開始使用
Cloud Volumes ONTAP

NetApp
June 11, 2024

目錄

開始使用

深入瞭解 Cloud Volumes ONTAP

利用 NetApp 技術、您可以最佳化雲端儲存成本與效能、同時強化資料保護、安全性與法規遵循。 Cloud Volumes ONTAP

不只是軟體的儲存應用裝置、可在雲端上執行功能完善的資料管理軟體。 Cloud Volumes ONTAP ONTAP它提供企業級儲存設備、具備下列主要功能：

- 儲存效率

  運用內建的重複資料刪除技術、資料壓縮、精簡配置及複製技術、將儲存成本降至最低。

- 高可用度

  確保雲端環境發生故障時、企業的可靠性和持續營運。

- 資料保護

  利用 NetApp 領先業界的複寫技術 SnapMirror 、將內部部署資料複寫到雲端、讓次要複本可輕鬆用於多種使用案例。 Cloud Volumes ONTAP

  Cloud Volumes ONTAP 也與 BlueXP 備份與還原整合、提供保護的備份與還原功能、以及雲端資料的長期歸檔。

  "深入瞭解 BlueXP 備份與還原"

- 資料分層

  在高效能與低效能儲存資源池之間隨需切換、而不需將應用程式離線。

- 應用程式一致性

  使用 NetApp SnapCenter 功能確保 NetApp Snapshot 複本的一致性。

  "深入瞭SnapCenter 解功能"

- 資料安全

  支援資料加密、並提供防範病毒和勒索軟體的功能。 Cloud Volumes ONTAP

- 隱私權法規遵循控管

  與 BlueXP 分類整合可協助您瞭解資料內容並識別敏感資料。

  "深入瞭解 BlueXP 分類"

不含適用於功能的授權 ONTAP 。 Cloud Volumes ONTAP

"檢視支援 Cloud Volumes ONTAP 的支援的支援功能"

"深入瞭 Cloud Volumes ONTAP 解功能"

支援的新部署 ONTAP 版本

在ONTAP 您建立全新Cloud Volumes ONTAP 的支援環境時、BlueXP可讓您從多個不同的支援版本中進行選擇。

此處列出的 Cloud Volumes ONTAP 版本以外的版本不適用於新部署。如需有關升級的資訊、請參閱 "支援的升級途徑"。

AWS

單一節點

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 正式
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 p6

HA配對

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 正式
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1

- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 p6

Azure

單一節點

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 正式
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6
- 9.5 p6

HA配對

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 正式
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6

Google Cloud

單一節點

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 正式
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

HA配對

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 正式
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

Amazon Web Services入門

在**AWS**中快速入門**Cloud Volumes ONTAP**

只要幾個步驟、Cloud Volumes ONTAP 就能開始使用AWS的功能。

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 AWS 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"。

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. 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。

3. 設定 S3 服務的 VPC 端點。

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

"深入瞭解網路需求"。

4 設定 **AWS KMS**

如果您想搭配 Cloud Volumes ONTAP 使用 Amazon 加密搭配使用、則必須確保存在作用中的客戶主金鑰（ CMK ）。您也必須新增 IAM 角色、將連接器的權限提供給作為 _key 使用者 _ 的連接器、以修改每個 CMK 的金鑰原則。 "深入瞭解"。

5 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

- "在AWS中從BlueXP建立連接器"
- "從AWS Marketplace建立連接器"
- "在內部部署安裝並設定 Connector"
- "Connector的AWS權限"

在**Cloud Volumes ONTAP AWS**中規劃您的不一樣組態

在 Cloud Volumes ONTAP AWS 中部署時、您可以選擇符合工作負載需求的預先設定系統、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。

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 AWS 地區的支援。 Cloud Volumes ONTAP "檢視支援區域的完整清單"。

您必須先啟用較新的 AWS 區域、才能在這些區域中建立及管理資源。 "瞭解如何啟用地區"。

選擇支援的本機區域

某些 AWS 本機區域（包括新加坡）支援 Cloud Volumes ONTAP 。選擇本機區域是選擇性的。

"檢視本機區域的完整清單"。
您必須先啟用本機區域、才能在這些區域中建立和管理資源。

"瞭解如何啟用本機區域"。

Phoenix 不是支援的本機區域。

選擇支援的執行個體

根據您選擇的授權類型、支援多種執行個體類型。 Cloud Volumes ONTAP

"AWS支援Cloud Volumes ONTAP 的支援組態"

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。

"AWS的儲存限制Cloud Volumes ONTAP"

在**AWS**中調整系統規模

調整 Cloud Volumes ONTAP 您的支援規模、有助於滿足效能與容量的需求。在選擇執行個體類型、磁碟類型和磁碟大小時、您應該注意幾個關鍵點：

執行個體類型

- 將工作負載需求與每個 EC2 執行個體類型的最大處理量和 IOPS 配對。
- 如果有多位使用者同時寫入系統、請選擇有足夠 CPU 來管理要求的執行個體類型。
- 如果您的應用程式大多讀取、請選擇具有足夠 RAM 的系統。
  - "AWS 文件： Amazon EC2 執行個體類型"
  - "AWS 文件： Amazon EBS 最佳化執行個體"

EBS 磁碟類型

EBS磁碟類型之間的差異較高、如下所示。若要深入瞭解EBS磁碟的使用案例、請參閱 "AWS 文件： EBS Volume 類型"。

- _通用SSD（GP3）_磁碟是成本最低的SSD、可在各種工作負載的成本與效能之間取得平衡。效能是以IOPS和處理量來定義。支援GP3磁碟Cloud Volumes ONTAP 的版本可搭配使用。9.7及更新版本。

  當您選取GP3磁碟時、BlueXP會填入預設的IOPS和處理量值、這些值會根據選取的磁碟大小提供相當於gp2磁碟的效能。您可以提高價值、以更高的成本獲得更好的效能、但我們不支援較低的值、因為這樣可能導致效能低落。簡而言之、請保留預設值或增加預設值。請勿降低。 "深入瞭解GP3磁碟及其效能"。

  請注意Cloud Volumes ONTAP 、此功能可搭配GP3磁碟支援Amazon EBS彈性磁碟區功能。 "深入瞭解彈性磁碟區支援"。

- _通用SSD（gp2）_磁碟可平衡各種工作負載的成本與效能。效能是以 IOPS 定義。
- _資源配置的IOPS SSD（IO1）_磁碟適用於需要以較高成本獲得最高效能的關鍵應用程式。

  請注意Cloud Volumes ONTAP 、支援Amazon EBS彈性Volume功能搭配IO1磁碟。 "深入瞭解彈性磁碟區支援"。

- _Throued Optimized HDD（ST1）_磁碟適用於經常存取的工作負載、這些工作負載需要以較低的價格提供快速且一致的處理量。

  使用處理量最佳化的HDD（ST1）時、不建議將資料分層至物件儲存設備。

EBS 磁碟大小

如果您選擇不支援的組態 "Amazon EBS彈性磁碟區功能"之後、您需要在啟動Cloud Volumes ONTAP 一套系統時選擇初始磁碟大小。之後、您就可以了 "讓BlueXP為您管理系統容量"但如果您想要的話 "自行建立集合體"請注意下列事項：

- 集合體中的所有磁碟大小必須相同。
- EBS 磁碟的效能與磁碟大小有關。大小決定 SSD 磁碟的基準 IOPS 和最大突發持續時間、以及 HDD 磁碟的基準和突發處理量。
- 最後、您應該選擇能提供所需 _ 持續效能 _ 的磁碟大小。
- 即使您選擇較大的磁碟（例如六個4 TiB磁碟）、也可能無法取得所有IOPS、因為EC2執行個體可能達到其頻寬限制。

  如需 EBS 磁碟效能的詳細資訊、請參閱 "AWS 文件： EBS Volume 類型"。

  如上所述、Cloud Volumes ONTAP 支援Amazon EBS彈性Volume功能的各種組態不支援選擇磁碟大小。 "深入瞭解彈性磁碟區支援"。

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 AWS中檢視系統資料的預設磁碟"。

連接器也需要系統磁碟。 "檢視Connector預設組態的詳細資料"。

準備在**Cloud Volumes ONTAP AWS Outpost**部署功能

如果您有 AWS Outpost 、您可以 Cloud Volumes ONTAP 在「工作環境」精靈中選取 Outpost VPC 、在該 Outpost 中部署功能不全。體驗與 AWS 中的任何其他 VPC 相同。請注意、您必須先在 AWS Outpost 部署 Connector 。

有幾項限制可以指出：

- 目前僅 Cloud Volumes ONTAP 支援單一節點的不支援系統
- 您可以搭配 Cloud Volumes ONTAP 使用的 EC2 執行個體僅限於您的據點所提供的項目
- 目前僅支援通用SSD（gp2）

收集網路資訊

在 Cloud Volumes ONTAP AWS 中啟動時、您需要指定 VPC 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。

單一**AZ**中的單一節點或**HA**配對

AWS 資訊	您的價值
區域	
VPC	
子網路	
安全性群組（如果使用您自己的）	

多個**AZs**中的**HA**配對

AWS 資訊	您的價值
區域	
VPC	
安全性群組（如果使用您自己的）	
節點 1 可用度區域	
節點 1 子網路	
節點 2 可用度區域	
節點 2 子網路	
中介可用度區域	
中介子網路	

AWS 資訊	您的價值
中介器的金鑰配對	
叢集管理連接埠的浮動 IP 位址	
節點 1 上資料的浮動 IP 位址	
節點 2 上資料的浮動 IP 位址	
浮動 IP 位址的路由表	

選擇寫入速度

BlueXP可讓您選擇Cloud Volumes ONTAP 適合的寫入速度設定。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。

設定您的網路

AWS 的網路需求 **Cloud Volumes ONTAP**

BlueXP負責Cloud Volumes ONTAP 設定功能完善的網路元件、例如IP位址、網路遮罩和路由。您需要確保可以存取傳出網際網路、有足夠的私有IP位址可用、有適當的連線位置等等。

一般要求

AWS 必須符合下列要求。

對節點的輸出網際網路存取 **Cloud Volumes ONTAP**

支援NetApp功能的支援節點需要外傳網際網路存取功能、此功能可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

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

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安全性群組允許連接埠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 嚴格的傳出規則以供支援、那麼Cloud Volumes ONTAP 您也必須確保支援透過連接埠3128建立_Outbound _連線的安全性群組。

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

HA 中介器的傳出網際網路存取

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

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

私有**IP**位址

BlueXP會自動分配所需的私有IP位址數量給Cloud Volumes ONTAP 整個過程。您必須確保網路有足夠的私有IP位址可用。

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。

單一節點系統的**IP**位址

BlueXP會將6個IP位址分配給單一節點系統。

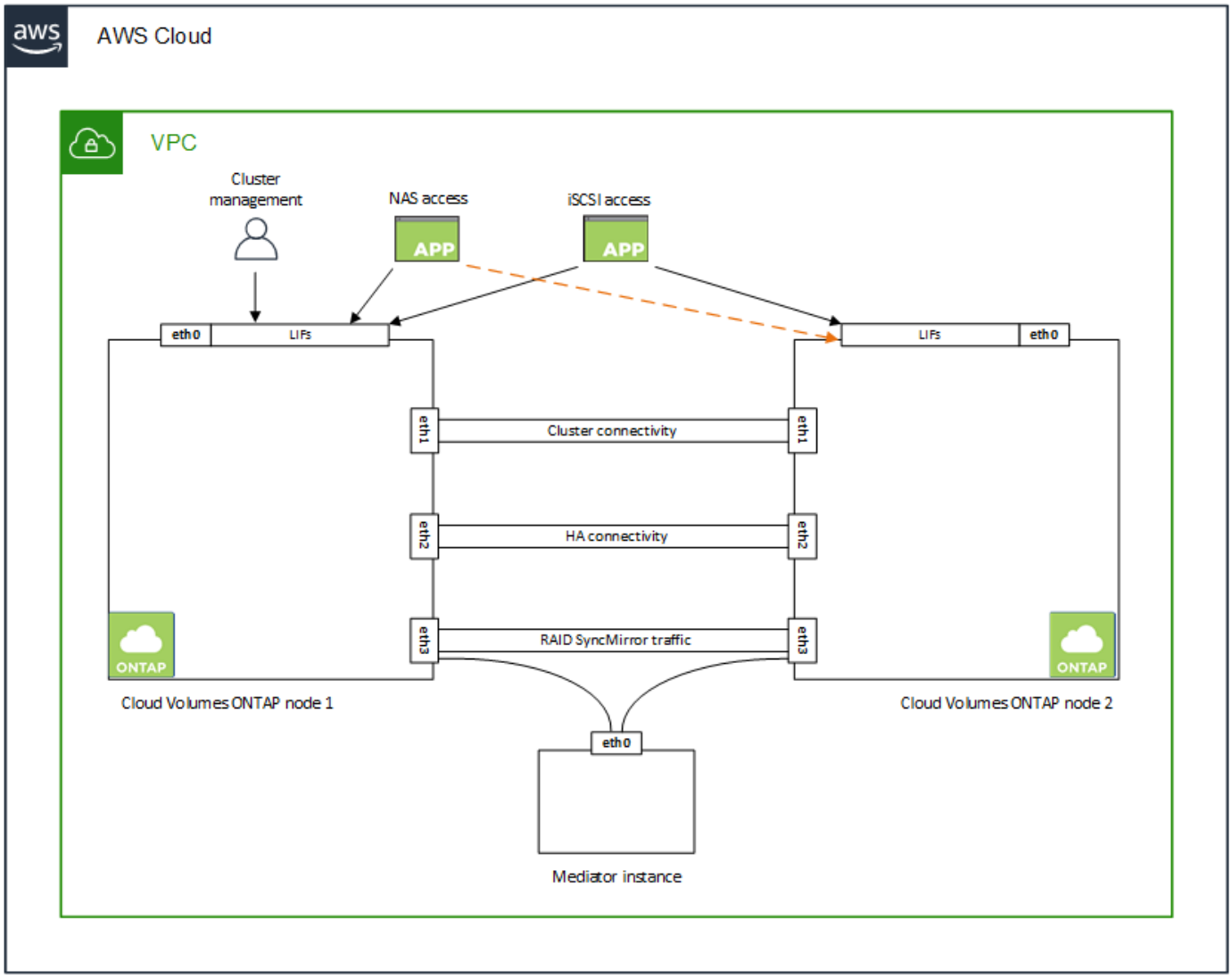
下表提供與每個私有IP位址相關聯的LIF詳細資料。

LIF	目的
叢集管理	整個叢集（HA配對）的管理管理。
節點管理	節點的管理管理。
叢集間	跨叢集通訊、備份與複寫。
NAS資料	透過NAS傳輸協定進行用戶端存取。
iSCSI資料	透過iSCSI傳輸協定進行用戶端存取。系統也用於其他重要的網路工作流程。此LIF為必填項目、不應刪除。

LIF	目的
儲存VM管理	儲存VM管理LIF可搭配SnapCenter 使用諸如VMware等管理工具。

HA配對的**IP**位址

HA配對比單一節點系統需要更多IP位址。這些IP位址分佈在不同的乙太網路介面上、如下圖所示：



HA配對所需的私有IP位址數目取決於您選擇的部署模式。部署在_onle_ AWS可用區域（AZ）中的HA配對需要15個私有IP位址、而部署在_multi__ AZs中的HA配對則需要13個私有IP位址。

下表提供與每個私有IP位址相關聯的LIF詳細資料。

HA配對的生命週數、在單一**AZ**中

LIF	介面	節點	目的
叢集管理	eth0	節點1	整個叢集（HA配對）的管理管理。
節點管理	eth0	節點1和節點2	節點的管理管理。
叢集間	eth0	節點1和節點2	跨叢集通訊、備份與複寫。

LIF	介面	節點	目的
NAS資料	eth0	節點1	透過NAS傳輸協定進行用戶端存取。
iSCSI資料	eth0	節點1和節點2	透過iSCSI傳輸協定進行用戶端存取。系統也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。
叢集連線能力	eth1	節點1和節點2	可讓節點彼此通訊、並在叢集內移動資料。
HA連線能力	eth2	節點1和節點2	在發生容錯移轉時、兩個節點之間的通訊。
RSMiSCSI流量	eth3	節點1和節點2	RAID SyncMirror 支援iSCSI流量、以及兩Cloud Volumes ONTAP 個支援節點與中介器之間的通訊。
中介者	eth0	中介者	節點與中介器之間的通訊通道、可協助進行儲存接管與恢復程序。

多個**AZs**中**HA**配對的**LIF**

LIF	介面	節點	目的
節點管理	eth0	節點1和節點2	節點的管理管理。
叢集間	eth0	節點1和節點2	跨叢集通訊、備份與複寫。
iSCSI資料	eth0	節點1和節點2	透過iSCSI傳輸協定進行用戶端存取。這些LIF也能管理節點之間的浮動IP位址移轉作業。這些生命是必要的、不應刪除。
叢集連線能力	eth1	節點1和節點2	可讓節點彼此通訊、並在叢集內移動資料。
HA連線能力	eth2	節點1和節點2	在發生容錯移轉時、兩個節點之間的通訊。
RSMiSCSI流量	eth3	節點1和節點2	RAID SyncMirror 支援iSCSI流量、以及兩Cloud Volumes ONTAP 個支援節點與中介器之間的通訊。
中介者	eth0	中介者	節點與中介器之間的通訊通道、可協助進行儲存接管與恢復程序。

部署在多個可用度區域時、會與多個生命區建立關聯 "浮動 IP 位址"、不計入AWS私有IP限制。

安全性群組

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

正在尋找Connector的相關資訊？ "檢視Connector的安全群組規則"

資料分層連線

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

當您建立 VPC 端點時、請務必選取與 Cloud Volumes ONTAP 該實例相對應的區域、 VPC 和路由表。您也必

須修改安全性群組、以新增允許流量到 S3 端點的傳出 HTTPS 規則。否則 Cloud Volumes ONTAP 、無法連線至 S3 服務。

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

連線**ONTAP** 至功能鏈接

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

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

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

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

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

VPC共享

從9.11.1版開始、Cloud Volumes ONTAP AWS支援搭配VPC共享功能的更新版、VPC共用功能可讓您的組織與其他AWS帳戶共用子網路。若要使用此組態、您必須設定AWS環境、然後使用API部署HA配對。

"瞭解如何在共用子網路中部署HA配對"。

多個 **AZs** 的 **HA** 配對需求

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

若要瞭解 HA 配對的運作方式、請參閱 "高可用度配對"。

可用度區域

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

每個可用區域都應有一個子網路。

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

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

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

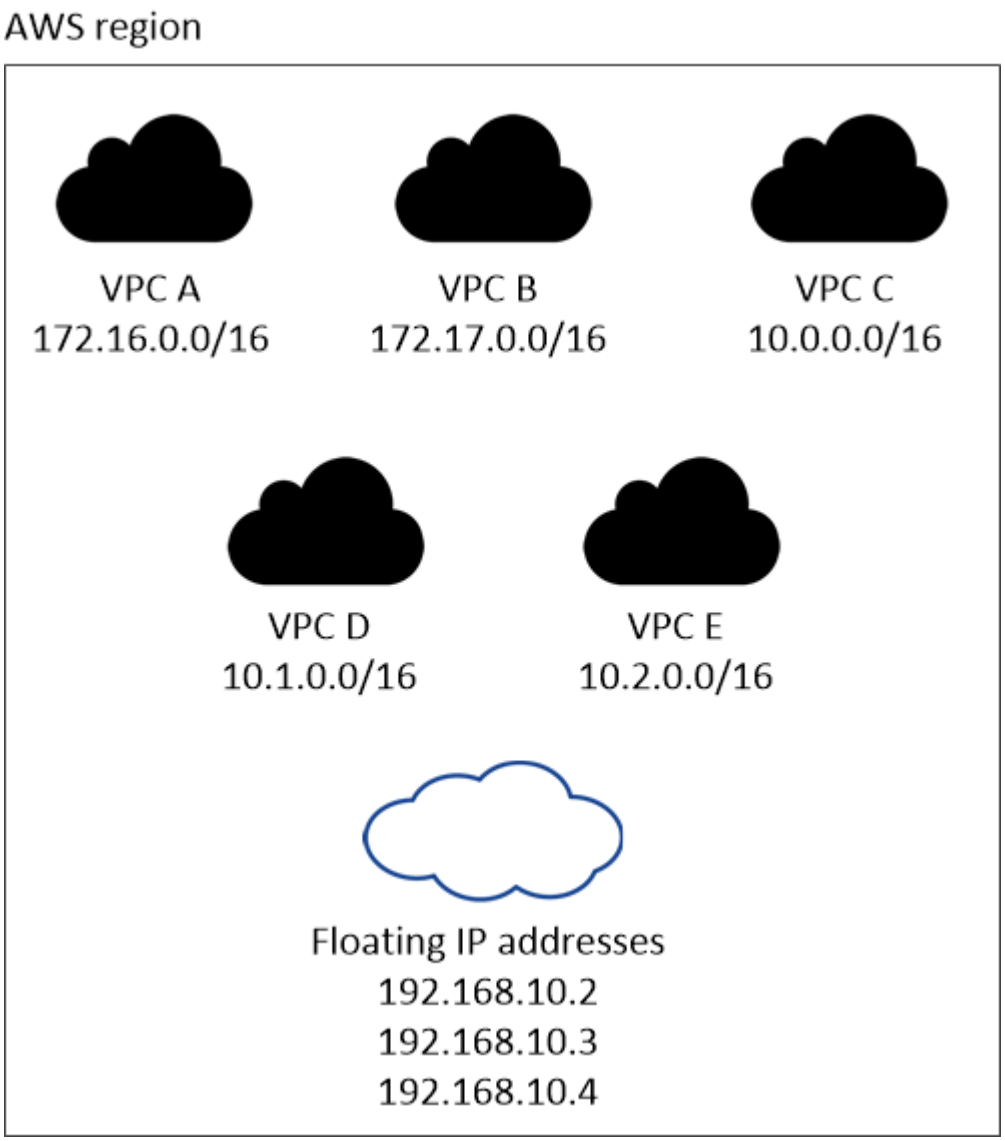
如果您使用 SnapDrive 適用於 Windows 的 SHIP 或 SnapCenter 搭配 HA 配對的 SHIP 、則 SVM 管理 LIF 需要一個浮動 IP 位址。

建立Cloud Volumes ONTAP 一套功能完善的運作環境時、您需要在BlueXP中輸入浮動IP位址。在啟動系統

時、BlueXP會將IP位址分配給HA配對。

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

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



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

傳輸閘道、可從 **VPC** 外部啟用浮動 **IP** 存取

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

路由表

在BlueXP中指定浮動IP位址之後、系統會提示您選取路由表、其中應包含通往浮動IP位址的路由。這可讓用戶端存取 HA 配對。

如果VPC中只有一個子網路路由表（主路由表）、則BlueXP會自動將浮動IP位址新增至該路由表。如果您有

多個路由表、在啟動 HA 配對時、請務必選取正確的路由表。否則、部分用戶端可能無法存取 Cloud Volumes ONTAP 功能不完全。

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

如需路由表的詳細資訊、請參閱 "AWS 文件：路由表"。

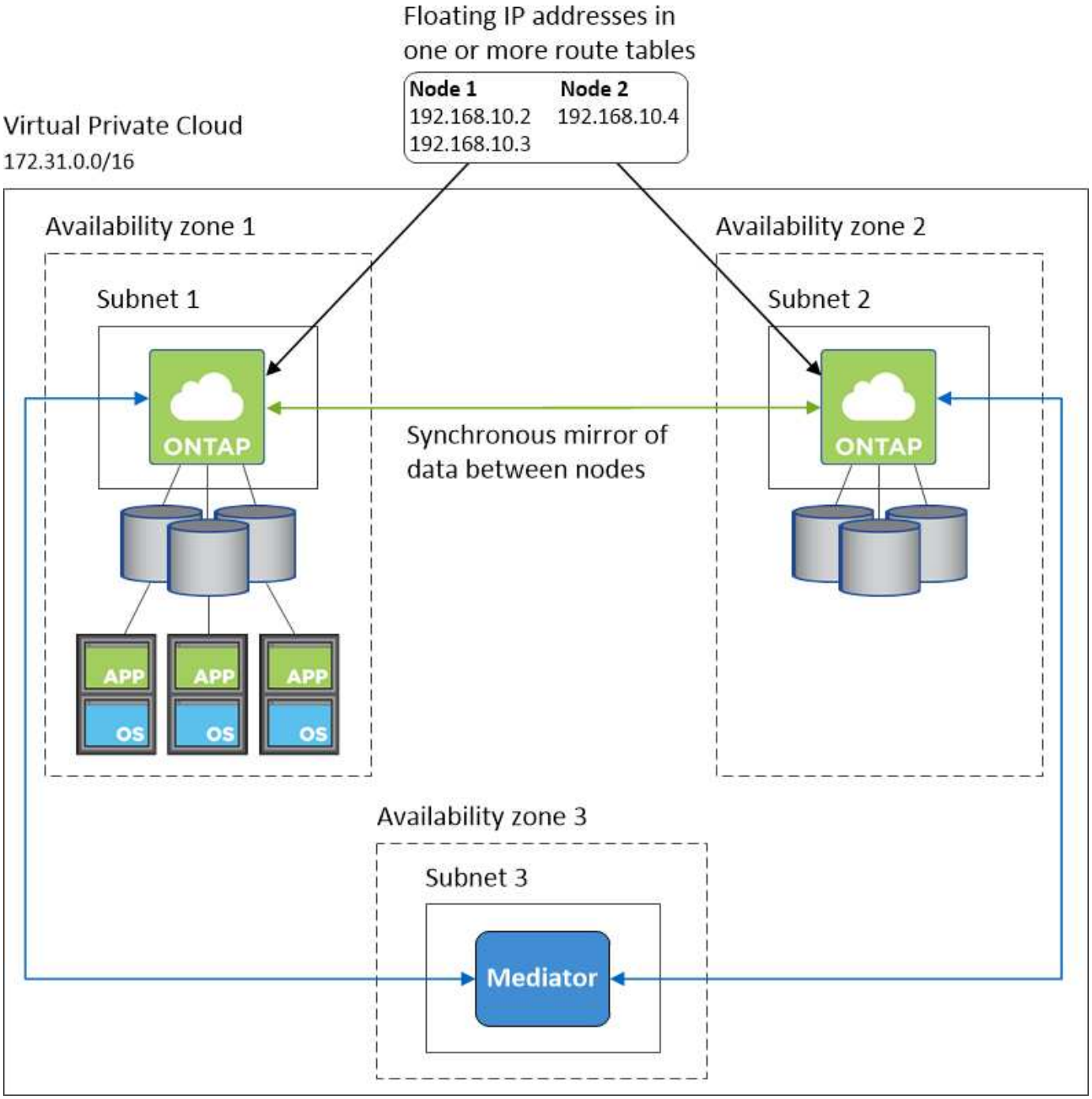
連線至 **NetApp** 管理工具

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

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

HA 組態範例

下圖說明多個AZs中HA配對的特定網路元件：三個可用度區域、三個子網路、浮動IP位址和路由表。



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"
- "AWS中的安全群組規則"

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

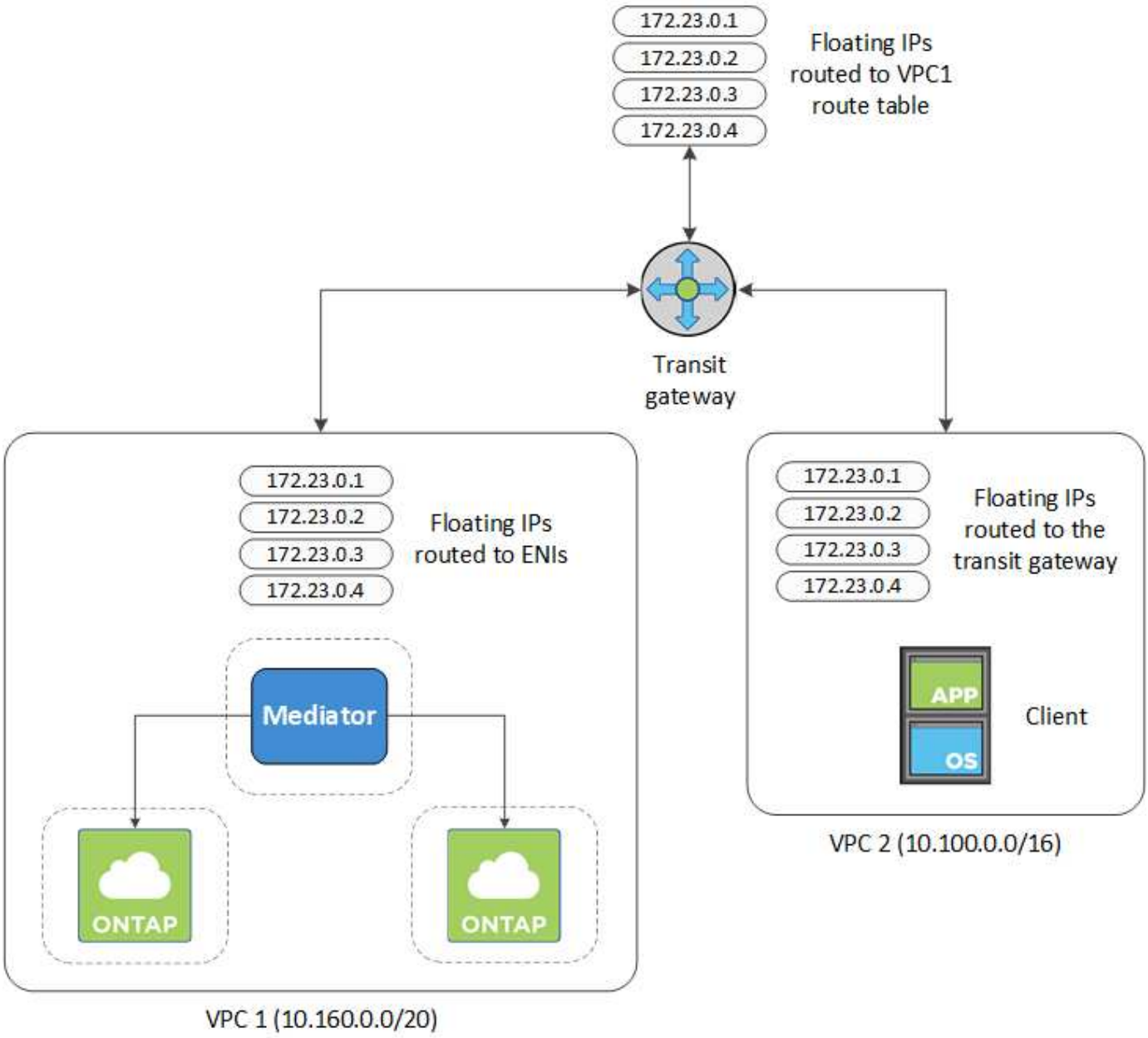
設定 AWS 傳輸閘道、以便存取 HA 配對 "浮動 IP 位址" 從 HA 配對所在的 VPC 外部。

