



Amazon Web Services 入門

Cloud Volumes ONTAP

NetApp
June 11, 2024

目錄

Amazon Web Services入門	1
在AWS中快速入門Cloud Volumes ONTAP	1
在Cloud Volumes ONTAP AWS中規劃您的不一樣組態	2
設定您的網路	6
設定 AWS KMS	26
設定IAM角色Cloud Volumes ONTAP 以供使用	29
在Cloud Volumes ONTAP AWS中設定適用於此功能的授權	38
在 Cloud Volumes ONTAP AWS 中啟動	45
在 AWS Secret Cloud 和 Top Secret Cloud 地區部署 Cloud Volumes ONTAP	57

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。

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 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。

- ["深入瞭解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"](#)。

- Throughput 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	
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

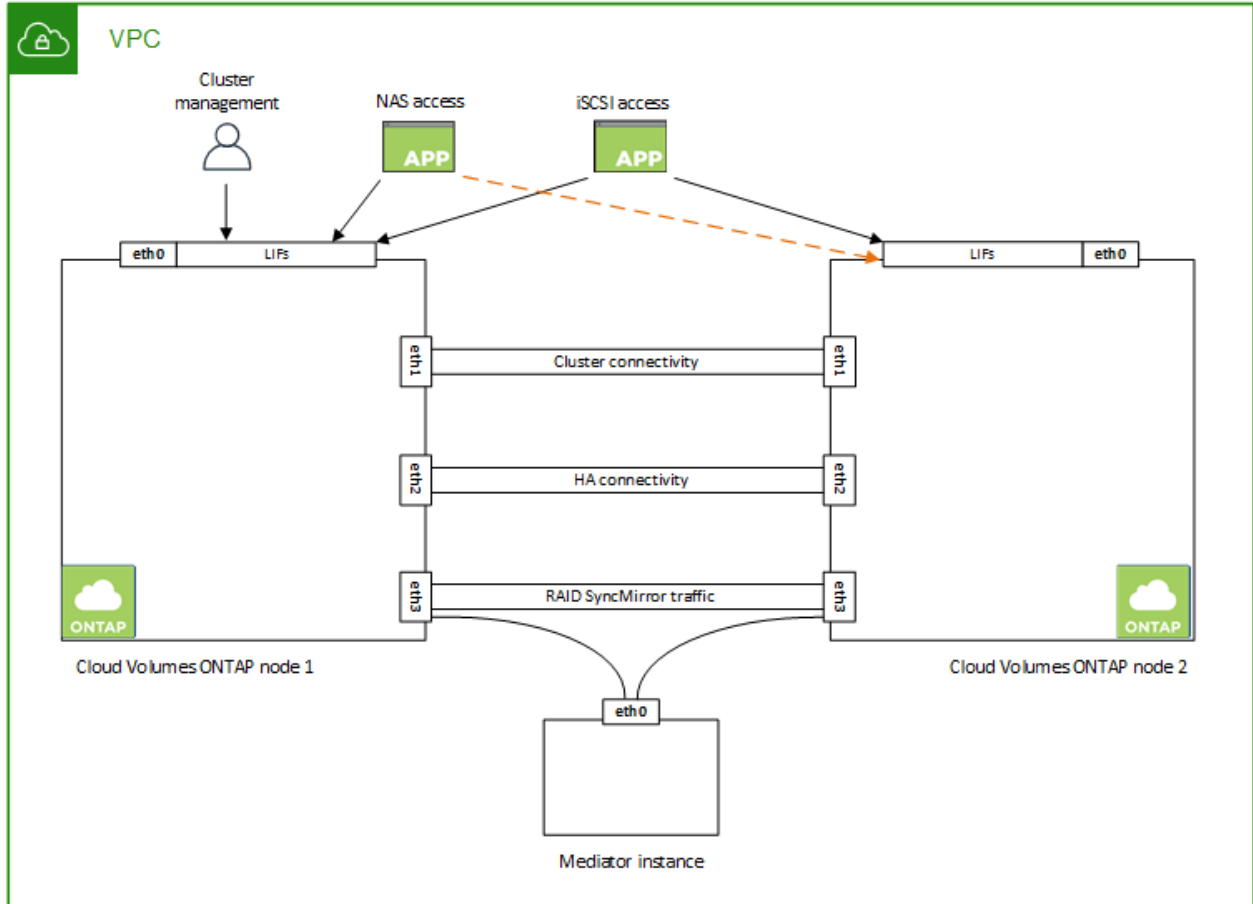
BlueXP會將6個IP位址分配給單一節點系統。

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。
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。
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。

