



NetApp Console入門

Cloud Volumes ONTAP

NetApp
February 13, 2026

This PDF was generated from <https://docs.netapp.com/zh-tw/storage-management-cloud-volumes-ontap/task-getting-started-azure.html> on February 13, 2026. Always check docs.netapp.com for the latest.

目錄

NetApp Console入門	1
Azure 中的Cloud Volumes ONTAP快速入門	1
在 Azure 中規劃您的Cloud Volumes ONTAP配置	1
選擇Cloud Volumes ONTAP許可證	2
選擇支援的區域	2
選擇受支援的 VM 類型	2
了解儲存限制	2
在 Azure 中調整系統大小	2
查看預設系統磁碟	3
收集網路資訊	3
選擇寫入速度	4
選擇卷使用情況設定檔	4
為Cloud Volumes ONTAP設定 Azure 網路	4
Cloud Volumes ONTAP的要求	4
控制台代理的要求	13
設定Cloud Volumes ONTAP以在 Azure 中使用客戶管理的金鑰	13
資料加密概述	13
Cloud Volumes ONTAP中的金鑰輪換	14
建立使用者分配的託管標識	15
建立金鑰保管庫並產生金鑰	15
建立使用加密金鑰的系統	16
在 Azure 中設定Cloud Volumes ONTAP許可	18
免費增值	18
基於容量的許可證	19
Keystone訂閱	23
基於節點的許可證	24
在 Azure 中為Cloud Volumes ONTAP啟用高可用性模式	24
在 Azure 中為Cloud Volumes ONTAP啟用 VMOrchestratorZonalMultiFD	26
在 Azure 中啟動Cloud Volumes ONTAP	26
在 Azure 中啟動單節點Cloud Volumes ONTAP系統	27
在 Azure 中啟動Cloud Volumes ONTAP HA 對	31
驗證 Azure 平台映像	37
針對Cloud Volumes ONTAP 的Azure 市場映像驗證	37
下載適用於Cloud Volumes ONTAP 的Azure 映像文件	37
從 Azure 市場匯出Cloud Volumes ONTAP的 VHD 映像	38
驗證文件簽名	44

NetApp Console入門

Azure 中的Cloud Volumes ONTAP快速入門

只需幾個步驟即可開始使用Cloud Volumes ONTAP for Azure。

1

建立控制台代理

如果你沒有 ["控制台代理"](#)但是，您需要建立一個。 ["了解如何在 Azure 中建立控制台代理"](#)

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

2

規劃您的配置

控制台提供符合您的工作負載要求的預先配置包，或者您可以建立自己的配置。如果您選擇自己的配置，您應該了解可用的選項。有關信息，請參閱["在 Azure 中規劃您的Cloud Volumes ONTAP配置"](#)。

3

設定網路

1. 確保您的 VNet 和子網路將支援控制台代理程式和Cloud Volumes ONTAP之間的連線。
2. 為NetApp AutoSupport啟用從目標 VPC 的出站網際網路存取。

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

["了解有關網路要求的更多信息"](#)。

4

啟動Cloud Volumes ONTAP

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

相關連結

- ["從控制台建立控制台代理"](#)
- ["從 Azure 市集建立控制台代理"](#)
- ["在 Linux 主機上安裝控制台代理軟體"](#)
- ["控制台如何處理權限"](#)

在 Azure 中規劃您的Cloud Volumes ONTAP配置

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

選擇Cloud Volumes ONTAP許可證

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

- ["了解Cloud Volumes ONTAP的授權選項"](#)
- ["了解如何設定許可"](#)

選擇支援的區域

大多數 Microsoft Azure 區域都支援Cloud Volumes ONTAP。 ["查看支援區域的完整列表"](#)。

選擇受支援的 VM 類型

Cloud Volumes ONTAP支援多種 VM 類型，視您選擇的授權類型而定。

["Azure 中Cloud Volumes ONTAP支援的配置"](#)

了解儲存限制

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

["Azure 中Cloud Volumes ONTAP的儲存限制"](#)

在 Azure 中調整系統大小

調整Cloud Volumes ONTAP系統的大小可以幫助您滿足效能和容量要求。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

查看受支援的虛擬機器類型 ["Cloud Volumes ONTAP發行說明"](#)然後查看有關每種受支援的 VM 類型的詳細資訊。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：記憶體最佳化虛擬機器大小"](#)

Azure 磁碟類型（單節點系統）

為Cloud Volumes ONTAP建立磁碟區時，您需要選擇Cloud Volumes ONTAP用作磁碟的底層雲端儲存。

單節點系統可以使用下列類型的 Azure 託管磁碟：

- 進階 SSD 託管磁碟 以更高的成本為 I/O 密集型工作負載提供高效能。
- 與高級 SSD 託管磁碟相比，高級 SSD v2 託管磁碟 以更低成本提供更高的效能和更低的延遲。
- 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 並且想要降低成本，那麼「標準 HDD 託管磁碟」是一個不錯的選擇。

有關這些磁碟用例的更多詳細信息，請參閱 ["Microsoft Azure 文件：Azure 中有哪些磁碟類型？"](#)。

具有 HA 對的 Azure 磁碟類型

HA 系統使用進階 SSD 共享託管磁碟，它們都以更高的成本為 I/O 密集型工作負載提供高效能。9.12.1 版本之前建立的 HA 部署使用進階頁面 blob。

Azure 磁碟大小

啟動 Cloud Volumes ONTAP 實例時，您必須選擇聚合的預設磁碟大小。NetApp Console 將此磁碟大小用於初始聚合，以及使用簡單設定選項時建立的任何其他聚合。您可以透過以下方式建立使用不同於預設磁碟大小的聚合：["使用進階分配選項"](#)。



聚合中的所有磁碟必須具有相同的大小。

選擇磁碟大小時，您應該考慮幾個因素。磁碟大小會影響您支付的儲存費用、您可以在聚合中建立的磁碟區的大小、Cloud Volumes ONTAP 可用的總容量以及儲存效能。

Azure Premium Storage 的效能與磁碟大小相關。更大的磁碟可提供更高的 IOPS 和吞吐量。例如，選擇 1 TiB 磁碟可以提供比 500 GiB 磁碟更好的效能，但成本更高。

標準儲存的磁碟大小之間沒有效能差異。您應該根據所需的容量來選擇磁碟大小。

請參閱 Azure 以了解按磁碟大小劃分的 IOPS 和吞吐量：

- ["Microsoft Azure：託管磁碟定價"](#)
- ["Microsoft Azure：Page Blob 定價"](#)

查看預設系統磁碟

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

["查看 Azure 中 Cloud Volumes ONTAP 系統資料的預設磁碟"](#)。



控制台代理還需要系統磁碟。["查看控制台代理預設配置的詳細信息"](#)。

收集網路資訊

在 Azure 中部署 Cloud Volumes ONTAP 時，您需要指定有關虛擬網路的詳細資訊。您可以使用工作表從管理員收集資訊。

Azure 資訊	你的價值
地區	
虛擬網路 (VNet)	
子網	
網路安全群組（如果使用您自己的）	

選擇寫入速度

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

選擇卷使用情況設定檔

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

NetApp儲存效率功能有以下優勢：

精簡配置

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

重複資料刪除

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

壓縮

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

為Cloud Volumes ONTAP設定 Azure 網路

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

Cloud Volumes ONTAP的要求

Azure 中必須符合下列網路需求。

出站互聯網訪問

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

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

Cloud Volumes ONTAP端點

Cloud Volumes ONTAP使用這些端點與各種服務進行通訊。

端點	適用於	目的	部署模式	不可用時的影響
\ https://netapp-cloud-account.auth0.com	驗證	用於控制台中的身份驗證。	標準和限制模式。	用戶身份驗證失敗，以下服務仍然不可用： • Cloud Volumes ONTAP服務 • ONTAP服務 • 協定和代理服務
https://vault.azure.net	金鑰保管庫	用於使用客戶管理金鑰 (CMK) 時從 Azure Key Vault 擷取客戶端金鑰。	標準、受限和私人模式。	Cloud Volumes ONTAP服務無法使用。
\ https://api.blueexp.net/app.com/tenancy	租賃	用於從控制台檢索Cloud Volumes ONTAP資源以授權資源和使用者。	標準和限制模式。	Cloud Volumes ONTAP資源和使用者未獲得授權。
\ https://mysupport.net/app.com/aods/asupmessage \ https://mysupport.net/app.com/asupprod/post/1.0/postAsup	AutoSupport	用於將AutoSupport遙測資料傳送給NetApp支援。	標準和限制模式。	AutoSupport資訊仍未送達。
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blueexpinfraproduct.eastus2.data.azurecr.io \ https://core.windows.net	公共區域	與 Azure 服務通訊。	標準、受限和私人模式。	Cloud Volumes ONTAP無法與 Azure 服務通訊以對 Azure 中的控制台執行特定操作。
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	中國區	與 Azure 服務通訊。	標準、受限和私人模式。	Cloud Volumes ONTAP無法與 Azure 服務通訊以對 Azure 中的控制台執行特定操作。

