



## 開始使用**Microsoft Azure** Cloud Volumes ONTAP

NetApp  
May 12, 2022

# 目錄

開始使用Microsoft Azure .....	1
Azure中的功能快速入門Cloud Volumes ONTAP .....	1
規劃 Cloud Volumes ONTAP Azure 的不一樣組態.....	1
Azure 的網路需求 Cloud Volumes ONTAP .....	4
設定Cloud Volumes ONTAP 支援使用Azure中客戶管理的金鑰.....	12
在 Cloud Volumes ONTAP Azure 中啟動 .....	14

# 開始使用Microsoft Azure

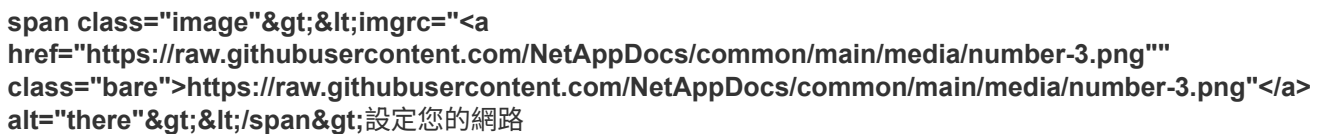
## Azure中的功能快速入門Cloud Volumes ONTAP

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

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"](#)。

當您建立第一個 Cloud Volumes ONTAP 運作環境時、如果您還沒有連接器、Cloud Manager 會提示您部署連接器。

Cloud Manager 提供符合工作負載需求的預先設定套件、您也可以建立自己的組態。如果您選擇自己的組態、應該瞭解可用的選項。 ["深入瞭解"](#)。

 設定您的網路

1. 確保您的 Vnet 和子網路可支援連接器與 Cloud Volumes ONTAP 支援的連接功能。
2. 啟用從目標 vnet 的傳出網際網路存取、讓 Connector 和 Cloud Volumes ONTAP 支援中心能夠連絡多個端點。

這個步驟很重要、因為連接器 Cloud Volumes ONTAP 無法在沒有外傳網際網路存取的情況下管理不穩定。如果您需要限制傳出連線、請參閱的端點清單 ["Connector 與 Cloud Volumes ONTAP the"](#)。

["深入瞭解網路需求"](#)。

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 Cloud Manager 建立 Connector"](#)
- ["從 Azure Marketplace 建立 Connector"](#)
- ["在 Linux 主機上安裝 Connector 軟體"](#)
- ["Cloud Manager具備權限的功能"](#)

## 規劃 Cloud Volumes ONTAP Azure 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。

檢視支援的區域

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"](#)。

## 選擇授權

有多種授權選項可供 Cloud Volumes ONTAP 選擇。每個選項都能讓您選擇符合需求的消費模式。"[深入瞭解 Cloud Volumes ONTAP 解適用於此功能的授權選項](#)"。

## 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

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。

HA 系統使用優質網頁。同時、單一節點系統可使用兩種 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 磁碟大小

啟動 Cloud Volumes ONTAP 時、您必須選擇集合體的預設磁碟大小。Cloud Manager 會將此磁碟大小用於初始 Aggregate、以及使用簡易資源配置選項時所建立的任何其他 Aggregate。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"](#)

### 選擇支援 Flash Cache 的組態

Azure 中的一個支援本地 NVMe 儲存設備的組態、可將其用作 \_Flash Cache 以獲得更好的效能。 Cloud Volumes ONTAP Cloud Volumes ONTAP ["深入瞭解 Flash Cache"](#)。

### 檢視預設系統磁碟

Cloud Manager除了儲存使用者資料之外、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"](#)。

### Azure 網路資訊工作表

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

Cloud Manager 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 Cloud Manager 中建立 Volume 時、您可以選擇啟用這些功能的設定檔、或是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。這包括連接器和 Cloud Volumes ONTAP 整個過程的網路功能。

### 需求 Cloud Volumes ONTAP

Azure 必須符合下列網路需求。

#### 傳出網際網路存取

支援向 NetApp 支援部門傳送訊息、以便主動監控儲存設備的健全狀況。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>