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

叢集管理介面和選用的 SVM 管理 LIF 也需要浮動 IP 位址。

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

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



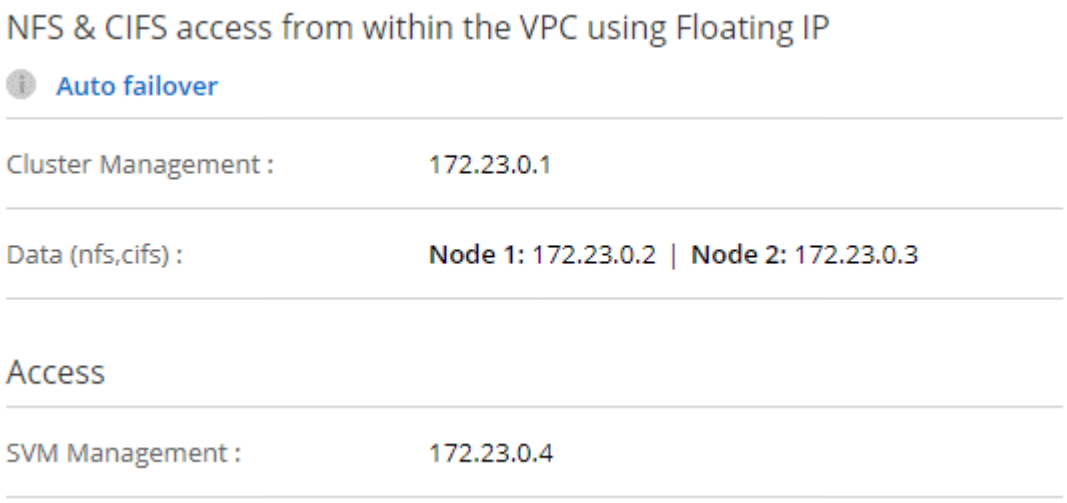
下列步驟說明如何設定類似的組態。

步驟

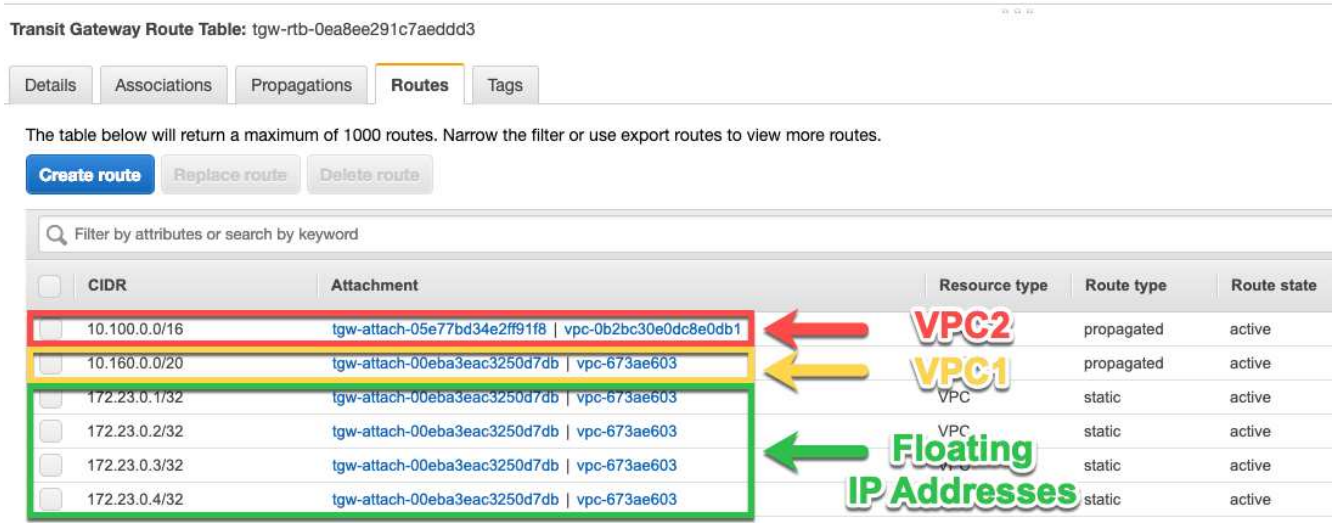
1. "建立傳輸閘道、並將 VPC 附加至閘道"。

2. 將VPC與傳輸閘道路由表建立關聯。
   a. 在* VPC*服務中、按一下* Transit Gateway Route Tables *。
   b. 選取路由表。
   c. 按一下「關聯」、然後選取「建立關聯」。
   d. 選擇要關聯的附件（VPC）、然後按一下*建立關聯*。
3. 指定 HA 配對的浮動 IP 位址、在傳輸閘道的路由表中建立路由。

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

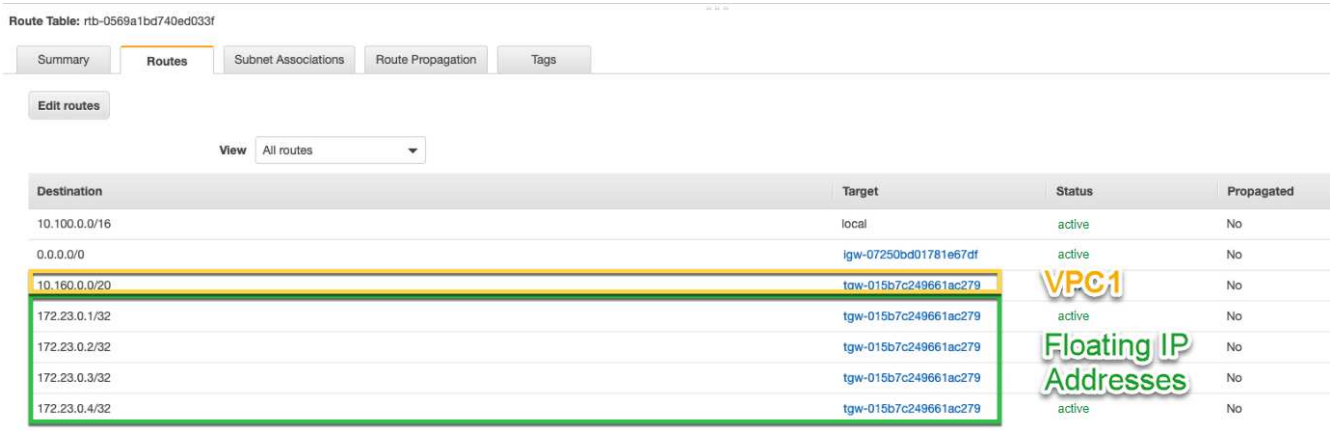


   下列範例影像顯示傳輸閘道的路由表。其中包括兩部 VPC 的 CIDR 區塊路由、 Cloud Volumes ONTAP 以及由 R1 使用的四個浮動 IP 位址。



4. 修改需要存取浮動 IP 位址的 VPC 路由表。
   a. 新增路由項目至浮動 IP 位址。
   b. 將路由項目新增至 HA 配對所在 VPC 的 CIDR 區塊。

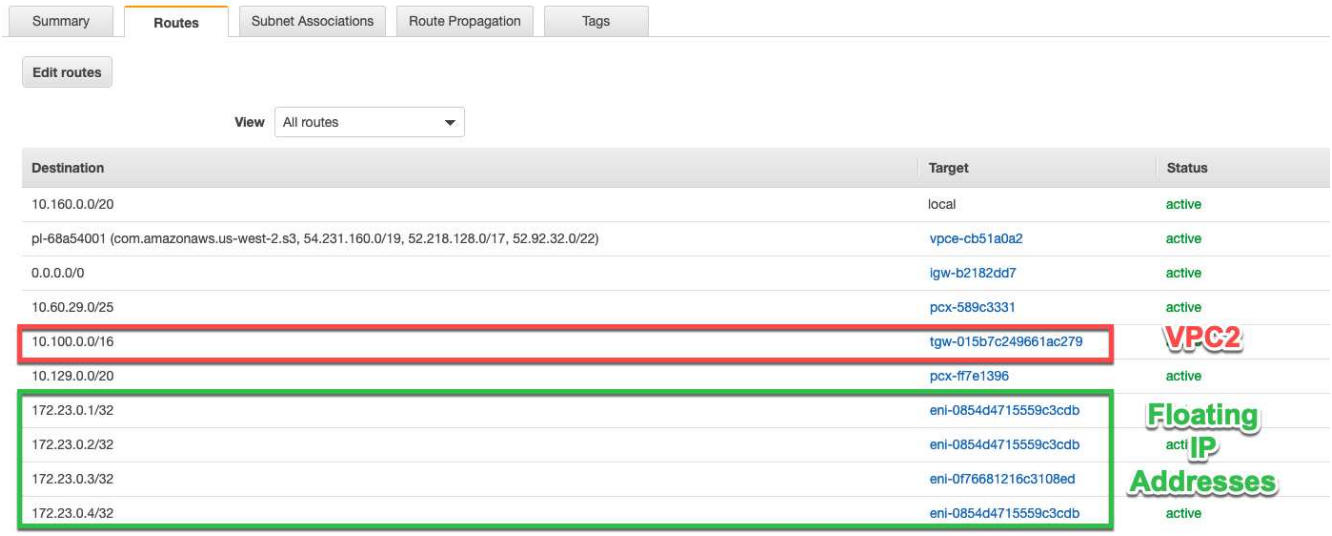
      下列範例影像顯示 VPC 2 的路由表、其中包括通往 VPC 1 的路由和浮動 IP 位址。



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

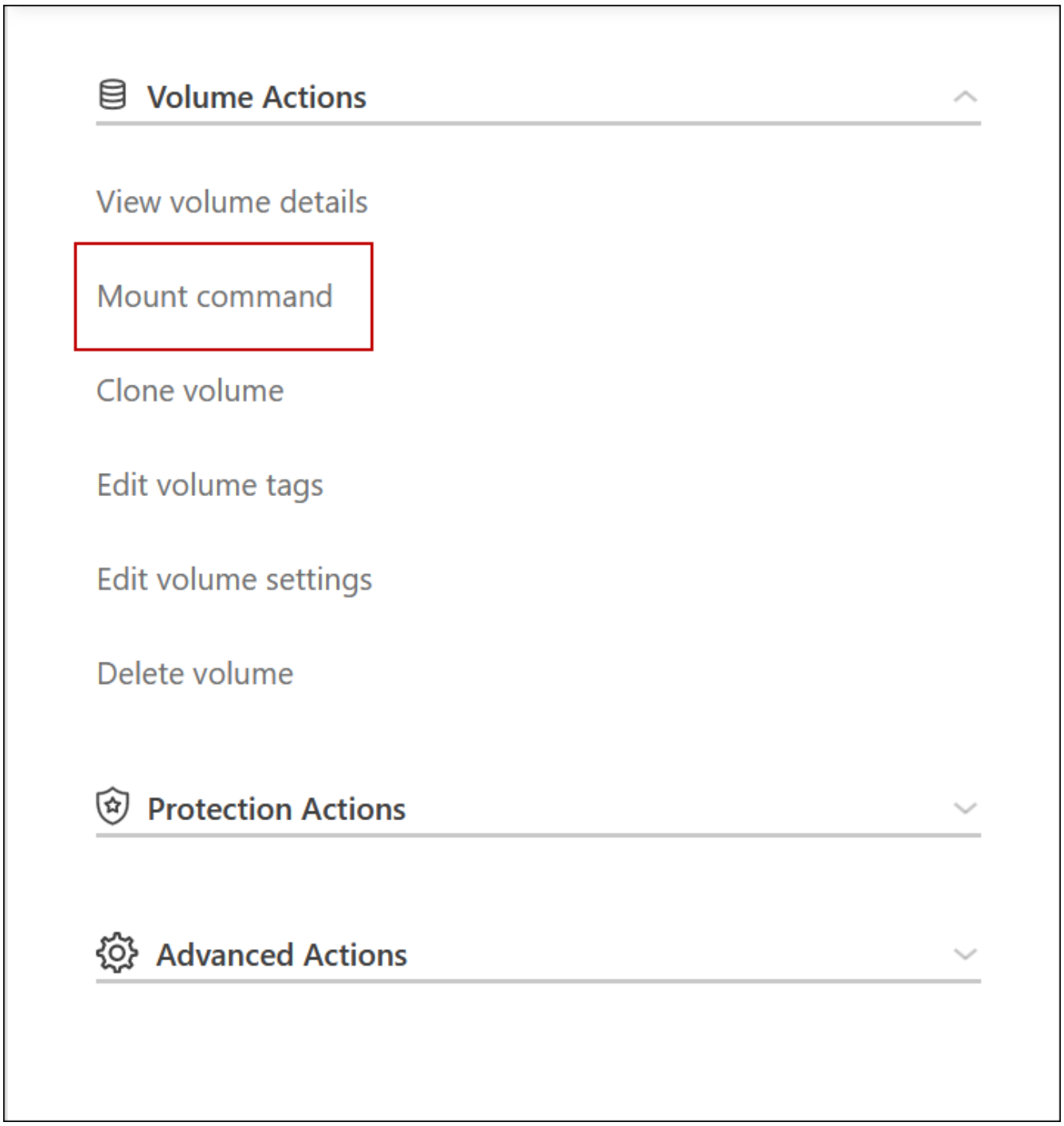
   此步驟非常重要、因為它會完成 VPC 之間的路由。

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



6. 將 VPC 的安全性群組設定更新為「所有流量」。
   a. 按一下 [虛擬私有雲] 底下的 [子網路] 。
   b. 按一下 * 路由表 * 索引標籤、為 HA 配對的其中一個浮動 IP 位址選取所需的環境。
   c. 按一下 * 安全性群組 * 。
   d. 選取 * 編輯輸入規則 * 。
   e. 按一下*新增規則*。
   f. 在 [類型] 下，選取 [* 所有流量] ，然後選取 VPC IP 位址。
   g. 按一下 * 儲存規則 * 以套用變更。
7. 使用浮動 IP 位址將磁碟區掛載到用戶端。

   您可以透過 BlueXP 中「管理磁碟區」面板下的 * 掛載命令 * 選項、在 BlueXP 中找到正確的 IP 位址。



8. 如果您要掛載NFS Volume、請設定匯出原則以符合用戶端VPC的子網路。

   "瞭解如何編輯Volume"。

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

在共享子網路中部署**HA**配對

從9.11.1版開始、Cloud Volumes ONTAP AWS支援搭配VPC共享功能的更新版、VPC共

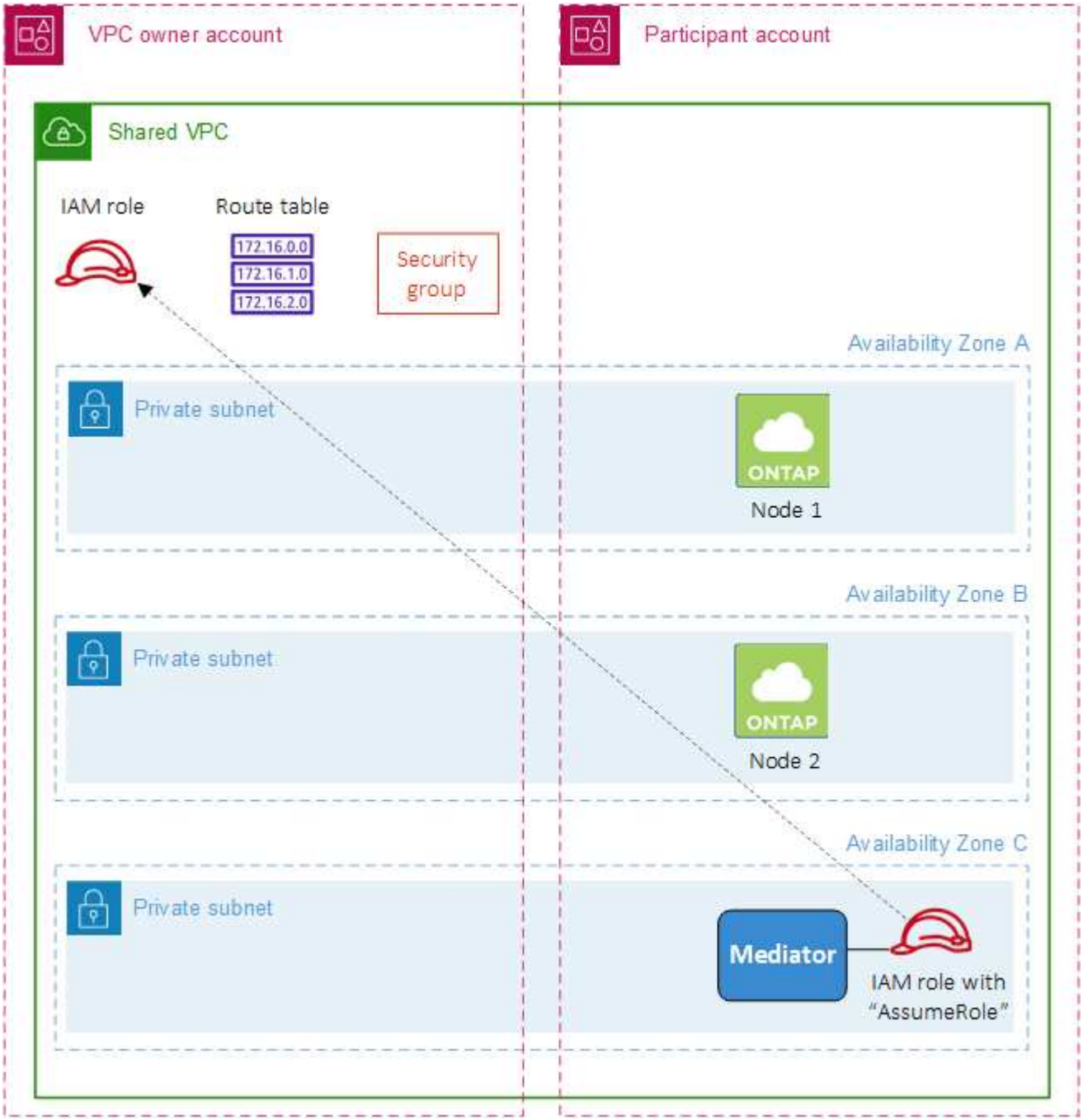
用功能可讓您的組織與其他AWS帳戶共用子網路。若要使用此組態、您必須設定AWS環境、然後使用API部署HA配對。

與 "VPC共享"、將一個功能豐富的全功能HA組態分佈於兩個帳戶：Cloud Volumes ONTAP

- VPC擁有者帳戶、擁有網路（VPC、子網路、路由表和Cloud Volumes ONTAP 保密群組）
- 參與者帳戶、其中EC2執行個體部署在共享子網路中（包括兩個HA節點和中介器）

若將某個版本部署在多個可用度區域中、HA中介程式需要特定權限、才能寫入VPC擁有者帳戶中的路由表。Cloud Volumes ONTAP您必須設定協調員可以承擔的IAM角色、以提供這些權限。

下圖顯示此部署所涉及的元件：



如下列步驟所述、您必須與參與者帳戶共用子網路、然後在VPC擁有者帳戶中建立IAM角色和安全性群組。

當您建立Cloud Volumes ONTAP 不協調作業環境時、BlueXP會自動建立IAM角色、並將其附加至協調者。此角色會假設您在VPC擁有者帳戶中建立的IAM角色、以便變更與HA配對相關的路由表。

步驟

1. 與參與者帳戶共用VPC擁有者帳戶中的子網路。

   若要在共用子網路中部署HA配對、必須執行此步驟。

   "AWS文件：共用子網路"

2. 在VPC擁有者帳戶中、建立Cloud Volumes ONTAP 一個安全群組以供使用。

   "請參閱Cloud Volumes ONTAP 安全性群組規則以瞭解相關資訊"。請注意、您不需要為HA中介者建立安全性群組。BlueXP能為您實現這項目標。

3. 在VPC擁有者帳戶中、建立包含下列權限的IAM角色：

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. 使用BlueXP API建立新Cloud Volumes ONTAP 的功能不全的工作環境。

   請注意、您必須指定下列欄位：

   - "安全性群組Id"

     「安全性GroupId」欄位應指定您在VPC擁有者帳戶中建立的安全性群組（請參閱上述步驟2）。

   - 「haParam」物件中的「assugerme勞力Arn」

     「assume勞力arn」欄位應包含您在VPC擁有者帳戶中建立的IAM角色ARN（請參閱上述步驟3）。

   例如：

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

+
"深入瞭Cloud Volumes ONTAP 解NetApp API"

AWS 的安全群組規則

BlueXP會建立AWS安全性群組、其中包括Cloud Volumes ONTAP 需要順利運作的傳入和傳出規則。您可能想要參照連接埠進行測試、或是想要使用自己的安全性群組。

規則 Cloud Volumes ONTAP

適用於此功能的安全性群組 Cloud Volumes ONTAP 需要傳入和傳出規則。

傳入規則

當您建立工作環境並選擇預先定義的安全性群組時、可以選擇允許下列其中一項的流量：

- *僅限選定VPC *：傳入流量的來源是VPC的子網路範圍（適用於Cloud Volumes ONTAP 整個系統）、以及連接器所在VPC的子網路範圍。這是建議的選項。
- 所有**VPC**：傳入流量的來源為0.00.0.0/0 IP範圍。

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	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
UDP	111.	遠端程序需要 NFS

傳輸協定	連接埠	目的
UDP	161-162	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

傳出規則

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
備份至 S3	TCP	5010.	叢集間 LIF	備份端點或還原端點	備份與還原備份至 S3 功能的作業
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 ）
	TCP	3000	節點管理 LIF	HA 中介	ZAPI 呼叫（ Cloud Volumes ONTAP 僅限 RHA ）
	ICMP	1.	節點管理 LIF	HA 中介	Keepive Alive （ Cloud Volumes ONTAP 僅限 HHA ）
組態備份	HTTP	80	節點管理 LIF	\http ：//Wese/occm/offboxconfig <connector-IP-address>	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%	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	UDP	162%	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

HA 協調器外部安全群組的規則

針對此功能、預先定義 Cloud Volumes ONTAP 的外部安全群組包括下列傳入和傳出規則。

傳入規則

HA中介器的預先定義安全性群組包括下列傳入規則。

傳輸協定	連接埠	來源	目的
TCP	3000	連接器的CIDR	從 Connector 進行 RESTful API 存取

傳出規則

HA 中介器的預先定義安全性群組會開啟所有傳出流量。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

HA 中介器的預先定義安全性群組包括下列傳出規則。

傳輸協定	連接埠	目的
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、只開啟 HA 中介者傳出通訊所需的連接埠。

傳輸協定	連接埠	目的地	目的
HTTP	80	AWS EC2執行個體上Connector的IP位址	下載中介程式升級
HTTPS	443..	ec2.amazonaws.com	協助進行儲存容錯移轉
UDP	53.	ec2.amazonaws.com	協助進行儲存容錯移轉

您可以建立介面 VPC 端點、從目標子網路到 AWS EC2 服務、而非開啟連接埠 443 和 53 。

HA組態內部安全性群組的規則

針對某個不穩定的HA組態、預先定義的內部安全群組Cloud Volumes ONTAP 包括下列規則。此安全性群組可在HA節點之間以及中介器與節點之間進行通訊。

BlueXP一律會建立此安全性群組。您沒有使用自己的選項。

傳入規則

預先定義的安全性群組包含下列傳入規則。

傳輸協定	連接埠	目的
所有流量	全部	HA 中介器與 HA 節點之間的通訊

傳出規則

預先定義的安全性群組包括下列傳出規則。

傳輸協定	連接埠	目的
所有流量	全部	HA 中介器與 HA 節點之間的通訊

Connector 規則

"檢視Connector的安全群組規則"

設定 **AWS KMS**

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

步驟

1. 確認存在作用中的客戶主金鑰（ CMK ）。

   CMK 可以是 AWS 託管的 CMK 、也可以是客戶託管的 CMK 。它可以與BlueXP和Cloud Volumes ONTAP Sfor相同的AWS帳戶、也可以位於不同的AWS帳戶中。

   "AWS 文件：客戶主要金鑰（ CMK ）"

2. 新增IAM角色、將權限提供給BlueXP做為_key使用者_、以修改每個CMK的金鑰原則。

   將IAM角色新增為主要使用者後、即可讓BlueXP擁有權限、可搭配Cloud Volumes ONTAP 使用CMK搭配使用。

   "AWS 文件：編輯金鑰"

3. 如果 CMK 位於不同的 AWS 帳戶、請完成下列步驟：

   a. 從 CMK 所在的帳戶移至 KMS 主控台。

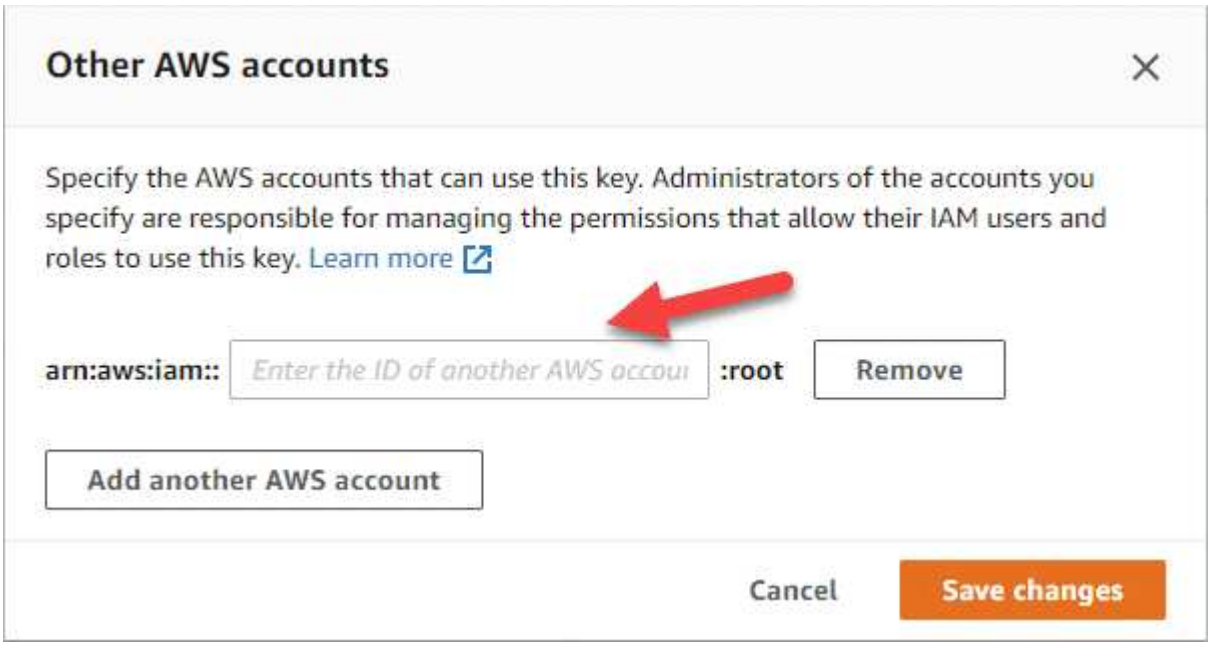
   b. 選取金鑰。

   c. 在「 * 一般組態 * 」窗格中、複製金鑰的 ARN 。

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

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

      在大多數情況下、這是BlueXP所在的帳戶。如果AWS中未安裝BlueXP、您將會為其提供AWS存取金鑰給BlueXP。



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

f. 建立包含下列權限的 IAM 原則。

g. 將原則附加至IAM角色或IAM使用者、以提供對BlueXP的權限。

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

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

+
如需此程序的其他詳細資料、請參閱 "AWS文件：允許其他帳戶的使用者使用KMS金鑰"。

4. 如果您使用由客戶管理的CMK、請將Cloud Volumes ONTAP 「IAM角色」新增為「_key使用者」、以修改CMK的金鑰原則。

   如果您在Cloud Volumes ONTAP 支援資料分層的情況下、想要加密儲存在S3儲存區中的資料、就必須執行

此步驟。

您需要在部署Cloud Volumes ONTAP 完時執行此步驟_after、因為IAM角色是在您建立工作環境時建立的。（當然、您可以選擇使用現有Cloud Volumes ONTAP 的ISIAM角色、因此可以在之前執行此步驟。）

"AWS 文件：編輯金鑰"

設定IAM角色Cloud Volumes ONTAP 以供使用

具有所需權限的IAM角色必須附加至每Cloud Volumes ONTAP 個節點。HA中介者也是如此。讓BlueXP為您建立IAM角色最簡單、但您可以使用自己的角色。

此工作為選用工作。當您建立Cloud Volumes ONTAP 一個運作環境時、預設選項是讓BlueXP為您建立IAM角色。如果貴企業的安全性原則要求您自行建立IAM角色、請遵循下列步驟。

AWS Secret Cloud 需要提供您自己的 IAM 角色。 "瞭解如何在Cloud Volumes ONTAP C2S中部署功能"。

步驟

1. 前往AWS IAM主控台。
2. 建立包含下列權限的IAM原則：
    - 適用於節點的基礎原則Cloud Volumes ONTAP

標準區域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud（美國）地區

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

最高機密區域

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

秘密區域

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- 適用於節點的備份原則Cloud Volumes ONTAP

  如果您計畫在 Cloud Volumes ONTAP 系統上使用 BlueXP 備份與還原、節點的 IAM 角色必須包含以下所示的第二個原則。

標準區域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud（美國）地區

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

最高機密區域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

秘密區域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- HA 中介

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "sts:AssumeRole",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. 建立IAM角色、並將您建立的原則附加至角色。

結果

現在您可以在建立新Cloud Volumes ONTAP 的運作環境時選擇IAM角色。

更多資訊

- "AWS文件：建立IAM原則"
- "AWS文件：建立IAM角色"