LIF	介面	節點	目的
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 ["高可用性配對"](#)。

可用性區域

此 HA 部署模式使用多個 AZs 來確保資料的高可用性。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。



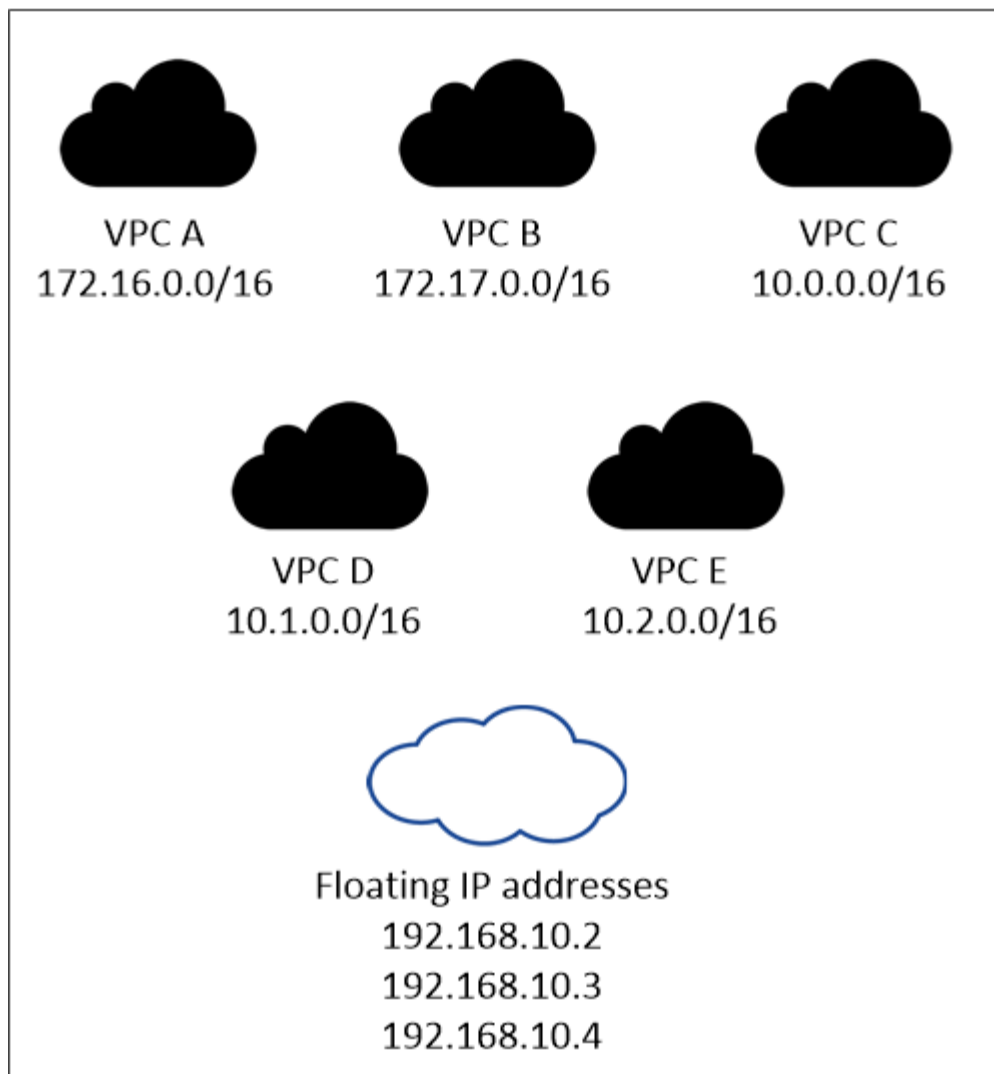
如果您使用 SnapDrive 適用於 Windows 的 SHIP 或 SnapCenter 搭配 HA 配對的 SHIP、則 SVM 管理 LIF 需要一個浮動 IP 位址。

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。

AWS region



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 相關聯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](#)。

