開始使用Microsoft Azure Cloud Volumes ONTAP

NetApp
June 11, 2024

目錄

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。

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 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"

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 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"。

4 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

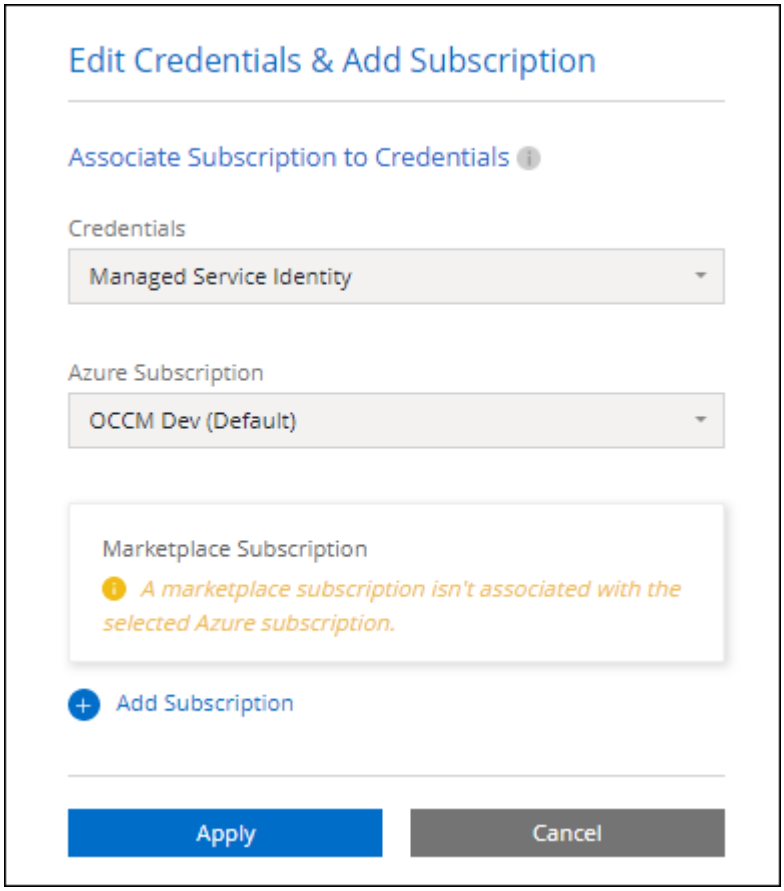
品"。

步驟

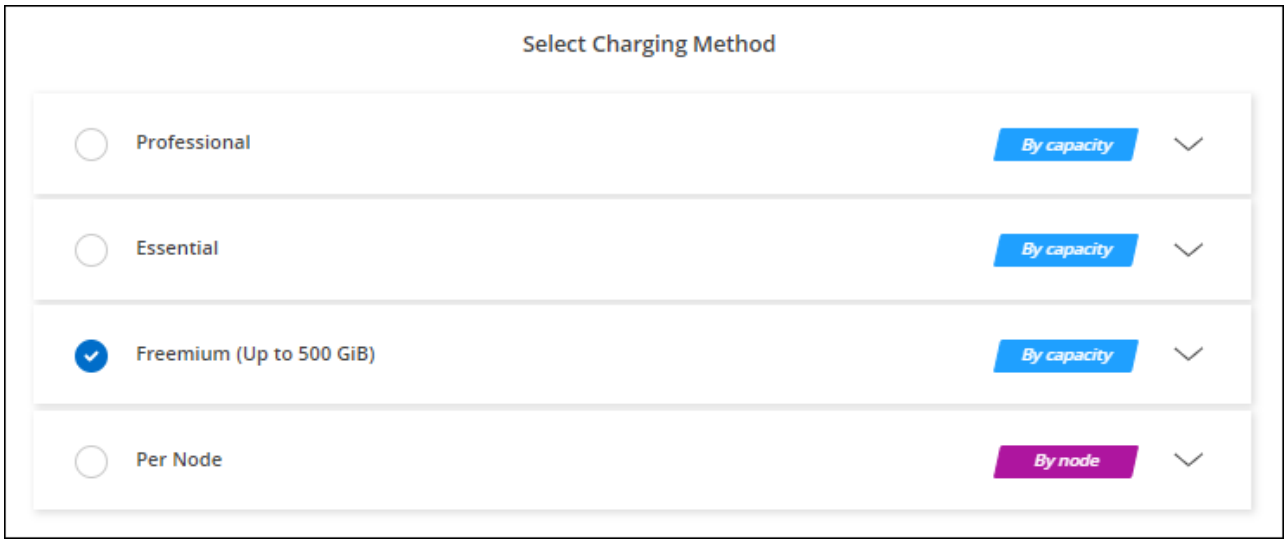
1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。

