Azure 管理

Cloud Volumes ONTAP

NetApp
February 13, 2026

目錄

Azure 管理

變更Cloud Volumes ONTAP的 Azure VM 類型

在 Microsoft Azure 中啟動Cloud Volumes ONTAP時，您可以從多種 VM 類型中進行選擇。如果您確定虛擬機器類型太小或太大，無法滿足您的需求，您可以隨時變更虛擬機器類型。

關於此任務

- 必須在Cloud Volumes ONTAP HA 對上啟用自動交還（這是預設）。如果不是，則操作將會失敗。

  "ONTAP 9 文件：用於設定自動交還的命令"

- 變更 VM 類型可能會影響 Microsoft Azure 服務費用。
- 此操作重新啟動Cloud Volumes ONTAP。

  對於單節點系統， I/O 會中斷。

  對於 HA 對來說，這種變化是無中斷的。 HA 對繼續提供數據。

NetApp Console透過啟動接管並等待返回來一次更改一個節點。 NetApp 的品質保證團隊在過程中對檔案的寫入和讀取進行了測試，並且沒有發現客戶端的任何問題。隨著連接的變化，在 I/O 層級觀察到一些重試，但應用層克服了 NFS/CIFS 連接的重新連接。

步驟

1. 在*系統*頁面上，選擇系統。
2. 在「概述」標籤上，按一下「功能」面板，然後按一下「**VM** 類型」旁邊的鉛筆圖示。

   如果您使用的是基於節點的即用即付 (PAYGO) 許可證，則可以透過點擊「許可證類型」旁邊的鉛筆圖示來選擇不同的許可證和 VM 類型。

3. 選擇 VM 類型，選取核取方塊以確認您了解變更的含義，然後按一下「變更」。

結果

Cloud Volumes ONTAP使用新設定重新啟動。

覆寫 Azure 中Cloud Volumes ONTAP HA 對的 CIFS 鎖

組織或帳戶管理員可以在NetApp Console中啟用一項設置，以防止在 Azure 維護事件期間出現Cloud Volumes ONTAP儲存復原問題。啟用此設定後， Cloud Volumes ONTAP將否決 CIFS 鎖定並重設活動的 CIFS 會話。

關於此任務

Microsoft Azure 會安排其虛擬機器的定期維護事件。當Cloud Volumes ONTAP HA 對上發生維護事件時，HA 對會啟動儲存接管。如果在此維護事件期間有活動的 CIFS 會話，則 CIFS 檔案上的鎖定可能會阻止儲存復原。