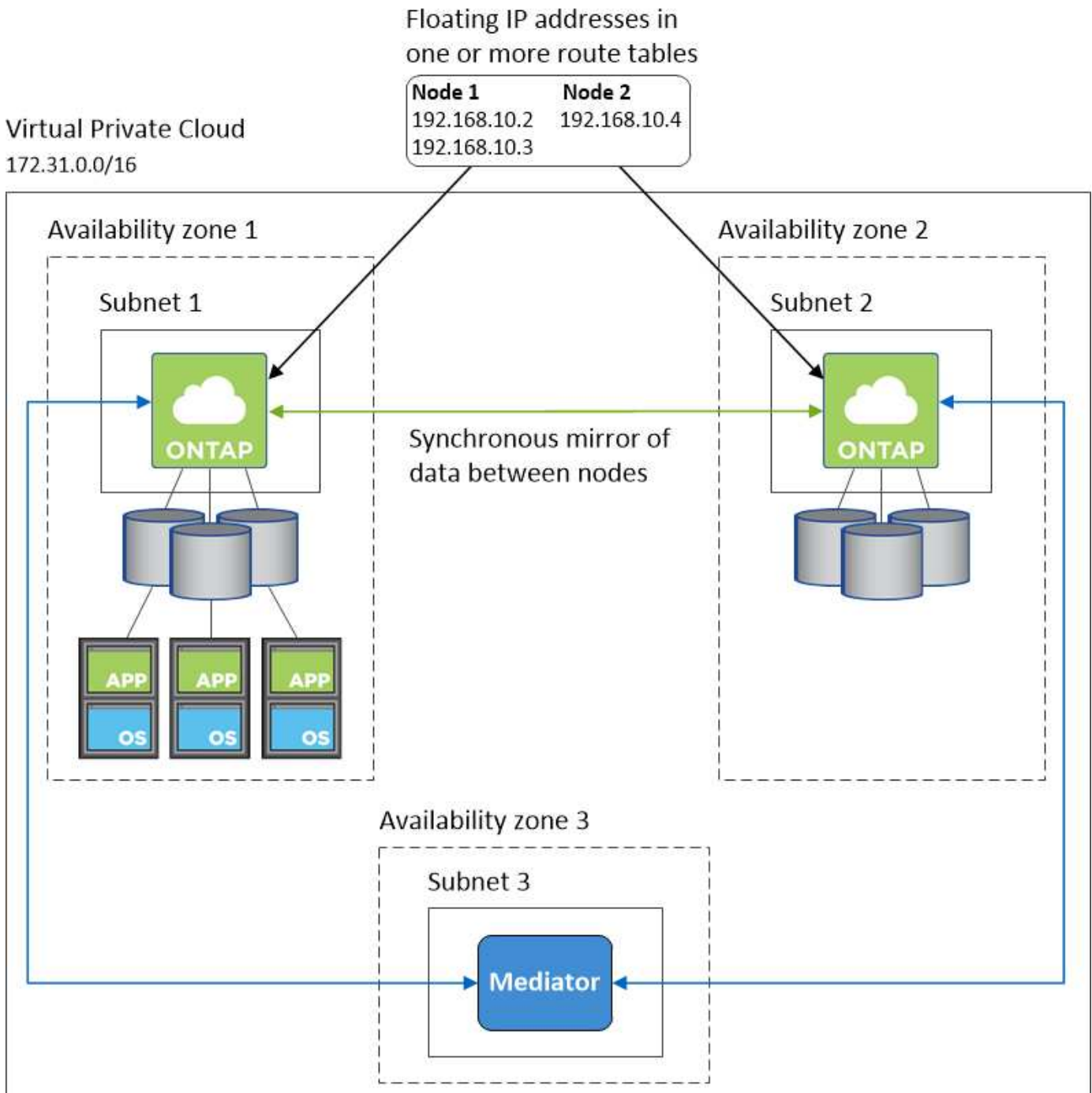
連線至 NetApp 管理工具

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

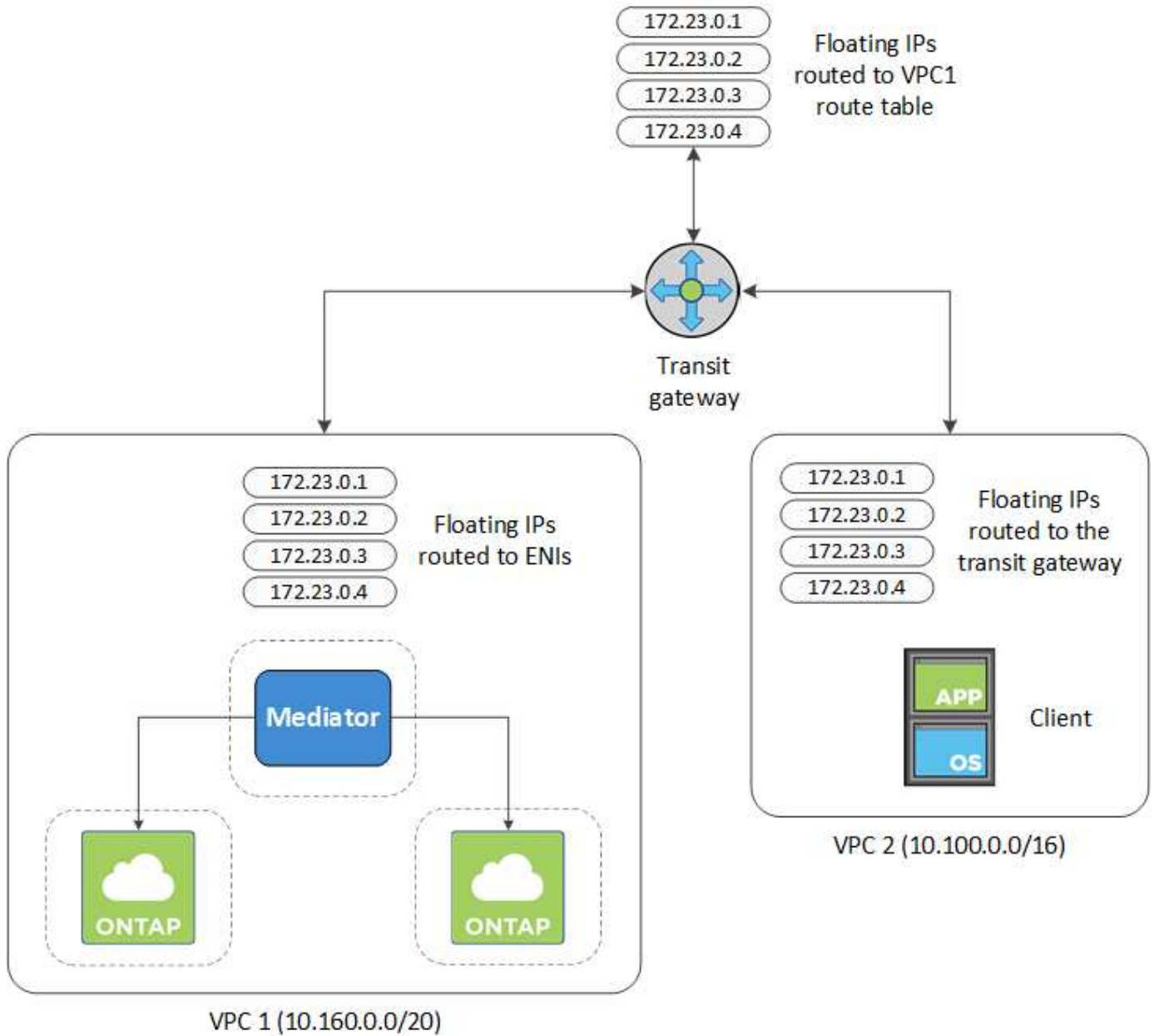
設定 AWS 傳輸閘道、以便存取 HA 配對 ["浮動 IP 位址"](#) 從 HA 配對所在的 VPC 外部。

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：

NFS & CIFS access from within the VPC using Floating IP

Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

Access

SVM Management : 172.23.0.4

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。

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

<input type="checkbox"/>	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8 vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
<input type="checkbox"/>	10.160.0.0/20	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC1	propagated	active
<input type="checkbox"/>	172.23.0.1/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.2/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.3/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.4/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active

Floating IP Addresses

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。

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1
Floating IP Addresses

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。

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-f7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-0f76681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