端點	適用於	目的	部署模式	不可用時的影響
https://management.microsoftazure.de \ https://login.microsoftonline.de \ https://blob.core.cloudapi.de \ https://core.cloudapi.de	德國地區	與 Azure 服務通訊。	標準、受限和私人模式。	Cloud Volumes ONTAP無法與 Azure 服務通訊以對 Azure 中的控制台執行特定操作。
https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	政府區域	與 Azure 服務通訊。	標準、受限和私人模式。	Cloud Volumes ONTAP無法與 Azure 服務通訊以對 Azure 中的控制台執行特定操作。
https://management.azure.microsoft.scloud \ https://login.microsoftonline.microsoft.scloud \ https://blob.core.microsoft.scloud \ https://core.microsoft.scloud	政府國防部區	與 Azure 服務通訊。	標準、受限和私人模式。	Cloud Volumes ONTAP無法與 Azure 服務通訊以對 Azure 中的控制台執行特定操作。

NetApp Console代理程式的網路代理程式配置

您可以使用NetApp Console代理程式的代理伺服器設定來啟用來自Cloud Volumes ONTAP 的外部網路存取。控制台支援兩種類型的代理：

- 明確代理：來自Cloud Volumes ONTAP 的出站流量使用在控制台代理的代理配置期間指定的代理伺服器的 HTTP 位址。管理員可能還配置了使用者憑證和根 CA 憑證以進行額外的身份驗證。Cloud Volumes ONTAP 顯式代理程式有可用的根 CA 證書，請確保使用 **"ONTAP CLI：安全性憑證安裝"**命令。
- 透明代理：網路配置為透過控制台代理的代理程式自動路由來自Cloud Volumes ONTAP 的出站流量。設定透明代理時，管理員只需要提供用於從Cloud Volumes ONTAP進行連接的根 CA 證書，而不是代理伺服器的 HTTP 位址。確保使用以下方式取得相同的根 CA 憑證並將其上傳到您的Cloud Volumes ONTAP系統 **"ONTAP CLI：安全性憑證安裝"**命令。

有關配置代理伺服器的信息，請參閱 **"配置控制台代理以使用代理伺服器"**。

IP 位址

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

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



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

單節點系統的 IP 位址

Console 會為單節點系統指派 5 或 6 個 IP 位址：

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



iSCSI IP 透過 iSCSI 協定提供客戶端存取。系統也將其用於其他重要的網路工作流程。此 LIF 是必需的，不應刪除。

- SVM 管理（可選 - 預設未配置）

HA 對的 IP 位址

控制台在部署期間將 IP 位址指派給 4 個 NIC（每個節點）。

請注意，NetApp Console 會在 HA 配對上建立 SVM 管理 LIF，但不會在 Azure 中的單節點系統上建立。

NIC0

- 節點管理IP
- 群集間 IP
- iSCSI IP



iSCSI IP 透過 iSCSI 協定提供客戶端存取。系統也將其用於其他重要的網路工作流程。此 LIF 是必需的，不應刪除。

NIC1

- 叢集網路IP

NIC2

- 叢集互連 IP (HA IC)

NIC3

- Pageblob NIC IP（磁碟存取）



NIC3 僅適用於使用頁 Blob 儲存的 HA 部署。

上述 IP 位址在故障轉移事件中不會遷移。

此外，還配置了 4 個前端 IP（FIP）以在故障轉移事件時進行遷移。這些前端 IP 位於負載平衡器中。

- 叢集管理 IP
- NodeA 資料 IP (NFS/CIFS)
- NodeB 資料 IP (NFS/CIFS)
- SVM 管理 IP

與 Azure 服務的安全連線

預設情況下，控制台啟用 Azure 專用鏈接，用於 Cloud Volumes ONTAP 和 Azure 頁 Blob 儲存帳戶之間的連接。

在大多數情況下，您無需執行任何操作 - 控制台會為您管理 Azure 專用連結。但是如果您使用 Azure 私人 DNS，則需要編輯設定檔。您還應該了解 Azure 中控制台代理程式的位置需求。

如果您的業務需要，您也可以停用專用連結連線。如果停用該鏈接，控制台會將 Cloud Volumes ONTAP 配置為使用服務端點。

["了解有關將 Azure Private Links 或服務端點與 Cloud Volumes ONTAP 結合使用的更多信息"](#)。

與其他 ONTAP 系統的連接

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

有關說明，請參閱 ["Microsoft Azure 文件：在 Azure 入口網站中建立網站到網站連接"](#)。

HA 互連埠

Cloud Volumes ONTAP HA 對包含 HA 互連，這使得每個節點能夠持續檢查其夥伴節點是否正常運行，並為對方的非揮發性記憶體鏡像日誌資料。HA 互連使用 TCP 連接埠 10006 進行通訊。

預設情況下，HA 互連 LIF 之間的通訊是開放的，且此連接埠沒有安全群組規則。但是，如果您在 HA 互連 LIF 之間建立防火牆，則需要確保 TCP 流量對連接埠 10006 開放，以便 HA 對可以正常運作。

Azure 資源組中只有一個 HA 對

您必須為在 Azure 中部署的每個 Cloud Volumes ONTAP HA 對使用一個專用資源群組。一個資源組中僅支援一個 HA 對。

如果您嘗試在 Azure 資源組中部署第二個 Cloud Volumes ONTAP HA 對，控制台會遇到連線問題。

安全群組規則

控制台建立 Azure 安全性群組，其中包含 Cloud Volumes ONTAP 成功執行的入站和出站規則。 ["查看控制台代理程式的安全性群組規則"](#)。

Cloud Volumes ONTAP的 Azure 安全性群組需要開啟適當的连接埠以進行節點之間的內部通訊。"[了解ONTAP內部端口](#)"。

我們不建議修改預先定義的安全性群組或使用自訂安全群組。但是，如果必須這樣做，請注意，部署過程要求Cloud Volumes ONTAP系統在自己的子網路內擁有完全存取權限。部署完成後，如果決定修改網路安全群組，請確保保持叢集連接埠和 HA 網路連接埠開放。這確保了Cloud Volumes ONTAP叢集內的無縫通訊（節點之間的任意通訊）。

單節點系統的入站規則

新增Cloud Volumes ONTAP系統並選擇預先定義安全性群組時，您可以選擇允許下列其中的流量：

- 僅限選定的 **VNet**：入站流量的來源是Cloud Volumes ONTAP系統的 VNet 子網路範圍和控制台代理程式所在的 VNet 子網路範圍。這是推薦的選項。
- 所有 **VNets**：入站流量的來源是 0.0.0.0/0 IP 範圍。
- 已停用：此選項限制對您的儲存帳戶的公共網路訪問，並停用Cloud Volumes ONTAP系統的資料分層。如果由於安全法規和政策，您的私人 IP 位址即使在同一個 VNet 內也不應該暴露，那麼建議使用此選項。

優先權和名稱	連接埠和協定	來源和目的地	描述
1000 入站_ssh	22 TCP	任意到任意	透過 SSH 存取叢集管理 LIF 或節點管理 LIF 的 IP 位址
1001 入站 http	80 TCP	任意到任意	使用叢集管理 LIF 的 IP 位址透過 HTTP 存取ONTAP System Manager Web 控制台
1002 inbound_111_tcp	111 TCP	任意到任意	NFS 的遠端過程調用
1003 inbound_111_udp	111 UDP	任意到任意	NFS 的遠端過程調用
1004 inbound_139	139 TCP	任意到任意	CIFS 的 NetBIOS 服務會話
1005 入站_161-162_tcp	161-162 TCP	任意到任意	簡單網路管理協議
1006 入站_161-162_udp	161-162 UDP	任意到任意	簡單網路管理協議
1007 inbound_443	443 TCP	任意到任意	使用叢集管理 LIF 的 IP 位址與控制台代理程式建立連線並透過 HTTPS 存取ONTAP System Manager Web 控制台
1008 inbound_445	445 TCP	任意到任意	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
1009 inbound_635_tcp	635 TCP	任意到任意	NFS 掛載
1010 inbound_635_udp	635 UDP	任意到任意	NFS 掛載
1011 inbound_749	749 TCP	任意到任意	Kerberos
1012 inbound_2049_tcp	2049 TCP	任意到任意	NFS 伺服器守護程式
1013 inbound_2049_udp	2049 UDP	任意到任意	NFS 伺服器守護程式

優先權和名稱	連接埠和協定	來源和目的地	描述
1014 inbound_3260	3260 TCP	任意到任意	透過 iSCSI 資料 LIF 進行 iSCSI 訪問
1015 入站_4045-4046_tcp	4045-4046 TCP	任意到任意	NFS 鎖定守護程式和網路狀態監視器
1016 入站_4045-4046_udp	4045-4046 UDP	任意到任意	NFS 鎖定守護程式和網路狀態監視器
1017 inbound_10000	10000 TCP	任意到任意	使用 NDMP 備份
1018 入站_11104-11105	11104-11105 TCP	任意到任意	SnapMirror資料傳輸
3000 入站拒絕_所有_tcp	任意連接埠 TCP	任意到任意	阻止所有其他 TCP 入站流量
3001 入站拒絕_所有_udp	任意連接埠 UDP	任意到任意	阻止所有其他 UDP 入站流量
65000 允許 VnetInBound	任意連接埠任意協定	虛擬網路到虛擬網路	來自 VNet 內部的入站流量
65001 允許 Azure 負載平衡器入站	任意連接埠任意協定	AzureLoadBalancer 到任意	來自 Azure 標準負載平衡器的資料流量
65500 拒絕所有入站	任意連接埠任意協定	任意到任意	阻止所有其他入站流量