如果啟用此設置， Cloud Volumes ONTAP將否決鎖定並重置活動的 CIFS 會話。因此，HA 對可以在這些維護事件期間完成儲存恢復。

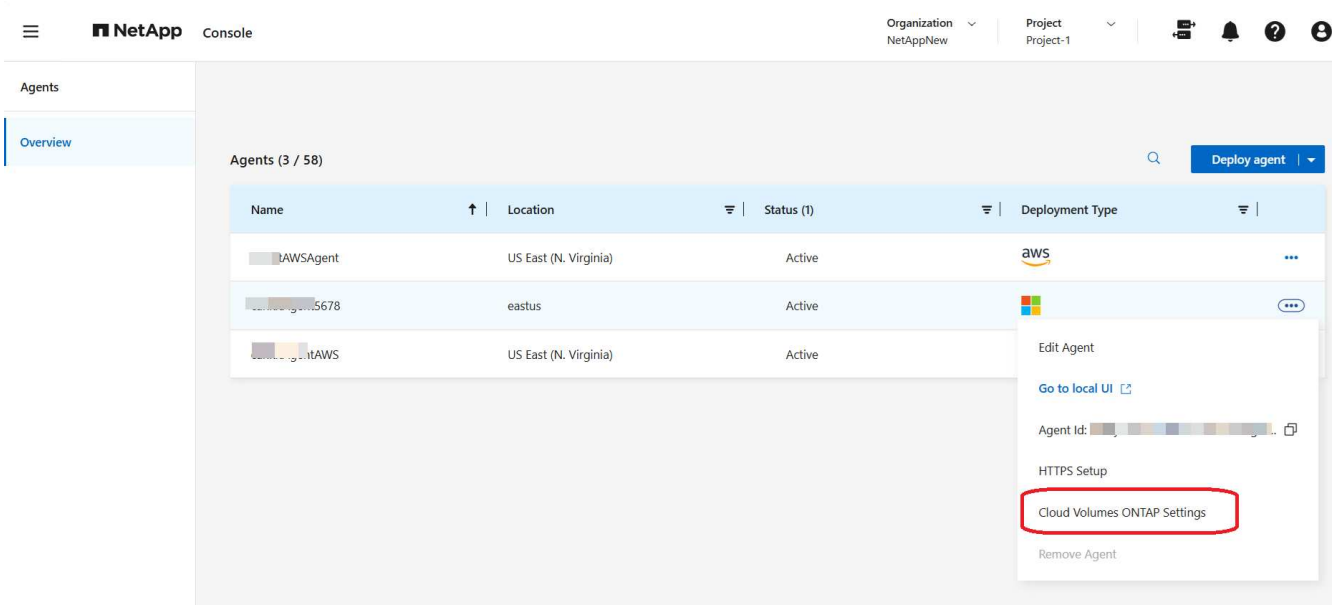
此過程可能會對 CIFS 用戶端造成破壞。 CIFS 用戶端未提交的資料可能會遺失。

開始之前

您需要先建立控制台代理，然後才能變更控制台設定。 "學習使用" 。

步驟

1. 從左側導覽窗格前往*管理>代理*。
2. 點選 ••• 管理Cloud Volumes ONTAP系統的控制台代理的圖示。
3. 選擇* Cloud Volumes ONTAP設定*。



4. 在「Azure」下，按一下「Azure HA 系統的 Azure CIFS 鎖定」。
5. 按一下複選框以啟用該功能，然後按一下“儲存”。

為Cloud Volumes ONTAP系統使用 Azure Private Link 或服務端點

Cloud Volumes ONTAP使用 Azure Private Link 連接到其關聯的儲存帳戶。如果需要，您可以停用 Azure Private Links 並改用服務端點。

概況

預設情況下， NetApp Console啟用 Azure Private Link 來建立Cloud Volumes ONTAP與其關聯儲存帳戶之間的連線。 Azure 專用連結可保護 Azure 中端點之間的連線並提供效能優勢。

