



Azure管理

Cloud Volumes ONTAP

NetApp
June 11, 2024

目錄

Azure管理	1
變更Azure VM類型Cloud Volumes ONTAP 以供使用	1
在Cloud Volumes ONTAP Azure中覆寫CIFS鎖、以利執行不需使用的功能	2
使用Azure私有連結或服務端點	3
正在移動資源群組	7
分離 Azure 中的 SnapMirror 流量	7

Azure管理

變更Azure VM類型Cloud Volumes ONTAP 以供使用

在Cloud Volumes ONTAP Microsoft Azure中啟動時、您可以從多種VM類型中進行選擇。您可以隨時變更VM類型、只要判斷其規模過小或過大、就能滿足您的需求。

關於這項工作

- 自動恢復必須在 Cloud Volumes ONTAP 一個「無法恢復的 HA 配對」上啟用（這是預設設定）。如果沒有、則作業將會失敗。

["供應說明文件：設定自動恢復的命令 ONTAP"](#)

- 變更VM類型可能會影響Microsoft Azure服務費用。
- 此作業會重新啟動 Cloud Volumes ONTAP 。

對於單一節點系統、I/O 會中斷。

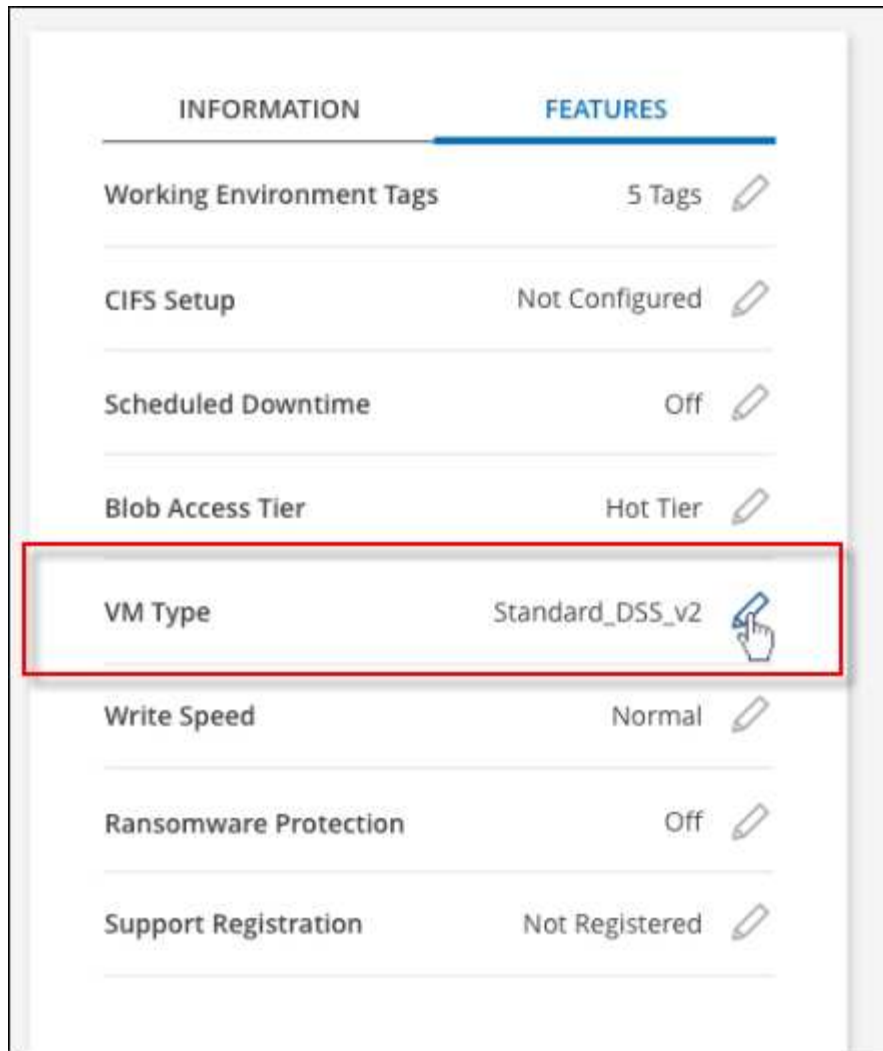
對於 HA 配對、變更不中斷營運。HA 配對可繼續提供資料。



BlueXP會主動啟動接管並等待回饋、一次只能正常變更一個節點。NetApp 的 QA 團隊在這段過程中測試了寫入和讀取檔案的能力、並未發現客戶端有任何問題。隨著連線變更、我們確實看到 I/O 層級的重試次數、但應用程式層卻取代了 NFS/CIFS 連線的這些短「重新連線」。