"瞭解如何驗AutoSupport 證功能"。

#### IP位址

Cloud Manager 會將下列 IP 位址分配給 Cloud Volumes ONTAP Azure 中的功能：

- 單一節點：5 個 IP 位址
- HA 配對：16 個 IP 位址

請注意、Cloud Manager 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。



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。

## 安全連線至 Azure 服務

Cloud Manager 可設定 vnet 服務端點和 Azure Private Link 端點、Cloud Volumes ONTAP 以便讓整個公司能夠私有連接至 Azure 服務。

### 服務端點

Cloud Manager 可讓 vnet 服務端點建立安全的連線、從 Cloud Volumes ONTAP 功能區到 Azure Blob 儲存設備、以便進行資料分層。不支援 Cloud Volumes ONTAP 其他服務端點、從功能到 Azure 服務皆不受支援。

如果 Cloud Manager 原則具有下列權限、Cloud Manager 可為您啟用 vnet 服務端點：

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

這些權限包含在最新版本中 ["Cloud Manager 原則"](#)。

如需設定資料分層的詳細資訊、請參閱 ["將冷資料分層至低成本物件儲存設備"](#)。

### 私有端點

根據預設、Cloud Manager 會在 Cloud Volumes ONTAP 支援 Azure 及其相關儲存帳戶的情況下、啟用 Azure Private Link 連線。Private Link 可保護 Azure 中端點之間的連線、並提供效能優勢。在大多數情況下、您完全不需要這麼做、Cloud Manager 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。您也可以視需要停用「私有連結」連線。

["深入瞭解如何搭配 Cloud Volumes ONTAP 使用 Azure 私有 Link 搭配使用功能"](#)。

## 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體的記錄資料。Cloud Volumes ONTAP HA 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「功能組」配對、Cloud Manager會發生連線問題。

## 安全性群組

您不需要建立安全性群組、因為Cloud Manager能幫您建立安全性群組。如果您需要使用自己的安全性群組規則、請參閱下列安全性群組規則。

## 安全性群組規則

Cloud Manager 會建立 Azure 安全性群組、其中包括 Cloud Volumes ONTAP 需要順利運作的傳入和傳出規則。您可能需要參照連接埠進行測試、或是偏好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。

## 單一節點系統的傳入規則

下列規則會允許流量、除非說明中註明會封鎖特定的傳入流量。

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、以 HTTPS 存取 System Manager 網路主控台
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
1012 inbound _2049_tcp	2049 TCP	任意	NFS 伺服器精靈



優先順序和名稱	連接埠與傳輸協定	來源與目的地	說明
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

下列規則會允許流量、除非說明中註明會封鎖特定的傳入流量。



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、以 HTTPS 存取 System Manager 網路主控台
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
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

優先順序和名稱	連接埠與傳輸協定	來源與目的地	說明
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協定從HTTPS變更為HTTP時、AutoSupport
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

服務	連接埠	傳輸協定	來源	目的地	目的
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

設定您的網路、讓 Connector 能夠管理公有雲環境中的資源和程序。最重要的步驟是確保從網際網路存取各種端點。



如果您的網路使用 Proxy 伺服器來進行所有與網際網路的通訊、您可以從「設定」頁面指定 Proxy 伺服器。請參閱 "[將 Connector 設定為使用 Proxy 伺服器](#)"。

### 連線至目標網路

連接器需要網路連線至您要部署 Cloud Volumes ONTAP 的 VPC 和 VNets 。

例如、如果您在公司網路中安裝 Connector 、則必須設定 VPN 連線至 VPC 或 vnet 、以便在其中啟動 Cloud Volumes ONTAP 更新。

### 傳出網際網路存取

連接器需要存取傳出網際網路、才能管理公有雲環境中的資源和程序。

端點	目的
<a href="https://support.netapp.com">https://support.netapp.com</a>	以取得授權資訊、並將AutoSupport 資訊傳送給NetApp支援部門。
<a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a>	在Cloud Manager中提供SaaS功能與服務。
<a href="https://cloudmanagerinfraproduct.azurecr.io">https://cloudmanagerinfraproduct.azurecr.io</a> <a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a>	升級Connector及其Docker元件。