如果需要，您可以將Cloud Volumes ONTAP設定為使用服務端點而不是 Azure Private Link。

無論採用哪種配置，控制台始終限制Cloud Volumes ONTAP和儲存帳戶之間的連接的網路存取。網路存取僅限

於部署Cloud Volumes ONTAP 的VNet 和部署控制台代理程式的 VNet。

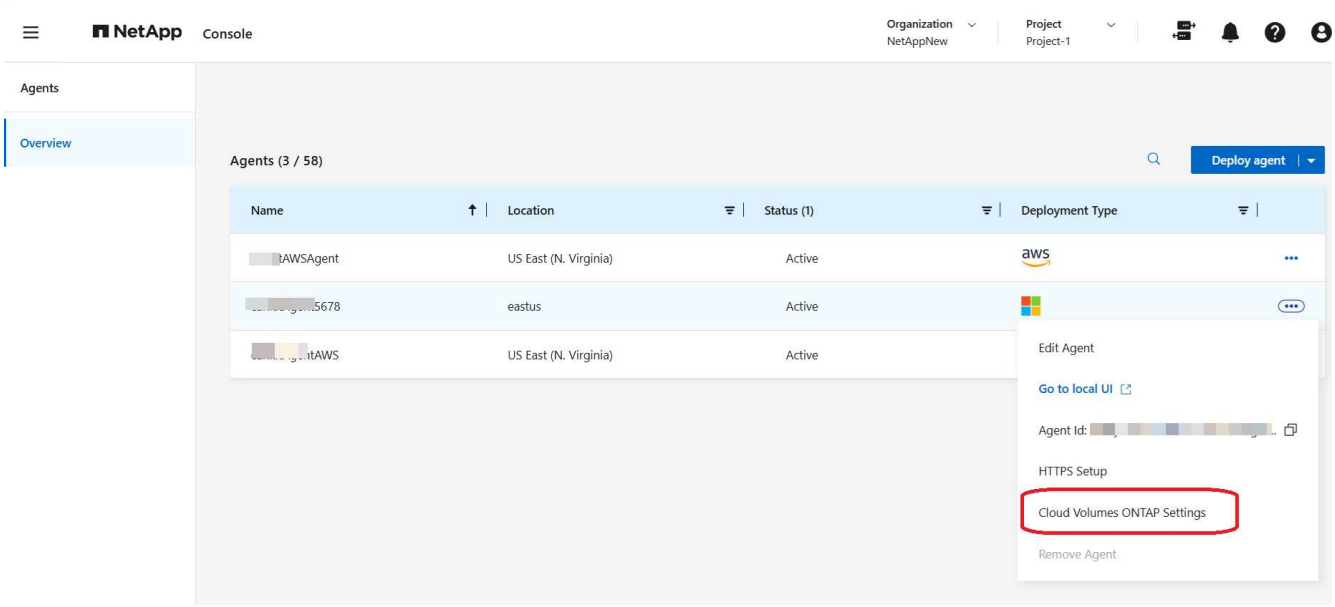
停用 **Azure Private Links** 並改用服務終點

如果您的業務需要，您可以在控制台中變更設置，以便將Cloud Volumes ONTAP配置為使用服務端點而不是 Azure Private Link。變更此設定適用於您建立的新Cloud Volumes ONTAP系統。服務端點僅支援"Azure 區域對"控制台代理程式和Cloud Volumes ONTAP VNet 之間。

控制台代理應部署在與其管理的Cloud Volumes ONTAP系統相同的 Azure 區域中，或部署在 "Azure 區域對"適用於Cloud Volumes ONTAP系統。

步驟

1. 從左側導覽窗格前往*管理>代理*。
2. 點選 ••• 管理Cloud Volumes ONTAP系統的控制台代理的圖示。
3. 選擇* Cloud Volumes ONTAP設定*。



4. 在「**Azure**」下，按一下「使用 **Azure** 專用連結」。
5. 取消選擇* Cloud Volumes ONTAP和儲存帳戶之間的專用連結連線*。
6. 點選“儲存”。

完成後

如果您停用了 Azure Private Links 且控制台代理程式使用代理伺服器，則必須啟用直接 API 流量。

"了解如何在控制台代理上啟用直接 API 流量"

使用 **Azure Private Links**

在大多數情況下，您無需執行任何操作即可設定與Cloud Volumes ONTAP 的Azure Private 連結。控制台為您管理 Azure 專用連結。但是如果您使用現有的 Azure 私人 DNS 區域，則需要編輯設定檔。