   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。

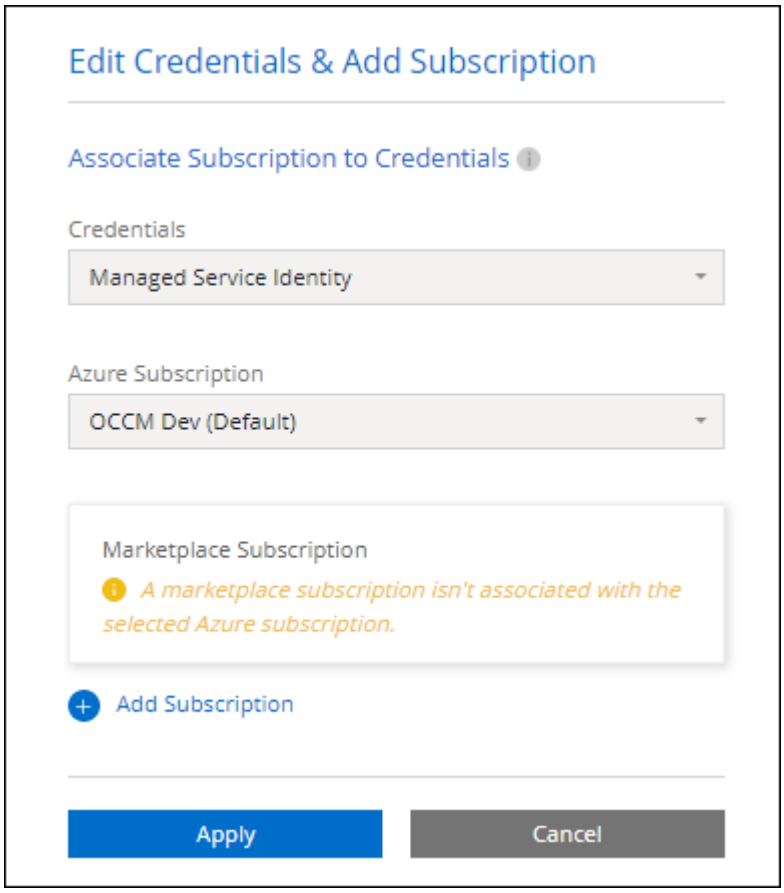
   您必須先從 BlueXP 數位錢包取得授權、才能搭配 Cloud Volumes ONTAP 使用。如有需要、您可以 "手動將授權新增至 BlueXP 數位錢包"。