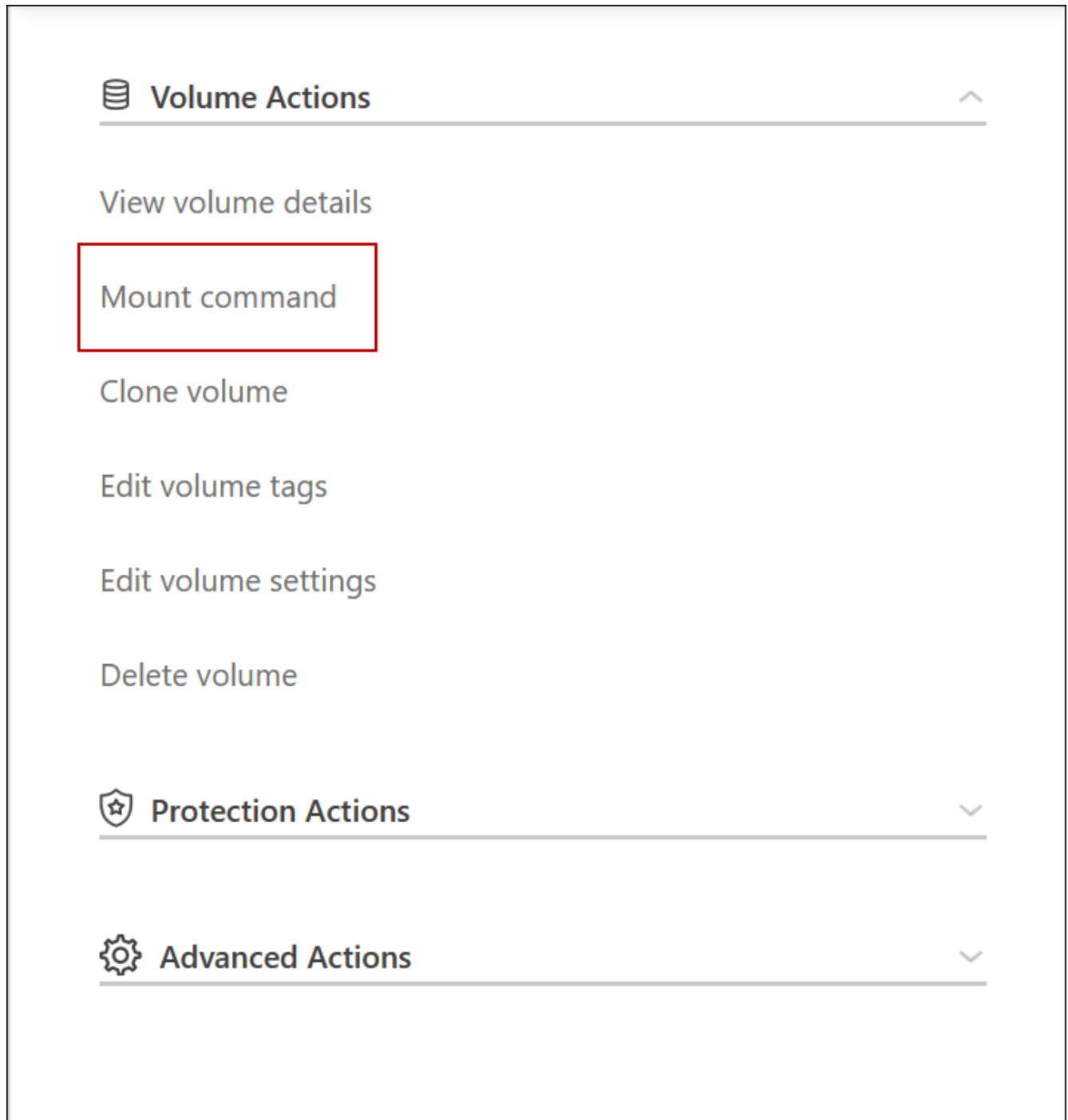
VPC2
Floating IP Addresses

6. 將 VPC 的安全性群組設定更新為「所有流量」。

- 按一下 [虛擬私有雲] 底下的 [子網路]。
- 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。
- 按一下 * 安全性群組 *。
- 選取 * 編輯輸入規則 *。
- 按一下 * 新增規則 *。
- 在 [類型] 下，選取 [* 所有流量]，然後選取 VPC IP 位址。
- 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