HA 系統的入站規則

新增Cloud Volumes ONTAP系統並選擇預先定義安全性群組時，您可以選擇允許下列其中的流量：

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



HA 系統的入站規則比單節點系統少，因為入站資料流量會經過 Azure Standard Load Balancer。因此，來自 Load Balancer 的流量應該保持開放狀態，如「AllowAzureLoadBalancerInBound」規則所示。

- 已停用：此選項限制對您的儲存帳戶的公共網路訪問，並停用Cloud Volumes ONTAP系統的資料分層。如果由於安全法規和政策，您的私人 IP 位址即使在同一個 VNet 內也不應該暴露，那麼建議使用此選項。

優先權和名稱	連接埠和協定	來源和目的地	描述
100 inbound_443	443 任何協議	任意到任意	使用叢集管理 LIF 的 IP 位址與控制台代理程式建立連線並透過 HTTPS 存取 ONTAP System Manager Web 控制台
101 inbound_111_tcp	111 任何協議	任意到任意	NFS 的遠端過程調用
102 inbound_2049_tcp	2049 任何協議	任意到任意	NFS 伺服器守護程式
111 入站_ssh	22 任何協議	任意到任意	透過 SSH 存取叢集管理 LIF 或節點管理 LIF 的 IP 位址

優先權和名稱	連接埠和協定	來源和目的地	描述
121 inbound_53	53 任何協議	任意到任意	DNS 和 CIFS
65000 允許 VnetInBound	任意連接埠任意協定	虛擬網路到虛擬網絡	來自 VNet 內部的入站流量
65001 允許 Azure 負載平衡器入站	任意連接埠任意協定	AzureLoadBalancer 到任意	來自 Azure 標準負載平衡器的資料流量
65500 拒絕所有入站	任意連接埠任意協定	任意到任意	阻止所有其他入站流量

出站規則

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

基本出站規則

Cloud Volumes ONTAP的預設安全群組包括以下出站規則。

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

高級出站規則

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



來源是Cloud Volumes ONTAP系統上的介面（IP 位址）。

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

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

控制台代理的要求

如果您尚未建立控制台代理，您也應該查看控制台代理的網路需求。

- ["查看控制台代理程式的網路要求"](#)
- ["Azure 中的安全性群組規則"](#)

相關主題

- ["驗證 Cloud Volumes ONTAP 的 AutoSupport 設置"](#)
- ["了解 ONTAP 內部端口"](#)。

設定 Cloud Volumes ONTAP 以在 Azure 中使用客戶管理的金鑰

使用具有 Microsoft 管理金鑰的 Azure 儲存服務加密，資料會在 Azure 中的 Cloud Volumes ONTAP 上自動加密。但是您可以按照本頁上的步驟使用您自己的加密金鑰。

資料加密概述

Cloud Volumes ONTAP 資料在 Azure 中自動使用 ["Azure 儲存服務加密"](#)。預設實作使用 Microsoft 管理的金鑰。無需設定。

如果您想將客戶管理的金鑰與Cloud Volumes ONTAP一起使用，則需要完成以下步驟：

1. 從 Azure 建立一個金鑰保管庫，然後在該保管庫中產生一個金鑰。
2. 從NetApp Console，使用 API 建立使用金鑰的Cloud Volumes ONTAP系統。

資料如何加密

控制台使用磁碟加密集，從而可以透過託管磁碟而不是頁面 blob 來管理加密金鑰。任何新的資料磁碟也使用相同的磁碟加密集。較低版本將使用 Microsoft 管理的金鑰，而不是客戶管理的金鑰。

建立配置為使用客戶管理金鑰的Cloud Volumes ONTAP系統後，Cloud Volumes ONTAP資料將如下加密。

Cloud Volumes ONTAP配置	用於密鑰加密的系統磁碟	用於密鑰加密的資料磁碟
單節點	• 引導 • 核 • NVRAM	• 根 • 數據
具有頁面 Blob 的 Azure HA 單可用性區域	• 引導 • 核 • NVRAM	沒有任何
具有共用託管磁碟的 Azure HA 單可用性區域	• 引導 • 核 • NVRAM	• 根 • 數據
具有共用託管磁碟的 Azure HA 多個可用性區域	• 引導 • 核 • NVRAM	• 根 • 數據

Cloud Volumes ONTAP的所有 Azure 儲存帳戶均使用客戶管理的金鑰加密。如果您想在建立儲存帳戶期間對其進行加密，則必須在Cloud Volumes ONTAP建立請求中建立並提供資源的 ID。這適用於所有類型的部署。如果您不提供，儲存帳戶仍將被加密，但控制台首先使用 Microsoft 管理的金鑰加密建立儲存帳戶，然後更新儲存帳戶以使用客戶管理的金鑰。

Cloud Volumes ONTAP中的金鑰輪換

配置加密金鑰時，必須使用 Azure 入口網站來設定並啟用自動金鑰輪替。建立並啟用新版本的加密金鑰可確保Cloud Volumes ONTAP可以自動偵測並使用最新的金鑰版本進行加密，確保您的資料保持安全而無需人工干預。

有關配置金鑰和設定金鑰輪換的信息，請參閱以下 Microsoft Azure 文件主題：

- ["在 Azure Key Vault 中配置加密金鑰自動輪換"](#)
- ["Azure PowerShell - 啟用客戶管理的金鑰"](#)



配置金鑰後，請確保已選擇 **"啟用自動旋轉"**，以便Cloud Volumes ONTAP可以在先前的金鑰過期時使用新的金鑰。如果您未在 Azure 入口網站上啟用此選項，Cloud Volumes ONTAP將無法自動偵測新金鑰，這可能會導致儲存設定問題。

建立使用者分配的託管標識

您可以選擇建立稱為使用者指派的託管識別碼的資源。這樣做可以讓您在建立Cloud Volumes ONTAP系統時加密您的儲存帳戶。我們建議在建立金鑰保管庫和產生金鑰之前建立此資源。

此資源具有以下 ID：userassignedidentity。

步驟

1. 在 Azure 中，前往 Azure 服務並選擇 託管識別。
2. 按一下“建立”。
3. 提供以下詳細資訊：
 - 訂閱：選擇訂閱。我們建議選擇與控制台代理的訂閱相同的訂閱。
 - 資源組：使用現有資源組或建立新的資源組。
 - 區域：可選，選擇與控制台代理相同的區域。
 - 名稱：輸入資源的名稱。
4. （可選）新增標籤。
5. 按一下“建立”。

建立金鑰保管庫並產生金鑰

金鑰保管庫必須位於您計劃建立Cloud Volumes ONTAP系統的相同 Azure 訂閱和區域中。

如果你建立了使用者分配的託管標識，在建立金鑰保管庫時，也應該為金鑰保管庫建立存取策略。

步驟

1. ["在 Azure 訂閱中建立金鑰保管庫"](#)。

請注意密鑰保管庫的以下要求：

- 密鑰保管庫必須與Cloud Volumes ONTAP系統位於同一區域。
- 應啟用以下選項：
 - 軟刪除（此選項預設為啟用，但不能停用）
 - 清除保護
 - **Azure Disk Encryption** 磁碟區加密（適用於單節點系統、多個區域中的 HA 配對以及 HA 單一 AZ 部署）



使用 Azure 客戶管理加密金鑰的前提是為金鑰保管庫啟用 Azure 磁碟加密。

- 如果建立了使用者指派的託管標識，則應啟用下列選項：

- 保險庫存取保單
2. 如果選擇了“保管庫存取原則”，請按一下“建立”為金鑰保管庫建立存取原則。如果沒有，請跳至步驟 3。
 - a. 選擇以下權限：
 - 得到
 - 清單
 - 解密
 - 加密
 - 解開密鑰
 - 包裝鍵
 - 核實
 - 符號
 - b. 選擇使用者指派的託管標識（資源）作為主體。
 - c. 審查並建立存取策略。
 3. ["在金鑰保管庫中產生金鑰"](#)。

請注意密鑰的以下要求：

- 金鑰類型必須是 *RSA*。
- 建議的 RSA 金鑰大小為 **2048**，但也支援其他大小。

建立使用加密金鑰的系統

建立金鑰保管庫並產生加密金鑰後，您可以建立配置為使用該金鑰的新 Cloud Volumes ONTAP 系統。這些步驟透過使用 API 來支援。

所需權限

如果您想要將客戶管理的金鑰與單節點 Cloud Volumes ONTAP 系統一起使用，請確保控制台代理具有下列權限：

```
"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"
```

["查看最新的權限列表"](#)

