Azure管理

Cloud Volumes ONTAP

NetApp
September 10, 2024

目录

Azure管理

更改 Cloud Volumes ONTAP 的 Azure VM 类型

在 Microsoft Azure 中启动 Cloud Volumes ONTAP 时，您可以从多种 VM 类型中进行选择。如果您确定虚拟机类型的大小不足或过大，则可以随时根据您的需要更改此虚拟机类型。

关于此任务

- 必须在 Cloud Volumes ONTAP HA 对上启用自动交还（这是默认设置）。否则，操作将失败。

  "ONTAP 9 文档：用于配置自动交还的命令"

- 更改虚拟机类型可能会影响 Microsoft Azure 服务费用。
- 该操作将重新启动 Cloud Volumes ONTAP 。

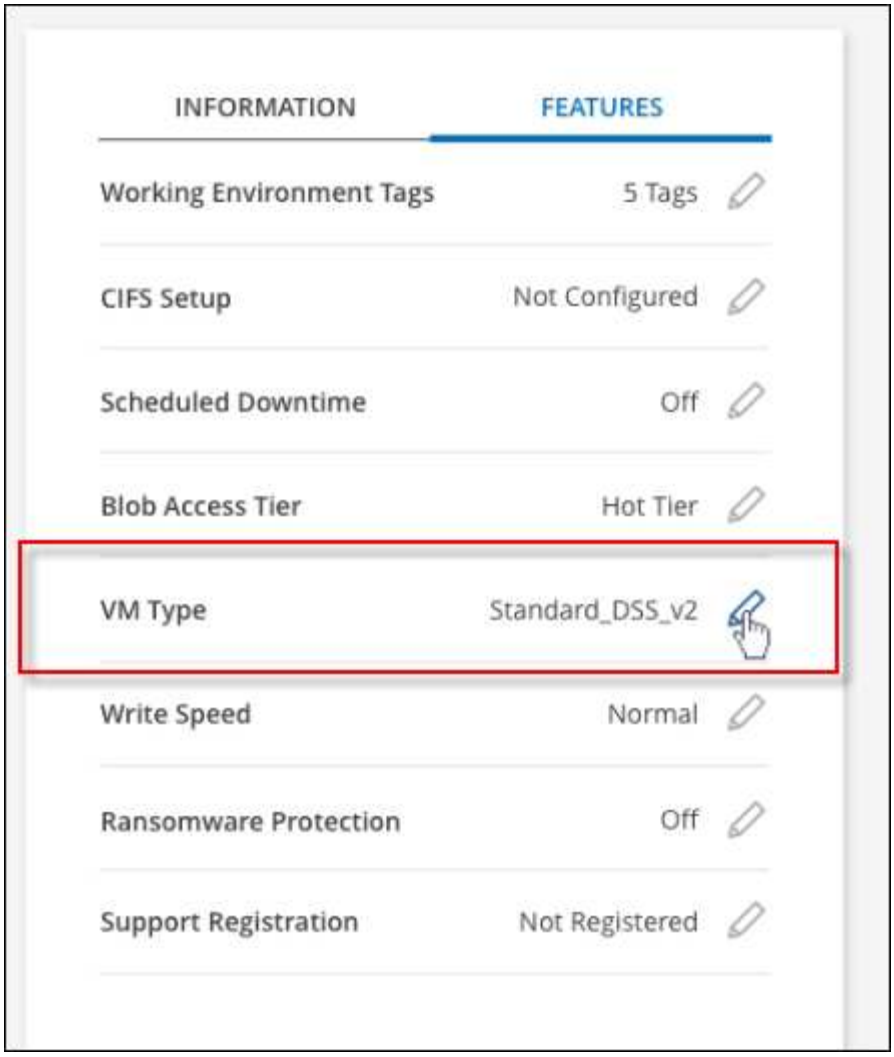
  对于单节点系统， I/O 中断。

  对于 HA 对、更改不会中断。HA 对继续为数据提供服务。

> BlueXP 通过启动接管并等待交还一次更改一个节点。在此过程中、NetApp的质量保证团队对文件的写入和读取进行了测试、未发现客户端存在任何问题。随着连接发生变化、我们会在I/O级别进行一些重试、但应用程序层克服了NFS/CCIFS连接的重新布线。