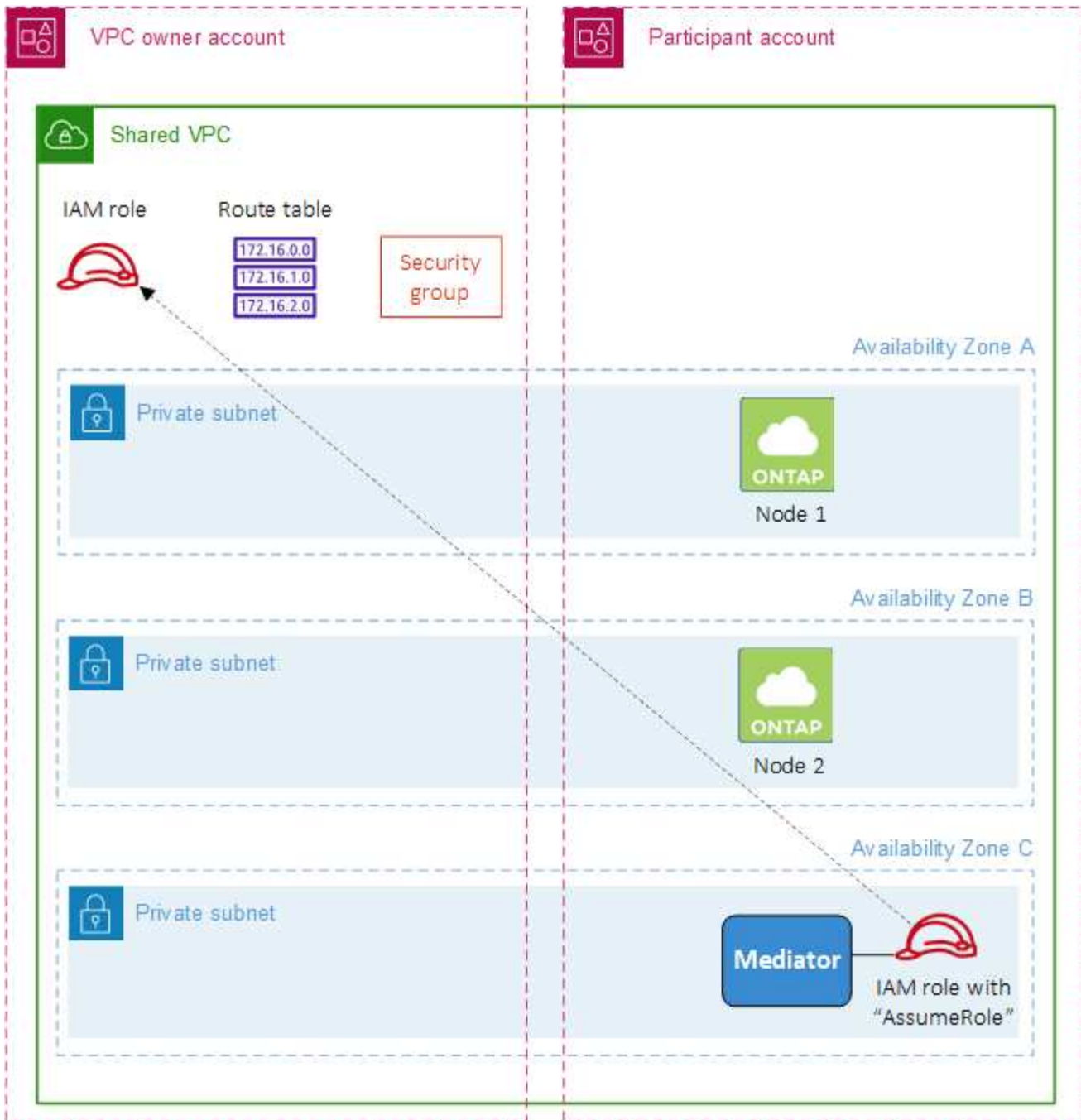
從9.11.1版開始、Cloud Volumes ONTAP AWS支援搭配VPC共享功能的更新版、VPC共用功能可讓您的組織與其他AWS帳戶共用子網路。若要使用此組態、您必須設定AWS環境、然後使用API部署HA配對。