步驟

1. 使用下列 API 呼叫取得 Azure 訂閱中的金鑰保管庫清單。

對於 HA 對：GET /azure/ha/metadata/vaults

對於單節點：GET /azure/vsa/metadata/vaults

記下*名稱*和*資源組*。您需要在下一個步驟中指定這些值。

["了解有關此 API 呼叫的更多信息"](#)。

2. 使用以下 API 呼叫取得保管庫中的金鑰清單。

對於 HA 對：GET /azure/ha/metadata/keys-vault

對於單節點：GET /azure/vsa/metadata/keys-vault

記下*keyName*。您需要在下一個步驟中指定該值（以及保險庫名稱）。

["了解有關此 API 呼叫的更多信息"](#)。

3. 使用下列 API 呼叫建立 Cloud Volumes ONTAP 系統。

a. 對於 HA 對：

POST /azure/ha/working-environments

請求主體必須包含以下欄位：

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



包括 ``userAssignedIdentity": " userAssignedIdentityId" 如果您建立此資源是為了用於儲存帳戶加密，則欄位。

["了解有關此 API 呼叫的更多信息"](#)。

b. 對於單節點系統：

POST /azure/vsa/working-environments

請求主體必須包含以下欄位：

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



包括 `"userAssignedIdentity": " userAssignedIdentityId"` 如果您建立此資源是為了用於儲存帳戶加密，則欄位。

["了解有關此 API 呼叫的更多信息"](#)。

結果

您有一個新的 Cloud Volumes ONTAP 系統，該系統配置為使用客戶管理的金鑰進行資料加密。

在 Azure 中設定 Cloud Volumes ONTAP 許可

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

免費增值

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

步驟

1. 從 NetApp Console 的左側導覽功能表中，選擇「儲存」>「管理」。
2. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
 - a. 在“詳細資訊和憑證”頁面上，按一下“編輯憑證”>“新增訂閱”，然後依照指示訂閱 Azure 市集中的即用即付產品。

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

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

- a. 返回控制台後，到達收費方式頁面時選擇「免費增值」。

Select Charging Method

☐	Professional	By capacity	▼
☐	Essential	By capacity	▼
☒	Freemium (Up to 500 GiB)	By capacity	▼
☐	Per Node	By node	▼

"[查看在 Azure 中啟動Cloud Volumes ONTAP 的逐步說明](#)"。

基於容量的許可證

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

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

- 從NetApp購買的授權（自帶授權 (BYOL)）
- Azure 市場提供的按小時付費 (PAYGO) 訂閱
- 年度合約

["了解有關基於容量的許可的更多信息"](#)。

以下部分介紹如何開始使用每種消費模型。

BYOL

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



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

步驟

1. ["聯絡NetApp銷售人員以取得許可證"](#)
2. ["將您的NetApp支援網站帳戶新增至控制台"](#)

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

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

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

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

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+

 Add Subscription

Apply

Cancel

- a. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。

Select Charging Method

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

["查看在 Azure 中啟動Cloud Volumes ONTAP 的逐步說明"](#)。

PAYGO 訂閱

透過訂閱雲端供應商市場提供的服務按小時付費。

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

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
 - a. 在“詳細資訊和憑證”頁面上，按一下“編輯憑證”>“新增訂閱”，然後依照指示訂閱 Azure 市集中的即用即付產品。

The screenshot shows a dialog box titled "Edit Credentials & Add Subscription". It has a section "Associate Subscription to Credentials" with an information icon. Below this are two dropdown menus: "Credentials" with "Managed Service Identity" selected, and "Azure Subscription" with "OCCM Dev (Default)" selected. A message box states: "Marketplace Subscription: A marketplace subscription isn't associated with the selected Azure subscription." Below the message is a "+ Add Subscription" link. At the bottom are "Apply" and "Cancel" buttons.

- b. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。

The screenshot shows a dialog box titled "Select Charging Method". It lists four options with radio buttons: "Professional" (selected), "Essential", "Freemium (Up to 500 GiB)", and "Per Node". To the right of each option is a button labeled "By capacity" (for the first three) or "By node" (for the last one), followed by a dropdown arrow.

["查看在 Azure 中啟動Cloud Volumes ONTAP 的逐步說明"](#)。



您可以從「設定」>「憑證」頁面管理與您的 Azure 帳戶相關聯的 Azure 市集訂閱。"[了解如何管理 Azure 帳戶和訂閱](#)"

年度合約

透過購買年度合約每年支付Cloud Volumes ONTAP 的費用。

步驟

1. 聯絡您的NetApp銷售代表購買年度合約。

該合約在 Azure 市場中以私人優惠的形式提供。

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

2. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
 - a. 在「詳細資料和憑證」頁面上，按一下「編輯憑證」>「新增訂閱」>「繼續」。
 - b. 在 Azure 入口網站中，選擇與您的 Azure 帳戶共用的年度計劃，然後按一下「訂閱」。
 - c. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。

Select Charging Method

☒ Professional	By capacity	▼
☐ Essential	By capacity	▼
☐ Freemium (Up to 500 GiB)	By capacity	▼
☐ Per Node	By node	▼

"[查看在 Azure 中啟動Cloud Volumes ONTAP 的逐步說明](#)"。

Keystone訂閱

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

步驟

1. 如果您尚未訂閱，"[聯絡NetApp](#)"
2. [聯絡NetApp](#) 以在控制台中授權您的使用者帳戶擁有一個或多個Keystone訂閱。
3. NetApp授權您的帳戶後，"[連結您的訂閱以用於Cloud Volumes ONTAP](#)"。
4. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。

- a. 當提示選擇充電方式時，選擇Keystone Subscription 充電方式。

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

["查看在 Azure 中啟動Cloud Volumes ONTAP 的逐步說明"](#)。

基於節點的許可證

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

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

在 Azure 中為Cloud Volumes ONTAP啟用高可用性模式

應啟用 Microsoft Azure 的高可用性 (HA) 模式，以減少非計畫性故障轉移時間並為Cloud Volumes ONTAP啟用 NFSv4 支援。在此模式下，您的Cloud Volumes ONTAP HA 節點可以在 CIFS 和 NFSv4 用戶端上的計劃外故障轉移期間實現較低（60 秒）的復原時間目標 (RTO)。

從Cloud Volumes ONTAP 9.10.1 開始，我們減少了在 Microsoft Azure 中執行的Cloud Volumes ONTAP HA 對的非計畫性故障轉移時間，並增加了對 NFSv4 的支援。若要讓這些增強功能可用於Cloud Volumes ONTAP，您

需要在 Azure 訂閱上啟用高可用性功能。

當需要在 Azure 訂閱上啟用功能時，NetApp Console 會提示您提供這些詳細資訊。

請注意以下事項：

- 您的 Cloud Volumes ONTAP HA 對的高可用性沒有問題。此 Azure 功能與 ONTAP 協同工作，以減少用戶端觀察到的因計劃外故障轉移事件而導致的 NFS 協定應用程式中斷時間。
- 啟用此功能不會對 Cloud Volumes ONTAP HA 造成破壞。
- 在您的 Azure 訂閱上啟用此功能不會為其他虛擬機器帶來問題。
- Cloud Volumes ONTAP 在 CIFS 和 NFS 用戶端上的叢集和 SVM 管理 LIF 故障轉移期間使用內部 Azure 負載平衡器。
- 啟用 HA 模式後，控制台每 12 小時掃描一次系統以更新內部 Azure 負載平衡器規則。

具有「擁有者」權限的 Azure 使用者可以從 Azure CLI 啟用該功能。

步驟

1. "從 [Azure 入口網站](#) 存取 [Azure Cloud Shell](#)"
2. 註冊高可用性模式功能：

```
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) 驗證該功能現在是否已註冊：

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

Azure CLI 應傳回類似以下內容的結果：

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

在 Azure 中為 Cloud Volumes ONTAP 啟用 VMOrchestratorZonalMultiFD

若要在本機冗餘儲存 (LRS) 單一可用區 (AZ) 中部署 VM 實例，您應該啟動 Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD` 您的訂閱功能。在高可用性 (HA) 模式下，此功能有助於在相同可用區域內的不同故障域中部署節點。

除非您啟動此功能，否則不會發生區域部署，且先前的 LRS 非區域部署將生效。

有關在單一可用區域中部署虛擬機器的信息，請參閱["Azure 中的高可用性對"](#)。

以具有「所有者」權限的使用者身分執行下列步驟：

步驟

1. 從 Azure 入口網站存取 Azure Cloud Shell。欲了解更多信息，請參閱 ["Microsoft Azure 文件：Azure Cloud Shell 入門"](#)。
2. 註冊 `Microsoft.Compute/VMOrchestratorZonalMultiFD` 透過執行以下命令來啟用此功能：

```
az 帳號設定 -s <Azure_subscription_name_or_ID> az 功能註冊 --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
```

3. 驗證註冊狀態及輸出範例：