在Cloud Volumes ONTAP AWS中設定適用於此功能的授權

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

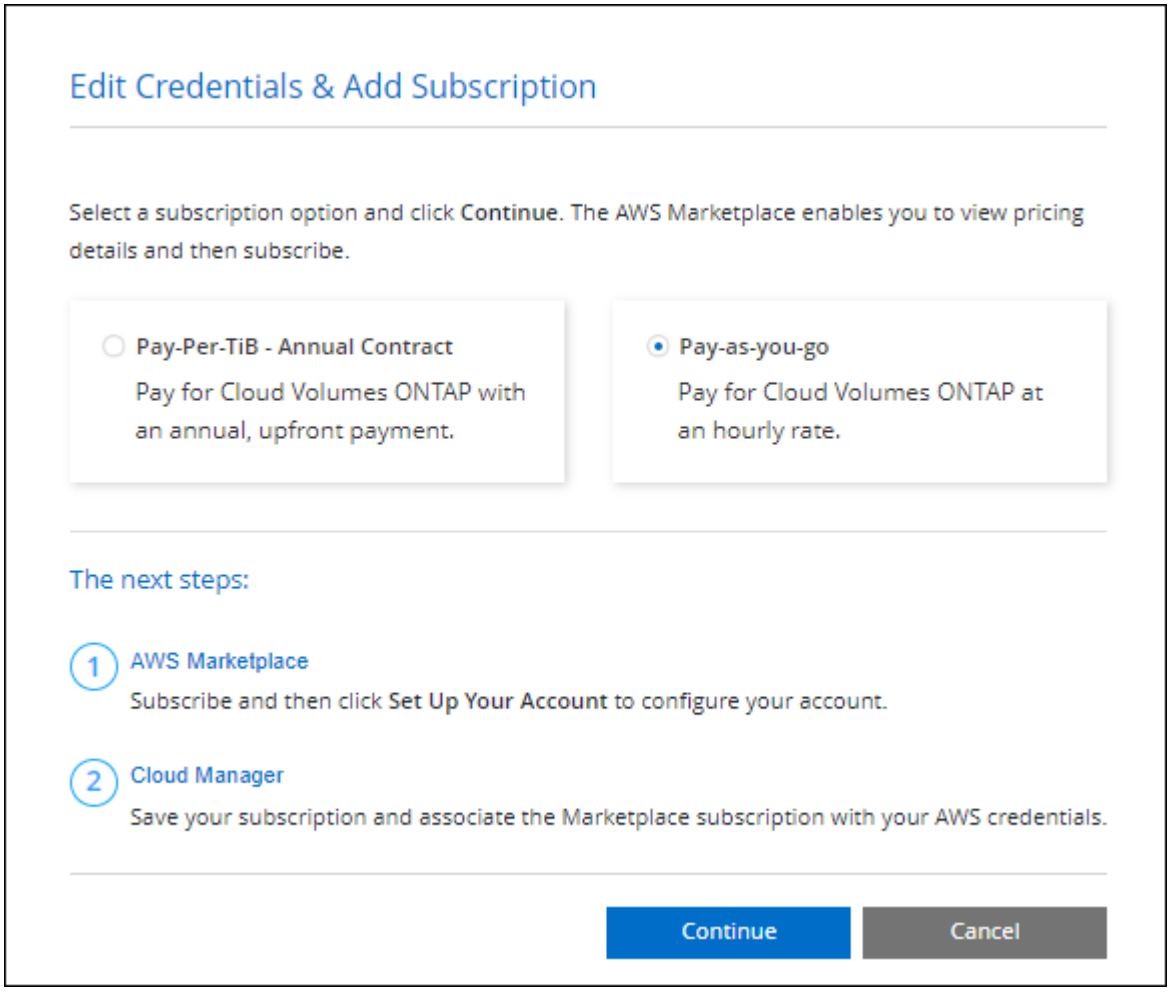
選擇Freemium產品、即可免費使用Cloud Volumes ONTAP 多達500 GiB的配置容量。 "深入瞭解Freemium產品"。

步驟

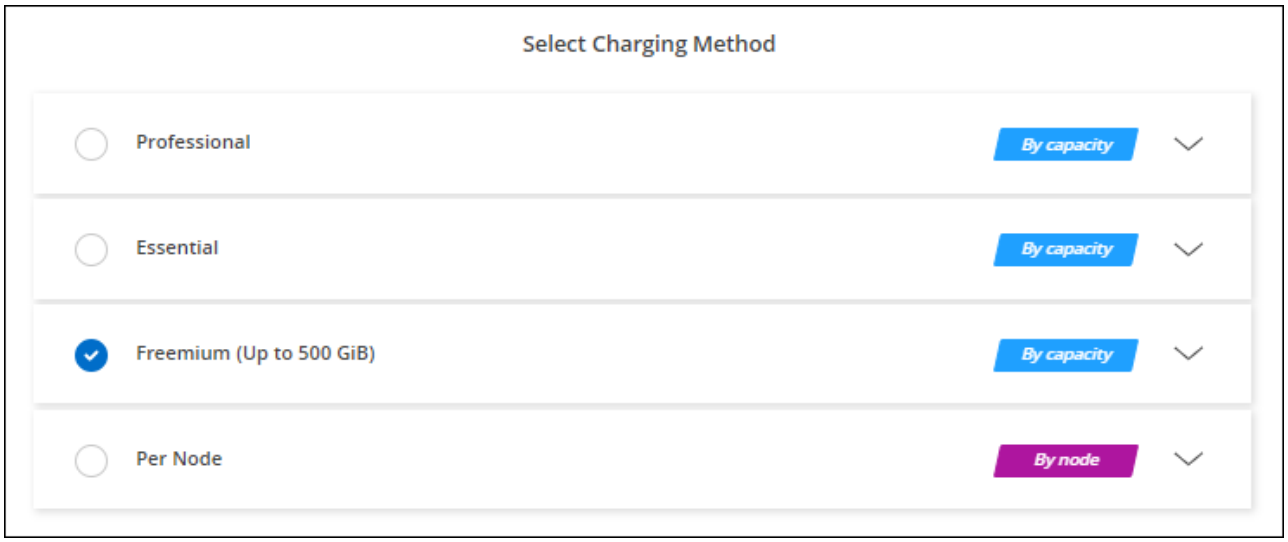
1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
    a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示訂閱AWS Marketplace中的隨

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"。



a. 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、以在Cloud Volumes ONTAP AWS中啟動功能"。

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AWS Marketplace訂閱時數小時隨付（PAYGO）
- AWS Marketplace的年度合約

"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"

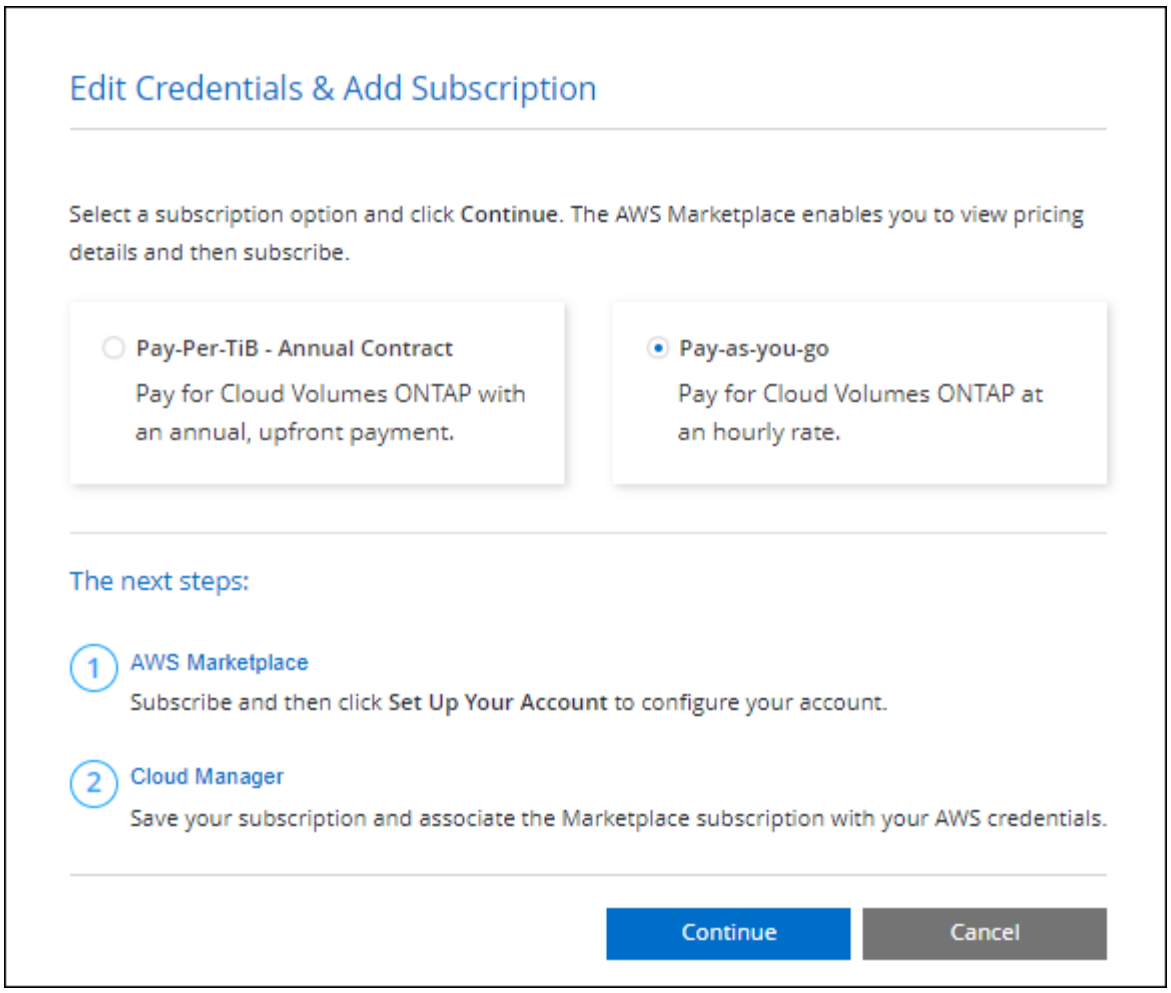
   BlueXP會自動查詢NetApp的授權服務、以取得NetApp 支援網站 與您的還原帳戶相關之授權的詳細資料。如果沒有錯誤、 BlueXP 會自動將授權新增至數位錢包。

   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"。

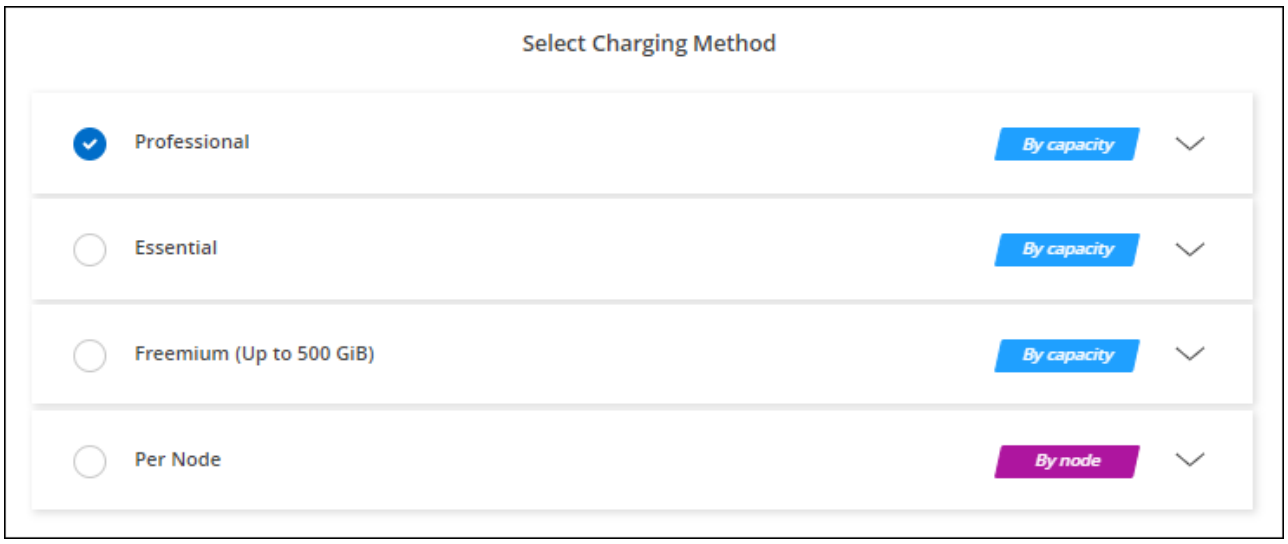
3. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。

   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AWS 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。



a. 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、以在Cloud Volumes ONTAP AWS中啟動功能"。

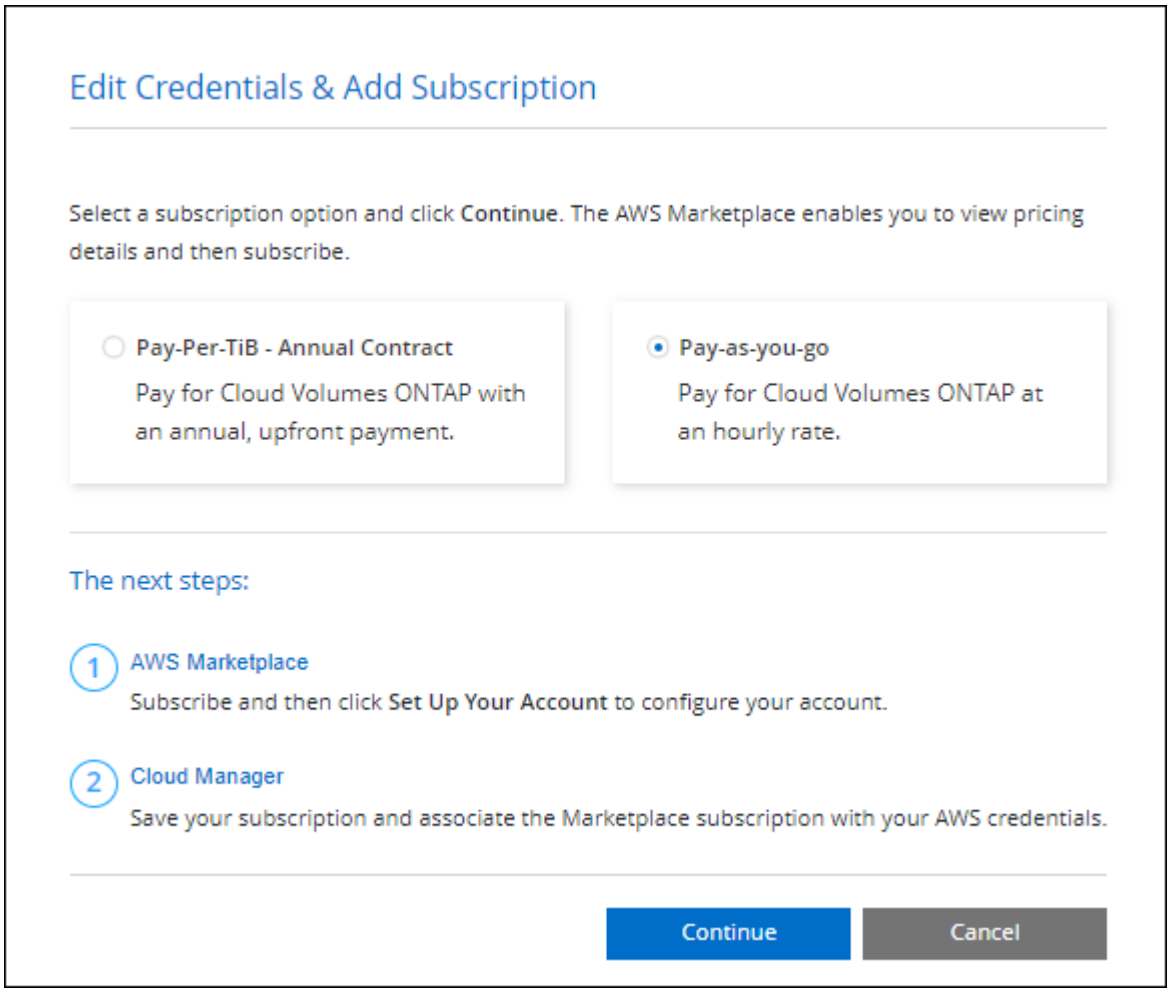
PAYGO訂閱

從雲端供應商的市場訂閱優惠、每小時支付一次。

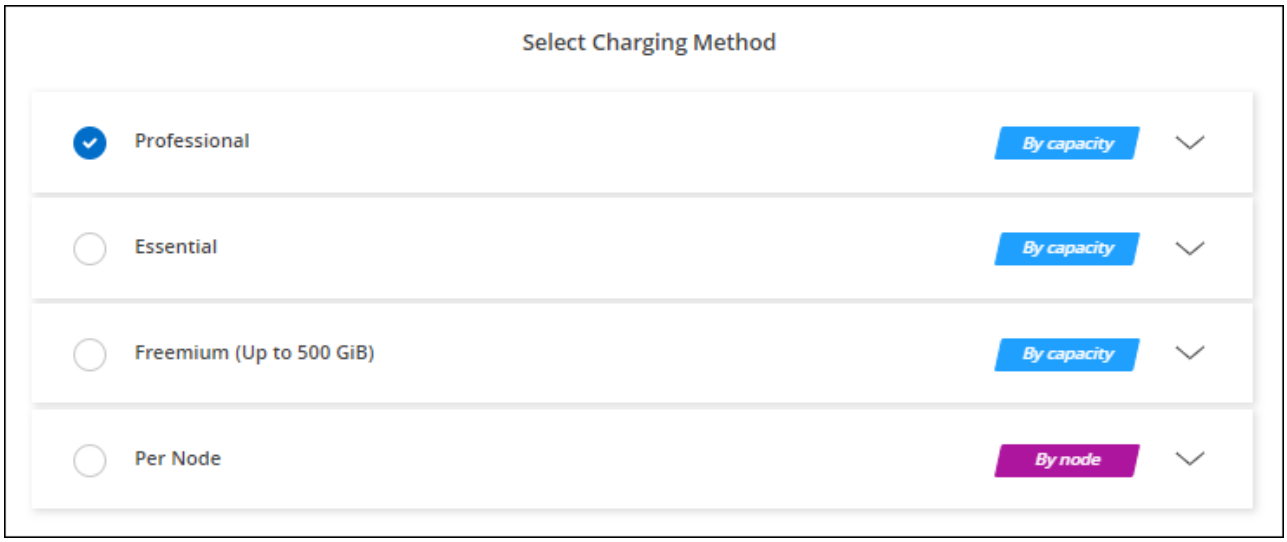
當您建立Cloud Volumes ONTAP 一個運作環境時、BlueXP會提示您訂閱AWS Marketplace提供的合約。該訂閱之後會與工作環境建立關聯、以便進行充電。您可以在其他工作環境中使用相同的訂閱。

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AWS 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、以在Cloud Volumes ONTAP AWS中啟動功能"。

您可以從「設定」>「認證」頁面管理與AWS帳戶相關的AWS Marketplace訂閱。 "瞭解如何管理AWS帳戶和訂閱"

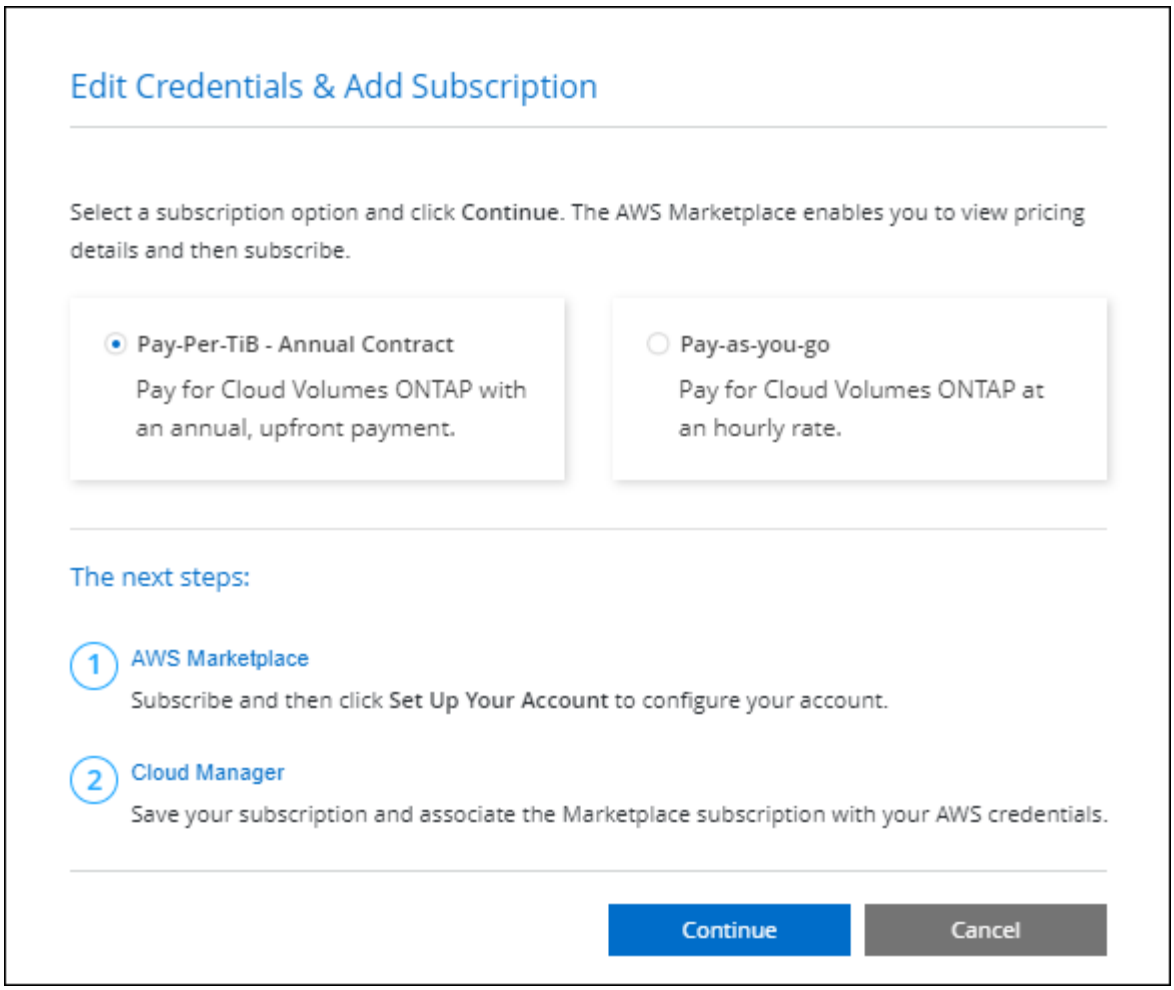
年度合約

每年向雲端供應商的市場購買一年一度的合約即可付款。

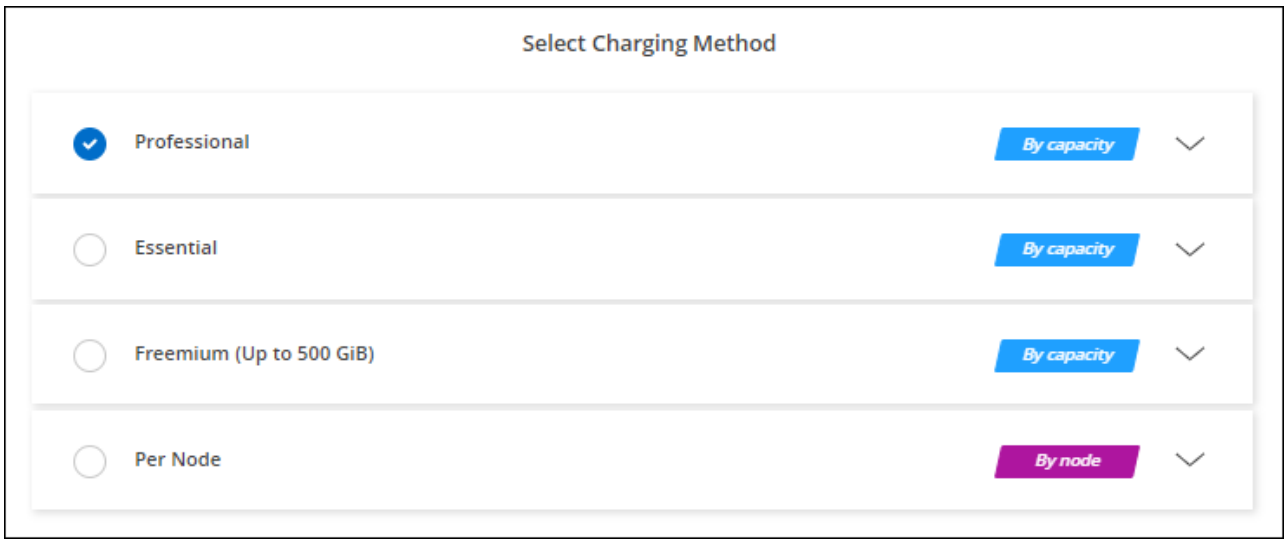
如同每小時訂閱、BlueXP會提示您訂閱AWS Marketplace提供的年度合約。

步驟

1. 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AWS Marketplace訂閱年度合約。



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。



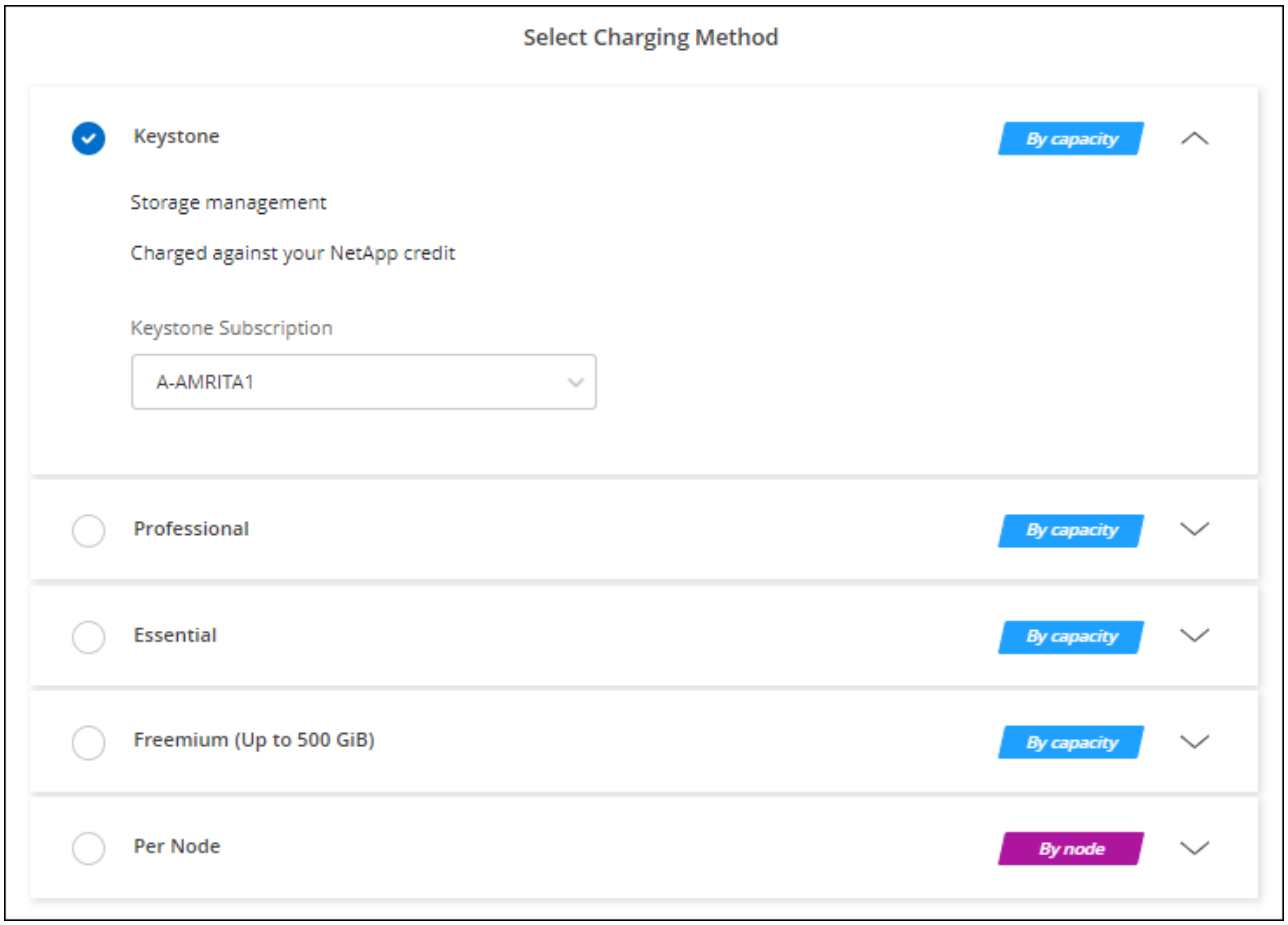
"請參閱逐步指示、以在Cloud Volumes ONTAP AWS中啟動功能"。

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、以在Cloud Volumes ONTAP AWS中啟動功能"。

在 Cloud Volumes ONTAP AWS 中啟動

您可以 Cloud Volumes ONTAP 在單一系統組態中或 AWS 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"。

- 瞭解您要使用的組態。

  您應該已做好準備、選擇組態、並從系統管理員取得 AWS 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"。

- 適用於CIFS組態的DNS與Active Directory。

  如需詳細資訊、請參閱 "AWS 的網路需求 Cloud Volumes ONTAP"。

在 **Cloud Volumes ONTAP AWS** 中啟動單一節點的效能不整系統

如果您想Cloud Volumes ONTAP 要在AWS中啟動功能、您需要在BlueXP中建立新的工作環境

關於這項工作

在您建立工作環境之後、BlueXP會立即在指定的VPC中啟動測試執行個體、以驗證連線能力。如果成功、BlueXP會立即終止執行個體、然後開始部署Cloud Volumes ONTAP 該系統。如果BlueXP無法驗證連線能力、則無法建立工作環境。測試執行個體為 T2.奈 米（預設 VPC 租賃）或 m3.medium （專屬 VPC 租賃）。

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 * Amazon Web Services* 和 * Cloud Volumes ONTAP 《單一節點 * 》。
4. 如果出現提示、 "建立連接器"。
5. * 詳細資料與認證 * ：選擇性地變更 AWS 認證資料與訂閱、輸入工作環境名稱、視需要新增標記、然後輸入密碼。