步骤

1. 在"画布"页面上、选择工作环境。
2. 在概述选项卡上、单击功能面板、然后单击*虚拟机类型*旁边的铅笔图标。



a. 如果您使用的是基于节点的PAYGO许可证、则可以选择通过单击*许可证类型*旁边的铅笔图标来选择其他许可证和VM类型。

3. 选择VM类型、选中复选框以确认您了解更改的含义、然后单击*更改*。

结果

Cloud Volumes ONTAP 会使用新配置重新启动。

覆盖Azure中Cloud Volumes ONTAP HA对的CIFS锁定

帐户管理员可以在BlueXP中启用一项设置、以防止在Azure维护事件期间出现Cloud Volumes ONTAP 存储交还问题。启用此设置后， Cloud Volumes ONTAP 将否决 CIFS 锁定并重置活动 CIFS 会话。

关于此任务

Microsoft Azure 会在其虚拟机上计划定期维护事件。在 Cloud Volumes ONTAP HA 对上发生维护事件时， HA 对将启动存储接管。如果在此维护事件期间存在活动的 CIFS 会话，则锁定 CIFS 文件可能会阻止存储交还。

如果启用此设置， Cloud Volumes ONTAP 将否决锁定并重置活动的 CIFS 会话。因此， HA 对可以在这些维护事件期间完成存储交还。

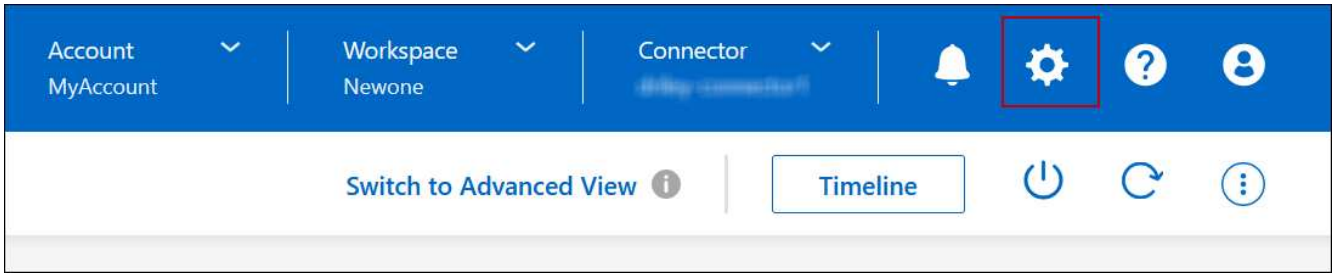
此过程可能会对 CIFS 客户端造成中断。未从 CIFS 客户端提交的数据可能会丢失。

您需要的内容

您需要先创建Connector、然后才能更改BlueXP设置。 "了解如何操作"。

步骤

1. 在BlueXP控制台的右上角，单击设置图标，然后选择*BlueXP Cloud Volumes ONTAP设置*。



2. 在 * Azure * 下，单击 * 适用于 Azure HA 工作环境的 Azure CIFS 锁定 * 。
3. 单击复选框以启用此功能，然后单击 * 保存 * 。

使用Azure专用链路或服务端点

Cloud Volumes ONTAP 使用Azure专用链路连接到其关联的存储帐户。如果需要、您可以禁用Azure专用链路、而改用服务端点。

概述

默认情况下、BlueXP会为Cloud Volumes ONTAP 与其关联存储帐户之间的连接启用Azure专用链路。Azure Private Link可确保Azure中端点之间的连接安全、并可提供性能优势。

如果需要、您可以将Cloud Volumes ONTAP 配置为使用服务端点、而不是Azure专用链路。

无论采用哪种配置、BlueXP都会始终限制Cloud Volumes ONTAP 与存储帐户之间的连接的网络访问。网络访问仅限于部署了Cloud Volumes ONTAP 的vNet和部署了连接器的vNet。