## 安全性群組規則

Connector 的安全性群組需要傳入和傳出規則。

### 傳入規則

連接埠	傳輸協定	目的
22	SSH	提供對 Connector 主機的 SSH 存取權
80	HTTP	提供從用戶端 Web 瀏覽器到本機使用者介面的 HTTP 存取
443..	HTTPS	提供 HTTPS 存取、從用戶端網頁瀏覽器存取本機使用者介面

### 傳出規則

Connector 的預先定義安全性群組會開啟所有傳出流量。如果可以接受、請遵循基本的傳出規則。如果您需要更嚴格的規則、請使用進階的傳出規則。

### 基本傳出規則

Connector 的預先定義安全性群組包括下列傳出規則。

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、僅開啟連接器傳出通訊所需的連接埠。



來源 IP 位址為 Connector 主機。

服務	連接埠	傳輸協定	目的地	目的
API 呼叫與 AutoSupport 功能	443..	HTTPS	傳出網際網路和 ONTAP 叢集管理 LIF	API將Azure和ONTAP VMware呼叫、Cloud Data Sense、勒索軟體服務、並將AutoSupport VMware訊息傳送給NetApp
DNS	53.	UDP	DNS	用於 Cloud Manager 的 DNS 解析

# 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. 在Cloud Manager中、使用API建立Cloud Volumes ONTAP 一個使用金鑰的功能不全的環境

## 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

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。

### HA 配對

- 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。
- 任何新的儲存帳戶（例如新增磁碟或集合體時）也會使用相同的金鑰。

### 單一節點

- 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。
- 對於根磁碟、開機磁碟和資料磁碟、Cloud Manager使用 "[磁碟加密集](#)"，可透過託管磁碟管理加密金鑰。
- 任何新的資料磁碟也會使用相同的磁碟加密集。
- NVRAM和核心磁碟是使用Microsoft管理的金鑰來加密、而非使用客戶管理的金鑰。

## 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。

### 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
- \* Azure磁碟加密、適用於Volume加密\* (Cloud Volumes ONTAP 僅適用於單一節點的整套系統)

## 2. "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Cloud Manager API可支援這些步驟。

如果您想要將客戶管理的金鑰與單一節點Cloud Volumes ONTAP 的作業系統搭配使用、請確定Cloud Manager 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"
```

您可以在上找到最新的權限清單 "[Cloud Manager 原則頁面](#)"。

HA配對不需要這些權限。

### 步驟

1. 請使用下列Cloud Manager 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Cloud Manager 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Cloud Manager API呼叫建立一套系統。

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"  
}
```