   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：

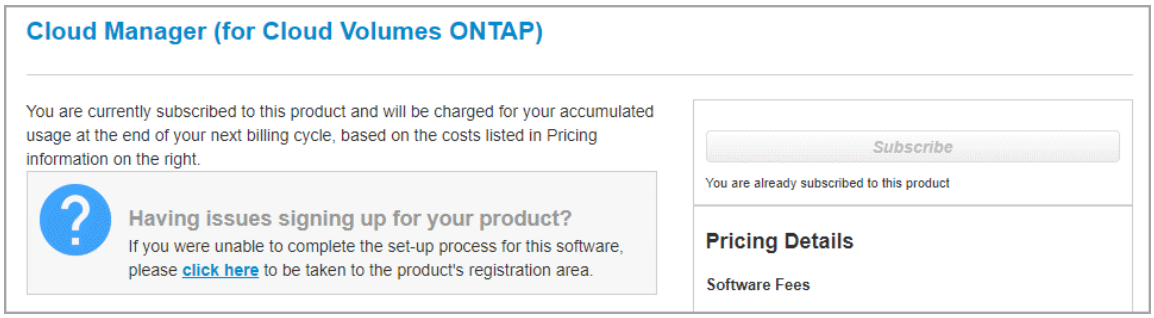
欄位	說明
工作環境名稱	BlueXP使用工作環境名稱來命名Cloud Volumes ONTAP 整個系統、以及Amazon EC2執行個體。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。
新增標記	AWS 標籤是 AWS 資源的中繼資料。BlueXP會將標記新增Cloud Volumes ONTAP 至該執行個體、以及與該執行個體相關聯的每個AWS資源。建立工作環境時、您最多可以從使用者介面新增四個標記、然後在建立之後新增更多標記。請注意、在建立工作環境時、 API 不會限制您使用四個標記。如需標記的相關資訊、請參閱 "AWS 文件：標記 Amazon EC2 資源"。
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
編輯認證資料	選擇與您要部署此系統之帳戶相關的AWS認證資料。您也可以將AWS Marketplace訂閱與此Cloud Volumes ONTAP 款作業系統建立關聯。 按一下*新增訂閱*、將所選認證資料與新的AWS Marketplace訂閱建立關聯。訂閱可以是一年一度的合約、或Cloud Volumes ONTAP 是以每小時的費率支付。 "瞭解如何將額外的AWS認證資料新增至BlueXP"。

下列影片說明如何將隨用隨付服務市場訂閱與 AWS 認證資料建立關聯：

從 AWS Marketplace 訂閱 BlueXP

如果多位 IAM 使用者使用相同的 AWS 帳戶、則每位使用者都需要訂閱。第一位使用者訂閱之後、 AWS Marketplace 會通知後續使用者他們已經訂閱、如下圖所示。雖然 AWS *account* 已有訂閱、但每個 IAM 使用者都需要將自己與該訂閱建立關聯。如果您看到以下訊息、請按一下*按一下此處*連結、前往BlueXP網站並完成程
序。



6. * 服務 * ：啟用或停用 Cloud Volumes ONTAP 您不想搭配使用的個別服務。
   - "深入瞭解 BlueXP 分類"
   - "深入瞭解 BlueXP 備份與還原"

   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：輸入您在中記錄的網路資訊 "AWS工作表"。

   下表說明您可能需要指導的欄位：

欄位	說明
VPC	如果您有 AWS Outpost 、 Cloud Volumes ONTAP 您可以選擇 Outpost VPC 、在該 Outpost 中部署單一節點的一套系統。體驗與 AWS 中的任何其他 VPC 相同。

欄位	說明
產生的安全性群組	如果讓BlueXP為您產生安全性群組、您必須選擇允許流量的方式： • 如果您選擇*僅限VPC*、則傳入流量的來源為所選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*、則傳入流量的來源為0.00.0.0/0 IP範圍。
使用現有的安全性群組	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. * 資料加密 * ：不選擇資料加密或 AWS 管理的加密。

   對於 AWS 管理的加密、您可以從帳戶或其他 AWS 帳戶中選擇不同的客戶主金鑰（ CMK ）。

   建立 Cloud Volumes ONTAP 一套系統後、您無法變更 AWS 資料加密方法。

   "瞭解如何設定 AWS KMS for Cloud Volumes ONTAP the 功能"。

   "深入瞭解支援的加密技術"。

9. 充電方法與**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"。
10. 《》（僅限AWS Marketplace年度合約）：請檢閱預設組態、然後按一下*「Continue」（繼續）或按一下「Change Configuration」（變更組態）*以選取您自己的組態。Cloud Volumes ONTAP

    如果您保留預設組態、則只需指定一個Volume、然後檢閱並核准組態。

11. 預先設定的套件：選取其中一個套件以快速啟動Cloud Volumes ONTAP 功能、或按一下*變更組態*以選取您自己的組態。

    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。

12. * IAM角色*：最好保留預設選項、讓BlueXP為您建立角色。

    如果您偏好使用自己的原則、就必須符合 "有關節點的原則要求 Cloud Volumes ONTAP"。

13. 授權：視Cloud Volumes ONTAP 需要變更此版本、並選取執行個體類型和執行個體租賃。

    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 。

14. 基礎儲存資源：選擇磁碟類型、設定基礎儲存設備、然後選擇是否要啟用資料分層。

    請注意下列事項：

    - 磁碟類型適用於初始磁碟區（和Aggregate）。您可以為後續磁碟區（和Aggregate）選擇不同的磁碟類

型。

- 如果您選擇GP3或IO1磁碟、則BlueXP會使用AWS中的彈性磁碟區功能、視需要自動增加基礎儲存磁碟容量。您可以根據儲存需求來選擇初始容量、Cloud Volumes ONTAP 並在部署完畢後加以修改。 "深入瞭解AWS對彈性磁碟區的支援"。
- 如果您選擇gp2或ST1磁碟、則可以針對初始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、選取磁碟大小。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。
- 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。

  "瞭解資料分層的運作方式"。

15. *寫入速度與WORM *：

    a. 如果需要、請選擇*正常*或*高速*寫入速度。

       "深入瞭解寫入速度"。

    b. 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。

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

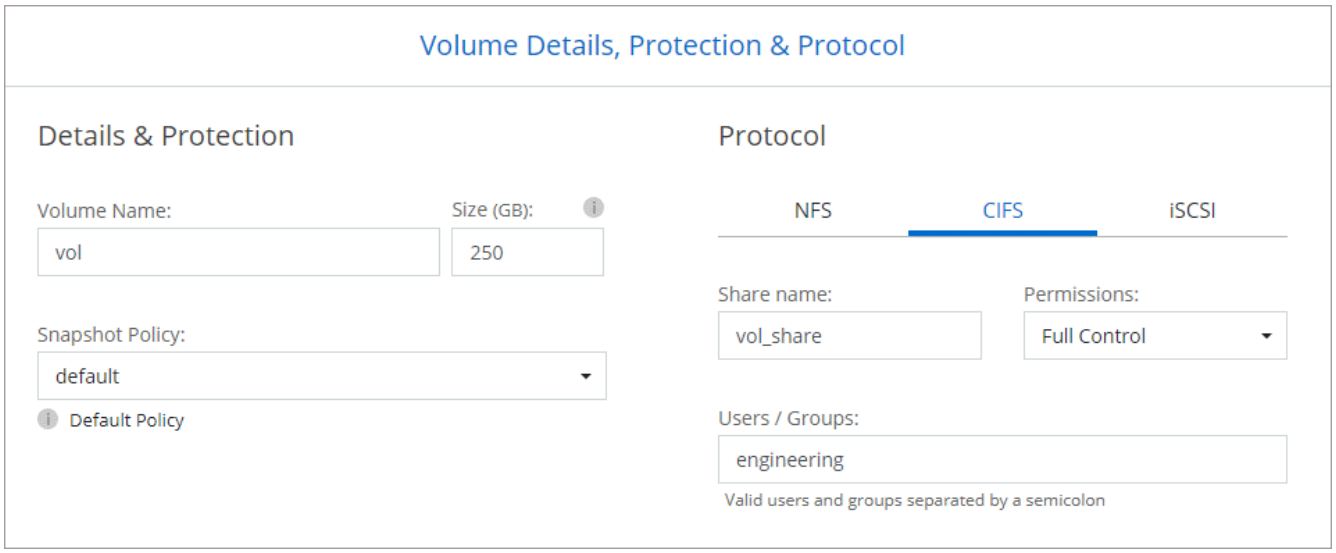
    "瞭解支援的用戶端傳輸協定和版本"。

    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 。

欄位	說明
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：



17. * 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。
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」。如果您將 AWS 託管 Microsoft AD 設定為 AD 伺服器 Cloud Volumes ONTAP 以供使用、您應該在此欄位中輸入 * OID=computers,O=corp* 。
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。

欄位	說明
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。

18. * 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、並編輯磁碟區分層原則。

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

19. * 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*以檢閱有關支援和BlueXP將購買的AWS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會啟動Cloud Volumes ONTAP 這個執行個體。您可以追蹤時間表的進度。

如果您在啟動 Cloud Volumes ONTAP 該實例時遇到任何問題、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 **Cloud Volumes ONTAP AWS** 中啟動一個「叢集 **HA** 配對」

如果您想要在Cloud Volumes ONTAP AWS中啟動一個「叢集HA配對」、您需要在BlueXP中建立HA工作環境。

限制

目前 AWS out貼 文不支援 HA 配對。

關於這項工作

在您建立工作環境之後、BlueXP會立即在指定的VPC中啟動測試執行個體、以驗證連線能力。如果成功、BlueXP會立即終止執行個體、然後開始部署Cloud Volumes ONTAP 該系統。如果BlueXP無法驗證連線能力、則無法建立工作環境。測試執行個體為 T2.奈 米（預設 VPC 租賃）或 m3.medium （專屬 VPC 租賃）。

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* Amazon Web Services*和* Cloud Volumes ONTAP 《*》HA *。

   有些 AWS 本機區域可供使用。

   您必須先啟用本機區域、並在 AWS 帳戶的本機區域中建立子網路、才能使用 AWS 本機區域。請遵循 * 選擇加入 AWS 本機區域 * 、並 * 將 Amazon VPC 延伸至中的本機區域 * 步驟 "AWS 教學課程「開始使用 AWS 本機區域部署低延遲應用程式」"。

   如果您執行的是 Connector 3.9.36 版或更低版本、則必須在 AWS EC2 主控台中、將下列權限新增至 AWS Connector 角色： DescribeAvailabilityZones 。
4. * 詳細資料與認證 * ：選擇性地變更 AWS 認證資料與訂閱、輸入工作環境名稱、視需要新增標記、然後輸入密碼。

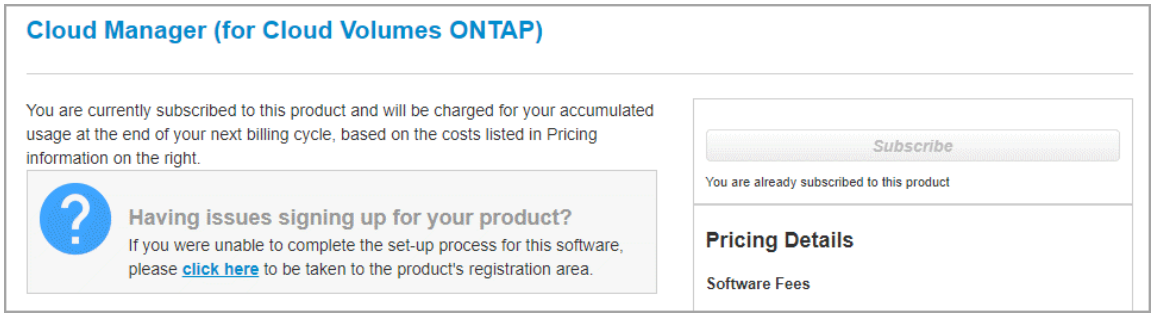
   本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

欄位	說明
工作環境名稱	BlueXP使用工作環境名稱來命名Cloud Volumes ONTAP 整個系統、以及Amazon EC2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。
新增標記	AWS 標籤是 AWS 資源的中繼資料。BlueXP會將標記新增Cloud Volumes ONTAP 至該執行個體、以及與該執行個體相關聯的每個AWS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記、然後在建立之後新增更多標記。請注意、在建立工作環境時、 API 不會限制您使用四個標記。如需標記的相關資訊、請參閱 "AWS 文件：標記 Amazon EC2 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。
編輯認證資料	選擇 AWS 認證資料和市場訂閱、以搭配此 Cloud Volumes ONTAP 款功能系統使用。 按一下*新增訂閱*、將所選認證資料與新的AWS Marketplace訂閱建立關聯。訂閱可以是一年一度的合約、或Cloud Volumes ONTAP 是以每小時的費率支付。 如果直接向NetApp（BYOL）購買授權、則無需訂閱AWS。 "瞭解如何將額外的AWS認證資料新增至BlueXP"。

   下列影片說明如何將隨用隨付服務市場訂閱與 AWS 認證資料建立關聯：

   從 AWS Marketplace 訂閱 BlueXP

如果多位 IAM 使用者使用相同的 AWS 帳戶、則每位使用者都需要訂閱。第一位使用者訂閱之後、 AWS Marketplace 會通知後續使用者他們已經訂閱、如下圖所示。雖然 AWS *account* 已有訂閱、但每個 IAM 使用者都需要將自己與該訂閱建立關聯。如果您看到以下訊息、請按一下*按一下此處*連結、前往BlueXP網站並完成程序。



5. * 服務 * ：讓服務保持啟用或停用您不想搭配 Cloud Volumes ONTAP 此作業系統使用的個別服務。
   - "深入瞭解 BlueXP 分類"
   - "深入瞭解 BlueXP 備份與還原"

   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 HA 組態。

   如需部署模型的總覽、請參閱 "適用於 AWS 的 HA Cloud Volumes ONTAP"。

7. 位置與連線（單一AZ）或*地區與VPC*（多個AZ）：輸入您在AWS工作表中記錄的網路資訊。

   下表說明您可能需要指導的欄位：

欄位	說明
產生的安全性群組	如果讓BlueXP為您產生安全性群組、您必須選擇允許流量的方式： • 如果您選擇*僅限VPC*、則傳入流量的來源為所選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*、則傳入流量的來源為0.00.0.0/0 IP範圍。
使用現有的安全性群組	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. * 連線能力與 SSH 驗證 * ：選擇 HA 配對與中介器的連線方法。
9. * 浮動 IPS* ：如果您選擇多個 AZs 、請指定浮動 IP 位址。

   該地區所有 VPC 的 IP 位址必須位於 CIDR 區塊之外。如需其他詳細資料、請參閱 "AWS 在 Cloud Volumes ONTAP 多個 AZs 中的功能需求"。

10. * 路由表 * ：如果您選擇多個 AZs 、請選取應包含浮動 IP 位址路由的路由表。

    如果您有多個路由表、請務必選取正確的路由表。否則、部分用戶端可能無法存取 Cloud Volumes ONTAP

此功能配對。如需路由表的詳細資訊、請參閱 "AWS 文件：路由表"。

11. * 資料加密 * ：不選擇資料加密或 AWS 管理的加密。

    對於 AWS 管理的加密、您可以從帳戶或其他 AWS 帳戶中選擇不同的客戶主金鑰（ CMK ）。

    建立 Cloud Volumes ONTAP 一套系統後、您無法變更 AWS 資料加密方法。

    "瞭解如何設定 AWS KMS for Cloud Volumes ONTAP the 功能"。

    "深入瞭解支援的加密技術"。

12. 充電方法與**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"。

13. 《》（僅限AWS Marketplace年度合約）：請檢閱預設組態、然後按一下*「Continue」（繼續）或按一下「Change Configuration」（變更組態）*以選取您自己的組態。Cloud Volumes ONTAP

    如果您保留預設組態、則只需指定一個Volume、然後檢閱並核准組態。

14. 預先設定的套件（僅限每小時或BYOL）：選取其中一個套件以快速啟動Cloud Volumes ONTAP 功能、或按一下*變更組態*以選取您自己的組態。

    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。

15. * IAM角色*：最好保留預設選項、讓BlueXP為您建立角色。

    如果您偏好使用自己的原則、就必須符合 "有關節點和 HA 中介器的原則要求 Cloud Volumes ONTAP"。

16. 授權：視Cloud Volumes ONTAP 需要變更此版本、並選取執行個體類型和執行個體租賃。

    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 。

17. 基礎儲存資源：選擇磁碟類型、設定基礎儲存設備、然後選擇是否要啟用資料分層。

    請注意下列事項：

    - 磁碟類型適用於初始磁碟區（和Aggregate）。您可以為後續磁碟區（和Aggregate）選擇不同的磁碟類型。
    - 如果您選擇GP3或IO1磁碟、則BlueXP會使用AWS中的彈性磁碟區功能、視需要自動增加基礎儲存磁碟容量。您可以根據儲存需求來選擇初始容量、Cloud Volumes ONTAP 並在部署完畢後加以修改。 "深入瞭解AWS對彈性磁碟區的支援"。
    - 如果您選擇gp2或ST1磁碟、則可以針對初始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、選取磁碟大小。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。
    - 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。

"瞭解資料分層的運作方式"。

18. *寫入速度與WORM *：

a. 如果需要、請選擇*正常*或*高速*寫入速度。

"深入瞭解寫入速度"。

b. 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。

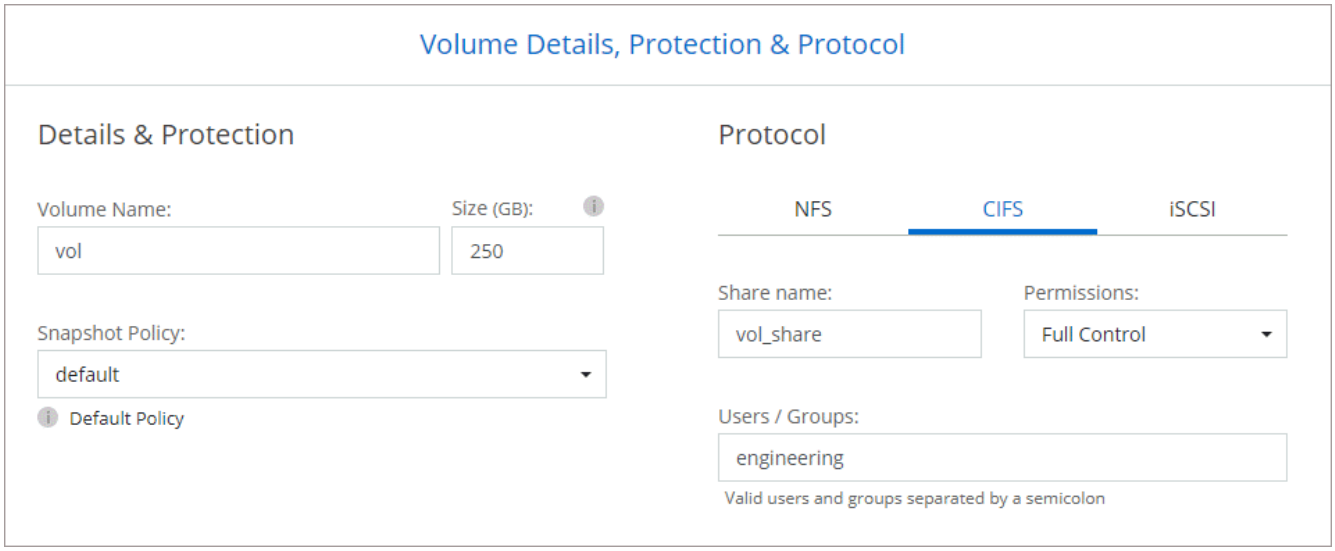
19. * 建立 Volume * ：輸入新磁碟區的詳細資料、或按一下 * 跳過 * 。

"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：



20. * CIFS 設定 * ：如果您選取 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。
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」。如果您將 AWS 託管 Microsoft AD 設定為 AD 伺服器 Cloud Volumes ONTAP 以供使用、您應該在此欄位中輸入 * OID=computers,O=corp* 。
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。

21. * 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、並編輯磁碟區分層原則。

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

22. * 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*以檢閱有關支援和BlueXP將購買的AWS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會啟動Cloud Volumes ONTAP 「更新HA配對」。您可以追蹤時間表的進度。

如果您在啟動 HA 配對時遇到任何問題、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 **AWS Secret Cloud** 和 **Top Secret Cloud** 地區部署 **Cloud Volumes ONTAP**

與標準 AWS 區域類似、您可以在中使用 BlueXP "AWS Secret Cloud" 和 "AWS Top Secret Cloud" 部署 Cloud Volumes ONTAP 、為您的雲端儲存設備提供企業級功能。AWS Secret Cloud 和 Top Secret Cloud 是美國特有的封閉區域智慧社群：本頁的指示僅適用於 AWS Secret Cloud 和 Top Secret Cloud 地區使用者。

開始之前

開始之前、請先檢閱 AWS Secret Cloud 和 Top Secret Cloud 中支援的版本、並瞭解 BlueXP 中的私有模式。

- 檢閱 AWS Secret Cloud 和 Top Secret Cloud 中支援的下列版本：
  - Cloud Volumes ONTAP 9.12.1 P2
  - Connector 3.9.32 版

    Connector是在Cloud Volumes ONTAP AWS中部署和管理功能所需的軟體。您將從安裝在Connector執行個體上的軟體登入BlueXP。AWS Secret Cloud 和 Top Secret Cloud 不支援 BlueXP 的 SaaS 網站。
- 瞭解私有模式

  在 AWS Secret Cloud 和 Top Secret Cloud 中、 BlueXP 以 _private 模式運作。在私有模式中、無法連線至 BlueXP SaaS 層。使用者可從 Connector 提供的網路型主控台、而非從 SaaS 層、在本機存取 BlueXP 。

  若要深入瞭解私有模式的運作方式、請參閱 "BlueXP 私有部署模式"。

步驟 **1** ：設定您的網路

設定AWS網路、Cloud Volumes ONTAP 使其能夠正常運作。

步驟

1. 選擇要在其中啟動Connector執行個體和Cloud Volumes ONTAP 例項的VPC和子網路。

2. 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。
3. 設定 S3 服務的 VPC 端點。

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

步驟 **2** ：設定權限

設定 IAM 原則和角色、為 Connector 和 Cloud Volumes ONTAP 提供在 AWS Secret Cloud 或 Top Secret Cloud 中執行動作所需的權限。

您需要IAM原則和IAM角色來執行下列各項：

- Connector執行個體
- 執行個體Cloud Volumes ONTAP
- 對於 HA 配對、 Cloud Volumes ONTAP HA 中介執行個體（如果您想要部署 HA 配對）

步驟

1. 移至AWS IAM主控台、然後按一下* Policies *。
2. 建立Connector執行個體的原則。

   您可以建立這些原則來支援 AWS 環境中的 S3 儲存區。稍後建立貯體時、請確定貯體名稱以開頭 `fabric-pool-`。這項要求同時適用於 AWS Secret Cloud 和 Top Secret Cloud 地區。

秘密區域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
```

```
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
```

```
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

最高機密區域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
```

```
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
```

```
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
```

```
        ]
}
```

3. 建立Cloud Volumes ONTAP 一套適用於此功能的原則。

秘密區域

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

最高機密區域

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

對於 HA 配對、如果您打算部署 Cloud Volumes ONTAP HA 配對、請為 HA 協調器建立原則。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

4. 使用角色類型Amazon EC2建立IAM角色、並附加您在先前步驟中建立的原則。

   建立角色：

   與原則類似、您應該有一個用於連接器的 IAM 角色、另一個用於 Cloud Volumes ONTAP 節點。
   對於 HA 配對：與原則類似、您應該有一個用於連接器的 IAM 角色、一個用於 Cloud Volumes ONTAP 節點、另一個用於 HA 協調器（如果您想要部署 HA 配對）。

   選取角色：

   啟動Connector執行個體時、您必須選取Connector IAM角色。從 BlueXP 建立 Cloud Volumes ONTAP 工作環境時、您可以為 Cloud Volumes ONTAP 選取 IAM 角色。
   對於 HA 配對、您可以在從 BlueXP 建立 Cloud Volumes ONTAP 工作環境時、為 Cloud Volumes ONTAP 和 HA 協調器選取 IAM 角色。

步驟 3 ：設定 AWS KMS

如果您想搭配 Cloud Volumes ONTAP 使用 Amazon 加密、請確保 AWS 金鑰管理服務（ KMS ）符合要求。

步驟

1. 請確定您的帳戶或其他AWS帳戶中存在使用中的客戶主金鑰（CMK）。

   CMK 可以是 AWS 託管的 CMK 、也可以是客戶託管的 CMK 。

2. 如果CMK位於AWS帳戶中、而該帳戶與您打算部署Cloud Volumes ONTAP 的帳戶不同、則您需要取得該金鑰的ARN。

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

3. 將Connector執行個體的IAM角色新增至CMK的主要使用者清單。

如此一來、BlueXP就有權將CMK搭配Cloud Volumes ONTAP 使用。

步驟 4 ：安裝 Connector 並設定 BlueXP

在開始使用 BlueXP 在 AWS 中部署 Cloud Volumes ONTAP 之前、您必須先安裝並設定 BlueXP Connector 。Connector讓BlueXP能夠管理公有雲環境中的資源和程序（包括Cloud Volumes ONTAP 整個過程）。

步驟

1. 取得由憑證授權單位（CA）簽署的根憑證（採用隱私權增強型郵件（PEF）Base - 64編碼的X・509格式）。請參閱貴組織的原則與程序、以取得該憑證。

   對於 AWS Secret Cloud 地區、您應該上傳 `NSS Root CA 2` 憑證、以及 Top Secret Cloud 的 `Amazon Root CA 4` 憑證：請務必僅上傳這些憑證、而非整個鏈結。憑證鏈結的檔案很大、上傳可能會失敗。如果您有其他憑證、您可以在稍後上傳、如下一步所述。

   您必須在設定程序期間上傳憑證。透過HTTPS傳送要求至AWS時、BlueXP會使用信任的憑證。

2. 啟動Connector執行個體：
   a. 前往適用於BlueXP的AWS Intelligence Community Marketplace頁面。
   b. 在「自訂啟動」索引標籤上、選擇從EC2主控台啟動執行個體的選項。
   c. 依照提示設定執行個體。

      設定執行個體時請注意下列事項：

      - 建議使用T3.xLarge。
      - 您必須選擇設定權限時所建立的 IAM 角色。
      - 您應該保留預設的儲存選項。
      - Connector所需的連線方法如下：SSH、HTTP和HTTPS。
3. 從連線至Connector執行個體的主機設定BlueXP：
   a. 開啟網頁瀏覽器並輸入 https://ipaddress 其中 ipaddress 是您安裝 Connector 的 Linux 主機的 IP 位址。
   b. 指定用於連線至AWS服務的Proxy伺服器。
   c. 上傳您在步驟1中取得的憑證。
   d. 選取 * 設定新的 BlueXP* 、然後依照提示設定系統。
      - 系統詳細資料：輸入Connector的名稱及您的公司名稱。
      - 建立管理使用者：建立系統的管理使用者。

        此使用者帳戶在本機系統上執行。無法透過BlueXP連線至驗證0服務。

      - * 審查 * ：檢閱詳細資料、接受授權合約、然後選取 * 設定 * 。
   e. 若要完成CA簽署憑證的安裝、請從EC2主控台重新啟動Connector執行個體。
4. 重新啟動Connector之後、請使用您在設定精靈中建立的系統管理員使用者帳戶登入。

步驟 **5** ：（選用）安裝私有模式憑證

此步驟對於 AWS Secret Cloud 和 Top Secret Cloud 地區為選用步驟、只有在您有其他憑證（除了您在前一步驟中安裝的根憑證）時才需要。

步驟

1. 列出現有的已安裝憑證。
   a. 若要收集 occm Container 泊塢視窗 ID （識別名稱為「 DS-occm-1 」）、請執行下列命令：

   ```
   docker ps
   ```

   b. 若要進入 occm 容器、請執行下列命令：

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   c. 若要從 "trust 儲存區密碼 " 環境變數收集密碼、請執行下列命令：

   ```
   env
   ```

   d. 若要列出信任存放區中所有已安裝的憑證、請執行下列命令、並使用上一步收集的密碼：

   ```
   keytool -list -v -keystore occm.truststore
   ```

2. 新增憑證。
   a. 若要收集 occm Container 泊塢視窗 id （識別名稱為「 DS-occm-1 」）、請執行下列命令：

   ```
   docker ps
   ```

   b. 若要進入 occm 容器、請執行下列命令：

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   將新的憑證檔案儲存在內。

   c. 若要從 "trust 儲存區密碼 " 環境變數收集密碼、請執行下列命令：

   ```
   env
   ```

   d. 若要將憑證新增至信任存放區、請執行下列命令、並使用上一步的密碼：

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. 若要檢查是否已安裝憑證、請執行下列命令：

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. 若要結束 occm 容器、請執行下列命令：