```
az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute { "id" : "/subscriptions/<ID>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiFD", "Compname" : " " "state" : "Registered" } , "type" : "Microsoft.Features/providers/features" }
```

在 Azure 中啟動 Cloud Volumes ONTAP

您可以透過在 NetApp Console 中建立 Cloud Volumes ONTAP 系統，在 Azure 中啟動單節點系統或 HA 配對。

開始之前

開始之前您需要以下內容。

- 已啟動並正在執行的控制台代理程式。
 - 你應該有一個 ["與您的系統關聯的控制台代理"](#)。
 - ["您應該準備好讓控制台代理程式始終處於運行狀態"](#)。
- 了解您想要使用的配置。

您應該有一個配置計劃，並且從管理員那裡獲得必要的 Azure 網路詳細資訊。有關詳細信息，請參閱["規劃您的 Cloud Volumes ONTAP 配置"](#)。

- 了解設定Cloud Volumes ONTAP許可所需的條件。

["了解如何設定許可"](#)。

關於此任務

當控制台在 Azure 中建立Cloud Volumes ONTAP系統時，它會建立多個 Azure 對象，例如資源群組、網路介面和儲存帳戶。您可以在精靈結束時查看資源摘要。



資料遺失的可能性

最佳做法是為每個Cloud Volumes ONTAP系統使用新的專用資源群組。

由於資料遺失的風險，不建議在現有的共用資源組中部署Cloud Volumes ONTAP。雖然控制台可以在部署失敗或刪除的情況下從共用資源群組中刪除Cloud Volumes ONTAP資源，但 Azure 使用者可能會意外從共用資源群組中刪除Cloud Volumes ONTAP資源。

在 Azure 中啟動單節點Cloud Volumes ONTAP系統

如果要在 Azure 中啟動單節點 Cloud Volumes ONTAP 系統，則需要在 Console 中建立單節點系統。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，點擊*新增系統*並依照指示操作。
3. 選擇位置：選擇*Microsoft Azure*和* Cloud Volumes ONTAP單一節點*。
4. 如果出現提示，["建立控制台代理"](#)。
5. 詳細資料和憑證：可選擇變更 Azure 憑證和訂閱，指定群集名稱，根據需要新增標籤，然後指定憑證。

下表描述了您可能需要指導的欄位：

場地	描述
系統名稱	控制台使用系統名稱來命名Cloud Volumes ONTAP系統和 Azure 虛擬機器。如果您選擇該選項，它也會使用該名稱作為預先定義安全性群組的前綴。
資源組標籤	標籤是 Azure 資源的元資料。當您在此欄位中輸入標籤時，控制台會將它們新增至與Cloud Volumes ONTAP系統關聯的資源群組。建立系統時，您可以從使用者介面新增多達四個標籤，然後可以在建立系統後新增更多標籤。請注意，在建立系統時，API 不會將您限制為四個標籤。有關標籤的信息，請參閱 "Microsoft Azure 文件：使用標籤來組織您的 Azure 資源" 。
使用者名稱和密碼	這些是Cloud Volumes ONTAP叢集管理員帳戶的憑證。您可以使用這些憑證透過ONTAP System Manager 或ONTAP CLI 連線到Cloud Volumes ONTAP。保留預設的_admin_使用者名稱或將其變更為自訂使用者名稱。
編輯憑證	您可以選擇不同的 Azure 憑證和不同的 Azure 訂閱來與此Cloud Volumes ONTAP系統一起使用。您需要將 Azure 市場訂閱與選定的 Azure 訂閱關聯，以便部署即用即付的Cloud Volumes ONTAP系統。 "了解如何新增憑證" 。

6. 服務：啟用或停用您想要或不想與Cloud Volumes ONTAP一起使用的單一服務。
 - ["了解有關NetApp Data Classification的更多信息"](#)

- ["了解有關NetApp Backup and Recovery的更多信息"](#)



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

7. 位置：選擇區域、可用區域、VNet 和子網，然後選取核取方塊以確認控制台代理程式和目標位置之間的網路連線。



對於中國區域，僅Cloud Volumes ONTAP 9.12.1 GA 和 9.13.0 GA 支援單節點部署。您可以將這些版本升級到Cloud Volumes ONTAP的更高補丁和版本，如下所示["Azure 中支援"](#)。如果您想在中國地區部署更高版本的Cloud Volumes ONTAP，請聯絡NetApp支援。中國地區僅支援直接從NetApp購買的許可證，不提供市場訂閱。

8. 連線：選擇新的或現有的資源群組，然後選擇是否使用預先定義的安全群組或使用您自己的安全群組。

下表描述了您可能需要指導的欄位：

場地	描述
資源組	為Cloud Volumes ONTAP建立新的資源組或使用現有的資源組。最佳做法是為Cloud Volumes ONTAP使用新的專用資源群組。雖然可以在現有的共享資源組中部署Cloud Volumes ONTAP，但由於資料遺失的風險，因此不建議這樣做。請參閱上面的警告以了解更多詳細資訊。  如果您使用的 Azure 帳戶具有 "所需權限"，如果部署失敗或刪除，控制台會從資源群組中刪除Cloud Volumes ONTAP資源。
產生的安全群組	如果您讓控制台為您產生安全性群組，則需要選擇如何允許流量： • 如果選擇*僅限選取的 VNet*，則入站流量的來源為選取 VNet 的子網路範圍和控制台代理程式所在的 VNet 的子網路範圍。這是推薦的選項。 • 如果選擇“所有 VNet”，則入站流量的來源為 0.0.0.0/0 IP 範圍。
使用現有的	如果您選擇現有的安全性群組，則它必須符合Cloud Volumes ONTAP要求。"查看預設安全群組"。

9. 收費方式和 **NSS** 帳戶：指定您想要在此系統中使用的收費選項，然後指定NetApp支援網站帳戶。

- ["了解Cloud Volumes ONTAP的授權選項"](#)。
- ["了解如何設定許可"](#)。

10. 預先配置套件：選擇其中一個套件來快速部署Cloud Volumes ONTAP系統，或點擊*建立我自己的設定*。

如果您選擇其中一個套餐，您只需指定一個卷，然後審核並批准配置。

11. 許可：如果需要，請變更Cloud Volumes ONTAP版本，並選擇虛擬機器類型。



如果所選版本有較新的候選版本、通用版本或修補程式版本，則BlueXP會在建立工作環境時將系統更新至該版本。例如，如果您選擇Cloud Volumes ONTAP 9.16.1 P3 並且 9.16.1 P4 可用，則會發生更新。更新不會從一個版本發生到另一個版本 - 例如，從 9.15 到 9.16。

12. 從 **Azure** 市集訂閱：如果控制台無法啟用Cloud Volumes ONTAP的程式部署，您將看到此頁面。請依照螢幕上所列的步驟操作。請參閱 ["以程式設計方式部署 Marketplace 產品"](#) 了解更多。
13. 底層儲存資源：選擇初始聚合的設定：磁碟類型、每個磁碟的大小以及是否應啟用資料分層到 Blob 儲存。

請注意以下事項：

- 如果在 VNet 中停用了對您的儲存帳戶的公共訪問，則您無法在Cloud Volumes ONTAP系統中啟用資料分層。有關信息，請參閱["安全群組規則"](#)。
- 磁碟類型適用於初始磁碟區。您可以為後續磁碟區選擇不同的磁碟類型。
- 磁碟大小適用於初始聚合中的所有磁碟以及使用簡單配置選項時控制台建立的任何其他聚合。您可以使用進階分配選項建立使用不同磁碟大小的聚合。

有關選擇磁碟類型和大小的協助，請參閱["在 Azure 中調整系統大小"](#)。

- 您可以在建立或編輯磁碟區時選擇特定的磁碟區分層策略。
- 如果您停用資料分層，則可以在後續聚合上啟用它。

["了解有關數據分層的更多信息"](#)。

14. 寫入速度與 **WORM**：

- a. 如有需要，請選擇*正常*或*高*寫入速度。

["了解有關寫入速度的更多信息"](#)。

- b. 如果需要，請啟動一次寫入、多次讀取 (WORM) 儲存。

此選項僅適用於某些 VM 類型。若要了解支援的 VM 類型，請參閱["HA 對許可證支援的配置"](#)。

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

["了解有關 WORM 存儲的更多信息"](#)。

- a. 如果您啟動 WORM 存儲，請選擇保留期限。

15. 建立磁碟區：輸入新磁碟區的詳細資料或點選*跳過*。

["了解支援的客戶端協定和版本"](#)。

此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

場地	描述
尺寸	您可以輸入的最大大小很大程度上取決於您是否啟用精簡配置，這使您能夠建立比目前可用的實體儲存更大的磁碟區。
存取控制（僅適用於 NFS）	導出策略定義了子網路中可以存取磁碟區的用戶端。預設情況下，控制台輸入一個提供對子網路中所有實例的存取權限的值。

場地	描述
權限和使用者/群組（僅適用於 CIFS）	這些欄位可讓您控制使用者和群組對共用的存取等級（也稱為存取控制清單或 ACL）。您可以指定本機或網域 Windows 使用者或群組，或 UNIX 使用者或群組。如果指定網域 Windows 使用者名，則必須使用網域\使用者名稱格式包含使用者的網域。
快照策略	Snapshot 副本策略指定自動建立的 NetApp Snapshot 副本的頻率和數量。NetApp Snapshot 副本是時間點檔案系統映像，它不會影響效能並且只需要最少的儲存空間。您可以選擇預設策略或無策略。對於瞬態數據，您可能會選擇無：例如，對於 Microsoft SQL Server，請選擇 tempdb。
進階選項（僅適用於 NFS）	為磁碟區選擇一個 NFS 版本：NFSv3 或 NFSv4。
啟動器群組和 IQN（僅適用於 iSCSI）	iSCSI 儲存目標稱為 LUN（邏輯單元），並以標準區塊裝置呈現給主機。啟動器群組是 iSCSI 主機節點名稱表，用於控制哪些啟動器可以存取哪些 LUN。iSCSI 目標透過標準乙太網路網路適配器 (NIC)、具有軟體啟動器的 TCP 卸載引擎 (TOE) 卡、融合網路適配器 (CNA) 或專用主機匯流排適配器 (HBA) 連接到網絡，並透過 iSCSI 限定名稱 (IQN) 進行識別。當您建立 iSCSI 磁碟區時，控制台會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，"使用 IQN 從主機連線到 LUN"。

下圖顯示了磁碟區建立精靈的第一頁：

Volume Details & Protection

Volume Name ?

ABDcv5689

Storage VM (SVM)

svm_...CVO1

Volume Size ? Unit

100

GiB

Snapshot Policy

default

default policy ?

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

場地	描述
DNS 主 IP 位址和輔助 IP 位址	為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 CIFS 伺服器將加入的網域的 Active Directory LDAP 伺服器和網域控制站所需的服務位置記錄 (SRV)。
要加入的 Active Directory 網域	您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。
授權加入網域的憑證	具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。
CIFS 伺服器 NetBIOS 名稱	AD 網域中唯一的 CIFS 伺服器名稱。

場地	描述
組織單位	AD 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。若要將 Azure AD 網域服務設定為 Cloud Volumes ONTAP 的 AD 伺服器，您應該在此欄位中輸入 OU=AADDC Computers 或 OU=AADDC Users https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou ["Azure 文件：在 Azure AD 網域服務託管網域中建立組織單位 (OU)"]
DNS 網域	Cloud Volumes ONTAP 儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。
NTP 伺服器	選擇「使用 Active Directory 網域」以使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器，那麼您應該使用 API。請參閱 "NetApp Console 自動化文檔" 了解詳情。請注意，只有在建立 CIFS 伺服器時才能設定 NTP 伺服器。建立 CIFS 伺服器後，它不可配置。

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

更多信息，請參閱["了解卷使用情況"](#)和["資料分層概述"](#)。

18. 審核並批准：審核並確認您的選擇。
- 查看有關配置的詳細資訊。
 - 按一下「更多資訊」以查看有關支援和控制台將購買的 Azure 資源的詳細資訊。
 - 選取*我明白...*複選框。
 - 按一下「開始」。

結果

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

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

如需更多協助，請訪問 ["NetApp Cloud Volumes ONTAP 支持"](#)。



部署程序完成後，請勿修改 Azure 入口網站中系統產生的 Cloud Volumes ONTAP 配置，尤其是系統標籤。對這些配置所做的任何變更都可能導致意外行為或資料遺失。

完成後

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

配額可讓您限制或追蹤使用者、群組或 qtree 使用的磁碟空間和檔案數量。

在 Azure 中啟動 Cloud Volumes ONTAP HA 對

如果您想在 Azure 中啟動 Cloud Volumes ONTAP HA 對，則需要在控制台中建立 HA 系統。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，點擊*新增系統*並依照指示操作。
3. 如果出現提示，["建立控制台代理"](#)。
4. 詳細資料和憑證：可選擇變更 Azure 憑證和訂閱，指定群集名稱，根據需要新增標籤，然後指定憑證。

下表描述了您可能需要指導的欄位：

場地	描述
系統名稱	控制台使用系統名稱來命名Cloud Volumes ONTAP系統和 Azure 虛擬機器。如果您選擇該選項，它也會使用該名稱作為預先定義安全性群組的前綴。
資源組標籤	標籤是 Azure 資源的元資料。當您在此欄位中輸入標籤時，控制台會將它們新增至與Cloud Volumes ONTAP系統關聯的資源群組。建立系統時，您可以從使用者介面新增多達四個標籤，然後可以在建立系統後新增更多標籤。請注意，在建立系統時，API 不會將您限制為四個標籤。有關標籤的信息，請參閱 "Microsoft Azure 文件：使用標籤來組織您的 Azure 資源" 。
使用者名稱和密碼	這些是Cloud Volumes ONTAP叢集管理員帳戶的憑證。您可以使用這些憑證透過ONTAP System Manager 或ONTAP CLI 連線到Cloud Volumes ONTAP。保留預設的_admin_使用者名稱或將其變更為自訂使用者名稱。