["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"  
}
```

+

["深入瞭解此API呼叫"](#)。

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 中啟動

您可以 Cloud Volumes ONTAP 在 Cloud Manager 中建立運作不正常的環境、在 Azure 中啟動單一節點系統或 HA 配對。

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"](#)。



- 瞭解在「新增工作環境」精靈中選擇特定授權選項所需的條件。["深入瞭解Cloud Volumes ONTAP 解關於功能驗證的資訊"](#)。

授權選項	需求	如何滿足需求
Freemium	需要Marketplace訂閱或NetApp支援網站 (NSS) 帳戶。	您可以從*詳細資料與認證*頁面訂閱雲端供應商的市場。您可以在「*充電方法」和「NSSAccount *」頁面上輸入您的NSS*帳戶。
專業或基本套件	需要Marketplace訂閱或容量型授權 (BYOL)。如果您的帳戶沒有有效的容量型授權、或是您的資源配置超過授權容量、建議您訂閱Marketplace以容量為基礎進行收費。	您可以從*詳細資料與認證*頁面訂閱雲端供應商的市場。如果您想要使用從NetApp購買的容量型授權 (BYOL)、您必須先將其新增至*數位錢包*。 <a href="#">"瞭解如何新增容量型BYOL授權"</a> 。
Keystone Flex 訂閱	您的帳戶必須獲得授權、而且訂閱必須啟用Cloud Volumes ONTAP 才能與效益管理系統搭配使用。	<p>a. mailto : <a href="mailto:ng-keystone-success@netapp.com">ng-keystone-success@netapp.com</a> [聯絡 NetApp]、以一或多個Keystone Flex 訂閱授權您的Cloud Manager使用者帳戶。</p> <p>b. NetApp授權您的帳戶之後、<a href="#">"連結您的訂閱內容以供Cloud Volumes ONTAP 搭配使用"</a>。</p> <p>c. 當您建立Cloud Volumes ONTAP 一個「叢集HA配對」時、請選擇Keystone Flex訂閱充電方法。</p>
每個節點授權	您必須訂閱Marketplace、否則必須自行攜帶授權 (BYOL)。此選項適用於現有訂閱或現有授權的客戶。不適用於新客戶。	如果您想要使用從NetApp購買的節點型授權 (BYOL)、您必須先將其新增至*數位錢包*。 <a href="#">"瞭解如何新增節點型BYOL授權"</a> 。您可以在「*充電方法」和「NSSAccount *」頁面上輸入您的NSS*帳戶。

Cloud Manager Cloud Volumes ONTAP 在 Azure 中建立一套功能完善的系統時、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Cloud Manager可在Cloud Volumes ONTAP 部署失敗或刪除時、從共用資源群組移除資源的功能、但Azure使用者可能會不小心從Cloud Volumes ONTAP 共用資源群組中刪除這些資源。

## 步驟

1. [[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。
2. \* 選擇位置 \* : 選擇 \* Microsoft Azure \* 與 \* Cloud Volumes ONTAP 《單一節點 \*》或 \* Cloud Volumes ONTAP 《高可用度 \*》。
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	Cloud Manager 會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。當您在此欄位中輸入標記時、Cloud Manager 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 " <a href="#">Microsoft Azure 說明文件：使用標籤來組織 Azure 資源</a> "。
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。" <a href="#">瞭解如何新增認證</a> "。

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

► <https://docs.netapp.com/zh-tw/cloud-manager-cloud-volumes->

[ontap//media/video\\_subscribing\\_azure.mp4](#) (video)

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Cloud Data Sense"](#)。
  - ["深入瞭解Cloud Backup"](#)。
  - ["深入瞭解監控服務"](#)。
6. 位置與連線：選取位置、資源群組、安全性群組、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。

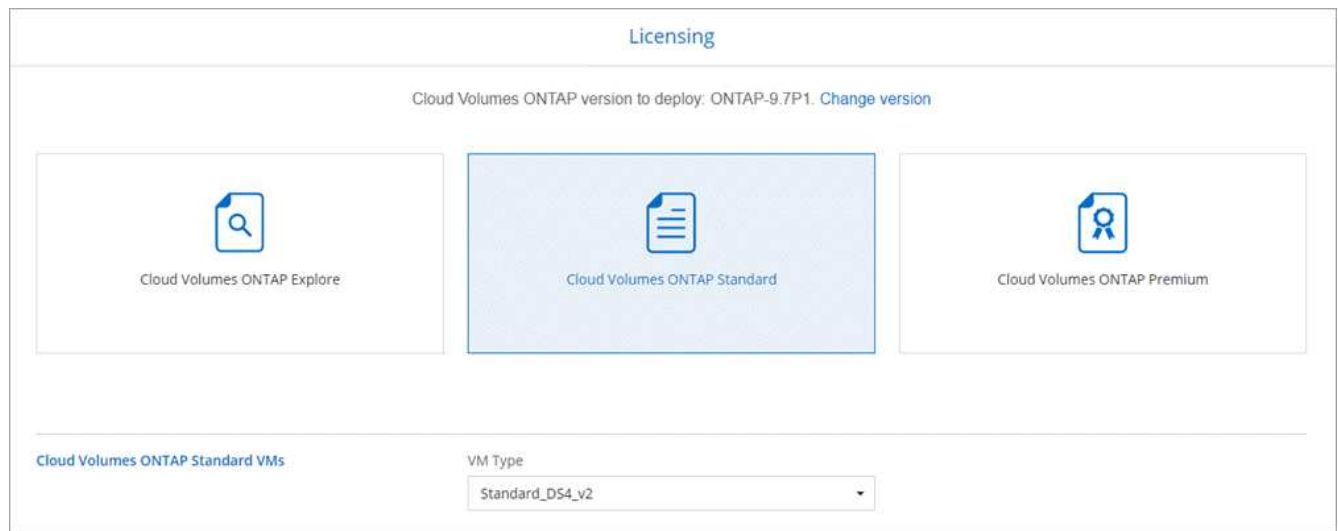
下表說明您可能需要指導的欄位：

欄位	說明
位置	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 、 Cloud Manager 會為您選擇一個。
資源群組	<p>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。</p> <p>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「功能組」配對、Cloud Manager會發生連線問題。</p> <div><p>如果您使用的Azure帳戶具有 <a href="#">"必要權限"</a>Cloud Manager可在Cloud Volumes ONTAP 部署失敗或刪除時、從資源群組移除不必要的資源。</p></div>
安全性群組	如果您選擇現有的安全群組、則必須符合Cloud Volumes ONTAP 下列需求： <a href="#">"檢視預設的安全性群組"</a> 。