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。

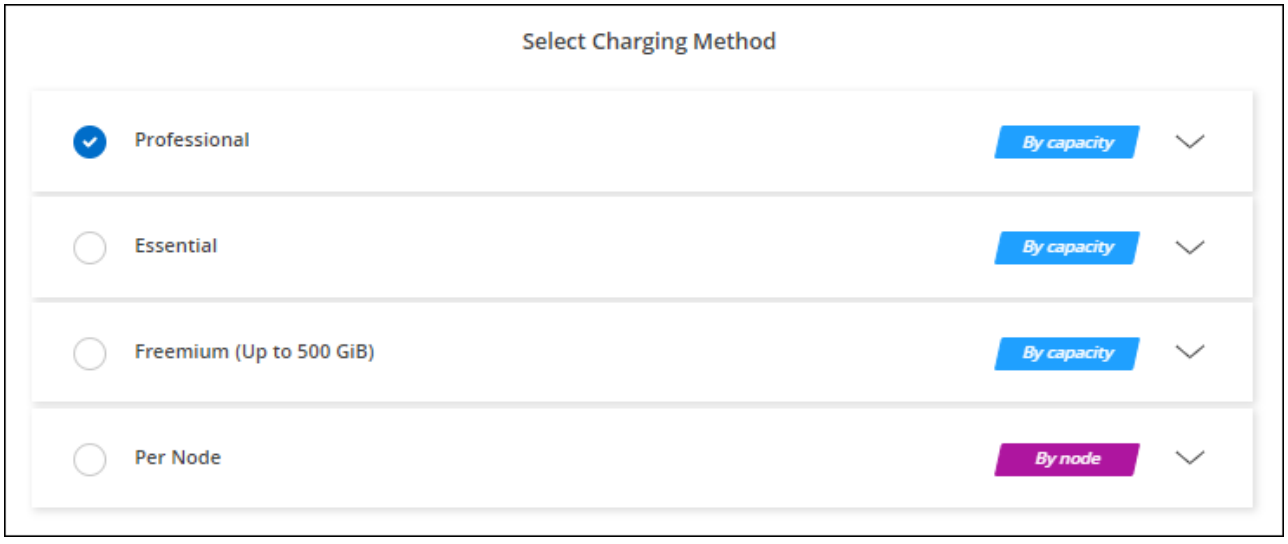
   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示訂閱Azure Marketplace中的隨