編輯憑證	您可以選擇不同的 Azure 憑證和不同的 Azure 訂閱來與此Cloud Volumes ONTAP系統一起使用。您需要將 Azure 市場訂閱與選定的 Azure 訂閱關聯，以便部署即用即付的Cloud Volumes ONTAP系統。 "了解如何新增憑證" 。

5. 服務：根據您是否要將各個服務與Cloud Volumes ONTAP一起使用來啟用或停用它們。
 - ["了解有關NetApp Data Classification的更多信息"](#)
 - ["了解有關NetApp Backup and Recovery的更多信息"](#)



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

6. HA部署模型：

- a. 選擇*單一可用區*或*多個可用區*。
 - 對於單一可用區域，請選擇 Azure 區域、可用區域、VNet 和子網路。

從Cloud Volumes ONTAP 9.15.1 開始，您可以在 Azure 中的單一可用區域 (AZ) 中以 HA 模式部署虛擬機器 (VM) 執行個體。您需要選擇支援此部署的區域和地理。如果區域或地理不支援區域部署，則遵循先前LRS的非區域部署模式。若要了解共享託管磁碟支援的配置，請參閱["具有共享託管磁碟的 HA 單可用區域配置"](#)。

- 對於多個可用區域，請選擇區域、VNet、子網路、節點 1 的區域以及節點 2 的區域。

- b. 選取*我已驗證網路連線...*複選框。

7. 連線：選擇新的或現有的資源群組，然後選擇是否使用預先定義的安全群組或使用您自己的安全群組。

下表描述了您可能需要指導的欄位：

場地	描述
資源組	為Cloud Volumes ONTAP建立新的資源組或使用現有的資源組。最佳做法是為Cloud Volumes ONTAP使用新的專用資源群組。雖然可以在現有的共享資源組中部署Cloud Volumes ONTAP，但由於資料遺失的風險，因此不建議這樣做。請參閱上面的警告以了解更多詳細資訊。 您必須為在 Azure 中部署的每個Cloud Volumes ONTAP HA 對使用專用資源群組。一個資源組中僅支援一個 HA 對。如果您嘗試在 Azure 資源組中部署第二個Cloud Volumes ONTAP HA 對，控制台會遇到連線問題。  如果您使用的 Azure 帳戶具有 "所需權限"，如果部署失敗或刪除，控制台會從資源群組中刪除Cloud Volumes ONTAP資源。
產生的安全群組	如果您讓控制台為您產生安全性群組，則需要選擇如何允許流量： • 如果選擇*僅限選取的 VNet*，則入站流量的來源為選取 VNet 的子網路範圍和控制台代理程式所在的 VNet 的子網路範圍。這是推薦的選項。 • 如果選擇“所有 VNets”，則入站流量的來源為 0.0.0.0/0 IP 範圍。
使用現有的	如果您選擇現有的安全性群組，則它必須符合Cloud Volumes ONTAP要求。查看預設安全群組。

8. 收費方式和 **NSS** 帳戶：指定您想要在此系統中使用的收費選項，然後指定NetApp支援網站帳戶。

- ["了解Cloud Volumes ONTAP的授權選項"](#)。
- ["了解如何設定許可"](#)。

9. 預先配置套件：選擇其中一個套件來快速部署Cloud Volumes ONTAP系統，或點擊*變更配置*。

如果您選擇其中一個套餐，您只需指定一個卷，然後審核並批准配置。

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



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

11. 從 **Azure** 市集訂閱：如果控制台無法啟用Cloud Volumes ONTAP的程式部署，請依照下列步驟操作。

12. 底層儲存資源：選擇初始聚合的設定：磁碟類型、每個磁碟的大小以及是否應啟用資料分層到 Blob 儲存。

請注意以下事項：

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

有關選擇磁碟大小的協助，請參閱["在 Azure 中調整系統大小"](#)。

- 如果在 VNet 中停用了對您的儲存帳戶的公共訪問，則您無法在Cloud Volumes ONTAP系統中啟用資料分層。有關信息，請參閱["安全群組規則"](#)。

- 您可以在建立或編輯磁碟區時選擇特定的磁碟區分層策略。
- 如果您停用資料分層，則可以在後續聚合上啟用它。

["了解有關數據分層的更多信息"](#)。

- 從Cloud Volumes ONTAP 9.15.0P1 開始，Azure 頁面 blob 不再支援新的高可用性對部署。如果您目前在現有的高可用性對部署中使用 Azure 頁 Blob，則可以移轉到 Edsv4 系列 VM 和 Edsv5 系列 VM 中較新的 VM 執行個體類型。

["詳細了解 Azure 中支援的配置"](#)。

13. 寫入速度與 **WORM**：

- 如有需要，請選擇*正常*或*高*寫入速度。

["了解有關寫入速度的更多信息"](#)。

- 如果需要，請啟動一次寫入、多次讀取 (WORM) 儲存。

此選項僅適用於某些 VM 類型。若要了解支援的 VM 類型，請參閱["HA 對許可證支援的配置"](#)。

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

["了解有關 WORM 存儲的更多信息"](#)。

- 如果您啟動 WORM 存儲，請選擇保留期限。

14. 與儲存和 **WORM** 的安全通訊：選擇是否啟用與 Azure 儲存帳戶的 HTTPS 連接，並啟動一次寫入、多次讀取 (WORM) 儲存（如果需要）。

HTTPS 連線從Cloud Volumes ONTAP 9.7 HA 對到 Azure 頁面 blob 儲存帳戶。請注意，啟用此選項可能會影響寫入效能。建立系統後，您無法變更設定。

["了解有關 WORM 存儲的更多信息"](#)。

如果啟用了資料分層，則無法啟用 WORM。

["了解有關 WORM 存儲的更多信息"](#)。

15. 建立磁碟區：輸入新磁碟區的詳細資料或點選*跳過*。

["了解支援的客戶端協定和版本"](#)。

此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

場地	描述
尺寸	您可以輸入的最大大小很大程度上取決於您是否啟用精簡配置，這使您能夠建立比目前可用的實體儲存更大的磁碟區。
存取控制（僅適用於 NFS）	導出策略定義了子網路中可以存取磁碟區的用戶端。預設情況下，控制台輸入一個提供對子網路中所有實例的存取權限的值。

場地	描述
權限和使用者/群組（僅適用於 CIFS）	這些欄位可讓您控制使用者和群組對共用的存取等級（也稱為存取控制清單或 ACL）。您可以指定本機或網域 Windows 使用者或群組，或 UNIX 使用者或群組。如果指定網域 Windows 使用者名，則必須使用網域\使用者名稱格式包含使用者的網域。
快照策略	Snapshot 副本策略指定自動建立的 NetApp Snapshot 副本的頻率和數量。NetApp Snapshot 副本是時間點檔案系統映像，它不會影響效能並且只需要最少的儲存空間。您可以選擇預設策略或無策略。對於瞬態數據，您可能會選擇無：例如，對於 Microsoft SQL Server，請選擇 tempdb。
進階選項（僅適用於 NFS）	為磁碟區選擇一個 NFS 版本：NFSv3 或 NFSv4。
啟動器群組和 IQN（僅適用於 iSCSI）	iSCSI 儲存目標稱為 LUN（邏輯單元），並以標準區塊裝置呈現給主機。啟動器群組是 iSCSI 主機節點名稱表，用於控制哪些啟動器可以存取哪些 LUN。iSCSI 目標透過標準乙太網路網路適配器 (NIC)、具有軟體啟動器的 TCP 卸載引擎 (TOE) 卡、融合網路適配器 (CNA) 或專用主機匯流排適配器 (HBA) 連接到網絡，並透過 iSCSI 限定名稱 (IQN) 進行識別。當您建立 iSCSI 磁碟區時，控制台會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，"使用 IQN 從主機連線到 LUN"。

下圖顯示了磁碟區建立精靈的第一頁：

Volume Details & Protection

Volume Name i

ABDcv5689

Storage VM (SVM)

svm_c...CVO1

Volume Size i

100

Unit

GiB

Snapshot Policy

default

default policy i

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

場地	描述
DNS 主 IP 位址和輔助 IP 位址	為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 CIFS 伺服器將加入的網域的 Active Directory LDAP 伺服器和網域控制站所需的服務位置記錄 (SRV)。
要加入的 Active Directory 網域	您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。
授權加入網域的憑證	具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。
CIFS 伺服器 NetBIOS 名稱	AD 網域中唯一的 CIFS 伺服器名稱。

場地	描述
組織單位	AD 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。若要將 Azure AD 網域服務設定為 Cloud Volumes ONTAP 的 AD 伺服器，您應該在此欄位中輸入 OU=AADD C Computers 或 OU=AADD C Users https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou ["Azure 文件：在 Azure AD 網域服務託管網域中建立組織單位 (OU)"]
DNS 網域	Cloud Volumes ONTAP 儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。
NTP 伺服器	選擇「使用 Active Directory 網域」以使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器，那麼您應該使用 API。請參閱 "NetApp Console 自動化文檔" 了解詳情。請注意，只有在建立 CIFS 伺服器時才能設定 NTP 伺服器。建立 CIFS 伺服器後，它不可配置。

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

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

18. 審核並批准：審核並確認您的選擇。

- 查看有關配置的詳細資訊。
- 按一下「更多資訊」以查看有關支援和控制台將購買的 Azure 資源的詳細資訊。
- 選取*我明白...*複選框。
- 按一下「開始」。

結果

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

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

如需更多協助，請訪問 ["NetApp Cloud Volumes ONTAP 支持"](#)。

完成後

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

配額可讓您限制或追蹤使用者、群組或 qtree 使用的磁碟空間和檔案數量。



部署程序完成後，請勿修改 Azure 入口網站中系統產生的 Cloud Volumes ONTAP 配置，尤其是系統標籤。對這些配置所做的任何變更都可能導致意外行為或資料遺失。

相關連結

[*在 Azure 中規劃 Cloud Volumes ONTAP 配置*](#) [*從 Azure 市場在 Azure 中部署 Cloud Volumes ONTAP*](#)

驗證 Azure 平台映像

針對Cloud Volumes ONTAP 的Azure 市場映像驗證

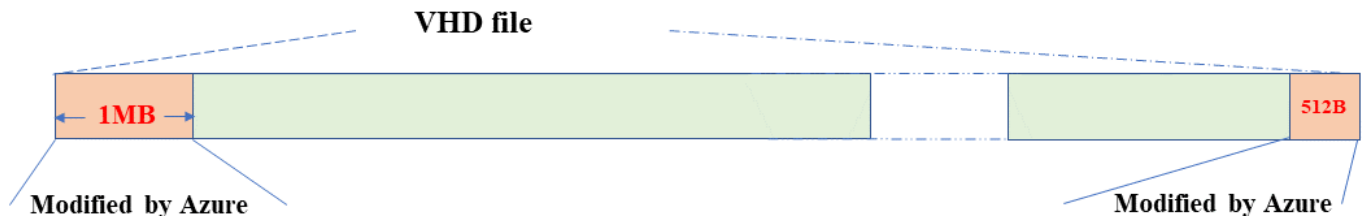
Azure 映像驗證符合增強的NetApp安全要求。驗證圖像檔案是一個簡單的過程。但是，Azure 映像簽署驗證需要特別注意 Azure VHD 映像文件，因為它在 Azure 市場中已更改。



Cloud Volumes ONTAP 9.15.0 及更高版本支援 Azure 映像驗證。

Azure 對已發布 VHD 檔案的更改

VHD 檔案開頭的 1 MB（1048576 位元組）和結尾的 512 位元組已被 Azure 修改。NetApp對剩餘的 VHD 檔案進行簽署。



在範例中，VHD 檔案為 10GB。NetApp簽署的部分標示為綠色（10 GB - 1 MB - 512 位元組）。

相關連結

- ["頁面錯誤部落格：如何使用 OpenSSL 進行簽署和驗證"](#)
- ["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 快速入門 - Bash | Microsoft Learn"](#)
- ["如何安裝 Azure CLI | Microsoft Learn"](#)
- ["az 儲存 blob 副本 | Microsoft Learn"](#)
- ["使用 Azure CLISign in— 登入與驗證 | Microsoft Learn"](#)

下載適用於Cloud Volumes ONTAP 的Azure 映像文件

您可以從 ["NetApp支援站點"](#)。

tar.gz 檔案包含圖像簽名驗證所需的檔案。除了 *tar.gz* 檔案之外，您還應該下載圖像的 *checksum* 檔案。校驗和檔案包含 `md5` 和 `sha256` *tar.gz* 檔案的校驗和。

步驟

1. 前往 ["NetApp支援網站上的Cloud Volumes ONTAP產品頁面"](#)並從*下載*部分下載所需的軟體版本。
2. 在Cloud Volumes ONTAP下載頁面上，按一下 Azure 映像檔的下載檔案並下載 *tar.gz* 檔案。

Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

Cloud Volumes ONTAP

Non-Restricted Countries

If you are upgrading to ONTAP 9.15.0P1, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

DOWNLOAD 9150P1_V_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

Restricted Countries

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

DOWNLOAD GCP-9-15-0P1_PKG.TAR.GZ [7.49 KB]

[View and download checksums](#)

DOWNLOAD AZURE-9-15-0P1_PKG.TAR.GZ [7.64 KB]

[View and download checksums](#)

3. 在 Linux 上，運行 `md5sum AZURE-<version>_PKG.TAR.GZ`。

在 macOS 上，運行 `sha256sum AZURE-<version>_PKG.TAR.GZ`。

4. 驗證 `md5sum` 和 `sha256sum` 值與下載的 Azure 映像中的值相符。

5. 在 Linux 和 macOS 上，使用以下命令提取 `tar.gz` 文件 ``tar -xzf`` 命令。

解壓縮後的 `tar.gz` 檔案包含摘要（.sig）檔案、公鑰憑證（.pem）檔案和鏈憑證（.pem）檔案。

提取 `tar.gz` 檔案後的範例輸出：