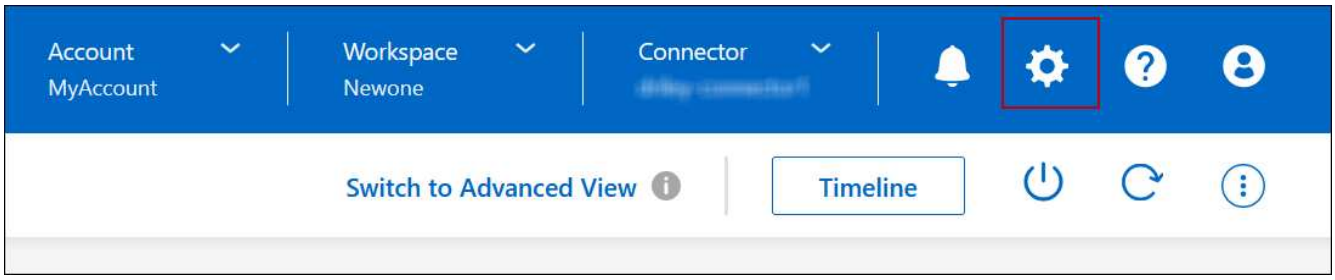
请禁用Azure专用链路并改用服务端点

如果您的企业需要、您可以更改BlueXP中的设置、以便将Cloud Volumes ONTAP 配置为使用服务端点、而不是Azure专用链路。更改此设置将适用场景 添加您创建的新Cloud Volumes ONTAP 系统。仅支持服务端点 "Azure区域对" 在连接器和Cloud Volumes ONTAP VNets之间。

此连接器应部署在与其管理的 Cloud Volumes ONTAP 系统所在的同一 Azure 区域或中 "Azure 区域对" 对于 Cloud Volumes ONTAP 系统。

步骤

1. 在BlueXP控制台的右上角，单击设置图标，然后选择*BlueXP Cloud Volumes ONTAP设置*。



2. 在 * Azure * 下，单击 * 使用 Azure 专用链接 * 。
3. 取消选择 * Cloud Volumes ONTAP 与存储帐户之间的专用链路连接 * 。
4. 单击 * 保存 * 。

完成后

如果禁用了Azure专用链路、并且Connector使用代理服务器、则必须启用直接API流量。

"了解如何在Connector上启用直接API流量"

使用Azure专用链路

在大多数情况下、您无需执行任何操作即可使用Cloud Volumes ONTAP 设置Azure专用链路。BlueXP为您管理Azure专用链路。但是、如果您使用现有Azure私有DNS区域、则需要编辑配置文件。

自定义DNS的要求

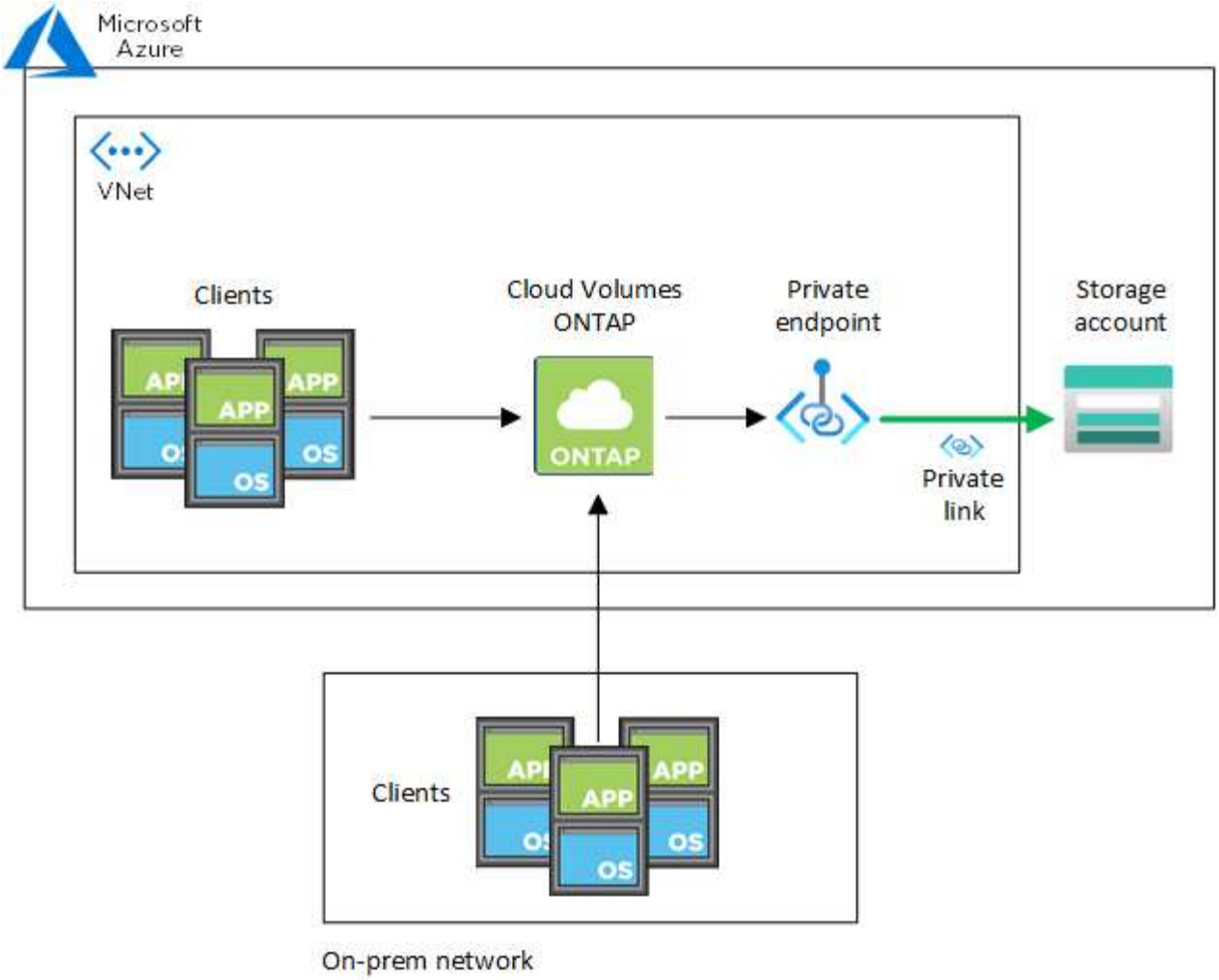
或者、如果您使用自定义DNS、则需要从自定义DNS服务器创建一个条件转发器来访问Azure专用DNS区域。要了解更多信息、请参见 "Azure有关使用DNS转发器的文档"。