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》"。

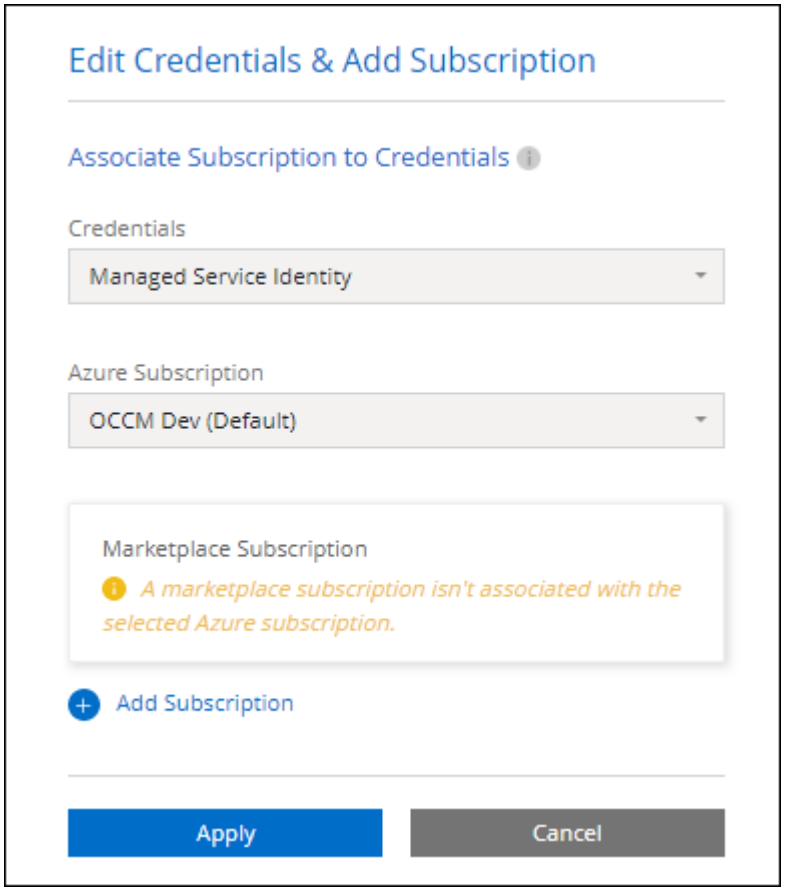
PAYGO訂閱

從雲端供應商的市場訂閱優惠、每小時支付一次。

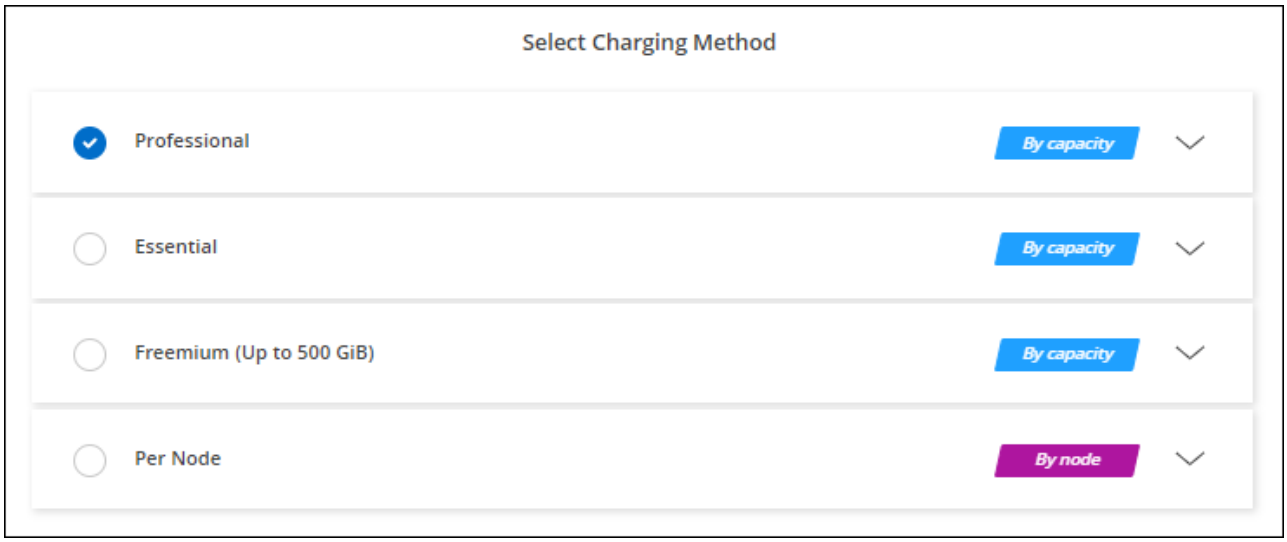
當您建立Cloud Volumes ONTAP 一個運作環境時、BlueXP會提示您訂閱Azure Marketplace提供的合約。該訂閱之後會與工作環境建立關聯、以便進行充電。您可以在其他工作環境中使用相同的訂閱。