```
exit
```

g. 若要重設 occm 容器、請執行下列命令：

```
docker restart <docker-id>
```

步驟 **6** ：新增授權至 **BlueXP** 數位錢包

如果您向 NetApp 購買授權、則需要將其新增至 BlueXP 數位錢包、以便在建立新的 Cloud Volumes ONTAP 系統時選取授權。數位錢包會將這些授權識別為未指派。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 按一下*未指派*。
4. 按一下「新增未指派的授權」。
5. 輸入授權的序號或上傳授權檔案。
6. 如果您還沒有使用許可檔案、則需要從 netapp.com 手動上傳使用許可檔案。
   a. 前往 "NetApp 授權檔案產生器" 並使用您的 NetApp 支援網站認證資料登入。
   b. 輸入您的密碼、選擇產品、輸入序號、確認您已閱讀並接受隱私權政策、然後按一下 * 提交 * 。
   c. 選擇您要透過電子郵件或直接下載來接收 serialNumber.NLF Json 檔案。
7. 按一下「 * 新增授權 * 」。

結果

BlueXP 將授權新增至數位錢包。授權將被識別為未指派、直到您將其與新Cloud Volumes ONTAP 的一套系統關聯為止。之後、授權便會移至數位錢包中的 BYOL 標籤。

步驟 **7** ：從 **BlueXP** 啟動 **Cloud Volumes ONTAP**

您可以在 BlueXP 中建立新的工作環境、在 AWS Secret Cloud 和 Top Secret Cloud 中啟動 Cloud Volumes ONTAP 執行個體。

開始之前

對於 HA 配對、必須有金鑰配對、才能啟用金鑰型 SSH 驗證給 HA 中介者。

步驟

1. 在「工作環境」頁面上、按一下「新增工作環境」。
2. 在 * 建立 * 下、選取 Cloud Volumes ONTAP 。

   對於 HA ：在 * 建立 * 下、選取 Cloud Volumes ONTAP 或 Cloud Volumes ONTAP HA 。
3. 完成精靈中的步驟以啟動Cloud Volumes ONTAP 整套系統。

> 在精靈中進行選擇時、請勿在 * 服務 * 下選取 * 資料感知與法規遵循 * 和 * 備份至雲端 * 。在 * 預先設定的封裝 * 下、選取 * 僅變更組態 * 、並確定您尚未選取任何其他選項。AWS Secret Cloud 和 Top Secret Cloud 地區不支援預先設定的套件、如果選取、您的部署將會失敗。

在多個可用性區域中部署 **Cloud Volumes ONTAP HA** 的注意事項

當您完成 HA 配對精靈時、請注意下列事項。

- 當您在多個可用性區域（ AZs ）中部署 Cloud Volumes ONTAP HA 時、應該設定傳輸閘道。請參閱 "設定 AWS 傳輸閘道"。
- 部署組態如下、因為在發佈時、 AWS Top Secret Cloud 只有兩個 AZs 可用：
  - 節點1：可用度區域A
  - 節點2：可用度區域B
  - 中介：可用度區域A或B

在單一和 **HA** 節點上部署 **Cloud Volumes ONTAP** 的注意事項

完成精靈時請注意下列事項：

- 您應該保留預設選項、以使用產生的安全性群組。

  預先定義的安全性群組包含Cloud Volumes ONTAP 一些規則、這些規則是讓整個公司順利運作所需的。如果您需要使用自己的安全性、請參閱下方的安全性群組一節。
- 您必須選擇在準備AWS環境時所建立的IAM角色。
- 基礎AWS磁碟類型適用於初始Cloud Volumes ONTAP 的流通量。

  您可以為後續磁碟區選擇不同的磁碟類型。
- AWS磁碟的效能與磁碟大小有關。

  您應該選擇能提供所需持續效能的磁碟大小。如需EBS效能的詳細資訊、請參閱AWS文件。
- 磁碟大小是系統上所有磁碟的預設大小。

> 如果您稍後需要不同的大小、可以使用「進階配置」選項來建立使用特定大小磁碟的集合體。

結果

BlueXP會啟動Cloud Volumes ONTAP 這個執行個體。您可以追蹤時間表的進度。

步驟 **8** ：安裝資料分層的安全性憑證

您必須手動安裝安全性憑證、才能在 AWS Secret Cloud 和 Top Secret Cloud 區域中進行資料分層。

開始之前

1. 建立 S3 儲存區。

   請確定貯體名稱以開頭 `fabric-pool-`. 例如 `fabric-pool-testbucket`。

2. 保留您安裝的根憑證 `step 4` 方便。

步驟

1. 從您安裝的根憑證複製文字 `step 4`。
2. 使用 CLI 安全連線至 Cloud Volumes ONTAP 系統。
3. 安裝根憑證。您可能需要按下 `ENTER` 金鑰多次：