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「assumeRoleArn」

「assumeRoleArn」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"
}
```

+

["深入瞭解Cloud Volumes ONTAP 解NetApp API"](#)

AWS 的安全性群組規則

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
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/offbo xconfig <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	1860 0 – 1869 9	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	1110 4.	叢集間 LIF	叢集間 LIF ONTAP	管理 SnapMirror 的叢集間通訊工作階段
	TCP	1110 5.	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"](#)

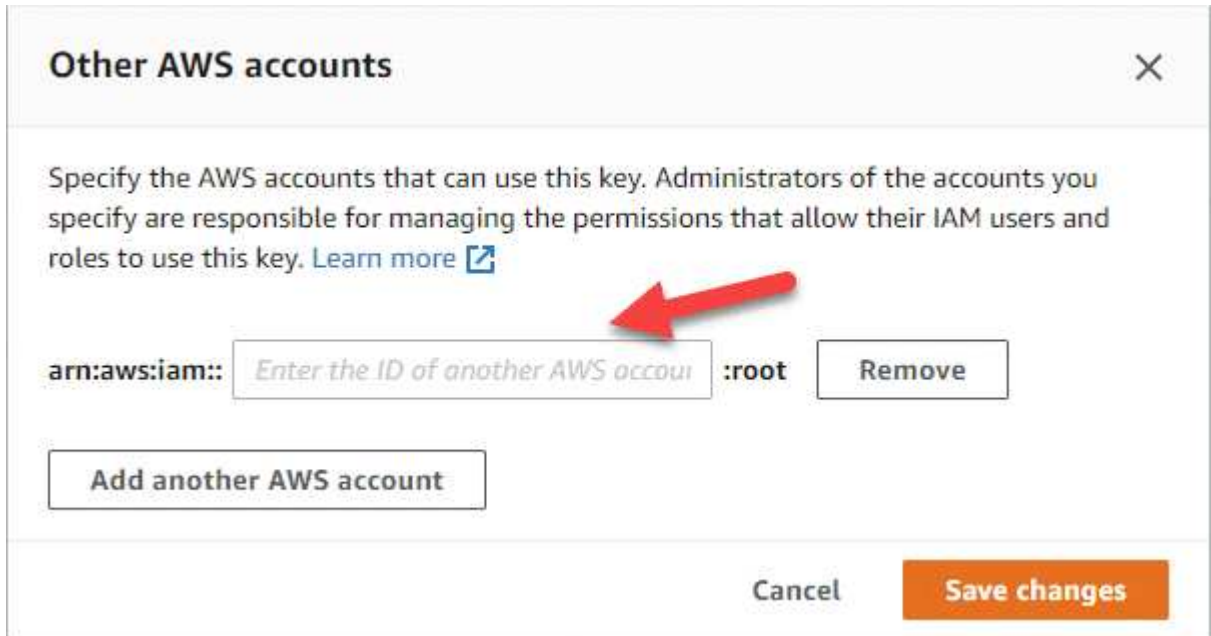
3. 如果 CMK 位於不同的 AWS 帳戶、請完成下列步驟：

- 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"](#)。

- 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IAM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"。

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue **Cancel**

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

Select Charging Method

Professional **By capacity** ▾

Essential **By capacity** ▾

Freemium (Up to 500 GiB) **By capacity** ▾

Per Node **By node** ▾

"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。

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract
 Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go
 Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 **AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 **Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue
Cancel

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。

Select Charging Method

<input checked="" type="radio"/>	Professional	By capacity ∨
<input type="radio"/>	Essential	By capacity ∨
<input type="radio"/>	Freemium (Up to 500 GiB)	By capacity ∨
<input type="radio"/>	Per Node	By node ∨

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

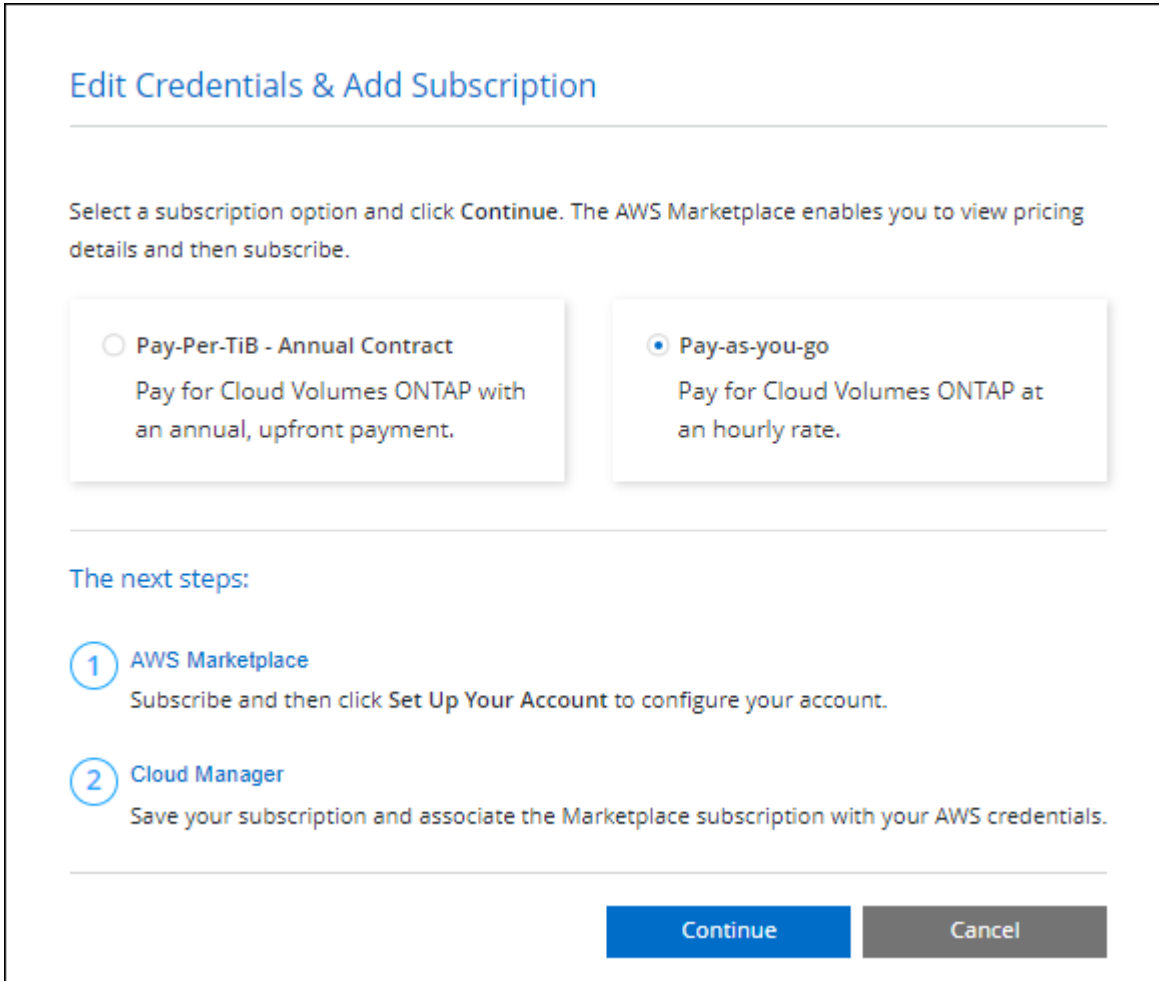
PAYGO訂閱

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。



Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

① **AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.

② **Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue **Cancel**

- 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。

Select Charging Method

<input checked="" type="radio"/> Professional	By capacity	∨
<input type="radio"/> Essential	By capacity	∨
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity	∨
<input type="radio"/> Per Node	By node	∨

"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。

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract
 Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go
 Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 **AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 **Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue
Cancel

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。

Select Charging Method

<input checked="" type="radio"/>	Professional	By capacity ▼
<input type="radio"/>	Essential	By capacity ▼
<input type="radio"/>	Freemium (Up to 500 GiB)	By capacity ▼
<input type="radio"/>	Per Node	By node ▼

"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](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。

Select Charging Method

Keystone By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1 v

Professional By capacity v