步驟

1. 在 Canvas 頁面上、選取工作環境。
2. 按一下 [概觀] 索引標籤上的 [功能] 面板，然後按一下 *VM 類型* 旁邊的鉛筆圖示。



a. 如果您使用的是節點型 PAYGO 授權、您可以選擇不同的授權和 VM 類型、方法是按一下 * 授權類型 * 旁的鉛筆圖示。

3. 選取 VM 類型、選取核取方塊以確認您瞭解變更的影響、然後按一下 * 變更 * 。

結果

以新組態重新開機。 Cloud Volumes ONTAP

在Cloud Volumes ONTAP Azure中覆寫CIFS鎖、以利執行不需使用的功能

帳戶管理員可在BlueXP中啟用一項設定、以防止Cloud Volumes ONTAP 在Azure維護活動期間發生有關還原儲存設備的問題。啟用此設定時 Cloud Volumes ONTAP 、不支援 CIFS 會鎖定並重設作用中的 CIFS 工作階段。

關於這項工作

Microsoft Azure 會排程在其虛擬機器上定期進行維護活動。當某個維護事件發生在Cloud Volumes ONTAP 一個不支援的HA配對上時、HA配對會啟動儲存設備接管。如果在此維護事件期間有作用中的CIFS工作階段、則CIFS檔案上的鎖定功能可能會妨礙儲存設備恢復。

如果啟用此設定、Cloud Volumes ONTAP 則會取消鎖定並重設作用中的 CIFS 工作階段。因此、HA配對可在這些維護事件期間完成儲存恢復。



此程序可能會對 CIFS 用戶端造成破壞。未從 CIFS 用戶端提交的資料可能會遺失。

您需要的產品

您必須先建立連接器、才能變更BlueXP設定。"瞭解方法"。

步驟

1. 在 BlueXP 主控台的右上角、按一下「設定」圖示、然後選取 * 「Cloud Volumes ONTAP 設定 *」。



2. 在* Azure 下、按一下 Azure CIFS Locks for Azure HA工作環境*。
3. 按一下核取方塊以啟用此功能、然後按一下「儲存」。

使用Azure私有連結或服務端點

使用Azure Private Link連線至相關儲存帳戶。Cloud Volumes ONTAP如有需要、您可以停用Azure私有連結、改用服務端點。

總覽

根據預設、BlueXP會啟用Azure Private Link、以便Cloud Volumes ONTAP 在支援的各個儲存帳戶之間建立連線。Azure Private Link可保護Azure中端點之間的連線安全、並提供效能優勢。

如有需要、您可以設定Cloud Volumes ONTAP 使用服務端點、而非Azure Private Link。

無論是哪一種組態、BlueXP都會限制Cloud Volumes ONTAP 存取網路、以利連接到各個儲存帳戶。網路存取僅限於Cloud Volumes ONTAP 部署了下列項目的vnet和部署Connector的vnet。