专用链路连接的工作原理

当BlueXP在Azure中部署Cloud Volumes ONTAP 时、它会在资源组中创建一个私有端点。专用端点与Cloud Volumes ONTAP 的存储帐户关联。因此，对 Cloud Volumes ONTAP 存储的访问会通过 Microsoft 主干网络进行。

如果客户端与 Cloud Volumes ONTAP 位于同一个 vNet 中，位于对等 VNets 中，或者使用专用 VPN 或 ExpressRoute 连接到 VNet ，则客户端访问将通过专用链路进行。

以下示例显示了客户端通过同一个 vNet 中的专用链路以及具有专用 VPN 或 ExpressRoute 连接的内部网络进行访问的情况。



如果连接器和Cloud Volumes ONTAP 系统部署在不同的VN中、则必须在部署连接器的vNet与部署Cloud Volumes ONTAP 系统的vNet之间设置vNet对等关系。

向**BlueXP**提供有关**Azure**私有**DNS**的详细信息

如果您使用 "Azure 专用 DNS"，然后您需要修改每个 Connector 上的配置文件。否则、BlueXP无法在Cloud Volumes ONTAP 与其关联存储帐户之间启用Azure专用链路连接。

请注意， DNS 名称必须与 Azure DNS 命名要求匹配 "如 Azure 文档中所示"。

步骤

1. 通过 SSH 连接到 Connector 主机并登录。
2. 导航到以下目录： /opt/application/netapp/cloudmanager/docker_occm/data
3. 通过使用以下关键字值对添加"user-private-dns-zone-settings"参数来编辑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
}
```

应在与"system-id"相同的级别输入参数、如下所示：

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

请注意、只有当专用DNS区域与Connector订阅不同时、才需要使用subscription关键字。

4. 保存文件并注销 Connector 。

   不需要重新启动。

启用故障回滚

如果在特定操作中、BlueXP无法创建Azure专用链路、则它将在没有Azure专用链路连接的情况下完成此操作。在创建新的工作环境（单节点或 HA 对）或对 HA 对执行以下操作时，可能会发生这种情况：创建新聚合，向现有聚合添加磁盘或在超过 32 TiB 时创建新存储帐户。

如果BlueXP无法创建Azure专用链路、您可以通过启用回滚来更改此默认行为。这有助于确保您完全符合公司的安全法规。

如果启用回滚、则BlueXP将停止此操作并回滚此操作中创建的所有资源。

您可以通过API或更新app.conf文件启用回滚。

*通过APi*启用回滚

步骤

1. 使用 `put /occm/config` API 调用与以下请求正文：

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

*通过更新app.conf启用回滚

步骤

1. 通过 SSH 连接到 Connector 主机并登录。
2. 导航到以下目录： /opt/application/netapp/cloudmanager/docker_occm/data
3. 通过添加以下参数和值来编辑app.conf：