```
$ 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
```

從 Azure 市場匯出 Cloud Volumes ONTAP 的 VHD 映像

一旦 VHD 映像發佈到 Azure 雲端，它就不再由 NetApp 管理。相反，已發布的圖像被放置在 Azure 市場上。當映像 Azure 市場上暫存和發佈時，Azure 會修改 VHD 開頭的 1 MB 和結尾的 512 位元組。要驗證 VHD 檔案的簽名，需要從 Azure 市場匯出 Azure 修改後的 VHD 鏡像。

開始之前

確保您的系統上安裝了 Azure CLI，或可以透過 Azure 入口網站使用 Azure Cloud Shell。有關如何安裝 Azure CLI 的詳細信息，請參閱 "[Microsoft 文件：如何安裝 Azure CLI](#)"。

步驟

1. 使用 `version_readme` 檔案的內容將系統上的 Cloud Volumes ONTAP 版本對應到 Azure 市場映像版本。Cloud Volumes ONTAP 版本由 ``buildname`` Azure 市場鏡像版本表示為 ``version`` 在版本映射中。

在下列範例中，Cloud Volumes ONTAP 版本 9.15.0P1 對應到 Azure 市場映像版本 9150.01000024.05090105。此 Azure 市場鏡像版本稍後用於設定鏡像 URN。

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

2. 確定要建立虛擬機器的區域。區域名稱用作 ``locName`` 設定市場影像的 URN 時的變數。若要列出可用區域，請執行以下命令：