```
security certificate install -type server-ca -cert-name <certificate-
name>
```

4. 出現提示時、輸入完整複製的文字、包括和寄件者 `----- BEGIN CERTIFICATE -----` 至 `----- END CERTIFICATE -----`。
5. 保留 CA 簽署數位憑證的複本、以供日後參考。
6. 保留 CA 名稱和憑證序號。
7. 為 AWS Secret Cloud 和 Top Secret Cloud 區域設定物件存放區： `set -privilege advanced -confirmations off`
8. 執行此命令以設定物件存放區。

   所有 Amazon 資源名稱（ ARN ）都應以後綴為後綴 `-iso-b`、例如 `arn:aws-iso-b`。例如、如果某個資源需要區域的 ARN 、對於 Top Secret Cloud 、請使用命名慣例 AS `us-iso-b` 適用於 `-server` 旗標。若為 AWS Secret Cloud 、請使用 `us-iso-b-1`。

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. 確認物件存放區已成功建立： `storage aggregate object-store show -instance`
10. 將物件存放區附加至 Aggregate 。每個新的集合體都應該重複此步驟： `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

開始使用Microsoft Azure

Azure中的功能快速入門Cloud Volumes ONTAP

只要幾個步驟、 Cloud Volumes ONTAP 就能開始使用適用於 Azure 的功能。


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 Azure 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"


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"。


設定您的網路

1. 確保您的 Vnet 和子網路可支援連接器與 Cloud Volumes ONTAP 支援的連接功能。
2. 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"。


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"
- "從 Azure Marketplace 建立 Connector"
- "在 Linux 主機上安裝 Connector 軟體"
- "BlueXP具備權限的功能"

在Cloud Volumes ONTAP Azure中規劃您的不一樣組態

在 Cloud Volumes ONTAP Azure 中部署時、您可以選擇符合工作負載需求的預先設定系統、也可以自行建立組態。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

大多數Microsoft Azure地區均支援此功能。Cloud Volumes ONTAP "檢視支援區域的完整清單"。

選擇支援的**VM**類型

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

"Azure支援Cloud Volumes ONTAP 的支援功能組態"

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。

"Azure的Cloud Volumes ONTAP 儲存限制"

在**Azure**中調整系統規模

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 VM 類型、磁碟類型和磁碟大小時、您應該注意幾個關鍵點：

虛擬機器類型

請查看中支援的虛擬機器類型 "發行說明 Cloud Volumes ONTAP" 然後檢閱每種受支援 VM 類型的詳細資料。請注意、每種 VM 類型都支援特定數量的資料磁碟。

- "Azure 文件：通用虛擬機器大小"
- "Azure 文件：記憶體最佳化的虛擬機器大小"

Azure磁碟類型搭配單一節點系統

當您建立 Cloud Volumes ONTAP 用於實現效能不均的磁碟區時、您需要選擇 Cloud Volumes ONTAP 底層的雲端儲存設備、以利將其用作磁碟。

單一節點系統可使用三種 Azure 託管磁碟：

- _Premium SSD 託管磁碟 _ 以更高的成本、為 I/O 密集的工作負載提供高效能。
- _ 標準 SSD 託管磁碟 _ 為需要低 IOPS 的工作負載提供一致的效能。
- 如果您不需要高 IOPS 、而且想要降低成本、那麼 _ 標準 HDD 託管磁碟 _ 是個不錯的選擇。

如需這些磁碟使用案例的其他詳細資料、請參閱 "Microsoft Azure 文件： Azure 提供哪些磁碟類型？"。

Azure磁碟類型搭配HA配對

HA系統使用優質的SSD共享託管磁碟、兩者都能以較高的成本為I/O密集型工作負載提供高效能。在9.12.1版本之前建立的HA部署會使用優質網頁。

Azure 磁碟大小

啟動 Cloud Volumes ONTAP 時、您必須選擇集合體的預設磁碟大小。BlueXP會將此磁碟大小用於初始Aggregate、以及當您使用簡易資源配置選項時所建立的任何其他集合體。您可以建立使用不同於預設磁碟大小的 Aggregate "使用進階配置選項"。

集合體中的所有磁碟大小必須相同。

在選擇磁碟大小時、您應該考量幾個因素。磁碟大小會影響您支付的儲存成本、您可以在集合體中建立的磁碟區大小、 Cloud Volumes ONTAP 可供使用的總容量、以及儲存效能。

Azure Premium Storage 的效能與磁碟大小有關。較大的磁碟可提供較高的 IOPS 和處理量。例如、選擇1個TiB磁碟可提供比500 GiB磁碟更好的效能、而且成本更高。

標準儲存設備的磁碟大小沒有效能差異。您應該根據所需的容量來選擇磁碟大小。

請參閱 Azure 、瞭解每個磁碟大小的 IOPS 與處理量：

- "Microsoft Azure ：託管磁碟定價"
- "Microsoft Azure ：網頁 Blobs 定價"

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 Azure中檢視系統資料的預設磁碟"。

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 Azure 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。

Azure 資訊	您的價值
區域	
虛擬網路（ vnet ）	
子網路	
網路安全群組（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。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。

Azure 的網路需求 Cloud Volumes ONTAP

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

需求 **Cloud Volumes ONTAP**

Azure 必須符合下列網路需求。

傳出網際網路存取

支援NetApp功能的支援節點需要外傳網際網路存取功能、此功能可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安全性群組允許連接埠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 嚴格的傳出規則以供支援、那麼Cloud Volumes ONTAP 您也必須確保支援透過連接埠3128建立_Outbound _連線的安全性群組。

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

IP位址

BlueXP會自動將所需數量的私有IP位址分配Cloud Volumes ONTAP 給Azure中的所有人。您必須確定網路有足夠的私有IP位址可用。

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 。

> 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。

單一節點系統的IP位址

BlueXP會將5或6個IP位址分配給單一節點系統：

- 叢集管理IP
- 節點管理IP
- SnapMirror的叢集間IP
- NFS/CIFS IP
- iSCSI IP

> iSCSI IP可透過iSCSI傳輸協定提供用戶端存取。系統也會將其用於其他重要的網路工作流程。此LIF為必填項目、不應刪除。

- SVM管理（選用-預設為未設定）

HA配對的IP位址

在部署期間、BlueXP會將IP位址分配給4個NIC（每個節點）。

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

網卡0

- 節點管理IP
- 叢集間IP
- iSCSI IP

> iSCSI IP可透過iSCSI傳輸協定提供用戶端存取。系統也會將其用於其他重要的網路工作流程。此LIF為必填項目、不應刪除。

網卡1

- 叢集網路IP

*網卡2 *

- 叢集互連IP（HA IC）
- NIC 3 *
- Pageblob NIC IP（磁碟存取）

NIC 3僅適用於使用網頁BLOB儲存設備的HA部署。

上述IP位址不會在容錯移轉事件上移轉。

此外、還設定4個前端IP（FIPS）在容錯移轉事件上進行移轉。這些前端IP位於負載平衡器中。

- 叢集管理IP
- 節點A資料IP（NFS/CIFS）
- 節點B資料IP（NFS/CIFS）
- SVM管理IP

安全連線至**Azure**服務

根據預設、BlueXP會啟用Azure Private Link、以便Cloud Volumes ONTAP 在支援鏈接的情況下連接到支援鏈接的畫面和Azure網頁BLOB儲存帳戶。

在大多數情況下、您無需做任何事、因為BlueXP會為您管理Azure Private Link。但如果您使用Azure私有DNS、則必須編輯組態檔。您也應該瞭解Azure中的Connector位置需求。

您也可以視業務需求而停用「私有連結」連線。如果您停用連結、則BlueXP會設定Cloud Volumes ONTAP 使用服務端點的功能。

"深入瞭解如何搭配Cloud Volumes ONTAP 使用Azure私有連結或服務端點搭配使用"。

連線至其他**ONTAP** 的系統

若要在Cloud Volumes ONTAP Azure中的某個系統與ONTAP 其他網路中的某些系統之間複寫資料、您必須在Azure vnet與其他網路（例如您的公司網路）之間建立VPN連線。

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

HA互連的連接埠

一個包含HA互連的「支援功能」配對、可讓每個節點持續檢查其合作夥伴是否正常運作、並鏡射另一個非揮發性記憶體的記錄資料。Cloud Volumes ONTAPHA互連使用TCP連接埠10006進行通訊。

依預設、HA互連生命體之間的通訊會開啟、而且此連接埠沒有安全性群組規則。但是、如果您在HA互連生命期之間建立防火牆、則必須確保TCP流量已開啟連接埠10006、如此HA配對才能正常運作。

Azure資源群組中只有一組**HA**配對

您必須使用_Dedicated資源群組來處理Cloud Volumes ONTAP 您在Azure中部署的每一組EHA。資源群組僅支援一個HA配對。

如果您嘗試在Cloud Volumes ONTAP Azure資源群組中部署第二個「鏈接HA配對」、則BlueXP會遇到連線問題。

安全性群組規則

BlueXP會建立Azure安全性群組、其中包含Cloud Volumes ONTAP 了順利運作所需的傳入和傳出規則。您可能想要參照連接埠進行測試、或是想要使用自己的安全性群組。

適用於此功能的安全性群組 Cloud Volumes ONTAP 需要傳入和傳出規則。

正在尋找Connector的相關資訊？ "檢視Connector的安全群組規則"

單一節點系統的傳入規則

當您建立工作環境並選擇預先定義的安全性群組時、可以選擇允許下列其中一項的流量：

- 僅限所選**vnet**：傳入流量的來源是vnet的子網路範圍、Cloud Volumes ONTAP 以及連接器所在vnet的子網路範圍。這是建議的選項。
- 所有**VNet**：傳入流量的來源為0.00.0.0/0 IP範圍。

優先順序和名稱	連接埠與傳輸協定	來源與目的地	說明
1000 inbound SSH	22 TCP	任意	SSH 存取叢集管理 LIF 的 IP 位址或節點管理 LIF
1001 inbound http	80 TCP	任意	使用叢集管理 LIF 的 IP 位址、以 HTTP 存取 System Manager Web 主控台
1002inbound （入站）_111_TCP	111 TCP	任意	遠端程序需要 NFS
1003 inbound _111_udp	111 udp	任意	遠端程序需要 NFS
1004 inbound （傳入）_139	139 TCP	任意	CIFS 的 NetBios 服務工作階段
1005inbound （傳入）_161-162 _tcp	161-162 TCP	任意	簡單的網路管理傳輸協定
1006 inbound （傳入）_161-162 _udp	161-162 udp	任意	簡單的網路管理傳輸協定
1007 inbound _443	443 TCP	任意	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
1008 inbound _445	445 TCP	任意	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
1009 inbound _6335_tcp	635 TCP	任意	NFS 掛載
1010 inbound _6335_udp	635 udp	任意	NFS 掛載
1011 inbound （傳入）_749	749 TCP	任意	Kerberos

優先順序和名稱	連接埠與傳輸協定	來源與目的地	說明
1012 inbound _2049_tcp	2049 TCP	任意	NFS 伺服器精靈
1013 inbound _2049_udp	2049 udp	任意	NFS 伺服器精靈
1014 inbound （傳入）_3260	3260 TCP	任意	透過 iSCSI 資料 LIF 存取 iSCSI
1015 inbound _4045-4046_tcp	4045-4046 TCP	任意	NFS 鎖定精靈和網路狀態監控
1016 inbound _4045-4046_udp	4045-4046 udp	任意	NFS 鎖定精靈和網路狀態監控
1017 inbound _10000	10000 TCP	任意	使用 NDMP 備份
1018 inbound （傳入）_11104-11105	11104-11105 TCP	任意	SnapMirror 資料傳輸
3000 inbound 拒絕 _all_tcp	任何連接埠 TCP	任意	封鎖所有其他 TCP 傳入流量
3001 inbound 拒絕 _all_udp	任何連接埠 udp	任意	封鎖所有其他的 UDP 傳入流量
65000 AllowVnetInBound	任何連接埠任何傳輸協定	虛擬網路至虛擬網路	來自 vnet 的傳入流量
65001 AllowAzureLoad BalancerInBound	任何連接埠任何傳輸協定	將 AzureLoadBalancer 移至任何	Azure Standard 負載平衡器的資料流量
65500 DenyAllInBound	任何連接埠任何傳輸協定	任意	封鎖所有其他傳入流量

HA 系統的傳入規則

當您建立工作環境並選擇預先定義的安全性群組時、可以選擇允許下列其中一項的流量：

- 僅限所選**vnet**：傳入流量的來源是vnet的子網路範圍、Cloud Volumes ONTAP 以及連接器所在vnet的子網路範圍。這是建議的選項。
- 所有**VNet**：傳入流量的來源為0.00.0.0/0 IP範圍。

HA 系統的傳入規則少於單一節點系統、因為傳入資料流量會流經 Azure Standard Load Balancer 。因此、來自負載平衡器的流量應開啟、如「 AllowAzureLoadBalancerInBound 」規則所示。

優先順序和名稱	連接埠與傳輸協定	來源與目的地	說明
100 inbound （傳入）_443	443 任何傳輸協定	任意	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
101 inbound （傳入）_111_TCP	111 任何傳輸協定	任意	遠端程序需要 NFS
102 inbound _2049_tcp	2049 任何傳輸協定	任意	NFS 伺服器精靈
111 inbound （傳入）_ssh	22 任何傳輸協定	任意	SSH 存取叢集管理 LIF 的 IP 位址或節點管理 LIF

優先順序和名稱	連接埠與傳輸協定	來源與目的地	說明
121inbound （傳入） _53	53 任何傳輸協定	任意	DNS 與 CIFS
65000 AllowVnetInBound	任何連接埠任何傳輸協定	虛擬網路至虛擬網路	來自 vnet 的傳入流量
65001 AllowAzureLoad BalancerInBound	任何連接埠任何傳輸協定	將 AzureLoadBalancer 移至任何	Azure Standard 負載平衡器的資料流量
65500 DenyAllInBound	任何連接埠任何傳輸協定	任意	封鎖所有其他傳入流量

傳出規則

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。

連接埠	傳輸協定	目的
全部	所有 TCP	所有傳出流量
全部	所有的 udp	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	連接埠	傳輸協定	來源	目的地	目的
Active Directory	88	TCP	節點管理 LIF	Active Directory 樹系	Kerberos V 驗證
	137.	UDP	節點管理 LIF	Active Directory 樹系	NetBios 名稱服務
	138	UDP	節點管理 LIF	Active Directory 樹系	NetBios 資料報服務
	139.	TCP	節點管理 LIF	Active Directory 樹系	NetBios 服務工作階段
	389	TCP 與 UDP	節點管理 LIF	Active Directory 樹系	LDAP
	445	TCP	節點管理 LIF	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	464.64	TCP	節點管理 LIF	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	464.64	UDP	節點管理 LIF	Active Directory 樹系	Kerberos 金鑰管理
	749	TCP	節點管理 LIF	Active Directory 樹系	Kerberos V 變更與設定密碼（ RPCSEC_GSS ）
	88	TCP	資料 LIF （ NFS 、 CIFS 、 iSCSI ）	Active Directory 樹系	Kerberos V 驗證
	137.	UDP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 名稱服務
	138	UDP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 資料報服務
	139.	TCP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 服務工作階段
	389	TCP 與 UDP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	LDAP
	445	TCP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	464.64	TCP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	464.64	UDP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos 金鑰管理
	749	TCP	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	連接埠	傳輸協定	來源	目的地	目的
組態備份	HTTP	80	節點管理 LIF	\http ：//Wese/occm/offboxconfig <connector-IP-address>	將組態備份傳送至Connector。 "深入瞭解組態備份檔案"。
DHCP	68	UDP	節點管理 LIF	DHCP	第一次設定的 DHCP 用戶端
DHCPS	67	UDP	節點管理 LIF	DHCP	DHCP 伺服器
DNS	53.	UDP	節點管理 LIF 與資料 LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	18600 – 18699	TCP	節點管理 LIF	目的地伺服器	NDMP 複本
SMTP	25	TCP	節點管理 LIF	郵件伺服器	可以使用 SMTP 警示 AutoSupport 來執行功能
SNMP	161.	TCP	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	161.	UDP	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	162%	TCP	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	162%	UDP	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
SnapMirror	11104.	TCP	叢集間 LIF	叢集間 LIF ONTAP	管理 SnapMirror 的叢集間通訊工作階段
	11105.	TCP	叢集間 LIF	叢集間 LIF ONTAP	SnapMirror 資料傳輸
系統記錄	514	UDP	節點管理 LIF	系統記錄伺服器	系統記錄轉送訊息

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"
- "Azure中的安全性群組規則"

設定Cloud Volumes ONTAP 支援使用Azure中客戶管理的金鑰

資料會使用在Cloud Volumes ONTAP Azure中的功能自動加密 "Azure 儲存服務加密" 使用Microsoft管理的金鑰。但您可以改用自己的加密金鑰、只要執行本頁的步驟即可。

資料加密總覽

Azure中的資料會使用自動加密Cloud Volumes ONTAP "Azure 儲存服務加密"。預設實作使用Microsoft管理的金鑰。無需設定。

如果您想要使用客戶管理的支援服務金鑰Cloud Volumes ONTAP 搭配使用、則必須完成下列步驟：

1. 從Azure建立金鑰保存庫、然後在該保存庫中產生金鑰

2. 從BlueXP中、使用API建立Cloud Volumes ONTAP 使用金鑰的功能不受影響的環境

金鑰旋轉

如果您建立新版的金鑰、Cloud Volumes ONTAP 則更新版本會自動使用最新的金鑰版本。

資料加密方式

BlueXP 使用磁碟加密集、可透過託管磁碟管理加密金鑰、而非分頁式分頁。任何新的資料磁碟也會使用相同的磁碟加密集。較低版本將使用Microsoft管理的金鑰、而非客戶管理的金鑰。

建立Cloud Volumes ONTAP 一個設定為使用客戶管理金鑰的功能完善的支援環境之後Cloud Volumes ONTAP 、即可將下列資料加密。

組態**Cloud Volumes ONTAP**	用於金鑰加密的系統磁碟	用於金鑰加密的資料磁碟
單一節點	• 開機 • 核心 • NVRAM	• 根目錄 • 資料
Azure HA 單一可用性區域、含頁面 Blobs	• 開機 • 核心 • NVRAM	無
Azure HA 單一可用性區域、含共用託管磁碟	• 開機 • 核心 • NVRAM	• 根目錄 • 資料
Azure HA 多個可用性區域、含共用託管磁碟	• 開機 • 核心 • NVRAM	• 根目錄 • 資料

所有的Azure儲存帳戶Cloud Volumes ONTAP 均使用客戶管理的金鑰進行加密。如果您想要在建立儲存帳戶期間加密、則必須在CVO建立要求中建立並提供資源ID。這適用於所有類型的部署。如果您未提供、儲存帳戶仍會加密、但BlueXP會先使用Microsoft管理的金鑰加密來建立儲存帳戶、然後再更新儲存帳戶以使用客戶管理的金鑰。

建立使用者指派的託管身分識別

您可以選擇建立稱為使用者指派之託管身分識別的資源。這樣做可讓您在建立 Cloud Volumes ONTAP 工作環境時加密儲存帳戶。建議您在建立金鑰資料保險箱和產生金鑰之前先建立此資源。

資源具有以下 ID ： `userassignedidentity`。

步驟

1. 在 Azure 中、前往 Azure 服務並選取 * 託管身分識別 * 。

2. 按一下「 * 建立 * 」。
3. 提供下列詳細資料：
   - * 訂閱 * ：選擇訂閱。我們建議您選擇與 Connector 訂閱相同的訂閱。
   - * 資源群組 * ：使用現有的資源群組或建立新的資源群組。
   - * 區域 * ：您也可以選擇與 Connector 相同的區域。
   - * 名稱 * ：輸入資源的名稱。
4. 您也可以新增標記。
5. 按一下「 * 建立 * 」。

建立金鑰保存庫並產生金鑰

金鑰庫必須位於您計畫建立Cloud Volumes ONTAP 此系統的同一個Azure訂閱和地區。

如果您 建立使用者指派的託管身分識別在建立金鑰資料保險箱時、您也應該為金鑰資料保險箱建立存取原則。

步驟

1. "在您的Azure訂閱中建立金鑰庫"。

   請注意金鑰庫的下列需求：

   - 金鑰保存庫必須與Cloud Volumes ONTAP 該系統位於相同的區域。
   - 應啟用下列選項：
     - 軟刪除（此選項預設為啟用、但不可停用）
     - 清除保護
     - 適用於**Volume**加密的**Azure**磁碟加密（適用於多個區域中的單一節點系統或HA配對）
   - 如果您建立使用者指派的託管身分識別、則應啟用下列選項：
     - * 資料保險箱存取原則 *
2. 如果您選取了 Vault 存取原則、請按一下「建立」來建立金鑰資料保險箱的存取原則。如果沒有、請跳至步驟 3 。
   a. 選取下列權限：
      - 取得
      - 清單
      - 解密
      - 加密
      - 解開密鑰
      - 換行鍵
      - 驗證
      - 簽署
   b. 選取使用者指派的託管身分識別（資源）做為主體。

c. 檢閱並建立存取原則。

3. "在金鑰保存庫中產生金鑰"。

   請注意金鑰的下列需求：

   - 金鑰類型必須為* RSA*。
   - 建議的RSA金鑰大小為* 2048*、但支援其他大小。

建立使用加密金鑰的工作環境

建立金鑰庫並產生加密金鑰之後、您可以建立Cloud Volumes ONTAP 新的、設定為使用金鑰的整套系統。使用BlueXP API可支援這些步驟。

必要權限

如果您想將客戶管理的金鑰與單一節點Cloud Volumes ONTAP 的一套系統整合、請確認BlueXP Connector具有下列權限：

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"檢視最新的權限清單"

步驟

1. 請使用下列BlueXP API呼叫、取得Azure訂閱中的金鑰保存清單。

   對於HA配對：「Get /azure/ha/mata/Vault」

   對於單一節點：「Get /azure/VSA/中繼資料/資料保存」

   請記下*名稱*和*資源群組*。您需要在下一步中指定這些值。

   "深入瞭解此API呼叫"。

2. 使用下列BlueXP API呼叫取得資料保險箱內的金鑰清單。

   對於HA配對：「Get /azure/ha/matmata/keys/Vault」

   對於單一節點：「Get /azure/VSA/中繼資料/金鑰庫」

   請記下*金鑰名稱*。您需要在下一步中指定該值（連同資料保險箱名稱）。

   "深入瞭解此API呼叫"。

3. 使用Cloud Volumes ONTAP 下列BlueXP API呼叫建立一個系統。

   a. 對於HA配對：

      「POST /azure/ha/辦公 環境」

      申請本文必須包含下列欄位：

      ```
      "azureEncryptionParameters": {
                    "key": "keyName",
                    "vaultName": "vaultName"
      }
      ```

      包括 "userAssignedIdentity": " userAssignedIdentityId" 如果您建立此資源以用於儲存帳戶加密、請輸入此欄位。

      "深入瞭解此API呼叫"。

   b. 對於單一節點系統：

      「POST /azure/VSA/工作環境」

      申請本文必須包含下列欄位：

      ```
      "azureEncryptionParameters": {
                    "key": "keyName",
                    "vaultName": "vaultName"
      }
      ```

      包括 "userAssignedIdentity": " userAssignedIdentityId" 如果您建立此資源以用於儲存帳戶加密、請輸入此欄位。

   "深入瞭解此API呼叫"。

結果

您有一個Cloud Volumes ONTAP 全新的支援系統、可設定使用客戶管理的金鑰進行資料加密。

在Cloud Volumes ONTAP Azure中設定for NetApp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

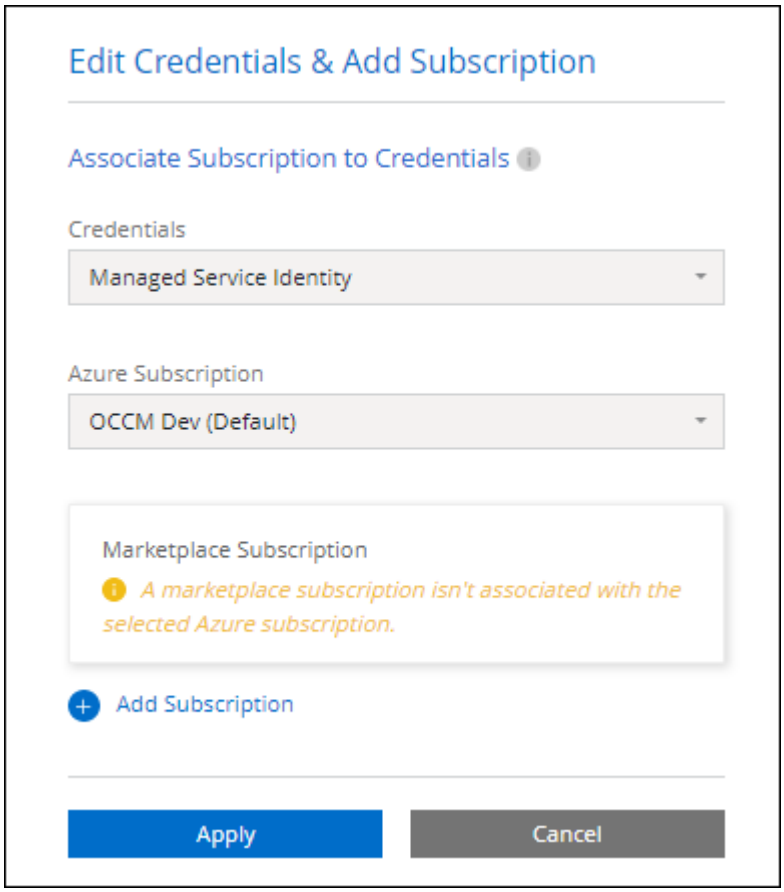
選擇Freemium產品、即可免費使用Cloud Volumes ONTAP 多達500 GiB的配置容量。 "深入瞭解Freemium產品"。

步驟

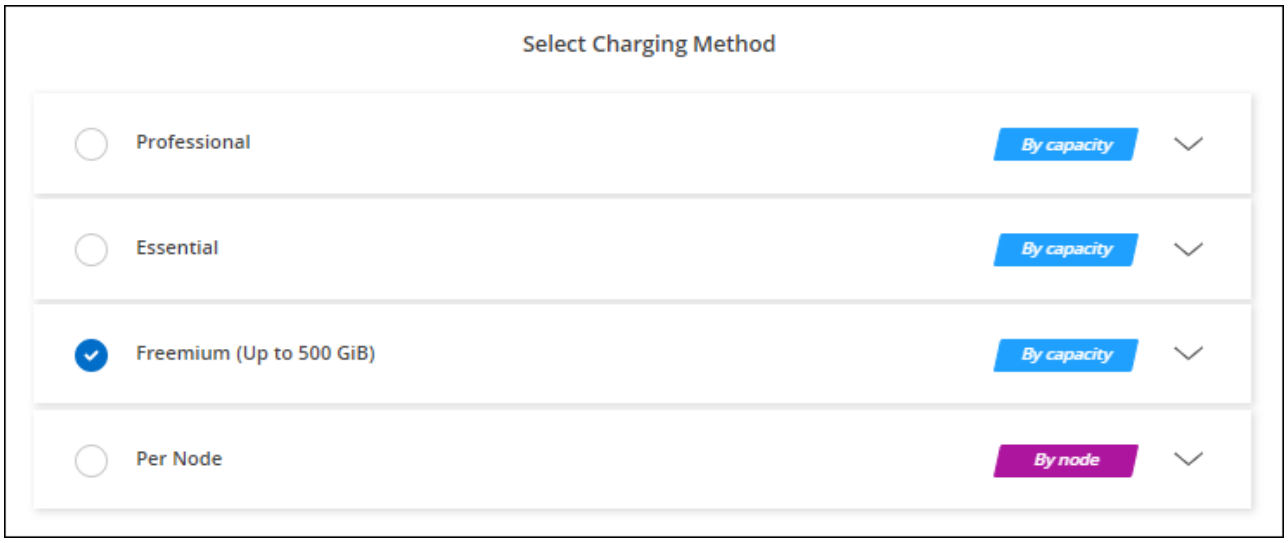
1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。

   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Azure 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"。



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



"請參閱Cloud Volumes ONTAP 逐步指示、以在Azure中推出《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）
- Azure Marketplace的每小時隨付隨付（PAYGO）訂閱
- 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"

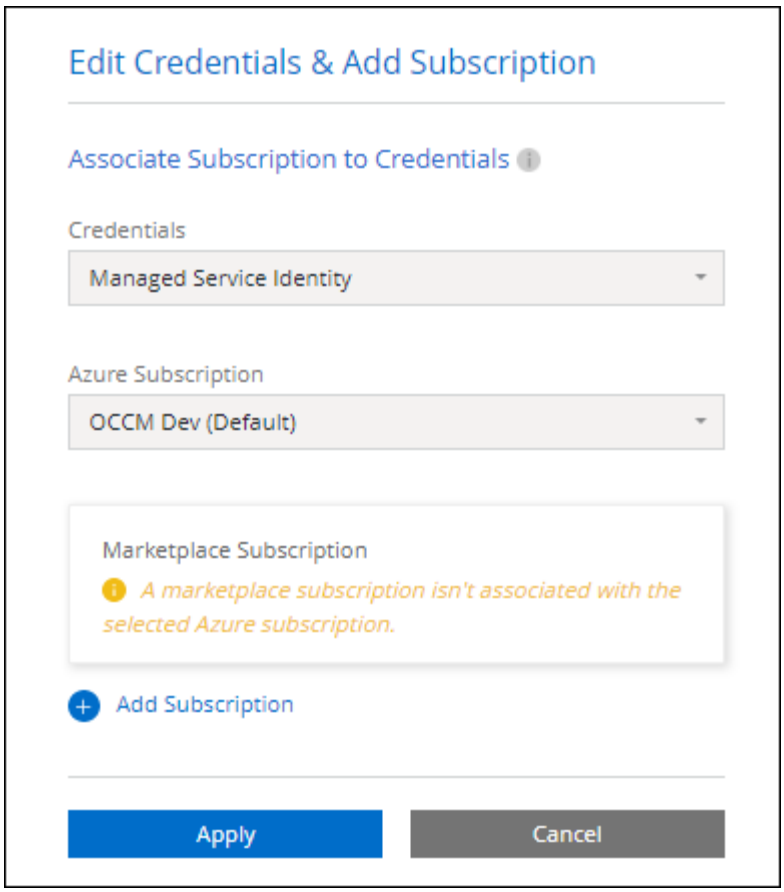
   BlueXP會自動查詢NetApp的授權服務、以取得NetApp 支援網站 與您的還原帳戶相關之授權的詳細資料。如果沒有錯誤、 BlueXP 會自動將授權新增至數位錢包。

   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"。

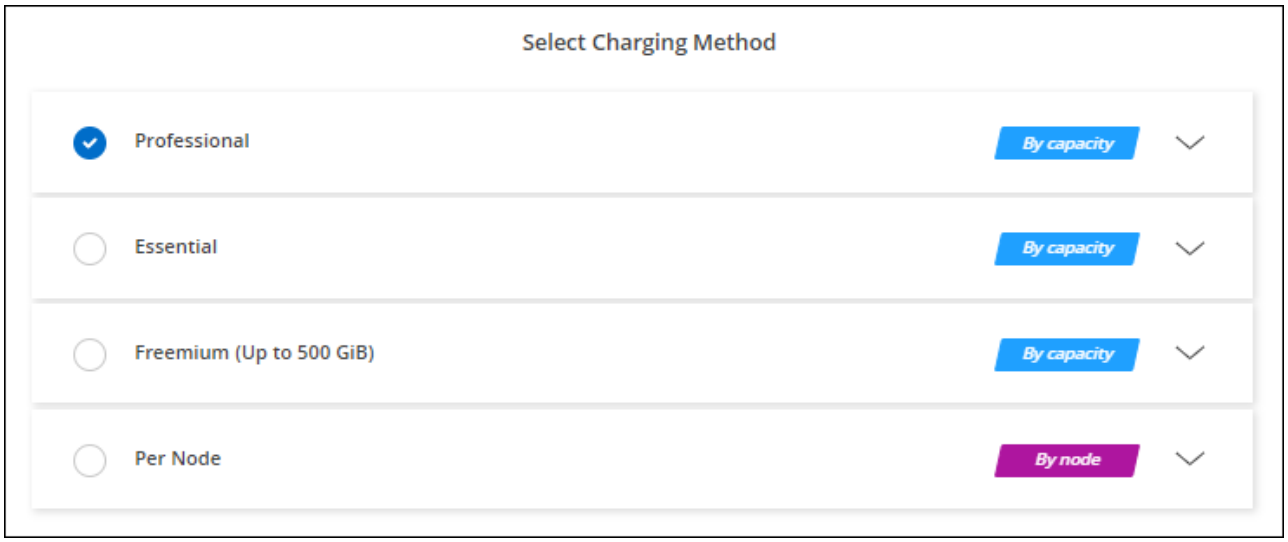
3. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。

   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Azure 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。



a. 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Cloud Volumes ONTAP 逐步指示、以在Azure中推出《功能不全》"。

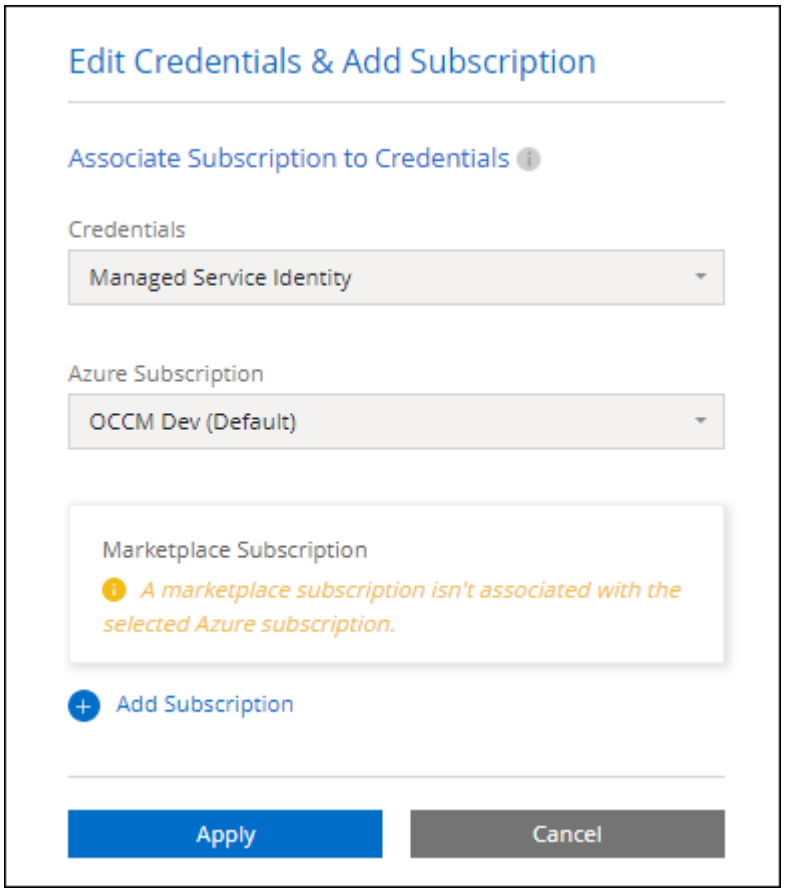
PAYGO訂閱

從雲端供應商的市場訂閱優惠、每小時支付一次。

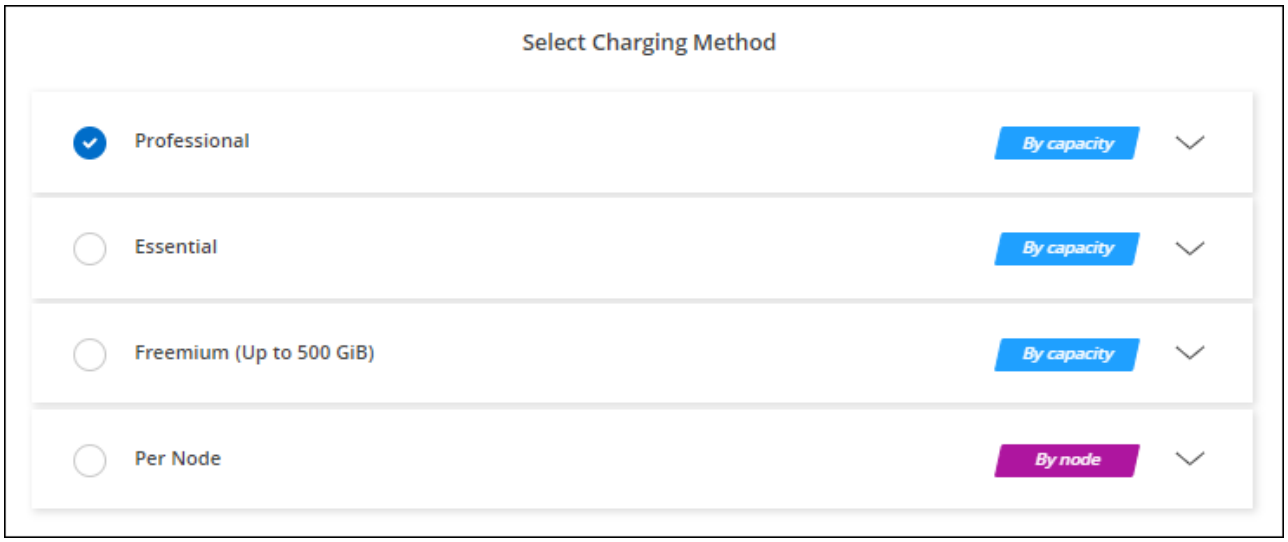
當您建立Cloud Volumes ONTAP 一個運作環境時、BlueXP會提示您訂閱Azure Marketplace提供的合約。該訂閱之後會與工作環境建立關聯、以便進行充電。您可以在其他工作環境中使用相同的訂閱。

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Azure 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Cloud Volumes ONTAP 逐步指示、以在Azure中推出《功能不全》"。

您可以從「設定」>「認證」頁面管理Azure Marketplace與Azure帳戶相關的訂閱。 "瞭解如何管理您的Azure帳戶和訂閱"

年度合約

購買年度合約、每年支付Cloud Volumes ONTAP 一份銷售費。

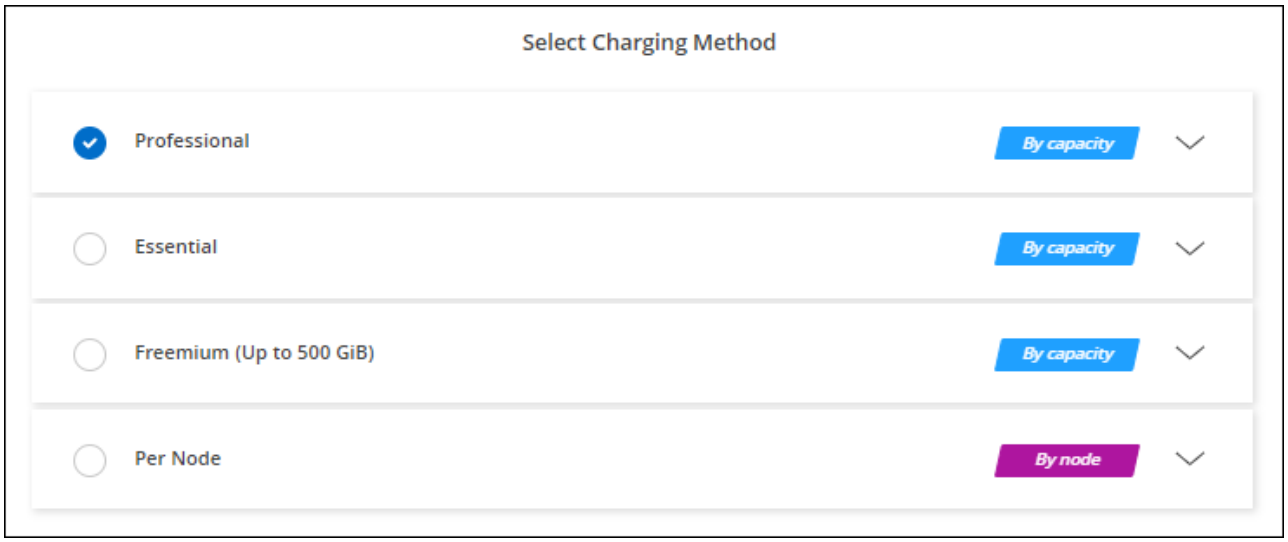
步驟

1. 請聯絡您的NetApp銷售代表以購買年度合約。

   該合約可在Azure Marketplace以_Private _優惠形式提供。

   NetApp與您分享私人優惠之後、您可以在工作環境建立期間、從Azure 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>繼續*。
   b. 在Azure入口網站中、選取與Azure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Cloud Volumes ONTAP 逐步指示、以在Azure中推出《功能不全》"。

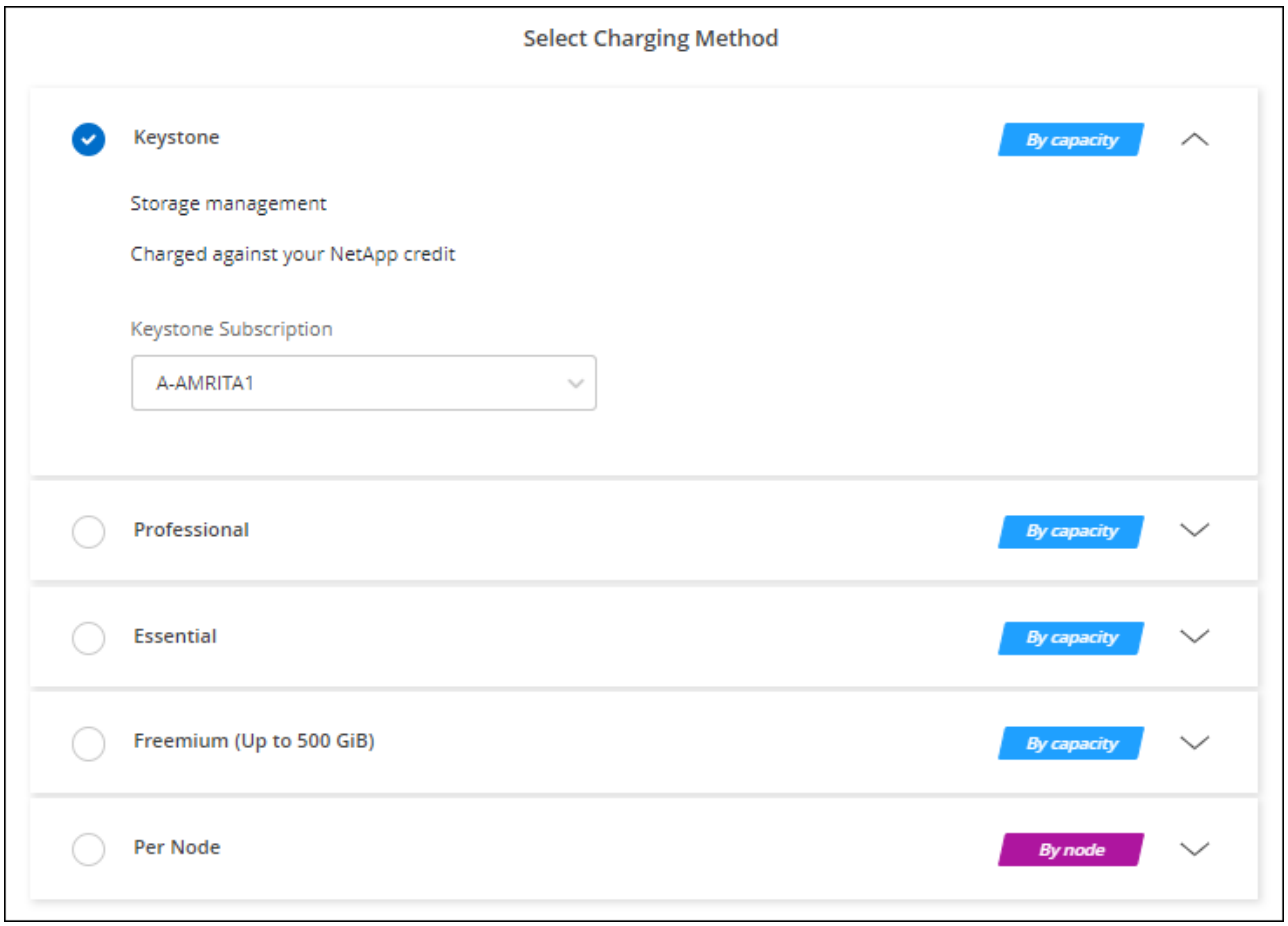
Keystone訂閱

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Cloud Volumes ONTAP 逐步指示、以在Azure中推出《功能不全》"。

在**Azure**中啟用高可用度模式

Microsoft Azure的高可用度模式應可減少非計畫性容錯移轉時間、並啟用NFSv4 for Cloud Volumes ONTAP 功能。

從發行版《S21》開始Cloud Volumes ONTAP 、我們縮短Cloud Volumes ONTAP 了在Microsoft Azure上執行的《21個HA配對》的非計畫性容錯移轉時間、並增加了對NFSv4的支援。若要讓Cloud Volumes ONTAP 這些增強功能適用於整個過程、您必須啟用Azure訂閱的高可用度功能。

當您需要在Azure訂閱中啟用此功能時、BlueXP會在必要行動訊息中提示您提供這些詳細資料。

請注意下列事項：

- 高可用度Cloud Volumes ONTAP 的不存在任何問題。此Azure功能可搭配ONTAP 使用、以減少因非計畫性容錯移轉事件而導致NFS傳輸協定的應用程式停機時間。
- 啟用此功能對Cloud Volumes ONTAP 功能不中斷運作、不中斷對功能的支援。
- 在您的Azure訂閱中啟用此功能、不會對其他VM造成問題。

具備「擁有者」權限的Azure使用者可從Azure CLI啟用此功能。

步驟

1. "從Azure Portal存取Azure Cloud Shell"
2. 註冊高可用度模式功能：

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. （可選）驗證功能是否已註冊：

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Azure CLI應傳回類似下列的結果：

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

在 **Cloud Volumes ONTAP Azure** 中啟動

您可以在Cloud Volumes ONTAP BlueXP中建立運作環境、在Azure中啟動單一節點系統或HA配對。

您需要的產品

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"。
- 瞭解您要使用的組態。

  您應該已經選擇組態、並從系統管理員取得 Azure 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"。

關於這項工作

當BlueXP在Cloud Volumes ONTAP Azure中建立一個功能完善的系統時、它會建立多個Azure物件、例如資源群組、網路介面和儲存帳戶。您可以在精靈結束時檢閱資源摘要。

> 資料遺失的可能性
>
> 最佳實務做法是針對每Cloud Volumes ONTAP 個系統使用新的專屬資源群組。
>
> 由於資料遺失的風險、不建議在 Cloud Volumes ONTAP 現有的共享資源群組中部署此功能。雖然在Cloud Volumes ONTAP 部署失敗或刪除的情況下、BlueXP可以從共用資源群組移除一些不必要的資源、但Azure使用者可能會不小心從Cloud Volumes ONTAP 共用資源群組中刪除一些不必要的資源。

在Cloud Volumes ONTAP Azure中啟動單一節點的不完整系統

如果您想要在Cloud Volumes ONTAP Azure中啟動單一節點的功能、您需要在BlueXP中建立單一節點的工作環境。

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* Microsoft Azure 和 Cloud Volumes ONTAP 《單一節點*》。
4. 如果出現提示、 "建立連接器"。
5. 詳細資料與認證：選擇性變更Azure認證與訂閱、指定叢集名稱、視需要新增標籤、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 整個系統、以及Azure虛擬機器。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。
資源群組標記	標記是 Azure 資源的中繼資料。在此欄位中輸入標記時、BlueXP會將標記新增至與Cloud Volumes ONTAP 該系統相關聯的資源群組。建立工作環境時、您最多可以從使用者介面新增四個標記、然後在建立之後新增更多標記。請注意、在建立工作環境時、 API 不會限制您使用四個標記。如需標記的相關資訊、請參閱 "Microsoft Azure 說明文件：使用標籤來組織 Azure 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。
[[video ）] 編輯認證資料	您可以選擇不同的 Azure 認證資料和其他 Azure 訂閱、以搭配此 Cloud Volumes ONTAP 款作業系統使用。您必須將 Azure Marketplace 訂閱與所選 Azure 訂閱建立關聯、才能部署隨用隨付 Cloud Volumes ONTAP 的功能。 "瞭解如何新增認證"。

下列影片說明如何將 Marketplace 訂閱與 Azure 訂閱建立關聯：

從 Azure Marketplace 訂閱 BlueXP

6. * 服務 * ：啟用或停用 Cloud Volumes ONTAP 您不想搭配使用的個別服務。
   - "深入瞭解 BlueXP 分類"
   - "深入瞭解 BlueXP 備份與還原"

   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：選取區域、可用度區域、vnet和子網路、然後選取核取方塊以確認連接器與目標位置之間的網路連線。

   對於單一節點系統、您可以選擇要部署 Cloud Volumes ONTAP 的可用度區域。如果您未選擇AZ、則BlueXP會為您選擇一個。

8. 連線能力：選擇新的或現有的資源群組、然後選擇是使用預先定義的安全性群組、還是使用自己的。

   下表說明您可能需要指導的欄位：

欄位	說明
資源群組	建立Cloud Volumes ONTAP 新的資源群組以供使用、或使用現有的資源群組。最佳實務做法是使用全新的資源群組 Cloud Volumes ONTAP 來進行支援。雖然可以在Cloud Volumes ONTAP 現有的共享資源群組中部署功能、但由於資料遺失的風險、不建議這麼做。如需詳細資料、請參閱上述警告。 如果您使用的Azure帳戶具有 "必要權限"、在Cloud Volumes ONTAP 部署失敗或刪除的情況下、BlueXP會從資源群組移除一些不必要的資源。
產生的安全性群組	如果讓BlueXP為您產生安全性群組、您必須選擇允許流量的方式： • 如果您選擇*選取的vnet only *、則傳入流量的來源是所選vnet的子網路範圍、以及連接器所在vnet的子網路範圍。這是建議的選項。 • 如果您選擇*所有VNet*、則傳入流量的來源為0.00.0.0/0 IP範圍。
使用現有的	如果您選擇現有的安全群組、則必須符合Cloud Volumes ONTAP 下列需求： "檢視預設的安全性群組"。

9. 充電方法與**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"。
10. * 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。

11. 授權：視Cloud Volumes ONTAP 需要變更此版本、然後選取虛擬機器類型。

    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 。

12. * 訂閱 Azure Marketplace* ：如果 BlueXP 無法啟用 Cloud Volumes ONTAP 的程式設計部署、您會看到此頁面。請依照畫面上列出的步驟進行。請參閱 "市場產品的程式化部署" 以取得更多資訊。

13. * 基礎儲存資源 * ：選擇初始 Aggregate 的設定：磁碟類型、每個磁碟的大小、以及是否應啟用資料分層至 Blob 儲存設備。

    請注意下列事項：

    - 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 Azure 中調整系統規模"。

    - 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。

      "深入瞭解資料分層"。

14. *寫入速度與WORM *：

    a. 如果需要、請選擇*正常*或*高速*寫入速度。

       "深入瞭解寫入速度"。

    b. 視需要啟動一次寫入、多次讀取（WORM）儲存設備。

       此選項僅適用於特定VM類型。若要瞭解支援哪些VM類型、請參閱 "HA配對授權的支援組態"。

       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。

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

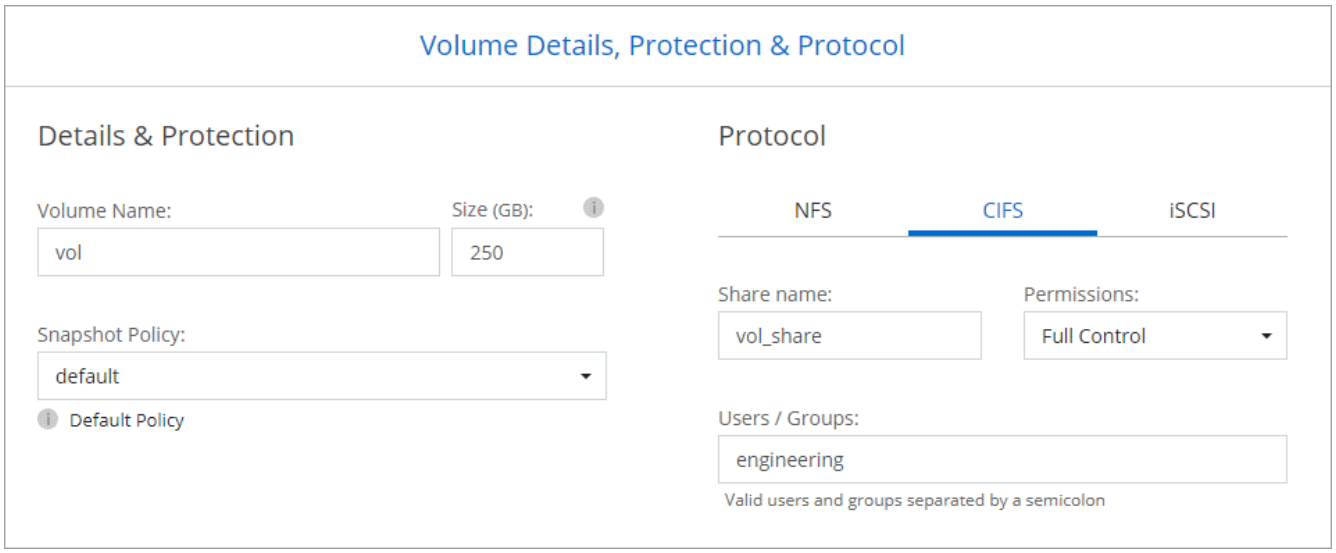
    "瞭解支援的用戶端傳輸協定和版本"。

    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。

欄位	說明
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：



16. * 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。
要加入的 Active Directory 網域	您要 CIFS 伺服器加入之 Active Directory （ AD ）網域的 FQDN 。

欄位	說明
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 Azure AD 網域服務設定為 Cloud Volumes ONTAP AD 伺服器以供使用、您應在此欄位中輸入 * OID=AADDC computers* 或 * OID=AADDC 使用者 *。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 說明文件：在 Azure AD 網域服務託管網域中建立組織單位（ OU ）"^]
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。

17. * 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 "瞭解 Volume 使用量設定檔" 和 "資料分層總覽"。

18. * 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將購買之Azure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Cloud Volumes ONTAP Azure中啟動一套功能完善的

如果您想要在Cloud Volumes ONTAP Azure中啟動一套功能不均的HA配對、您必須在BlueXP中建立HA工作環境。

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. 如果出現提示、 "建立連接器"。
4. 詳細資料與認證：選擇性變更Azure認證與訂閱、指定叢集名稱、視需要新增標籤、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 整個系統、以及Azure虛擬機器。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。
資源群組標記	標記是 Azure 資源的中繼資料。在此欄位中輸入標記時、BlueXP會將標記新增至與Cloud Volumes ONTAP 該系統相關聯的資源群組。建立工作環境時、您最多可以從使用者介面新增四個標記、然後在建立之後新增更多標記。請注意、在建立工作環境時、 API 不會限制您使用四個標記。如需標記的相關資訊、請參閱 "Microsoft Azure 說明文件：使用標籤來組織 Azure 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。
[[video ）] 編輯認證資料	您可以選擇不同的 Azure 認證資料和其他 Azure 訂閱、以搭配此 Cloud Volumes ONTAP 款作業系統使用。您必須將 Azure Marketplace 訂閱與所選 Azure 訂閱建立關聯、才能部署隨用隨付 Cloud Volumes ONTAP 的功能。 "瞭解如何新增認證"。

   下列影片說明如何將 Marketplace 訂閱與 Azure 訂閱建立關聯：

   從 Azure Marketplace 訂閱 BlueXP

5. * 服務 * ：啟用或停用 Cloud Volumes ONTAP 您不想搭配使用的個別服務。
   - "深入瞭解 BlueXP 分類"
   - "深入瞭解 BlueXP 備份與還原"

   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*：
   a. 選擇*單一可用度區域*或*多個可用度區域*。
   b. 位置與連線（單一AZ）及*地區與連線*（多個AZs）
      - 對於單一AZ、請選取一個地區、vnet和子網路。

- 對於多個AZs、請為節點1選取區域、vnet、子網路、區域、為節點2選取區域。

c. 選取「我已驗證網路連線能力...」核取方塊。

7. 連線能力：選擇新的或現有的資源群組、然後選擇是使用預先定義的安全性群組、還是使用自己的。

   下表說明您可能需要指導的欄位：

欄位	說明
資源群組	建立Cloud Volumes ONTAP 新的資源群組以供使用、或使用現有的資源群組。最佳實務做法是使用全新的資源群組 Cloud Volumes ONTAP 來進行支援。雖然可以在Cloud Volumes ONTAP 現有的共享資源群組中部署功能、但由於資料遺失的風險、不建議這麼做。如需詳細資料、請參閱上述警告。 您必須使用專屬的資源群組來處理Cloud Volumes ONTAP 您在Azure中部署的每個「EHA配對」。資源群組僅支援一個HA配對。如果您嘗試在Cloud Volumes ONTAP Azure資源群組中部署第二個「鏈接HA配對」、則BlueXP會遇到連線問題。 如果您使用的Azure帳戶具有 "必要權限"、在Cloud Volumes ONTAP 部署失敗或刪除的情況下、BlueXP會從資源群組移除一些不必要的資源。
產生的安全性群組	如果讓BlueXP為您產生安全性群組、您必須選擇允許流量的方式： • 如果您選擇*選取的vnet only *、則傳入流量的來源是所選vnet的子網路範圍、以及連接器所在vnet的子網路範圍。這是建議的選項。 • 如果您選擇*所有VNet*、則傳入流量的來源為0.00.0.0/0 IP範圍。
使用現有的	如果您選擇現有的安全群組、則必須符合Cloud Volumes ONTAP 下列需求： "檢視預設的安全性群組"。

8. 充電方法與**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 一個作業系統、或按一下*變更組態*。

   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、然後選取虛擬機器類型。

    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. 從**Azure Marketplace**訂閱：如果BlueXP無法啟用Cloud Volumes ONTAP 程式化部署的功能、請依照下列步驟進行。

12. * 基礎儲存資源 * ：選擇初始 Aggregate 的設定：磁碟類型、每個磁碟的大小、以及是否應啟用資料分層至 Blob 儲存設備。

    請注意下列事項：

    - 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。

      如需選擇磁碟大小的說明、請參閱 "在Azure中調整系統規模"。

    - 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。

      "深入瞭解資料分層"。

13. *寫入速度與WORM *：

    a. 如果需要、請選擇*正常*或*高速*寫入速度。

       "深入瞭解寫入速度"。

    b. 視需要啟動一次寫入、多次讀取（WORM）儲存設備。

       此選項僅適用於特定VM類型。若要瞭解支援哪些VM類型、請參閱 "HA配對授權的支援組態"。

       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。

14. *安全通訊至儲存設備與WORM *：選擇是否啟用HTTPS連線至Azure儲存帳戶、並視需要啟動一次寫入、多次讀取（WORM）儲存設備。

    HTTPS連線是Cloud Volumes ONTAP 從一個畫面9.7 HA配對到Azure網頁blob儲存帳戶。請注意、啟用此選項可能會影響寫入效能。您無法在建立工作環境之後變更設定。

    "深入瞭解 WORM 儲存設備"。

    如果資料分層已啟用、則無法啟用 WORM 。

    "深入瞭解 WORM 儲存設備"。

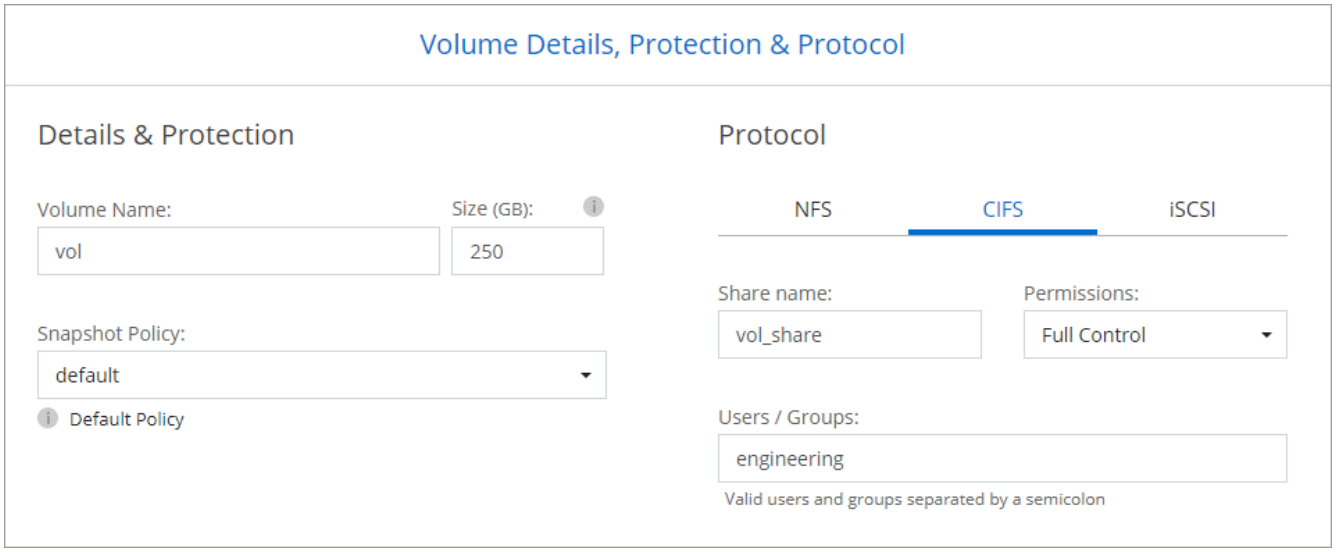
15. * 建立 Volume * ：輸入新磁碟區的詳細資料、或按一下 * 跳過 * 。

    "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：



16. * 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。

欄位	說明
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 Azure AD 網域服務設定為 Cloud Volumes ONTAP AD 伺服器以供使用、您應在此欄位中輸入 * OID=AADDC computers* 或 * OID=AADDC 使用者 *。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 說明文件：在 Azure AD 網域服務託管網域中建立組織單位（ OU ）"^]
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。

17. * 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"。

18. * 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將購買之Azure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。

Azure 平台影像驗證

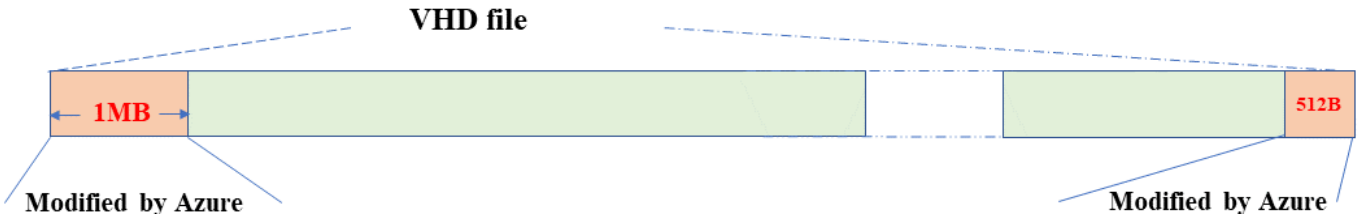
Azure 影像驗證總覽

Azure 影像驗證符合增強的 NetApp 安全要求。雖然驗證映像檔案是一項簡單的程序、但 Azure 映像簽章驗證確實需要特別的資料、才能將其傳送至知名的 Azure VHD 映像檔、因為 Azure 市場已進行了一次替代。

Cloud Volumes ONTAP 軟體 9.15.0 版或更新版本支援 Azure 影像驗證。

Azure 對已發佈 VHD 檔案的變更

Azure 修改了領先業界的 1MB （ 1048576 位元組）和結束 512 位元組 VHD 檔案。NetApp 映像簽署會略過前導的 1MB 並結束 512 個位元組、然後簽署剩餘的 VHD 映像部分。



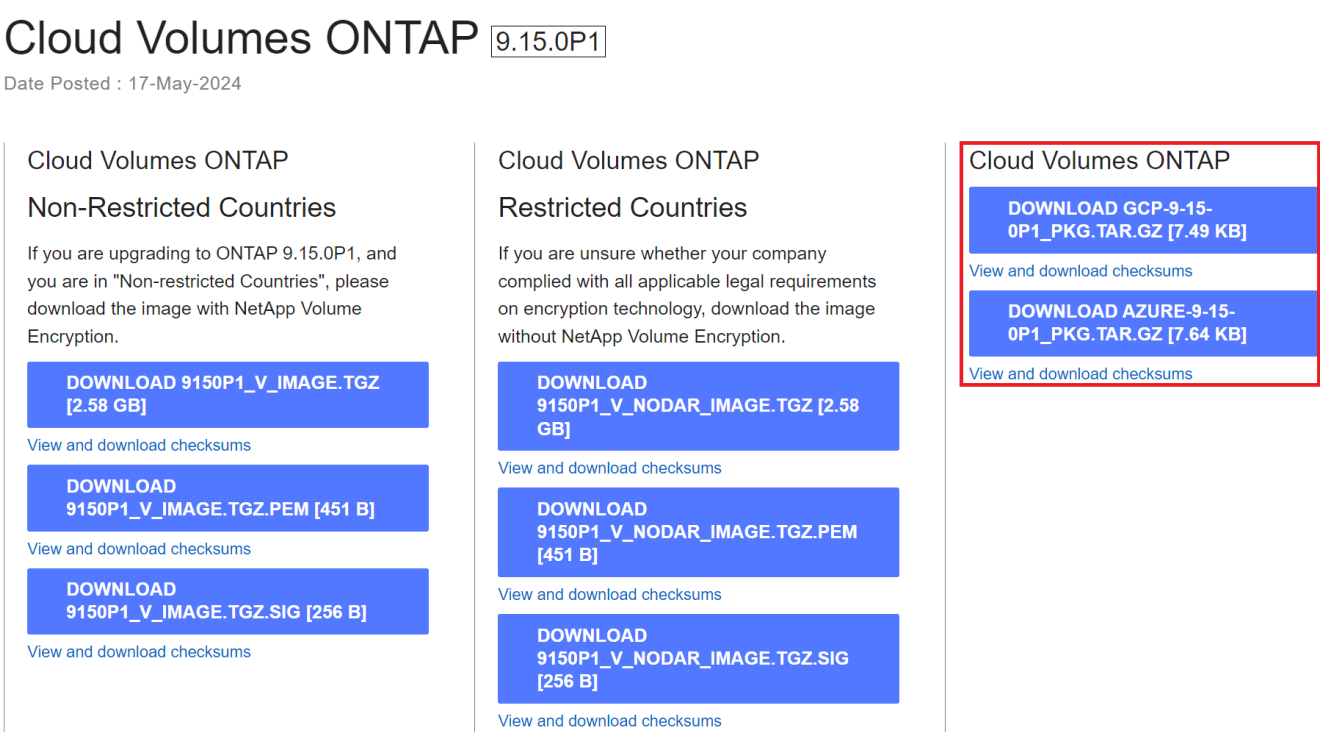
例如、上圖顯示大小為 10GB 的 VHD 檔案。但 NetApp 簽署部分會以綠色標示、大小為 10GB - 1MB - 512B 。

下載 Azure Image Digest File

Azure Image Digest File 可從下載 "NetApp 支援網站"。下載檔案為 tar.gz 格式、包含用於影像簽章驗證的檔案。

步驟

1. 前往 "NetApp 支援網站 上的 Cloud Volumes ONTAP 產品頁面" 並在「下載」區段下載所需的軟體版本。
2. 在 Cloud Volumes ONTAP 下載頁面下、按一下 Azure 影像摘要檔案的 * 下載按鈕 * 、即可下載 TAR 。 gz 檔案。



3. 對於 Linux 和 MacOS 、您必須執行下列步驟、才能取得下載 Azure Image Digest 檔案的 md5sum 和 shav256sum 。
   a. 若為 md5sum 、請輸入 `md5sum` 命令。
   b. 若為 shaf256sum 、請輸入 `sha256sum` 命令。
4. 驗證 `md5sum` 和 `sha256sum` 值符合 Azure Image Digest File 下載。
5. 在 Linux 和 Mac OS 上、執行 `tar -xzf` 擷取 tar.gz 檔案的命令。

   擷取的 TAR 。 gz 檔案包含摘要檔案（ .sig ）、公開金鑰憑證檔案（ .pem ）和鏈結憑證檔案（ .pem ）。

   。列出解壓縮 tar.gz 檔案的結果 *

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

映像從 **Azure Marketplace** 匯出

一旦 VHD 映像發佈至 Azure 雲端、該映像就不再由 NetApp 管理。而是將發佈的映像放在 Azure 市場上。Azure 對 VHD 的領先 1MB 和結尾 512B 的變更是在 Azure 市場上分段及發佈映像時發生的。若要驗證 VHD 檔案的簽章、 Azure 修改的 VHD 映像必須先從 Azure 市場匯出。

您需要的產品

您必須在系統上安裝必要的程式。

- Azure CLI 已安裝、或 Azure Cloud Shell 透過 Azure 入口網站隨時可供使用。

  如需如何安裝 Azure CLI 的詳細資訊、請參閱 "Azure 說明文件：如何安裝 Azure CLI"。

步驟

1. 使用 version_readme.Me 檔案的內容、將 ONTAP 版本對應至 Azure 市場映像版本。

   對於版本 _ 讀我檔案中列出的每個版本對應、 ONTAP 版本以「 buildname 」表示、 Azure 市場映像版本以「 version 」表示。

   例如、在下列版本 _ 讀我檔案中、 ONTAP 版本「 9.15.0P1 」對應至 Azure 市場映像版本「 9150.01000024.05090105 」。此 Azure 市場映像版本稍後會用於設定映像 URN 。

   ```
   [
       {
           "buildname": "9.15.0P1",
           "publisher": "netapp",
           "version": "9150.01000024.05090105"
       }
   ]
   ```

2. 識別您要建立 VM 的區域名稱。

   設定市場映像的 URN 時、此區域名稱會用作「 locName 」變數的值。

   a. 若要接收可用區域的清單、請輸入 `az account list-locations -o table` 命令。

      在下表中、區域名稱稱為「名稱」欄位。

   ```
   $ az account list-locations -o table
   DisplayName               Name                 RegionalDisplayName
   ------------------------  -------------------
   -------------------------------------
   East US                   eastus               (US) East US
   East US 2                 eastus2              (US) East US 2
   South Central US          southcentralus       (US) South Central US
   ...
   ```

3. 請從下表中檢閱對應 VM 部署類型的 SKU 名稱。

   當設定市場映像的 URN 時、 SKU 名稱會用作「 skuName 」變數的值。

   例如、單一節點部署應使用「 ONTAP 雲端 byol 」 SKU 名稱。

VM 部署類型	SKU 名稱
單一節點	ONTAP 雲端
高可用度	ONTAP 雲端 _ byol_ha

4. ONTAP 版本和 Azure 市場映像對應完成後、即可透過 Azure Cloud Shell 或 Azure CLI 、從 Azure 市場匯出 VHD 檔案。

透過 **Azure** 入口網站上的 **Azure Cloud Shell** 匯出 **VHD** 檔案

1. 從 Azure Cloud Shell 將市場映像匯出至 vhd （ image2 、例如 9150.01000024.05090105.vhd ）、然後下載至您的本機機器（例如 Linux 機器或 Windows PC ）。

按一下以顯示