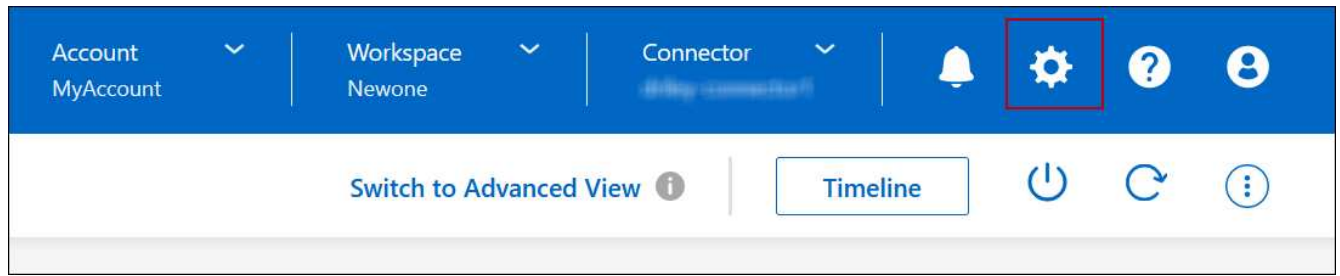
停用Azure私有連結、改用服務端點

如果貴企業需要、您可以變更BlueXP中的設定、使Cloud Volumes ONTAP 其設定使用服務端點、而非Azure私有連結。變更此設定會套用Cloud Volumes ONTAP 至您所建立的新版資訊系統。服務端點僅在中受支援 "Azure區域配對" 連接器與Cloud Volumes ONTAP 胎心之間。

連接器應部署在Cloud Volumes ONTAP 其所管理的或所管理的各個系統所在的Azure區域 "Azure區域配對" 適用於整個系統。Cloud Volumes ONTAP

步驟

1. 在 BlueXP 主控台的右上角、按一下「設定」圖示、然後選取 * 「Cloud Volumes ONTAP 設定 *」。



2. 在* Azure 下、按一下*使用**Azure Private Link**。
3. 取消選擇* Cloud Volumes ONTAP 在不同時使用*私有連結的情況下、連接到儲存帳戶*。
4. 按一下「* 儲存 *」。

完成後

如果您停用Azure私有連結、且Connector使用Proxy伺服器、則必須啟用直接API流量。

["瞭解如何在Connector上啟用直接API流量"](#)

使用**Azure**私有連結

在大多數情況下、您不需要做任何事、就能使用Cloud Volumes ONTAP 下列功能來設定Azure私有連結：
：BlueXP會為您管理Azure私有連結。但如果您使用現有的Azure私有DNS區域、則必須編輯組態檔。

自訂**DNS**的需求

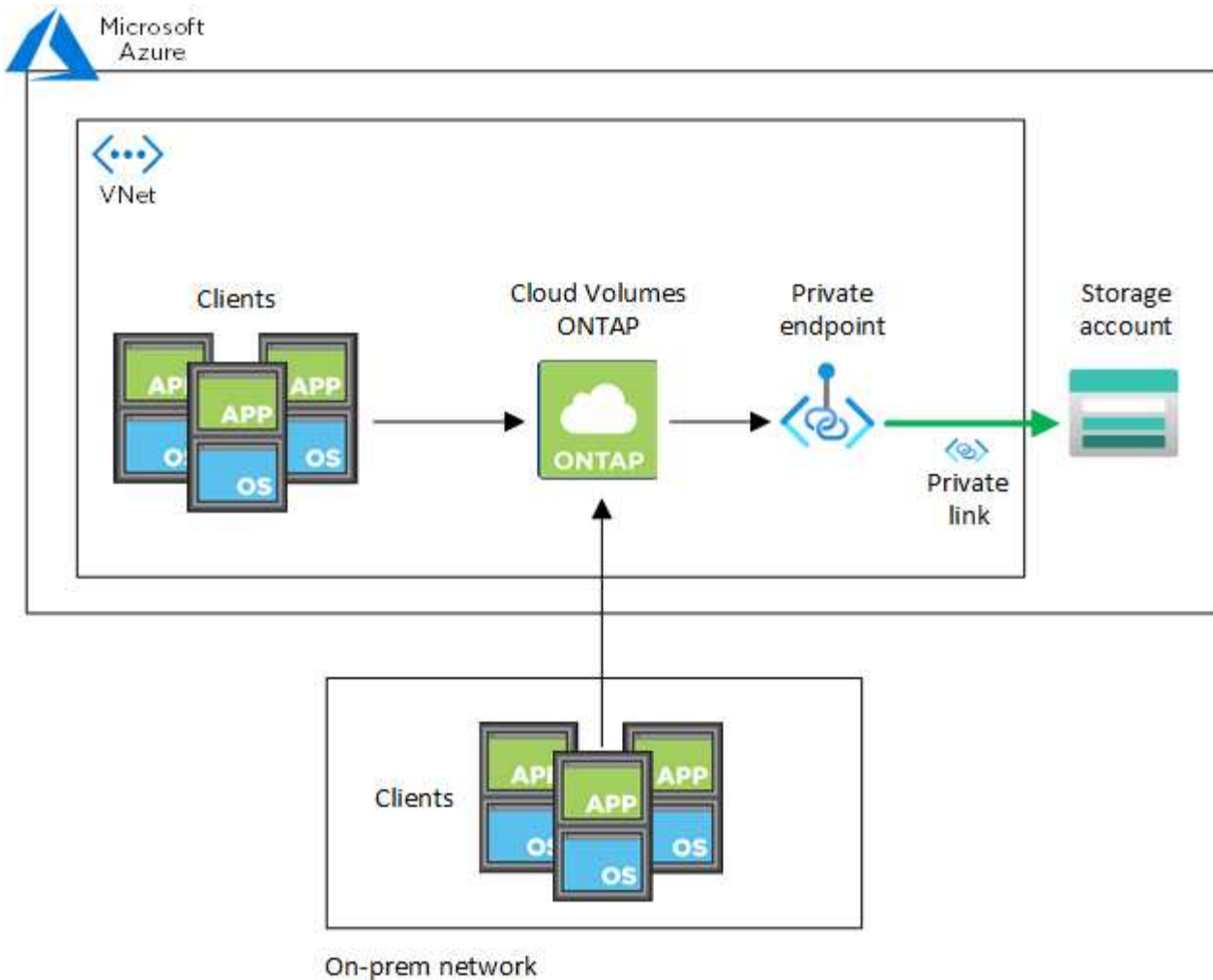
或者、如果您使用自訂DNS、則需要從自訂DNS伺服器建立條件轉寄站、以前往Azure私有DNS區域。若要深入瞭解、請參閱 ["Azure關於使用DNS轉寄站的文件"](#)。