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。

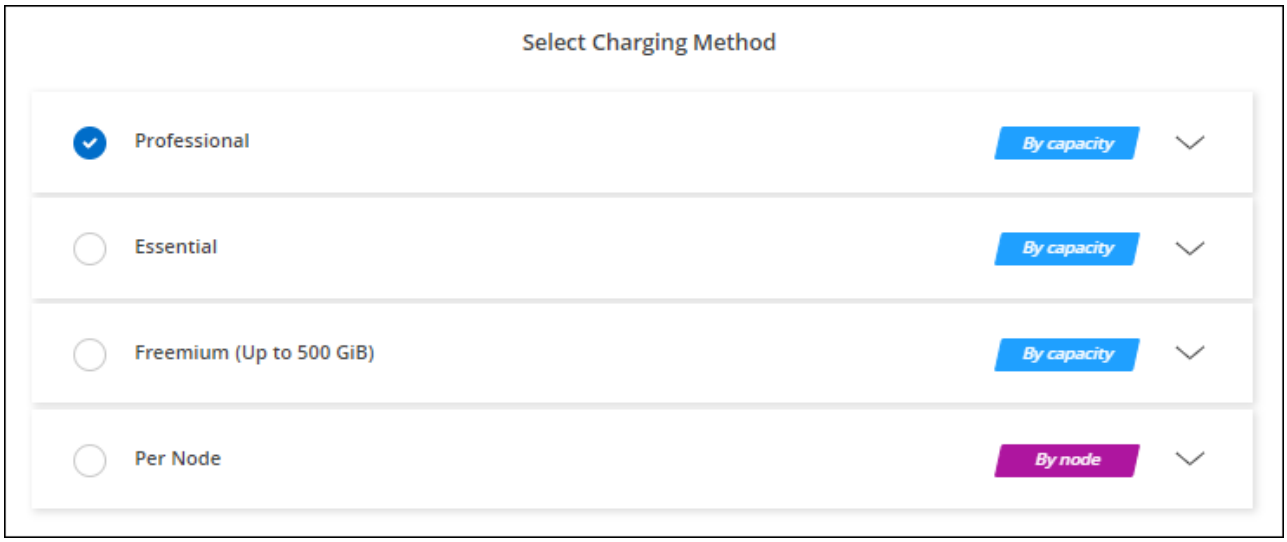
步驟

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。



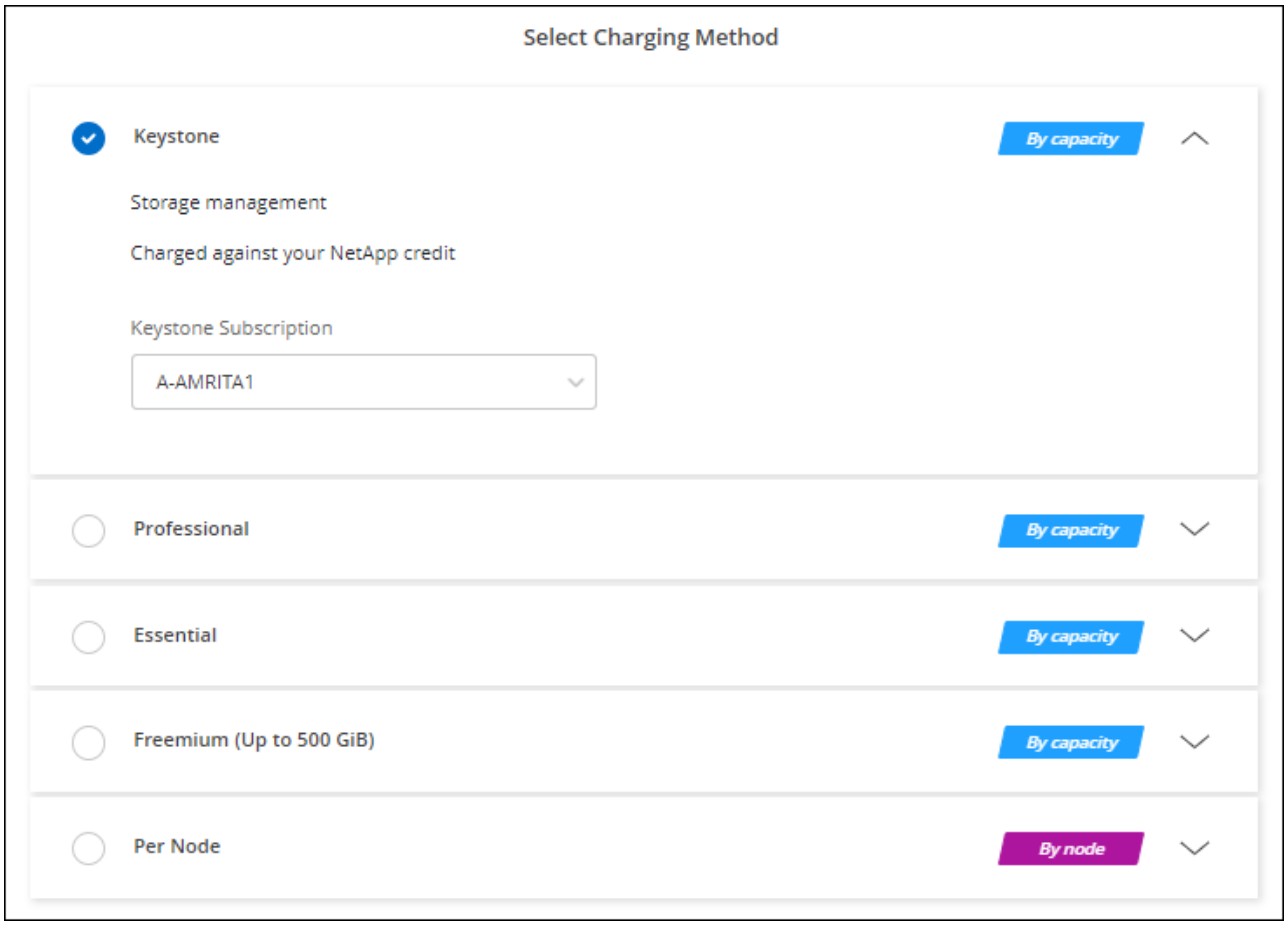
"請參閱Cloud Volumes ONTAP 逐步指示、以在Azure中推出《功能不全》"。