自訂 **DNS** 的要求

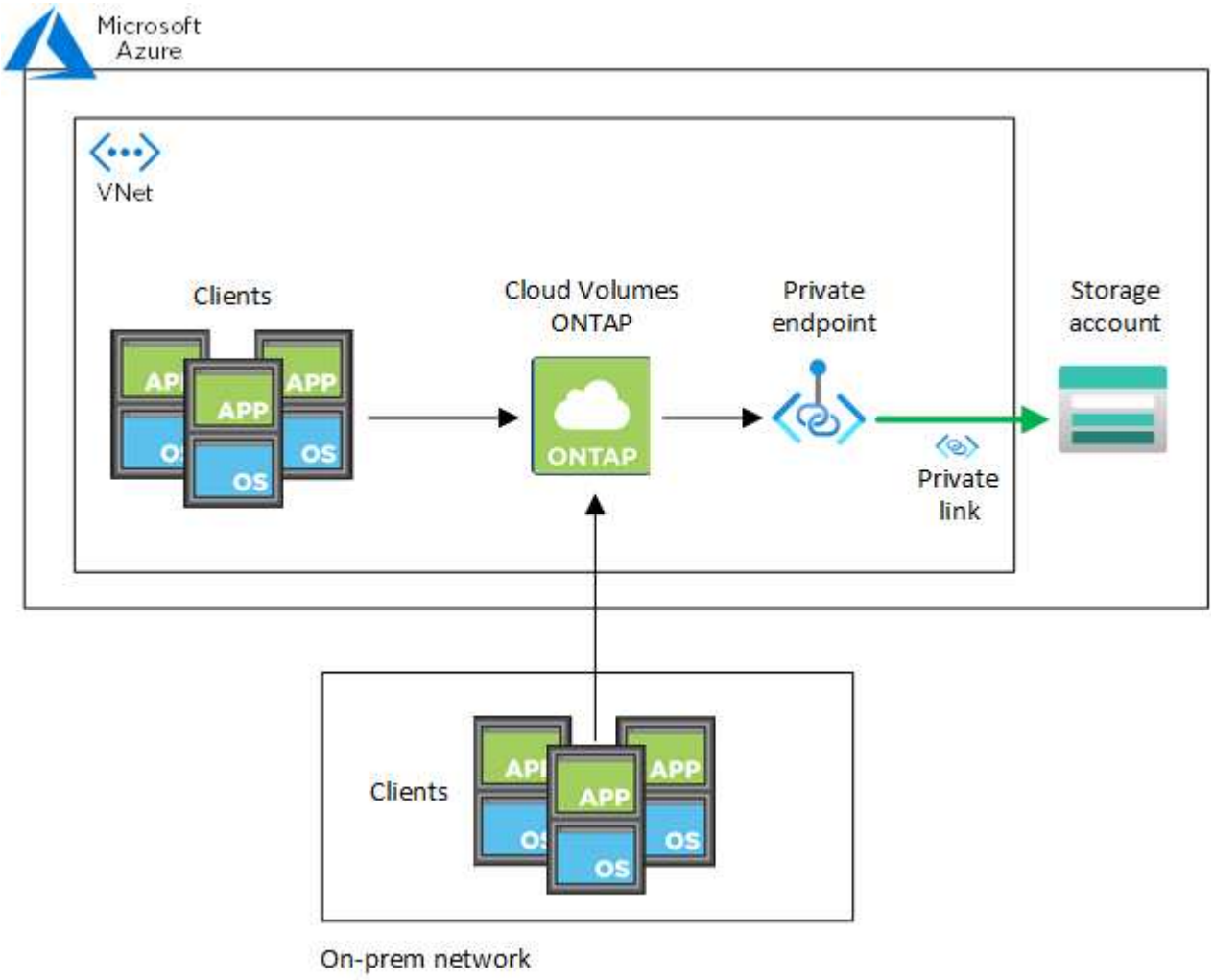
或者，如果您使用自訂 DNS，則需要從自訂 DNS 伺服器建立至 Azure 私人 DNS 區域的條件轉送器。要了解更多信息，請參閱"Azure 關於使用 DNS 轉送器的文檔"。

專用連結連接的工作原理

當控制台在 Azure 中部署Cloud Volumes ONTAP時，它會在資源組中建立一個私有端點。私有端點與Cloud Volumes ONTAP 的儲存帳戶相關聯。因此，對Cloud Volumes ONTAP儲存的存取需要透過 Microsoft 主幹網路。

當客戶端與Cloud Volumes ONTAP位於同一 VNet 內、位於對等 VNet 內或位於本機網路中時，用戶端存取將透過專用連結進行。

以下範例展示了用戶端如何透過專用連結從同一 VNet 內部以及從具有專用 VPN 或 ExpressRoute 連接的本機網路存取。



如果控制台代理程式和Cloud Volumes ONTAP系統部署在不同的 VNet 中，則必須在部署控制台代理程式的 VNet 和部署Cloud Volumes ONTAP系統的 VNet 之間設定 VNet 對等連線。