私有連結連線的運作方式

當BlueXP在Cloud Volumes ONTAP Azure中部署時、它會在資源群組中建立一個私有端點。私有端點與Cloud Volumes ONTAP 用於實現功能不均的儲存帳戶相關聯。因此Cloud Volumes ONTAP 、存取資料可透過Microsoft主幹網路存取。

當用戶端與Cloud Volumes ONTAP S時 位於相同的vnet內、在連接VNet的對等網路內、或在使用私有VPN或ExpressRoute連線至vnet的內部部署網路中、用戶端存取會透過私有連結進行。

以下範例顯示用戶端透過私有連結從同一個Vnet存取、以及從內部網路存取具有私有VPN或ExpressRoute連線的權限。



如果連接器和Cloud Volumes ONTAP 物件系統部署在不同的VNets中、則您必須在部署連接器的vnet和Cloud Volumes ONTAP 部署了該系統的vnet之間設定vnet對等關係。

提供您Azure私有DNS的詳細資料給BlueXP

如果您使用 "Azure 私有 DNS"然後您需要修改每個 Connector 上的組態檔。否則、BlueXP無法在Cloud Volumes ONTAP 支援的儲存帳戶之間啟用Azure Private Link連線。

請注意、DNS 名稱必須符合 Azure DNS 命名需求 "如 Azure 文件所示"。

步驟

1. SSH 連接至 Connector 主機並登入。
2. 瀏覽至下列目錄：`/opp/application/netapp/cloudmanager/docker_occm/data`
3. 使用下列關鍵字-值配對新增「user-Private - DNS"區域設定參數、以編輯app.conf：

```
"user-private-dns-zone-settings" : {
  "resource-group" : "<resource group name of the DNS zone>",
  "subscription" : "<subscription ID>",
  "use-existing" : true,
  "create-private-dns-zone-link" : true
}
```

此參數應與「system-id」輸入的層級相同、如下所示：

```
"system-id" : "<system ID>",
"user-private-dns-zone-settings" : {
```

請注意、只有當私有DNS區域的訂閱與Connector不同時、才需要訂購關鍵字。

4. 儲存檔案並登出 Connector 。

不需要重新開機。

在故障時啟用復原功能

如果BlueXP無法建立Azure私有連結做為特定行動的一部分、則在不使用Azure私有連結連線的情況下完成此動作。當建立新的工作環境（單一節點或HA配對）、或是HA配對上發生下列動作時、就會發生這種情況：建立新的Aggregate、新增磁碟至現有的Aggregate、或是在超過32 TiB時建立新的儲存帳戶。