```
az account list-locations -o table
```

在此表中，區域名稱出現在 ``Name`` 場地。

```
$ 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. 查看下表中對應 Cloud Volumes ONTAP 版本和 VM 部署類型的 SKU 名稱。SKU 名稱用作 ``skuName`` 設定市場影像的 URN 時的變數。

例如，所有採用 Cloud Volumes ONTAP 9.15.0 的單節點部署都應使用 ``ontap_cloud_byol`` 作為 SKU 名稱。

* Cloud Volumes ONTAP 版本*	透過虛擬機器部署	SKU 名稱
9.17.1 及更高版本	Azure 市場	ontap_cloud_direct_gen2
9.17.1 及更高版本	NetApp Console	ontap_cloud_gen2
9.16.1	Azure 市場	ontap_cloud_direct
9.16.1	主機	ontap_cloud

9.15.1	主機	ontap_cloud
9.15.0	控制台，單節點部署	ontap_cloud_byol
9.15.0	控制台、高可用性 (HA) 部署	ontap_cloud_byol_ha

4. 對應ONTAP版本和 Azure 市場映像後，使用 Azure Cloud Shell 或 Azure CLI 從 Azure 市場匯出 VHD 檔案。

使用 Linux 上的 Azure Cloud Shell 匯出 VHD 文件

從 Azure Cloud Shell，將市場映像匯出至 VHD 檔案（例如，`9150.01000024.05090105.vhd`），然後下載到本機 Linux 系統。執行下列步驟從 Azure 市場取得 VHD 映像。

步驟

1. 設定市場圖像的 URN 和其他參數。URN 格式為 `<publisher>:<offer>:<sku>:<version>`。或者，您可以列出 NetApp 市場圖像來確認正確的圖像版本。

```
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
...
```

2. 從市場映像建立一個具有匹配映像版本的新託管磁碟：

```
PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnfl"
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
```

3. 將 VHD 檔案從託管磁碟匯出到 Azure 儲存體。建立具有適當存取等級的容器。在這個例子中，我們使用了一個名為 `vm-images` 和 `Container` 訪問級別。從 Azure 入口網站取得儲存帳戶存取金鑰：儲存帳戶 > **examplesaname** > 存取金鑰 > **key1** > **key** > 顯示 > **<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

```

4. 將產生的映像下載到您的 Linux 系統。使用 `wget` 下載 VHD 檔案的指令：

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

URL 遵循標準格式。為了實現自動化，您可以獲得如下所示的 URL 字串。或者，您可以使用 Azure CLI `az` 命令來取得 URL。範例 URL：<https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd>]

5. 清理託管磁碟

```

PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName

```

使用 Linux 上的 Azure CLI 匯出 VHD 文件

使用本機 Linux 系統的 Azure CLI 將市場映像匯出到 VHD 檔案。

步驟

1. 登入 Azure CLI 並列出市場圖像：

```
% az login --use-device-code
```

2. 要登錄，請使用網頁瀏覽器開啟頁面 <https://microsoft.com/devicelogin> 並輸入驗證碼。

```
% 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"
},
...
```

3. 從具有匹配映像版本的市場映像建立新的託管磁碟。

```
% 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.bluepinfraprod.eastus2.data.azurecr.io/xxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluepinfraprod.eastus2.data.azurecr.io/xxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
```

為了使流程自動化，需要從標準輸出中提取 SAS。請參閱相應文件以獲取指導。

4. 從託管磁碟匯出 VHD 檔案。

- a. 建立具有適當存取等級的容器。在此範例中，名為 `vm-images` 和 `Container` 使用訪問級別。
- b. 從 Azure 入口網站取得儲存帳戶存取金鑰：儲存帳戶 > **examplesaname** > 存取金鑰 > **key1** > **key** > 顯示 > **<copy>**

您也可以使用 `az` 此步驟的命令。

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxxx"
% 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": "\"0xxxxxxxxxxxxxxxxxxxx\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. 檢查 blob 副本的狀態。

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
  "copy": {
    "completionTime": null,
    "destinationSnapshot": null,
    "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx",
    "incrementalCopy": null,
    "progress": "10737418752/10737418752",
    "source": "https://md-
xxxxxx.blueexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "status": "success",
    "statusDescription": null
  },
....
```

6. 將生成的映像下載到您的 Linux 伺服器。

```
wget <URL of file examplesaname/Containers/vm-  
images/9150.01000024.05090105.vhd>
```

URL 遵循標準格式。為了實現自動化，您可以獲得如下所示的 URL 字串。或者，您可以使用 Azure CLI `az` 命令來取得 URL。範例 URL：https://examplesaname.bluelxpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. 清理託管磁碟

```
az disk revoke-access --name $diskName --resource-group $diskRG  
az disk delete --name $diskName --resource-group $diskRG --yes
```

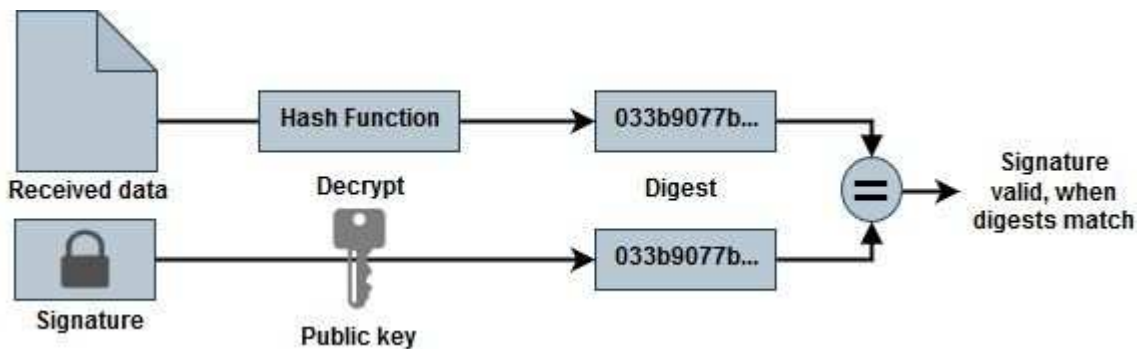
驗證文件簽名

針對**Cloud Volumes ONTAP** 的**Azure** 市場映像簽章驗證

Azure 映像驗證過程透過剝離 VHD 檔案的開頭 1 MB 和結尾 512 位元組，然後套用雜湊函數來產生摘要檔案。為了匹配簽章程序，使用 `_sha256_` 進行雜湊。

文件簽章驗證工作流程摘要

以下是文件簽章驗證工作流程的概述。



- 從 ["NetApp支援站點"](#) 並提取摘要 (.sig) 文件、公鑰證書 (.pem) 文件和鍵證書 (.pem) 文件。請參閱["下載 Azure 映像摘要文件"](#) 了解更多。
- 信任鏈的驗證。
- 從公鑰憑證 (.pem) 中提取公鑰 (.pub)。
- 使用提取的公鑰解密摘要檔案。
- 將結果與從圖像檔案中刪除開頭 1 MB 和結尾 512 位元組後建立的臨時檔案的新生成的摘要進行比較。此步驟透過使用 OpenSSL 命令列工具執行。OpenSSL CLI 工具會在檔案比對成功或失敗時顯示對應的訊息。

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

在 Linux 上驗證匯出的 VHD 檔案簽章包括驗證信任鏈、編輯檔案和驗證簽章。

步驟

1. 從下載 Azure 映像檔 ["NetApp支援站點"](#)並提取摘要 (.sig) 文件、公鑰證書 (.pem) 文件和鏈證書 (.pem) 文件。

參考 ["下載 Azure 映像摘要文件"](#)了解更多。

2. 驗證信任鏈。

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

3. 刪除 VHD 檔案開頭的 1 MB (1,048,576 位元組) 和結尾的 512 位元組。使用時 tail，這 -c +K`選項從檔案的第 K 個位元組產生位元組。因此，它將 1048577 傳遞給 `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 從憑證中提取公鑰，並使用簽署檔案和公鑰驗證剝離的檔案 (sign.tmp)。

命令提示字元根據驗證顯示指示成功或失敗的訊息。

```
% 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
```

驗證 macOS 上 Cloud Volumes ONTAP 的 Azure 市場映像簽名

在 Linux 上驗證匯出的 VHD 檔案簽章包括驗證信任鏈、編輯檔案和驗證簽章。

步驟

1. 從下載 Azure 映像檔 ["NetApp 支援站點"](#) 並提取摘要 (.sig) 文件、公鑰證書 (.pem) 文件和鏈證書 (.pem) 文件。

參考 ["下載 Azure 映像摘要文件"](#) 了解更多。

2. 驗證信任鏈。

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

3. 刪除 VHD 檔案開頭的 1MB (1,048,576 位元組) 和結尾的 512 位元組。使用時 tail，這 -c +K 選項從檔案的第 K 個位元組產生位元組。因此，它將 1048577 傳遞給 tail -c。請注意，在 macOS 上，tail 指令可能需要大約十分鐘才能完成。

```
% 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 從憑證中提取公鑰，並使用簽署檔案和公鑰驗證剝離的檔案 (sign.tmp)。命令提示字元根據驗證顯示指示成功或失敗的訊息。

```
% 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
```

版權資訊

Copyright © 2026 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。