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。

欄位	說明
[[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。

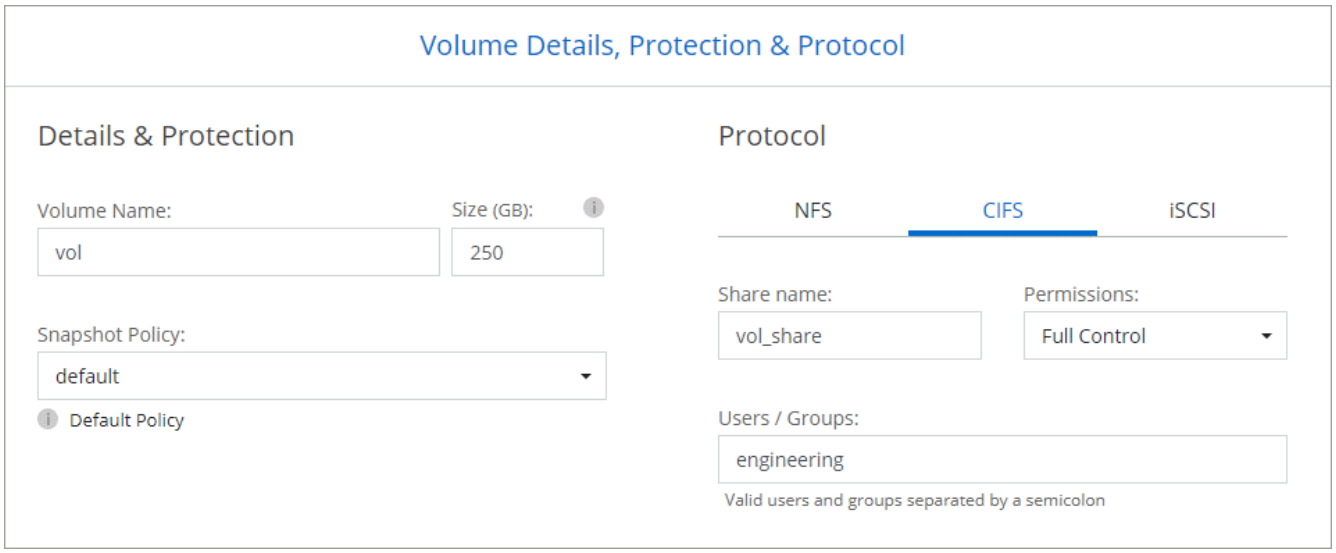
15. * 建立 Volume * ：輸入新磁碟區的詳細資料、或按一下 * 跳過 * 。

"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。
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 。
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"。