如果BlueXP無法建立Azure私有連結、您可以啟用復原功能來變更此預設行為。這有助於確保您完全符合貴公司的安全法規。

如果您啟用復原、則BlueXP會停止動作、並回溯作為行動一部分所建立的所有資源。

您可以透過API或更新app.conf檔案來啟用復原功能。

*透過API*啟用復原功能

步驟

1. 請使用「PUT /occm/config（放入/occm/config）API呼叫與下列要求內容：

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

更新app.conf以啟用復原功能

步驟

1. SSH 連接至 Connector 主機並登入。
2. 瀏覽至下列目錄：/opp/application/netapp/cloudmanager/docker_occm/data
3. 新增下列參數和值以編輯 app.conf：


```
"rollback-on-private-link-failure": true
. 儲存檔案並登出 Connector 。
```

不需要重新開機。

正在移動資源群組

支援 Azure 資源群組移動、但工作流程僅發生在 Azure 主控台。Cloud Volumes ONTAP

您可以在同一 Azure 訂閱中、將工作環境從一個資源群組移至 Azure 中的其他資源群組。不支援在不同 Azure 訂閱之間移動資源群組。

步驟

1. 從* Canvas* 移除工作環境。

若要瞭解如何移除工作環境、請參閱 ["移除 Cloud Volumes ONTAP 運作環境"](#)。

2. 在 Azure 主控台執行資源群組搬移。

若要完成移動、請參閱 ["將資源移至新的資源群組或訂閱 Microsoft Azure 文件中"](#)。

3. 在* Canvas* 中、探索工作環境。
4. 在工作環境的資訊中尋找新的資源群組。

結果

工作環境及其資源（VM、磁碟、儲存帳戶、網路介面、快照）位於新的資源群組中。

分離 Azure 中的 SnapMirror 流量

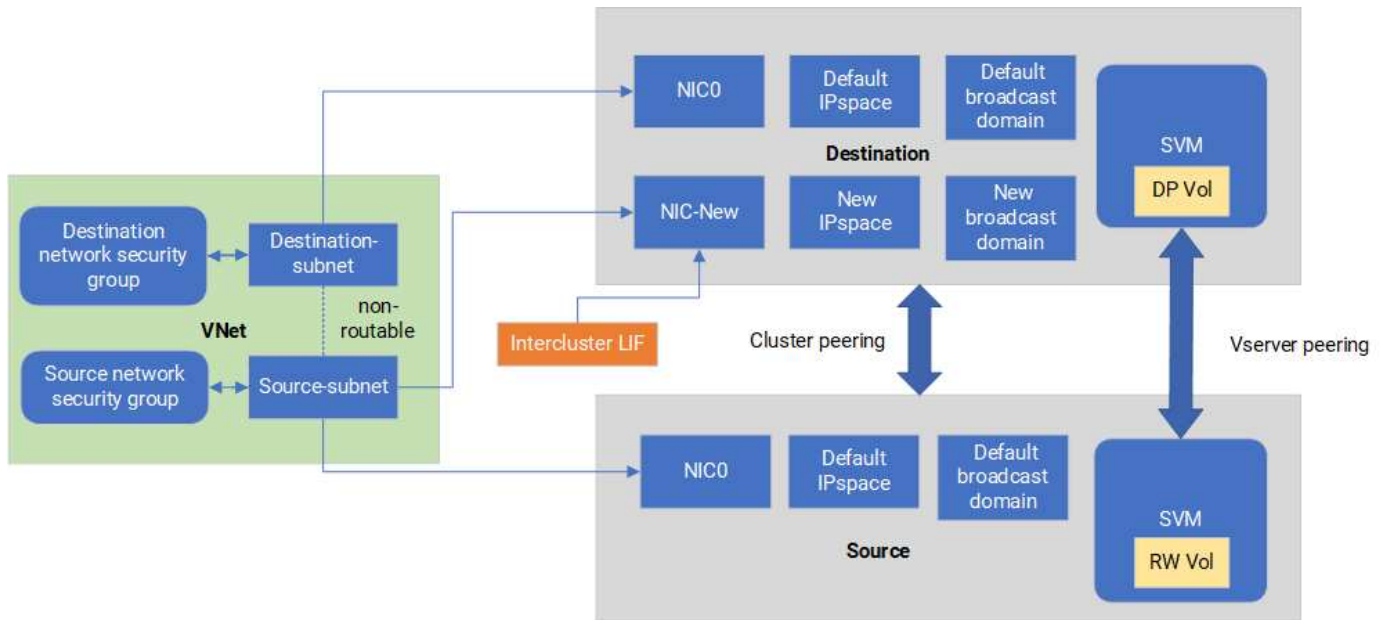
有了 Azure 中的 Cloud Volumes ONTAP、您可以將 SnapMirror 複寫流量與資料和管理流量區隔。若要將 SnapMirror 複寫流量與資料流量區隔、您需要新增網路介面卡（NIC）、相關的叢集間 LIF 和不可路由的子網路。