提供有關 **Azure** 專用 **DNS** 的詳細信息

如果你使用 "Azure 專用 DNS"，那麼就需要在每個Console代理上修改一個設定檔。否則，控制台無法設定Cloud Volumes ONTAP與其關聯儲存帳戶之間的 Azure Private Link 連線。

請注意，DNS 名稱必須符合 Azure DNS 命名要求 "如 Azure 文件所示"。

步驟

1. 透過 SSH 連接到控制台代理主機並登入。
2. 導航至 `/opt/application/netapp/cloudmanager/docker_occm/data`目錄。
3. 編輯 `app.conf`透過添加 `user-private-dns-zone-settings`具有以下關鍵字-值對的參數：

```
"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
}
```

這 `subscription`僅當私有 DNS 區域與控制台代理的訂閱不同時才需要關鍵字。

4. 儲存檔案並登出控制台代理程式。

不需要重新啟動。

啟用故障回滾

如果控制台無法在特定操作中建立 Azure 專用鏈接，它將在沒有 Azure 專用連結連接的情況下完成此操作。建立新系統（單一節點或 HA 對）時，或在 HA 對上執行以下操作時，可能會發生這種情況：建立新聚合、向現有聚合新增磁碟或在超過 32 TiB 時建立新的儲存帳戶。

如果控制台無法建立 Azure 專用鏈接，您可以透過啟用回溯來變更此預設行為。這有助於確保您完全遵守公司的安全規定。

如果啟用回滾，控制台將停止該操作並回滾作為該操作的一部分所建立的所有資源。

您可以透過 API 或更新 app.conf 檔案來啟用回滾。

透過 **API** 啟用回滾

步

1. 使用 `PUT /occm/config`具有以下請求主體的 API 呼叫：

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

透過更新 **app.conf** 啟用回滾

步驟

1. 透過 SSH 連接到控制台代理的主機並登入。
2. 導覽至以下目錄：/opt/application/netapp/cloudmanager/docker_occm/data
3. 編輯 app.conf，新增以下參數和值：

```
 "rollback-on-private-link-failure": true
. 儲存檔案並登出控制台代理程式。
```

不需要重新啟動。

在 Azure 控制台中移動Cloud Volumes ONTAP的 Azure 資源組

Cloud Volumes ONTAP支援 Azure 資源組移動，但工作流程僅在 Azure 控制台中進行。

您可以將Cloud Volumes ONTAP系統從同一 Azure 訂閱內的一個資源群組移至 Azure 中的另一個資源群組。不支援在不同的 Azure 訂閱之間行動資源群組。

步驟

1. 刪除Cloud Volumes ONTAP系統。請參閱"刪除Cloud Volumes ONTAP系統" 。
2. 在 Azure 控制台中執行資源組移動。

   若要完成移動，請參閱"Microsoft Azure 文件中的“將資源移至新的資源群組或訂閱”"。
3. 在*系統*頁面上，發現系統。
4. 在系統資訊中尋找新的資源組。