```
#Azure Cloud Shell on Azure portal to get VHD image from Azure
Marketplace
a) Set the URN and other parameters of the marketplace image. URN is
with format "<publisher>:<offer>:<sku>:<version>". Optionally, a
user can list NetApp marketplace images to confirm the proper image
version.
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName
$pubName -Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...

b) Create a new managed disk from the Marketplace image with the
matching image version
PS /home/user1> $diskName = “9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = “fnf1”
PS /home/user1> az disk create -g $diskRG -n $diskName --image
-reference $urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds
3600 --access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-
Json)[0].accessSas

c) Export a VHD from the managed disk to Azure Storage
Create a container with proper access level. As an example, a
container named 'vm-images' with 'Container' access level is used
here.
Get storage account access key, on Azure portal, 'Storage
Accounts'/'examplesaname'/'Access Key'/'key1'/'key'/'show'/<copy>.
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
```

```
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri
$diskAccessSAS -DestContainer $containerName -DestContext
$destContext -DestBlob $destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container
$containerName –Context $destContext -Blob $destBlobName

d) Download the generated image to your server, e.g., a Linux
machine.
Use "wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>".
The URL is organized in a formatted way. For automation tasks, the
following example could be used to derive the URL string. Otherwise,
Azure CLI 'az' command could be issued to get the URL, which is not
covered in this guide. URL Example:
https://examplesaname.blob.core.windows.net/vm-
images/9150.01000024.05090105.vhd

e) Clean up the managed disk
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG
-DiskName $diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