關於 Azure 中的 SnapMirror 流量分隔

根據預設、BlueXP 會在相同子網路上的 Cloud Volumes ONTAP 部署中設定所有 NIC 和生命。在此類組態中、SnapMirror 複寫流量和資料與管理流量使用相同的子網路。分離 SnapMirror 流量會利用無法路由傳送至現有子網路的額外子網路、用於資料和管理流量。

圖 1.

下圖顯示 SnapMirror 複寫流量與其他 NIC、相關的叢集間 LIF 和單一節點部署中不可路由的子網路之間的分隔。HA 配對部署稍有不同。



開始之前

請檢閱下列考量事項：

- 您只能將單一 NIC 新增至 Cloud Volumes ONTAP 單一節點或 HA 配對部署（VM 執行個體）、以進行 SnapMirror 流量分隔。
- 若要新增 NIC、您部署的 VM 執行個體類型必須有未使用的 NIC。
- 來源叢集和目的地叢集應可存取相同的虛擬網路（vnet）。目的地叢集是 Azure 中的 Cloud Volumes ONTAP 系統。來源叢集可以是 Azure 中的 Cloud Volumes ONTAP 系統、也可以是 ONTAP 系統。

步驟 1：建立額外的 NIC 並附加至目的地 VM

本節提供如何建立其他 NIC 並將其附加至目的地 VM 的說明。目的地 VM 是 Azure 中 Cloud Volumes ONTAP 的單一節點或 HA 配對系統、您可以在其中設定額外的 NIC。

步驟

1. 在 ONTAP CLI 中、停止節點。

```
dest::> halt -node <dest_node-vm>
```

2. 在 Azure 入口網站中、檢查 VM（節點）狀態是否已停止。

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. 使用 Azure Cloud Shell 中的 Bash 環境來停止節點。

- a. 停止節點。

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

- b. 取消分配節點。

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. 設定網路安全性群組規則、使兩個子網路（來源叢集子網路和目的地叢集子網路）無法彼此路由。

- a. 在目的地 VM 上建立新的 NIC 。
- b. 尋找來源叢集子網路的子網路 ID 。

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet-name <vnet> --query id
```

- c. 在目的 VM 上建立新的 NIC 、並提供來源叢集子網路的子網路 ID 。在此輸入新 NIC 的名稱。

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new> --subnet <id_from_prev_command> --accelerated-networking true
```

- d. 儲存私有 IP 位址。此 IP 位址 <new_added_nic_primary_addr> 用於在中建立叢集間 LIF [廣播網域](#)、新 NIC 的叢集間 LIF 。

5. 將新的 NIC 連接至 VM 。

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics <dest_node-vm-nic-new>
```

6. 啟動 VM（節點）。

```
az vm start --resource-group <dest_node-rg> --name <dest_node-vm>
```

7. 在 Azure 入口網站中、前往 * 網路 * 並確認新的 NIC（例如 NIC 新的）存在且已啟用加速網路連線。

```
az network nic list --resource-group azure-59806175-60147103-azure-rg --query "[].{NIC: name, VM: virtualMachine.id}"
```

對於 HA 配對部署、請針對合作夥伴節點重複這些步驟。

步驟 2：為新 NIC 建立新的 IPspace、廣播網域和叢集間 LIF

叢集間生命體的獨立 IPspace 可在叢集之間進行複寫的網路功能之間提供邏輯分隔。

請使用 ONTAP CLI 執行下列步驟。

步驟

1. 建立新的 IPspace (new_IPSpace) 。

```
dest::> network ipspace create -ip-space <new_ipspace>
```

2. 在新的 IPspace (new_IPSpace) 上建立廣播網域、然後新增 NIC 新連接埠。