結果

系統及其資源（虛擬機器、磁碟、儲存帳戶、網路介面、快照）位於新的資源群組中。

在 Azure 中隔離SnapMirror流量

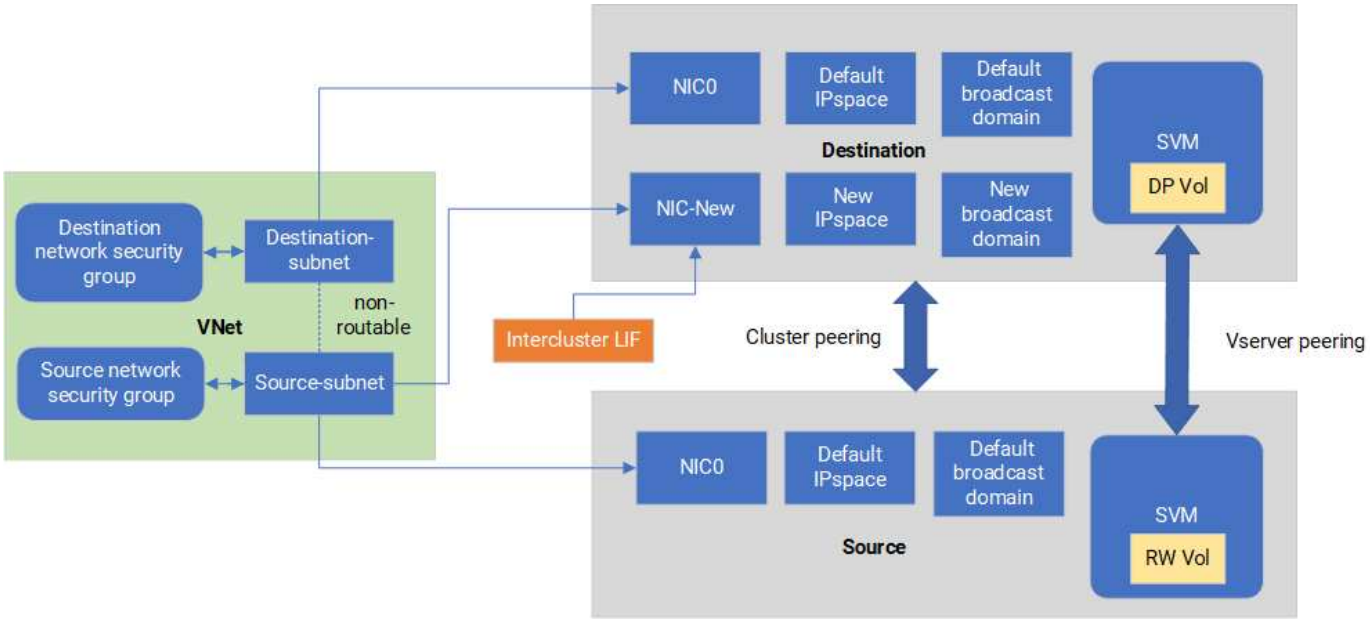
使用 Azure 中的Cloud Volumes ONTAP ，您可以將SnapMirror複製流量與資料和管理流量分開。為了將SnapMirror複製流量與資料流量隔離，您需要新增一個新的網路介面卡 (NIC)、一個相關的群集間 LIF 和一個不可路由的子網路。

關於 Azure 中的SnapMirror流量隔離

預設情況下， NetApp Console會在相同子網路上設定Cloud Volumes ONTAP部署中的所有 NIC 和 LIF。在這樣的設定中， SnapMirror複製流量和資料和管理流量使用相同的子網路。隔離SnapMirror流量利用了無法路由到用於資料和管理流量的現有子網路的額外子網路。

圖 1

下圖顯示了在單一節點部署中，使用附加 NIC、關聯的群集間 LIF 和不可路由子網路對SnapMirror複製流量進行隔離。 HA 對部署略有不同。



開始之前

回顧以下注意事項：

- 您只能向Cloud Volumes ONTAP單節點或 HA 對部署（VM 實例）新增單一 NIC 以實現SnapMirror流量隔離。
- 若要新增新的 NIC，您部署的 VM 實例類型必須具有未使用的 NIC。
- 來源叢集和目標叢集應該可以存取同一個虛擬網路 (VNet)。目標叢集是 Azure 中的Cloud Volumes ONTAP系統。來源叢集可以是 Azure 中的Cloud Volumes ONTAP系統或ONTAP系統。

步驟 1：建立額外的 NIC 並連接到目標 VM

本節提供有關如何建立附加 NIC 並將其附加到目標 VM 的說明。目標 VM 是 Azure 中Cloud Volumes ONTAP中的單節點或 HA 對系統，您要設定額外的 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 環境停止節點。
   a. 停止節點。

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

b. 解除分配節點。

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

4. 設定網路安全群組規則，讓兩個子網路（來源叢集子網路和目標叢集子網路）互不可達。
   a. 在目標虛擬機器上建立新的 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. 使用來源叢集子網路的子網路 ID 在目標虛擬機器上建立新的 NIC。在這裡輸入新 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. 保存私有IP位址。此 IP 位址 <new_added_nic_primary_addr> 用於在廣播域，新 NIC 的群集間 LIF。
5. 將新的 NIC 附加到 VM。