從本機 **Linux** 機器透過 **Azure CLI** 匯出 **VHD** 檔案

1. 從本機 Linux 機器透過 Azure CLI 將市場映像匯出至 vhd 。

按一下以顯示

```
#Azure CLI on local Linux machine to get VHD image from Azure
Marketplace
a) Login Azure CLI and list marketplace images
% az login --use-device-code
To sign in, use a web browser to open the page
https://microsoft.com/devicelogin and enter the code XXXXXXXXX to
authenticate.

% az vm image list --all --publisher netapp --offer netapp-ontap-
cloud --sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...

b) Create a new managed disk from the Marketplace image with the
matching image version
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level
Read --name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxx"
}

% export diskAccessSAS="https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxx"
#To automate the process, the SAS needs to be extracted from the
standard output. This is not included in this guide.
```

```
c) export vhd from managed disk
Create a container with proper access level. As an example, a
container named 'vm-images' with 'Container' access level is used
here.
Get storage account access key, on Azure portal, 'Storage
Accounts'/'examplesaname'/'Access Key'/'key1'/'key'/'show'/<copy>.
There should be az command that can achieve the same, but this is
not included in this guide.
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS
--destination-container $containerName --account-name
$storageAccountName --account-key $storageAccountKey --destination
-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}

#to check the status of the blob copying
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.blob.core.windows.net/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
```

```
    },
....

d) Download the generated image to your server, e.g., a Linux
machine.
Use "wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>".
The URL is organized in a formatted way. For automation tasks, the
following example could be used to derive the URL string. Otherwise,
Azure CLI 'az' command could be issued to get the URL, which is not
covered in this guide. URL Example:
https://examplesaname.blob.core.windows.net/vm-
images/9150.01000024.05090105.vhd

e) Clean up the managed disk
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

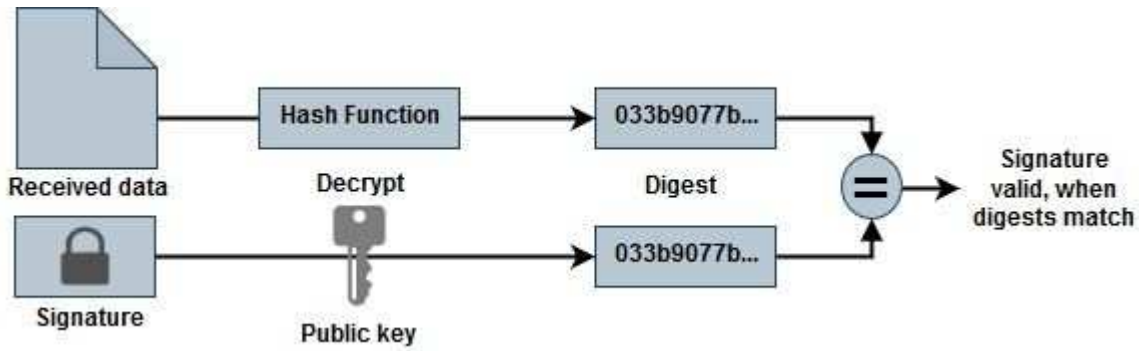
檔案簽章驗證

檔案簽章驗證

Azure 影像驗證程序將使用雜湊功能、從 VHD 檔案產生內含前導式 1MB 等量區塊的摘要、並結束 512B 等量區塊區塊區塊。為了符合簽署程序、使用 SHA256 進行雜湊。您需要從 VHD 檔案移除前導式 1MB 和最終版 512B 、然後驗證 VHD 檔案的其餘部分。

檔案簽章驗證工作流程摘要

以下是檔案簽章驗證工作流程程序的概觀。



- 從下載 Azure Image Digest 檔案 "NetApp 支援網站" 然後擷取摘要檔案（ .SIG ）、公開金鑰憑證檔案（ .pem ）和鏈結憑證檔案（ .pem ）。

  請參閱 "下載 Azure Image Digest File" 以取得更多資訊。

- 驗證信任鏈結。

- 從公開金鑰憑證（ .pem ）擷取公開金鑰（ .pub ）。
- 解壓縮的公開金鑰用於解密摘要檔案。然後將結果與從映像檔案建立的新未加密暫存檔案摘要進行比較、並移除前導式 1MB 與結尾 512 位元組的檔案。

  此步驟可透過下列 openssl 命令來達成。

  - 一般 CLI 聲明如下所示：

    ```
    openssl dgst -verify <public_key> -keyform <form> <hash_function>
    -signature <digest_file> -binary <temporary_file>
    ```

  - 如果檔案相符、則 Openssl CLI 工具會顯示「驗證成功」訊息、如果檔案不符、則會顯示「驗證失敗」訊息。

Linux 上的檔案簽章驗證

您可以依照下列步驟驗證匯出的 VHD 檔案簽章適用於 Linux 。

步驟

1. 從下載 Azure Image Digest 檔案 "NetApp 支援網站" 然後擷取摘要檔案（ .SIG ）、公開金鑰憑證檔案（ .pem ）和鏈結憑證檔案（ .pem ）。

   請參閱 "下載 Azure Image Digest File" 以取得更多資訊。

2. 驗證信任鏈結。

   ```
   % openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
   Certificate-9.15.0P1_azure.pem
   Certificate-9.15.0P1_azure.pem: OK
   ```

3. 移除前導的 1MB （ 1048576 位元組）、並結束 512 位元組的 VHD 檔案。

   如果使用「 tail 」、選項「 -c +K 」會以指定檔案的 KTH 位元組開始輸出位元組。因此、 1048577 會傳送至 'tail -c 。

   ```
   % tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
   % head -c -512 ./sign.tmp.tail > sign.tmp
   % rm ./sign.tmp.tail
   ```

4. 使用 openssl 從憑證擷取公開金鑰、並使用簽章檔案和公開金鑰驗證等量分佈的檔案（ sign.tmp ）。

   如果輸入檔通過驗證、則會顯示命令
   " 驗證正常 " 。否則將顯示「驗證失敗」。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 清理工作區。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Mac OS 上的檔案簽章驗證

您可以依照下列步驟、驗證 Mac OS 匯出的 VHD 檔案簽章。

步驟

1. 從下載 Azure Image Digest 檔案 "NetApp 支援網站" 然後擷取摘要檔案（ .SIG ）、公開金鑰憑證檔案（ .pem ）和鏈結憑證檔案（ .pem ）。

   請參閱 "下載 Azure Image Digest File" 以取得更多資訊。

2. 驗證信任鏈結。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 移除前導的 1MB （ 1048576 位元組）、並結束 512 位元組的 VHD 檔案。

   如果使用「 tail 」、選項「 -c +K 」會以 KTH 位元組開始輸出位元組
   指定檔案的。因此、 1048577 會傳送至 'tail -c 。大約需要 13 分鐘
   以在 Mac OS 上完成 tail 命令。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. 使用 openssl 從憑證擷取公開金鑰、並驗證等量分割

檔案（ sign.tmp ）、含簽章檔案和公開金鑰。

如果輸入檔案通過驗證、命令會顯示「驗證正常」。
否則將顯示「驗證失敗」。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 清理工作區。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

何處可以找到 **Azure** 影像驗證的其他資訊

如需 Azure 影像驗證的其他資訊、請參閱下列連結。以下連結將帶您前往非 NetApp 網站。

參考資料

- "網頁故障部落格：如何使用 OpenSSL 簽署及驗證"
- "使用 Azure Marketplace 映像為 Azure Stack Edge Pro GPU 建立 VM 映像 | Microsoft Learn"
- "使用 Azure CLI 將託管磁碟匯出 / 複製到儲存帳戶 | Microsoft Learn"
- "Azure Cloud Shell Quickstart - Bash | Microsoft Learn"
- "如何安裝 Azure CLI | Microsoft Learn"
- "AZ 儲存資源膨脹複本 | Microsoft Learn"
- "使用 Azure CLI 登入：登入與驗證 | Microsoft Learn"

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**中調整系統規模

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：

「kipSvmManagementLif: 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。

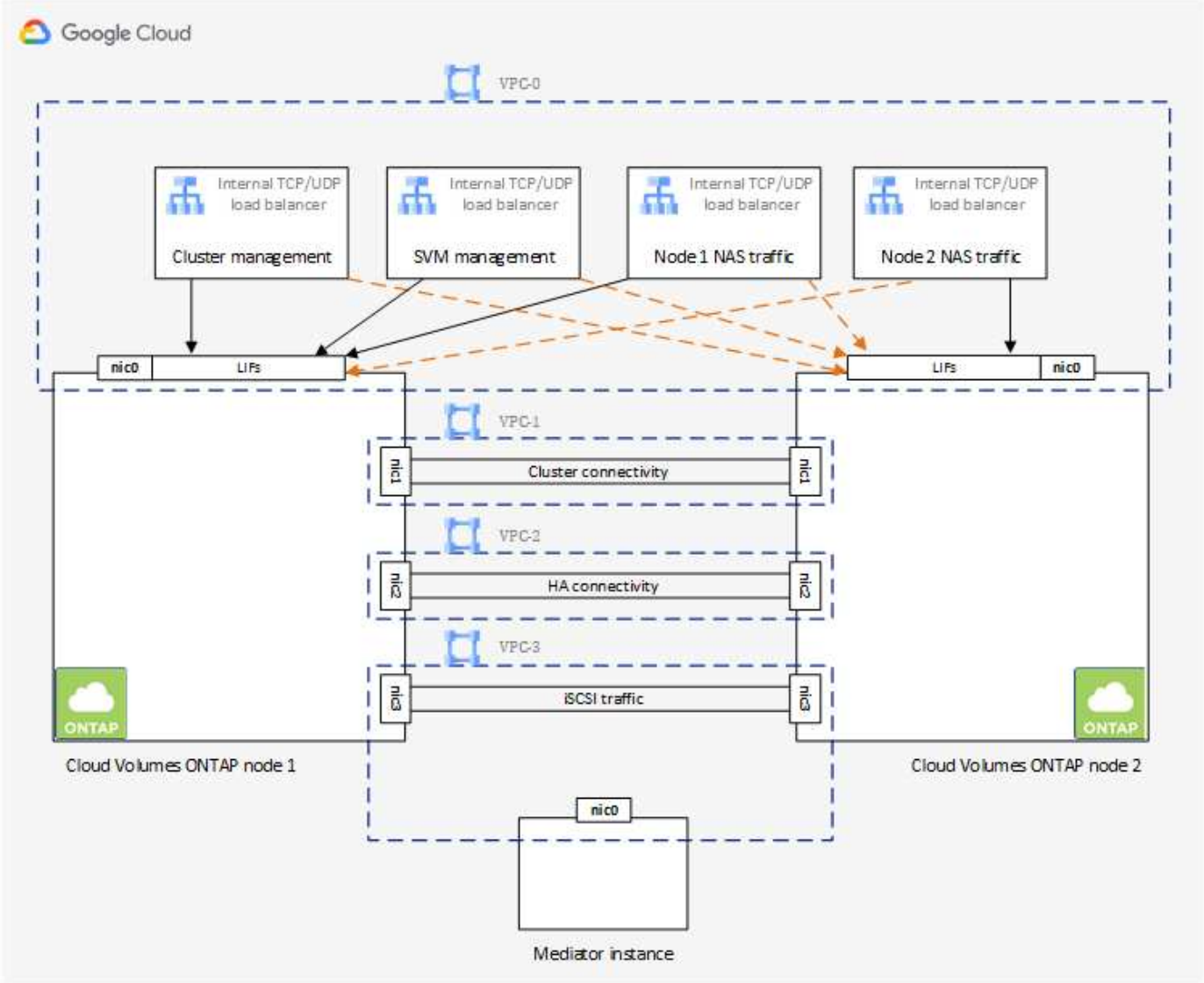
  此部署模式可降低成本、因為各區域之間不需支付任何資料出口費用。

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：

「kipSvmManagementLif: 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：

「kipSvmManagementLif: 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" 您必須在部署 Cloud Volumes ONTAP 的 Google Cloud 子網路中停用。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。您可能想要參考連接埠以進行測試、或是想要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	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	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

傳出規則

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 ：//Wese/occm/offboxconfig <connector-IP-address>	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 %	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	UDP	162 %	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

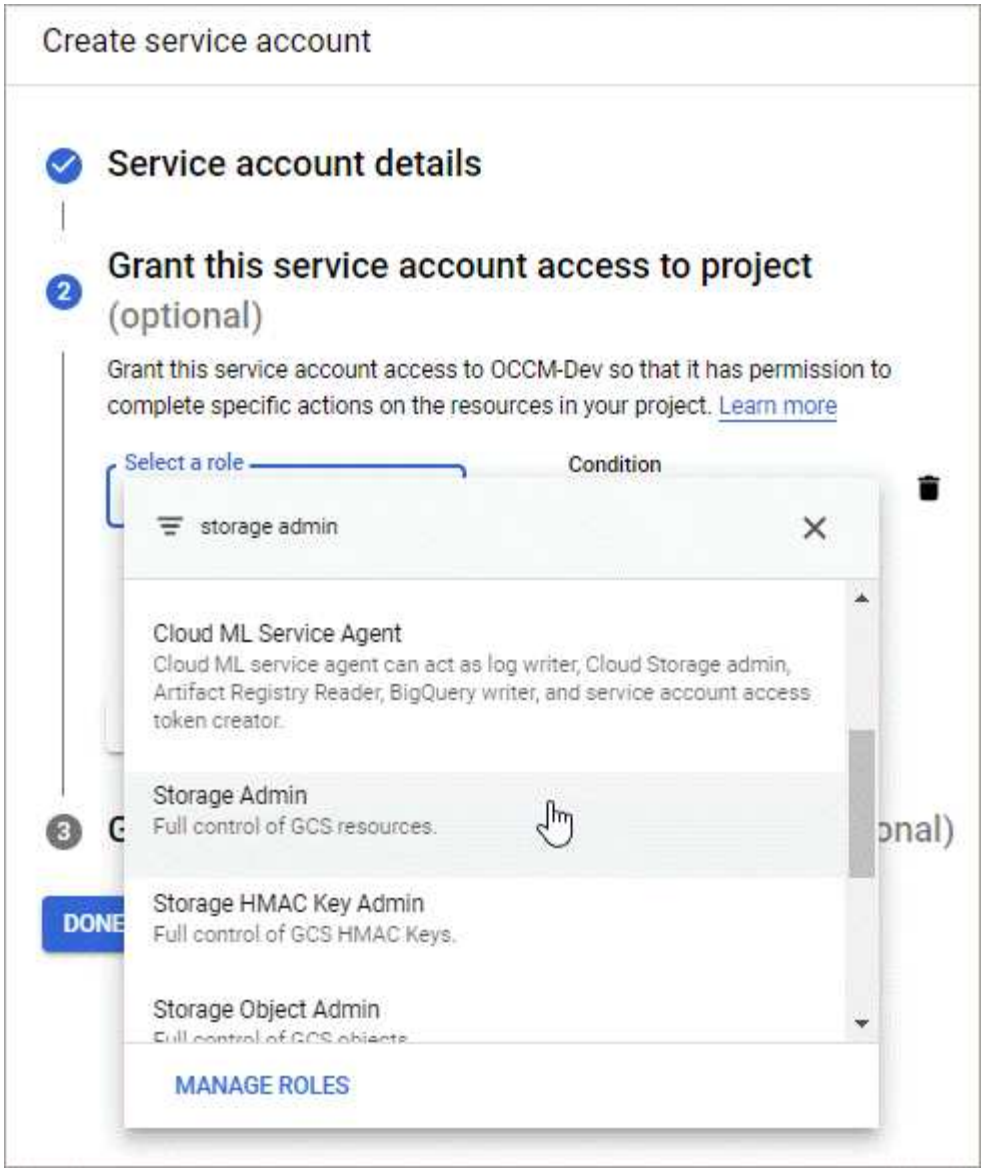
下列兩種用途需要Google Cloud服務帳戶：Cloud Volumes ONTAP第一個是啟用時 "資料分層" 將冷資料分層至Google Cloud中的低成本物件儲存設備。第二個是啟用時 "BlueXP備份與還原" 將磁碟區備份至低成本的物件儲存設備。

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。

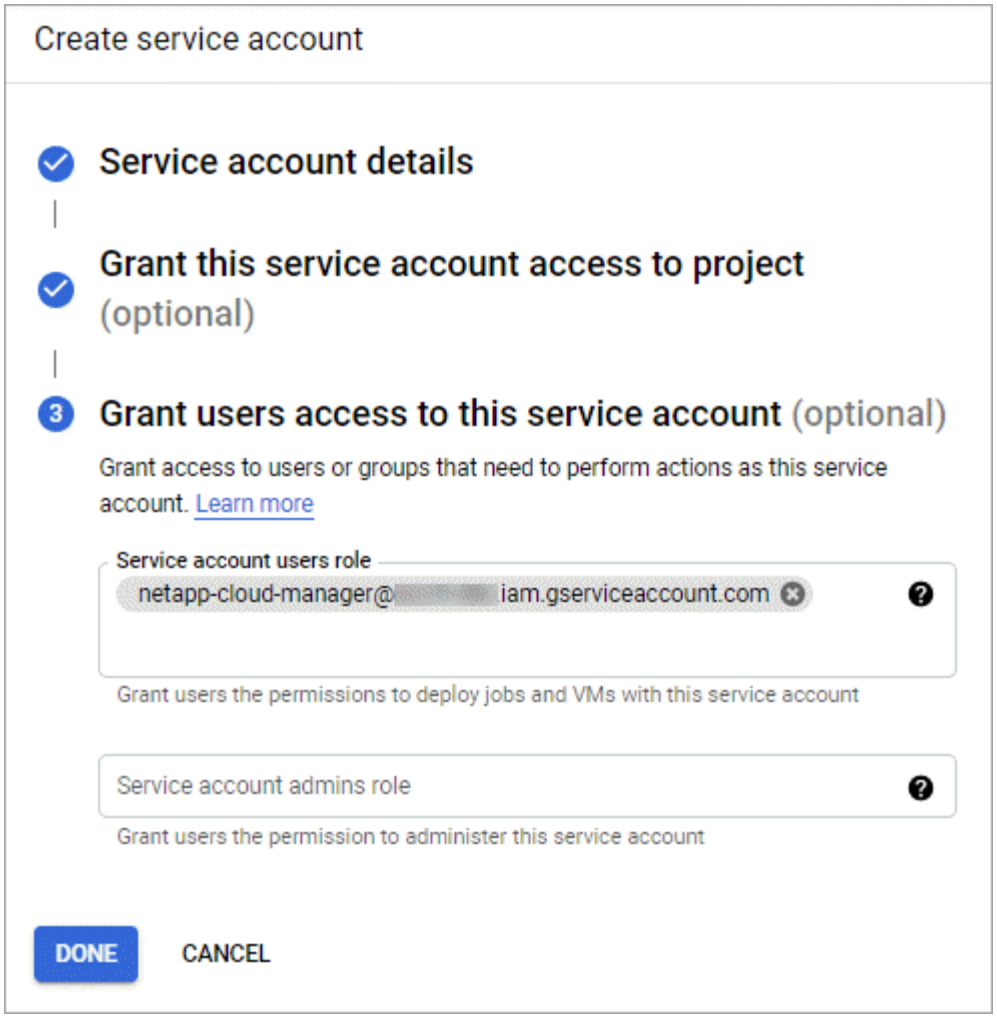
步驟

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。



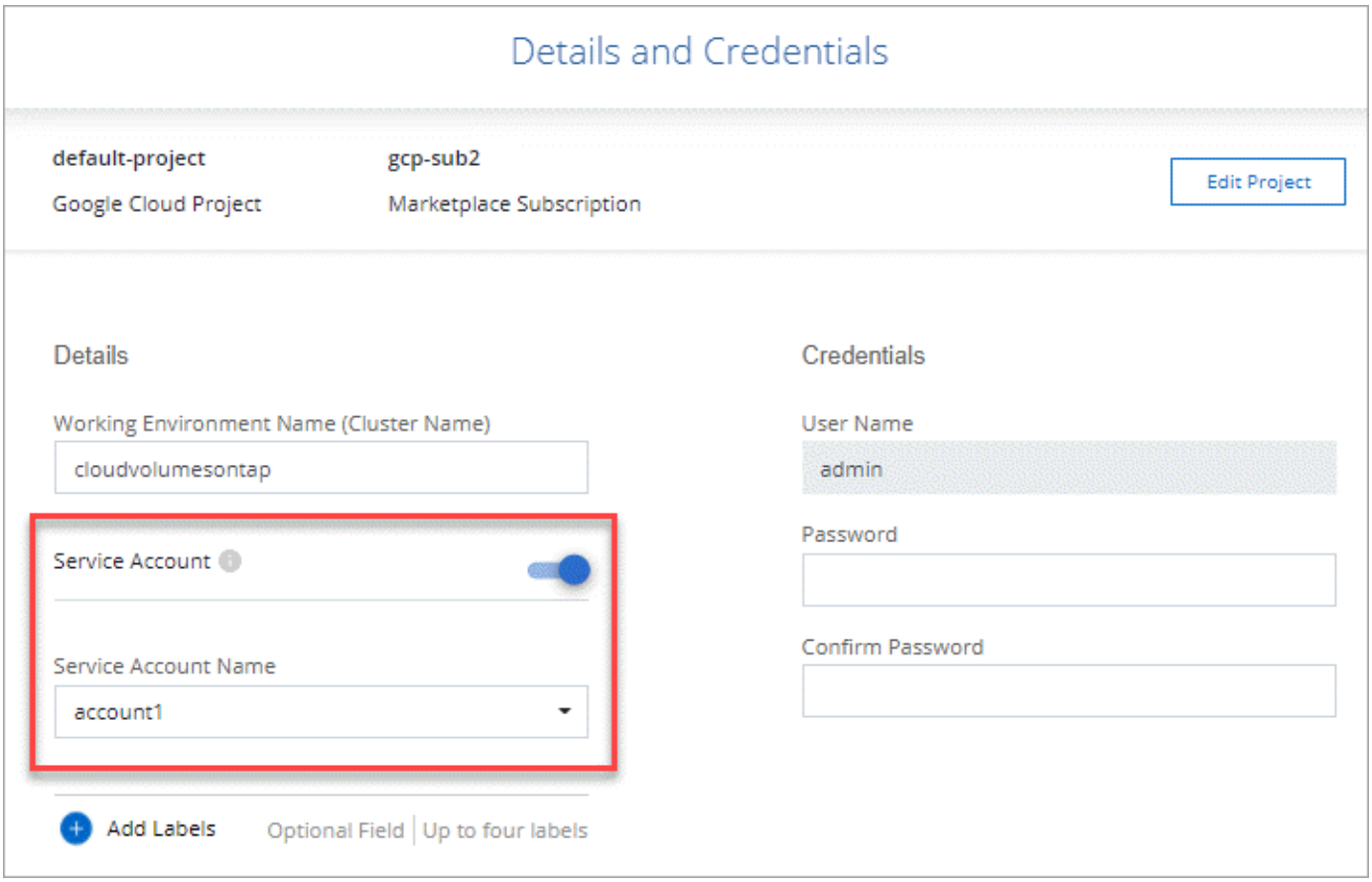
c. 授予使用者此服務帳戶的存取權：將Connector服務帳戶新增為_Service Account User_至此新的服務帳戶。

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. 若要取得金鑰的「ID」、請叫用「/GCP / VSA /中繼資料/ GCP加密金鑰」API呼叫的「Get」命令、或在GCP主控台的金鑰上選擇「Copy Resource Name」（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"。

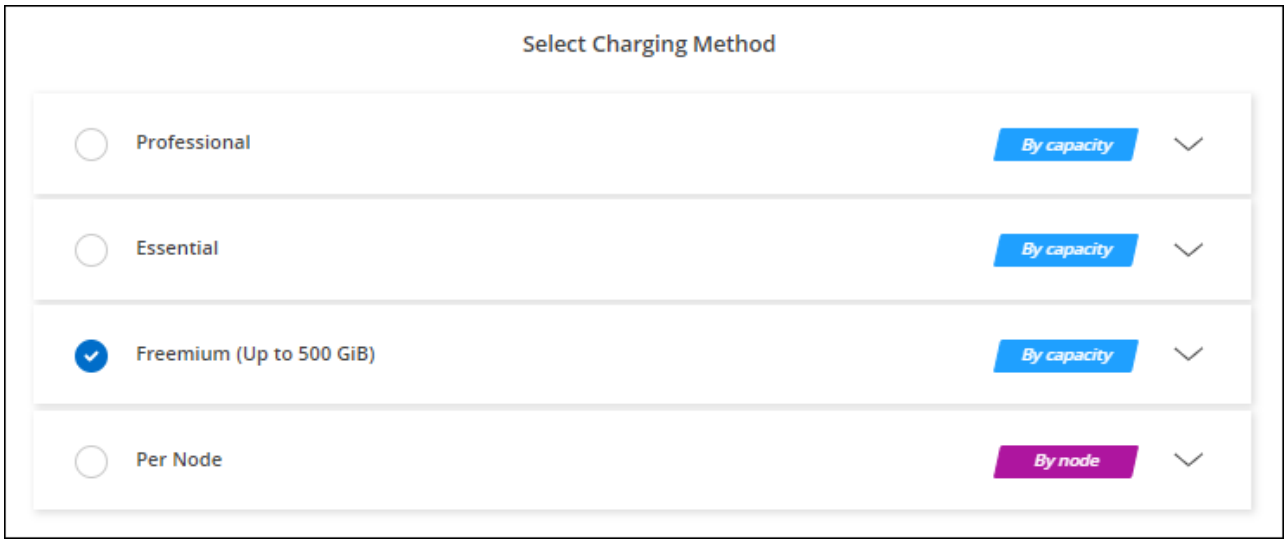
步驟

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"

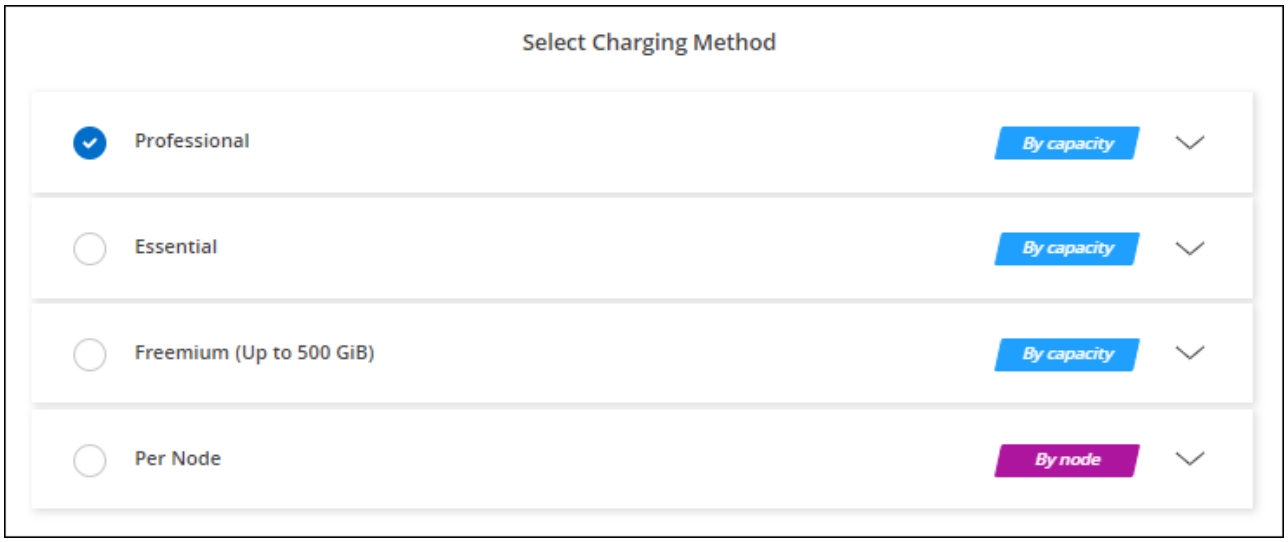
   BlueXP會自動查詢NetApp的授權服務、以取得NetApp 支援網站 與您的還原帳戶相關之授權的詳細資料。如果沒有錯誤、 BlueXP 會自動將授權新增至數位錢包。

   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」"。

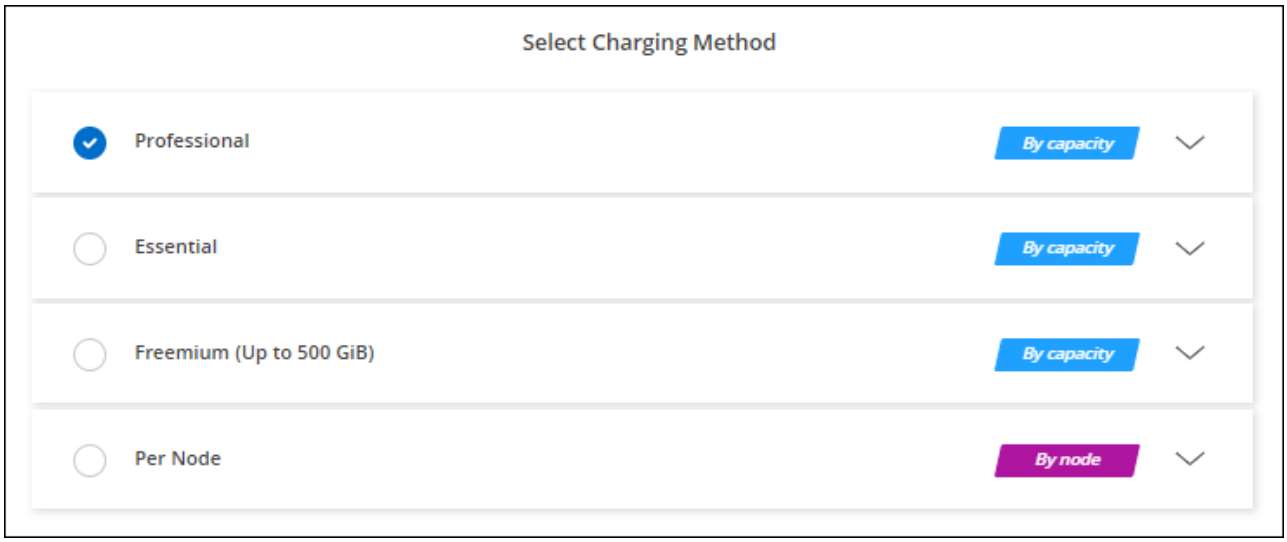
PAYGO訂閱

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。

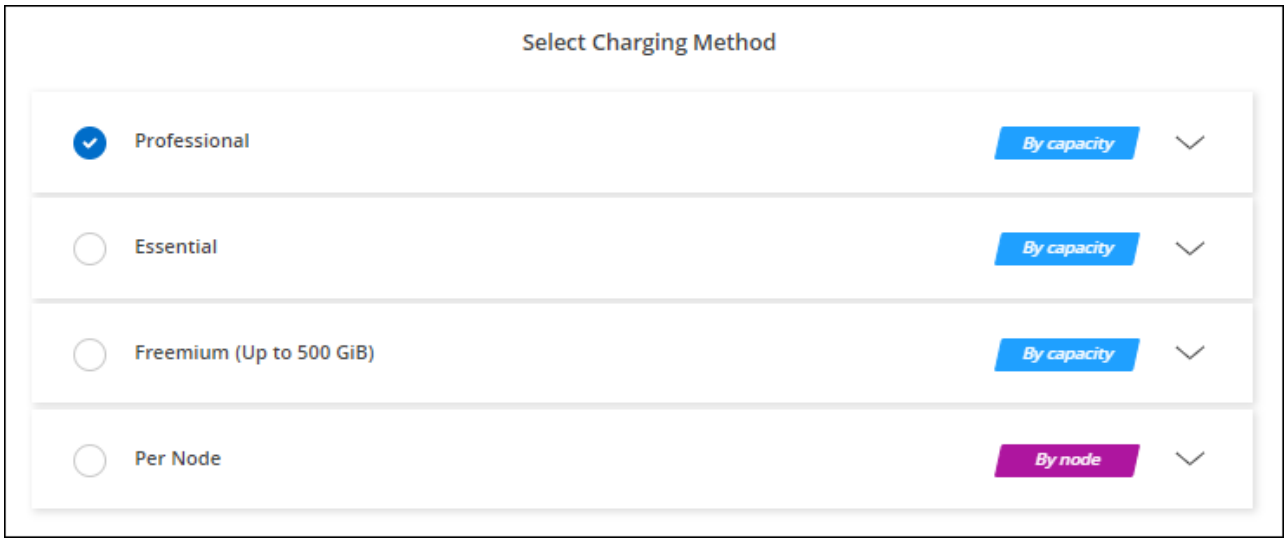
步驟

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。



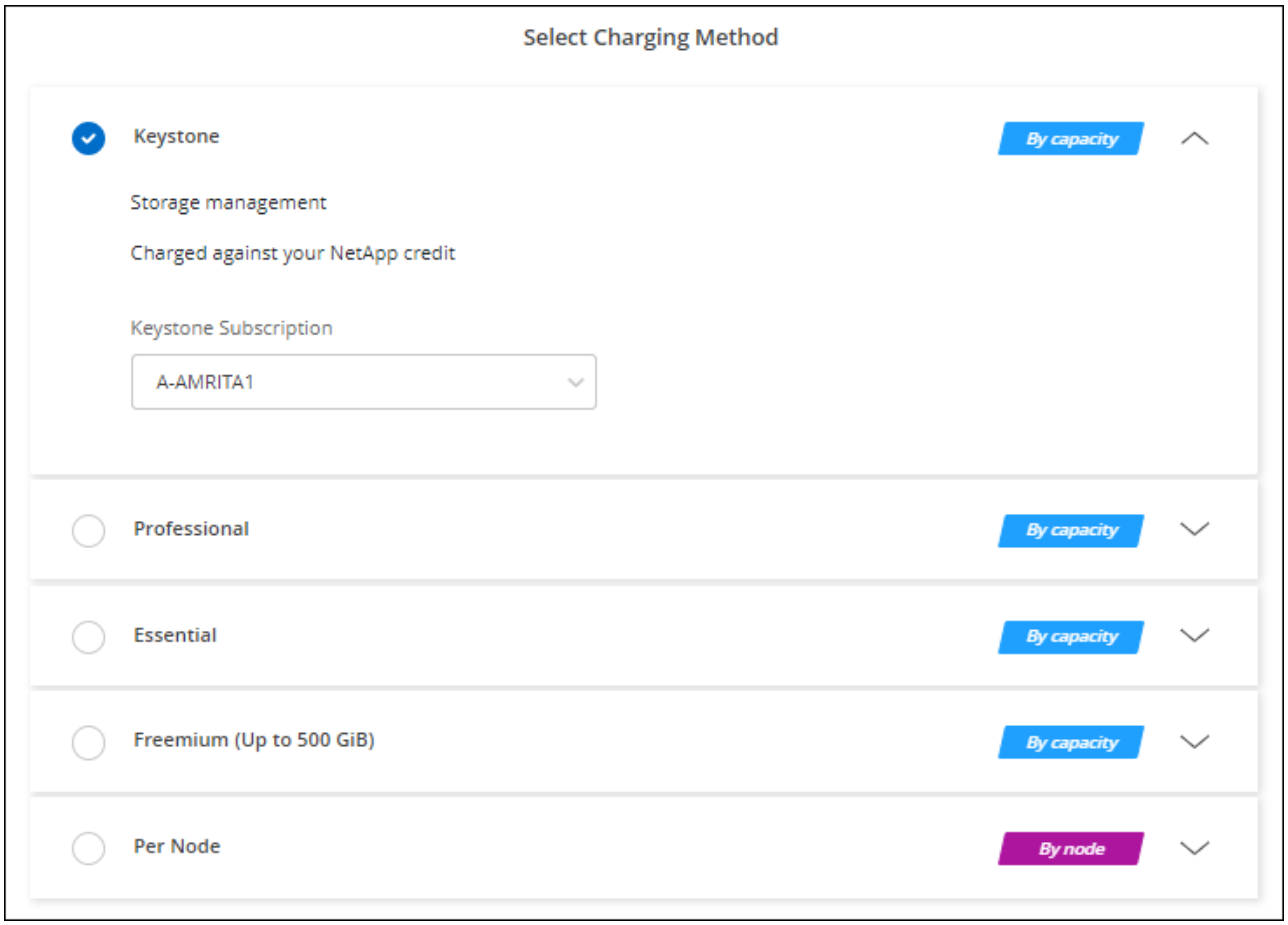
"請參閱逐步指示Cloud Volumes ONTAP 、在Google Cloud中啟動「功能不全」"。

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。

從 Google Cloud Marketplace 訂閱 BlueXP

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. 充電方法與**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"。

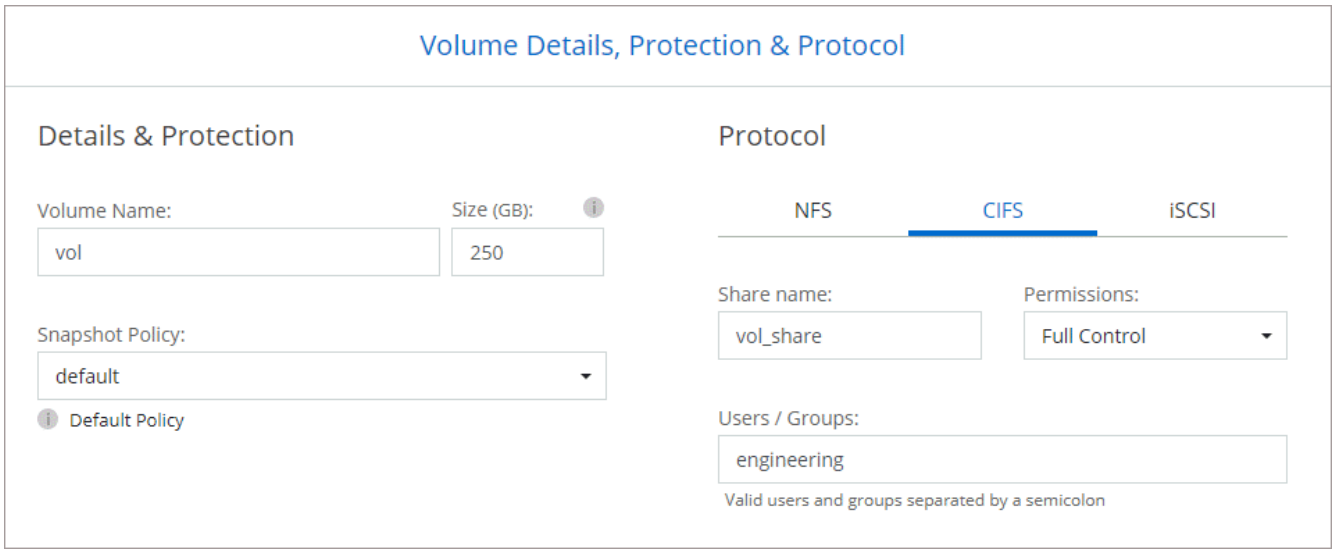
14. * 建立 Volume * ：輸入新磁碟區的詳細資料、或按一下 * 跳過 * 。

    "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 * 。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["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。
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"。

欄位	說明
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。

從 Google Cloud Marketplace 訂閱 BlueXP

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. 充電方法與**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 * 。

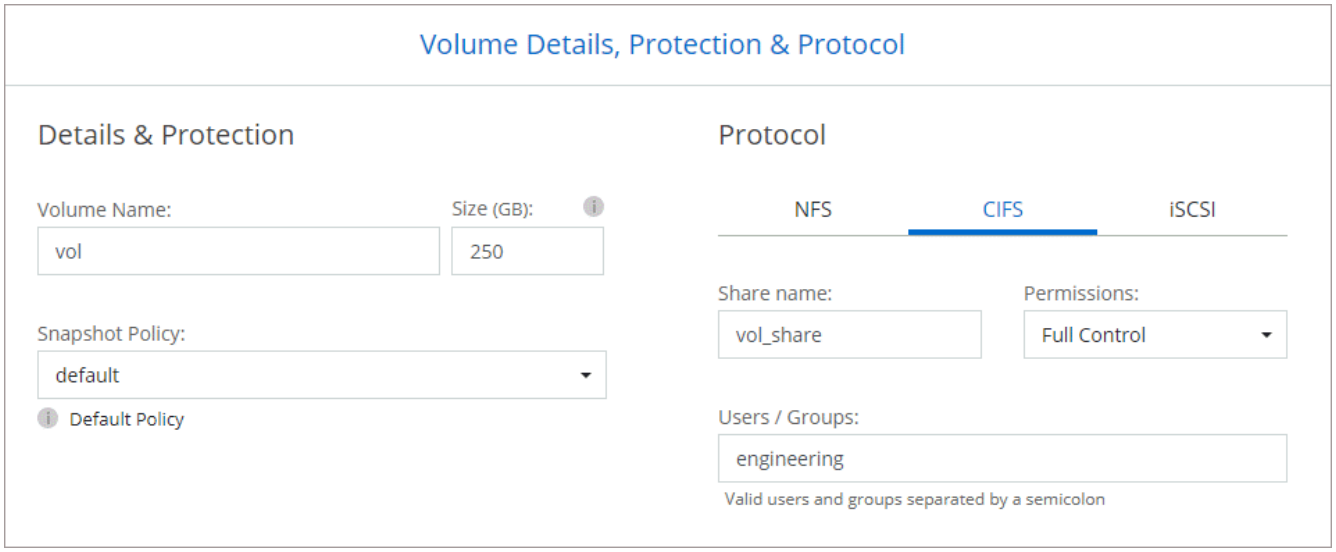
"瞭解支援的用戶端傳輸協定和版本"。

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 * 。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["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

```
$ 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

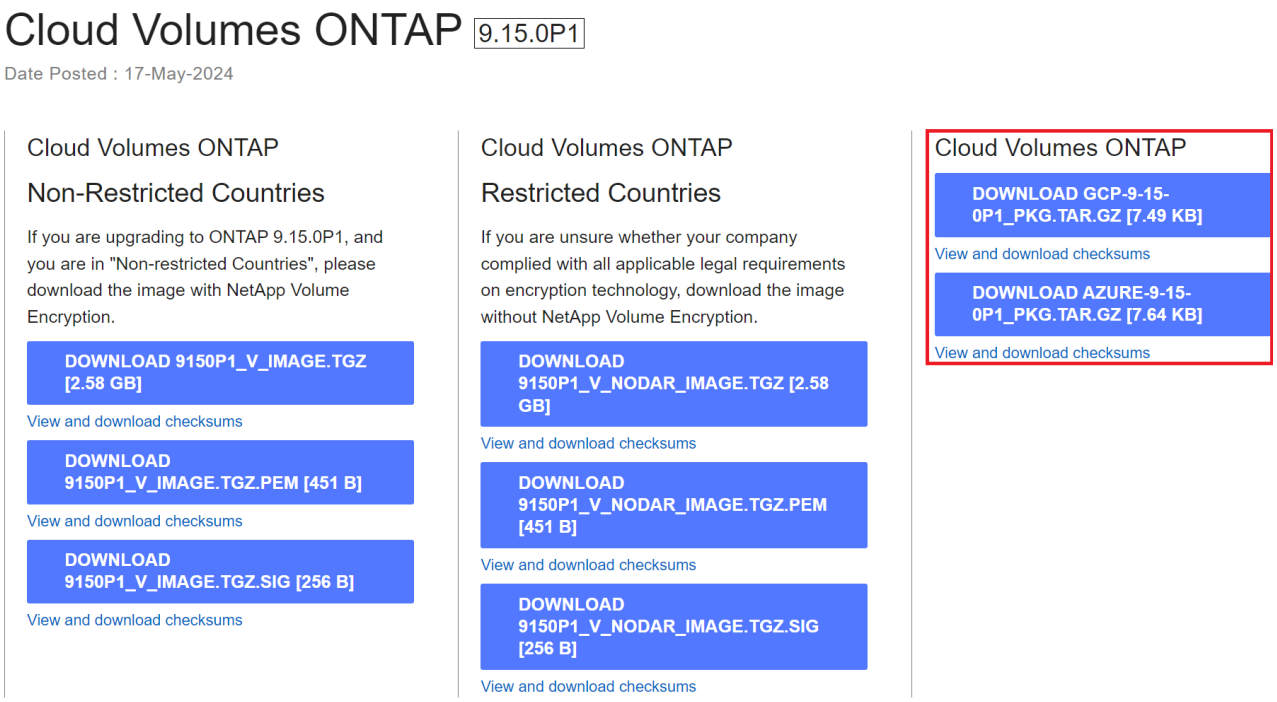
驗證Google Cloud簽署的映像

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。

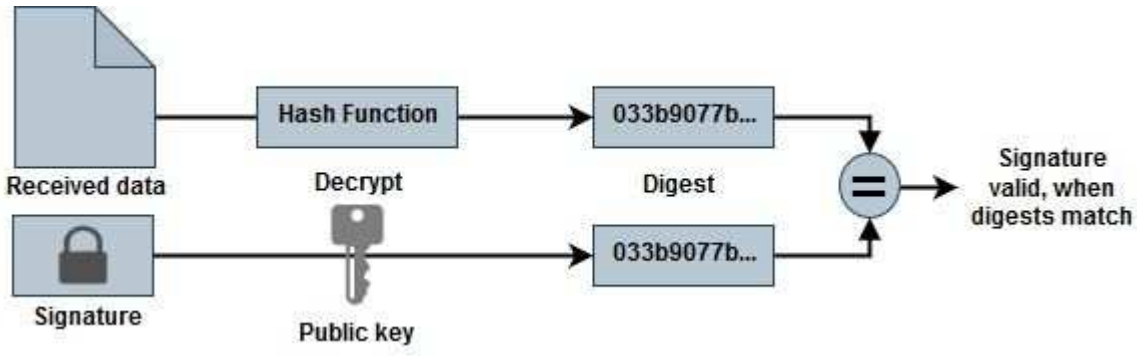
簽署映像驗證工作流程摘要

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

```
# 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

```
# 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
```