7. 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。
  - ["瞭解這些充電方法"](#)。
  - ["瞭解精靈中您想要使用的授權方法所需的內容"](#)。
8. \* 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。

9. \* 授權 \* : 視 Cloud Volumes ONTAP 需要變更版本、選取授權、然後選取虛擬機器類型。



如果您在啟動系統之後需要變更、您可以稍後修改授權或虛擬機器類型。



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、Cloud Manager 會在建立工作環境時、將系統更新至該版本。例如、如果您選取 Cloud Volumes ONTAP 了「供應的是」「供應的是」「供應的是」「供應的是」「供應的是」、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。

10. \* 從 Azure Marketplace 訂閱 \*：如果 Cloud Manager 無法以程式設計方式部署 Cloud Volumes ONTAP 功能、請依照下列步驟進行。
11. \* 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 Cloud Manager 在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"](#)。

12. \* 寫入速度與 WORM \*（僅限單節點系統）：選擇 \* 正常 \* 或 \* 高速 \* 寫入速度、並視需要啟動一次寫入、多次讀取（WORM）儲存設備。

["深入瞭解寫入速度"](#)。

如果啟用雲端備份或啟用資料分層、則無法啟用 WORM。

["深入瞭解 WORM 儲存設備"](#)。

13. \* 安全通訊至儲存設備與 WORM \*（僅限 HA）：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 從一個名為「支援速度」的鏈接至 Azure 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"](#)。

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

["瞭解支援的用戶端傳輸協定和版本"](#)。

本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

欄位	說明
尺寸	您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。
存取控制（僅適用於 NFS）	匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、Cloud Manager 會輸入一個值、讓您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 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）、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 Volume 時、Cloud Manager 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、 <a href="#">"使用 IQN 從主機連線至 LUN"</a> 。

下圖顯示 CIFS 傳輸協定的「Volume」（磁碟區）頁面：

Volume Details, Protection & Protocol

### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy: 

default

Default Policy

### Protocol

NFS
CIFS
iSCSI

Share name:  Permissions: 

Full Control

Users / Groups:

Valid users and groups separated by a semicolon

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

欄位	說明
DNS 主要和次要 IP 位址	提供 CIFS 伺服器名稱解析的 DNS 伺服器 IP 位址。列出的 DNS 伺服器必須包含所需的服務位置記錄 (SRV), 才能找到 CIFS 伺服器要加入之網域的 Active Directory LDAP 伺服器和網域控制器。
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 * 。 <a href="https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou">https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou</a> ["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 <a href="#">"Cloud Manager 自動化文件"</a> 以取得詳細資料。請注意、您只能在建立 CIFS 伺服器時設定 NTP 伺服器。您建立 CIFS 伺服器之後、就無法進行設定。

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

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

17. \* 審查與核准 \*：檢閱並確認您的選擇。

- a. 檢閱組態的詳細資料。
- b. 按一下 \* 更多資訊 \* 以檢閱 Cloud Manager 將購買的支援與 Azure 資源詳細資料。

c. 選取「\* 我瞭解 ... \*」核取方塊。

d. 按一下「\* 執行 \*」。

Cloud Manager 部署 Cloud Volumes ONTAP 了這個功能。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。



## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.