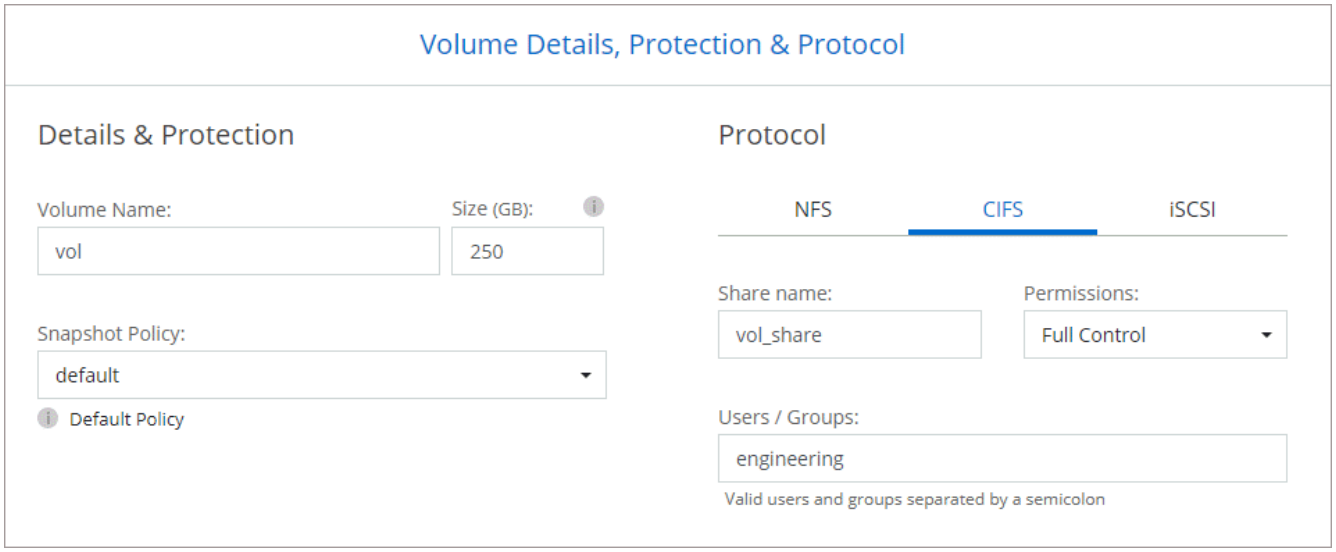
15. * 建立 Volume * ：輸入新磁碟區的詳細資料、或按一下 * 跳過 * 。

"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。
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