```
 "rollback-on-private-link-failure": true
. 保存文件并注销 Connector 。
```

不需要重新启动。

移动资源组

Cloud Volumes ONTAP 支持Azure资源组移动、但工作流仅在Azure控制台中执行。

您可以在同一Azure订阅中将工作环境从一个资源组移动到Azure中的其他资源组。不支持在不同Azure订阅之间移动资源组。

步骤

1. 从*画布*中删除工作环境。

   要了解如何删除工作环境，请参见"删除 Cloud Volumes ONTAP 工作环境"。

2. 在Azure控制台中执行资源组移动。

   要完成移动、请参见 "将资源移动到Microsoft Azure文档中的新资源组或订阅"。

3. 在*画布*中、了解工作环境。
4. 在工作环境信息中查找新资源组。

结果

工作环境及其资源(VM、磁盘、存储帐户、网络接口、快照)位于新资源组中。

在Azure中隔离SnapMirror流量

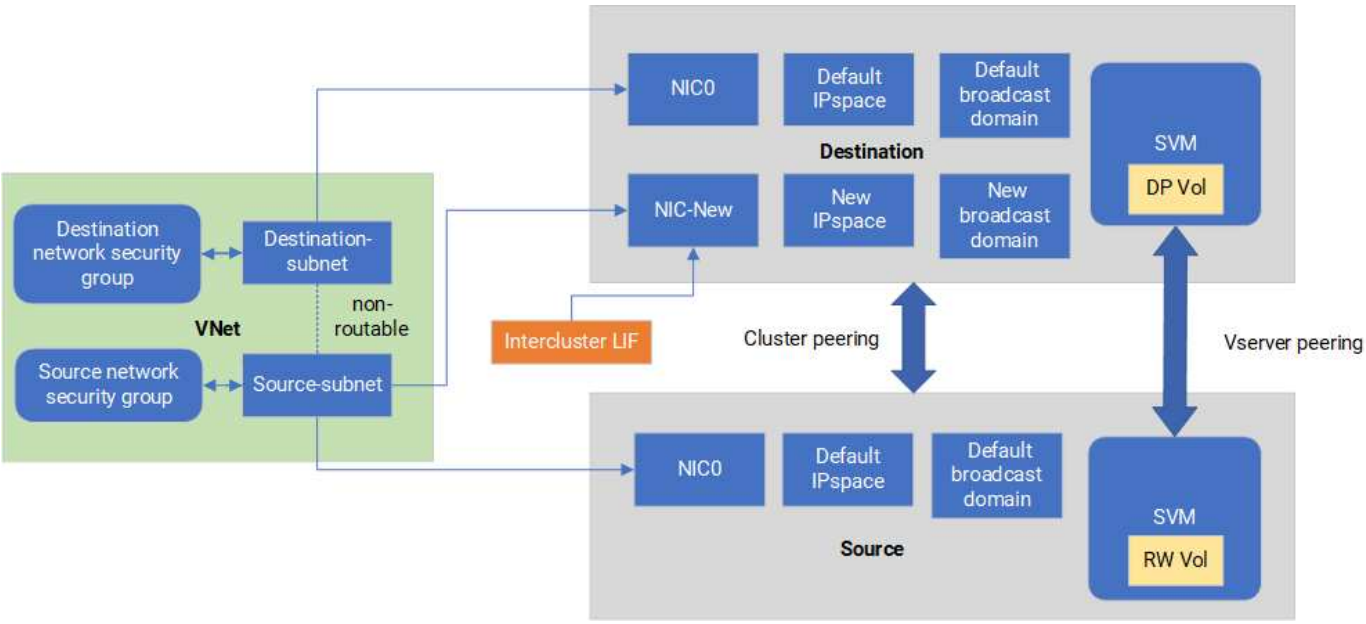
借助Azure中的Cloud Volumes ONTAP、您可以将SnapMirror复制流量与数据和管理流量隔离。要将SnapMirror复制流量与数据流量隔离、您需要添加一个新的网络接口卡(Network Interface Card、NIC)、一个关联的集群间LIF和一个不可路由的子网。

关于Azure中的SnapMirror流量隔离

默认情况下、BlueXP会在同一子网上配置Cloud Volumes ONTAP部署中的所有NIC和LUN。在此类配置中、SnapMirror复制流量以及数据和管理流量使用同一子网。隔离SnapMirror流量会利用一个不可路由到用于数据和管理流量的现有子网的额外子网。

图**1.**

下图显示了在单节点部署中使用附加NIC、关联的集群间LIF和不可路由子网隔离SnapMirror复制流量的情况。HA对部署略有不同。



开始之前

请查看以下注意事项：

- 您只能将一个NIC添加到Cloud Volumes ONTAP单节点或HA对部署(VM实例)中、以实现SnapMirror流量隔离。
- 要添加新的NIC、您部署的VM实例类型必须具有未使用的NIC。
- 源集群和目标集群应能够访问同一个虚拟网络(vNet)。目标集群是Azure中的Cloud Volumes ONTAP系统。源集群可以是Azure中的Cloud Volumes ONTAP系统、也可以是ONTAP系统。

第1步：创建一个额外的NIC并连接到目标虚拟机

本节介绍如何创建其他NIC并将其连接到目标VM。目标VM是Azure中Cloud Volumes ONTAP中要设置其他NIC的单节点或HA对系统。

步骤

1. 在ONTAP命令行界面中、停止节点。

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

2. 在Azure门户中、检查虚拟机(节点)状态是否为已停止。