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

6. 啟動虛擬機器（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-new）存在並且加速網路已啟用。

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

對於 HA 對部署，請對合作夥伴節點重複這些步驟。

步驟 2：為新 NIC 建立新的 IP 空間、廣播域和群集間 LIF

群集間 LIF 的單獨 IP 空間為群集間複製的網路功能提供了邏輯分離。

使用ONTAP CLI 執行以下步驟。

步驟

1. 建立新的 IP 空間（new_ipspace）。

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

2. 在新的 IP 空間（new_ipspace）上建立廣播網域並新增 nic-new 連接埠。

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

3. 對於單節點系統，新增連接埠為 *e0b*。對於使用託管磁碟的 HA 配對部署，新增連接埠為 *e0d*。對於使用分頁 Blob 的 HA 配對部署，新增連接埠為 *e0e*。請使用節點名稱，而非 VM 名稱。執行 `node show`以尋找節點名稱。

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

4. 在新的廣播域 (new_bd) 和新的 NIC (nic-new) 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. 驗證新的集群間 LIF 的建立。

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

對於 HA 對部署，請對合作夥伴節點重複這些步驟。

步驟 3：驗證來源系統和目標系統之間的叢集對等連接

本節提供有關如何驗證來源系統和目標系統之間的對等關係的說明。

使用ONTAP CLI 執行以下步驟。

步驟

1. 驗證目標群集的群集間 LIF 是否可以對來源群集的群集間 LIF 執行 ping 操作。由於目標群集執行此命令，因此目標 IP 位址是來源上的群集間 LIF IP 位址。

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

2. 驗證來源集群的集群間 LIF 是否可以 ping 通目標集群的集群間 LIF。目標是在目標上建立的新 NIC 的 IP 位址。

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

對於 HA 對部署，請對合作夥伴節點重複這些步驟。

步驟 4：在來源系統和目標系統之間建立 SVM 對等連接

本節提供如何在來源系統和目標系統之間建立 SVM 對等的說明。

使用ONTAP CLI 執行以下步驟。

步驟

1. 使用來源集群間 LIF IP 位址作為目標在目標上建立集群對等 `-peer-addrs`。對於 HA 對，列出兩個節點的來源群集間 LIF IP 位址作為 `-peer-addrs`。

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

2. 輸入並確認密碼。
3. 使用目標群集 LIF IP 位址作為來源群集的 IP 位址，在來源上建立群集對等連接 `peer-addrs`。對於 HA 對，列出兩個節點的目標群集間 LIF IP 位址作為 `-peer-addrs`。

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

4. 輸入並確認密碼。
5. 檢查集群是否對等。

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

成功的對等連線在可用性欄位中顯示 可用。

6. 在目標上建立 SVM 對等連線。來源 SVM 和目標 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 對等連線。

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

8. 檢查 SVM 是否已對等。

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

同行國家顯示*peered* 和對等應用程式顯示*snapmirror*.

步驟 5：在來源系統和目標系統之間建立SnapMirror複製關係

本節提供如何在來源系統和目標系統之間建立SnapMirror複製關係的說明。

要移動現有的SnapMirror複製關係，必須先中斷現有的SnapMirror複製關係，然後再建立新的SnapMirror複製關係。

使用ONTAP CLI 執行以下步驟。

步驟

1. 在目標 SVM 上建立資料保護磁碟區。

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

2. 在目標上建立SnapMirror複製關係，其中包括複製的SnapMirror策略和計劃。

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

3. 在目標上初始化SnapMirror複製關係。

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

4. 在ONTAP CLI 中，透過執行以下命令驗證SnapMirror關係狀態：

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

關係狀態是 `Snapmirrored`關係的健康是 `true`。

5. 可選：在ONTAP CLI 中，執行以下命令查看SnapMirror關係的操作記錄。

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

或者，您可以掛載來源磁碟區和目標卷，將檔案寫入來源卷，並驗證磁碟區是否複製到目標磁碟區。

版權資訊

商標資訊