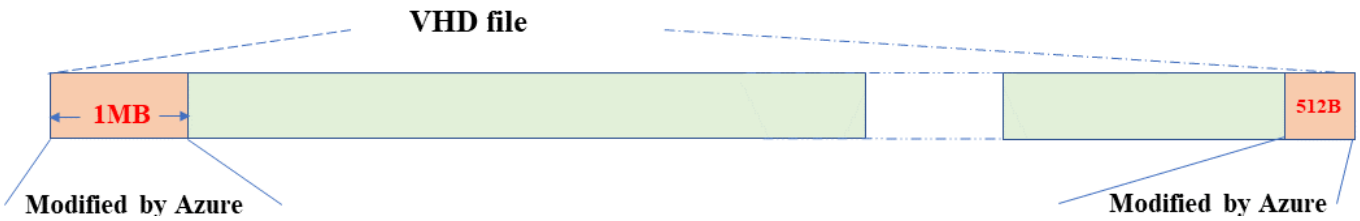
Azure 影像驗證總覽

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。



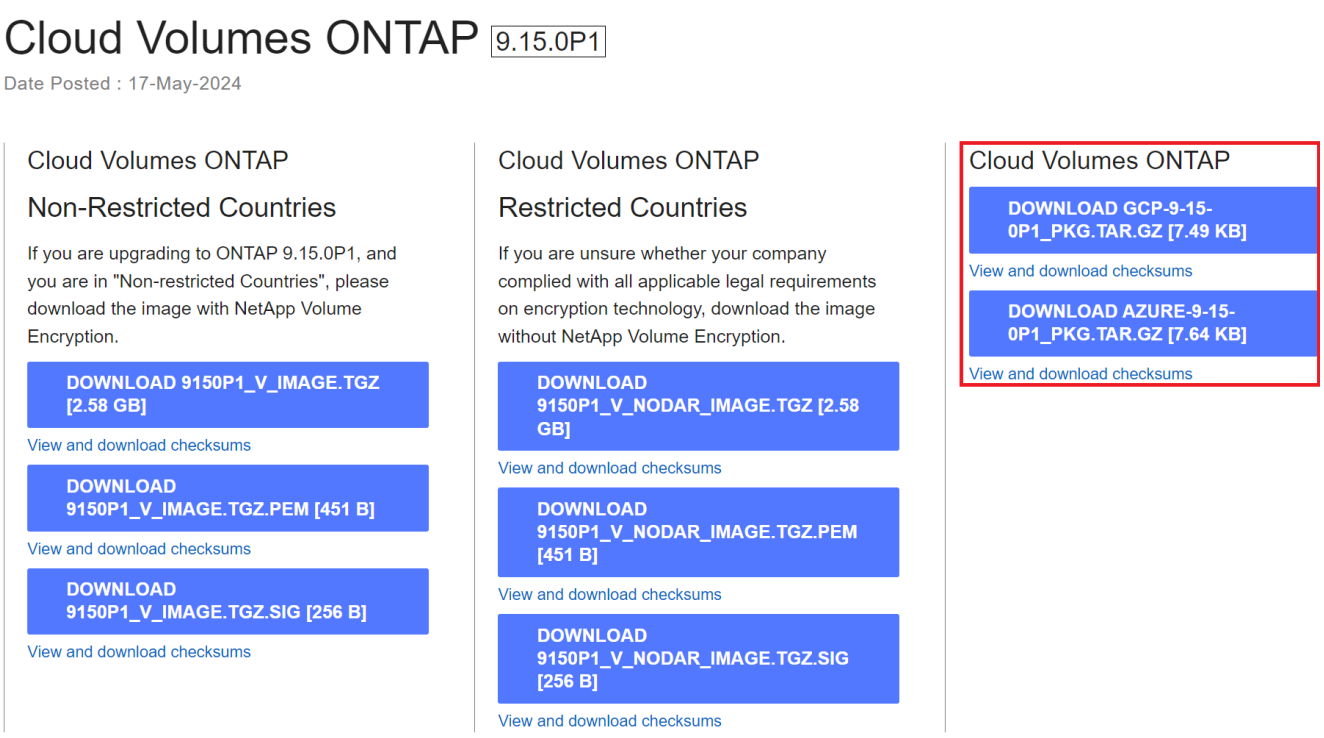
例如、上圖顯示大小為 10GB 的 VHD 檔案。但 NetApp 簽署部分會以綠色標示、大小為 10GB - 1MB - 512B 。

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

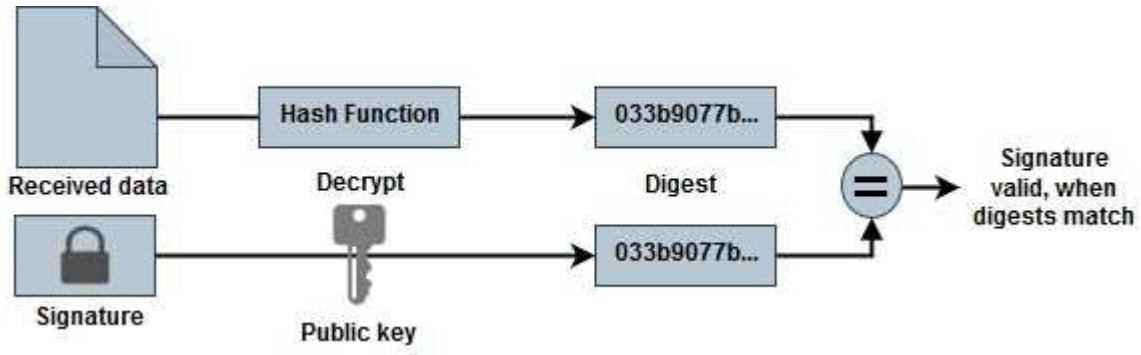
檔案簽章驗證

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"