Essential By capacity v

Freemium (Up to 500 GiB) By capacity v

Per Node By node v

"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	<p>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。</p> <p>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。</p> <p>"瞭解如何將額外的AWS認證資料新增至BlueXP"。</p>

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。



Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

? **Having issues signing up for your product?**
If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

Subscribe

You are already subscribed to this product

Pricing Details

Software Fees

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	<p>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：</p> <ul style="list-style-type: none"> • 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	<p>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。"深入瞭解Cloud Volumes ONTAP 解適用於此功能的防火牆規則"。</p>

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。

◦ ["深入瞭解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 目標可透過標準以太網路介面卡 (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：

Volume Details, Protection & Protocol

Details & Protection

Volume Name: Size (GB):

Snapshot Policy:

Default Policy

Protocol

NFS
 CIFS
 iSCSI

Share name: Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

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	<p>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。</p> <p>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。</p>

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。



Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

?

Having issues signing up for your product?

If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

Subscribe

You are already subscribed to this product

Pricing Details

Software Fees

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： <ul style="list-style-type: none"> • 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。 " 深入瞭解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。

- ["深入瞭解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 目標可透過標準以太網路介面卡 (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：

Volume Details, Protection & Protocol

Details & Protection	Protocol
<p>Volume Name: <input style="width: 200px;" type="text" value="vol"/></p> <p>Size (GB): <input style="width: 80px;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 150px;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> NFS CIFS iSCSI </p> <p>Share name: <input style="width: 150px;" type="text" value="vol_share"/></p> <p>Permissions: <input style="width: 150px;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 200px;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

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。

```
{
  "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 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>`

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

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

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

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

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

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

商標資訊

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