```
dest::> network port show
```

3. 對於單節點系統、新增的連接埠為 e0b。對於具有託管磁碟的 HA 配對部署、新增的連接埠為 e0d。對於具有頁面 Blobs 的 HA 配對部署、新增的連接埠為 e0e。使用節點名稱而非 VM 名稱。執行即可找到節點名稱 node show。

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500  
-ip-space <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. 在新的廣播網域 (new_bd) 和新的 NIC (NIC 新) 上建立叢集間 LIF。

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-  
lif> -service-policy default-intercluster -address  
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask  
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. 驗證新叢集間 LIF 的建立。

```
dest::> net int show
```

對於 HA 配對部署、請針對合作夥伴節點重複這些步驟。

步驟 3：驗證來源和目的地系統之間的叢集對等關係

本節提供如何驗證來源和目的地系統之間對等關係的指示。

請使用 ONTAP CLI 執行下列步驟。

步驟

1. 確認目的地叢集的叢集間 LIF 可以 ping 通來源叢集的叢集間 LIF 。由於目的地叢集執行此命令、因此目的地 IP 位址是來源上的叢集間 LIF IP 位址。

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. 確認來源叢集的叢集間 LIF 可以 ping 通目的地叢集的叢集間 LIF 。目的地是在目的地上建立的新 NIC 的 IP 位址。

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

對於 HA 配對部署、請針對合作夥伴節點重複這些步驟。

步驟 4：在來源與目的地系統之間建立 SVM 對等關係

本節提供如何在來源與目的地系統之間建立 SVM 對等關係的指示。

請使用 ONTAP CLI 執行下列步驟。

步驟

1. 使用來源叢集間 LIF IP 位址做為、在目的地上建立叢集對等關係 `-peer-addr`s。對於 HA 配對、請將兩個節點的來源叢集間 LIF IP 位址列為 `-peer-addr`s。

```
dest::> cluster peer create -peer-addr <10.161.189.6> -ipspace
<new_ipspace>
```

2. 輸入並確認通行密碼。
3. 使用目的地叢集 LIF IP 位址做為、在來源上建立叢集對等關係 `peer-addr`s。對於 HA 配對、請將兩個節點的目的地叢集間 LIF IP 位址列為 `-peer-addr`s。

```
src::> cluster peer create -peer-addr <10.161.189.18>
```

4. 輸入並確認通行密碼。
5. 檢查叢集是否已對等連接。

```
src::> cluster peer show
```

在可用度欄位中成功的對等顯示 * 可用 *。

6. 在目的地上建立 SVM 對等關係。來源和目的地 SVM 都應該是資料 SVM。

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. 接受 SVM 對等關係。

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. 請檢查 SVM 是否有問題。

```
dest::> vserver peer show
```

對等狀態顯示 **peered** 並顯示對等應用程式 **snapmirror**。

步驟 5：在來源與目的地系統之間建立 SnapMirror 複寫關係

本節提供如何在來源與目的地系統之間建立 SnapMirror 複寫關係的指示。

若要移動現有的 SnapMirror 複寫關係、您必須先中斷現有的 SnapMirror 複寫關係、然後再建立新的 SnapMirror 複寫關係。

請使用 ONTAP CLI 執行下列步驟。

步驟

1. 在目的地 SVM 上建立資料保護的 Volume。

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. 在目的地上建立 SnapMirror 複寫關係、其中包括 SnapMirror 原則和複寫排程。

```
dest::> snapmirror create -source-path src_svm:src_vol -destination
-path dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. 初始化目的地上的 SnapMirror 複寫關係。

```
dest::> snapmirror initialize -destination-path <dest_svm:new_dest_vol>
```

4. 在 ONTAP CLI 中、執行下列命令以驗證 SnapMirror 關係狀態：

```
dest::> snapmirror show
```

關係狀態為 Snapmirrored 而關係的健全狀況就是 true。

5. 可選：在 ONTAP CLI 中，運行以下命令查看 SnapMirror 關係的操作歷史記錄。

```
dest::> snapmirror show-history
```

或者、您可以掛載來源和目的地磁碟區、將檔案寫入來源磁碟區、並驗證磁碟區是否正在複寫到目的地。

版權資訊

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

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

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

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

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

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

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

商標資訊

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