```
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环境停止节点。
   a. 停止节点。

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

b. 取消分配此节点。

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

4. 配置网络安全组规则、使两个子网(源集群子网和目标集群子网)不可相互路由。
   a. 在目标虚拟机上创建新的NIC。
   b. 查找源集群子网的子网ID。

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

   c. 在目标VM上使用源集群子网的子网ID创建新NIC。在此输入新NIC的名称。

```
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privateIPAddress。此IP地址<new_added_nic_primary_addr>用于在中创建集群间LIF 广播域、新NIC的集群间LIF。
5. 将新的NIC连接到虚拟机。

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

6. 启动虚拟机(节点)。

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

7. 在Azure门户中，转至*Networking*并确认新的NIC (例如NIC-NEW)已存在，并且已启用加速网络。

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

对于HA对部署、请对配对节点重复上述步骤。

第2步：为新NIC创建新的IP空间、广播域和集群间LIF

集群间的独立IP空间可在各个网络功能之间实现逻辑隔离、以便在集群之间进行复制。

使用ONTAP命令行界面执行以下步骤。

步骤

1. 创建新的IP空间(new_ipspace)。

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

2. 在新IP空间(new_ipspace)上创建广播域并添加NIC新端口。

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

3. 对于单节点系统、新添加的端口为_e0b_。对于使用受管磁盘的HA对部署、新添加的端口为_e0d_。对于使用页面Blobs的HA对部署、新添加的端口为_e0e_。请使用节点名称、而不是VM名称。通过运行查找节点名称 `node show`。

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

4. 在新广播域(new_bd)和新NIC (nic-new)上创建集群间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. 验证是否已创建新的集群间LIF。

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

对于HA对部署、请对配对节点重复上述步骤。

第3步：验证源系统和目标系统之间的集群对等关系

本节介绍如何验证源系统与目标系统之间的对等关系。

使用ONTAP命令行界面执行以下步骤。

步骤

1. 验证目标集群的集群间LIF是否可以对源集群的集群间LIF执行ping操作。由于目标集群会执行此命令、因此目标IP地址是源上的集群间LIF IP地址。

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

2. 验证源集群的集群间LIF是否可以对目标集群的集群间LIF执行ping操作。目标是在目标上创建的新NIC的IP地址。

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

对于HA对部署、请对配对节点重复上述步骤。

第4步：在源系统和目标系统之间创建SVM对等关系

本节介绍如何在源系统和目标系统之间创建SVM对等关系。

使用ONTAP命令行界面执行以下步骤。

步骤

1. 使用源集群间LIF IP地址作为在目标上创建集群对等关系 `-peer-addrs`。对于HA对、将两个节点的源集群间LIF IP地址列为 `-peer-addrs`。

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

2. 输入并确认密码短语。
3. 使用目标集群LIF IP地址作为在源上创建集群对等关系 `peer-addrs`。对于HA对、将两个节点的目标集群间LIF IP地址列为 `-peer-addrs`。

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

4. 输入并确认密码短语。
5. 检查集群是否已建立对等状态。

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

成功建立对等关系后、可用性字段中会显示*可用*。

6. 在目标上创建SVM对等关系。源和目标SVM均应为数据SVM。

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

7. 接受SVM对等。

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

8. 检查SVM是否已对等。

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

对等状态显示 **peered***和对等应用程序显示 ***snapmirror**

第5步：在源系统和目标系统之间创建SnapMirror复制关系

本节介绍如何在源系统和目标系统之间创建SnapMirror复制关系。

要移动现有SnapMirror复制关系、必须先中断现有SnapMirror复制关系、然后再创建新的SnapMirror复制关系。

使用ONTAP命令行界面执行以下步骤。

步骤

1. 在目标SVM上创建受数据保护的卷。

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

2. 在目标上创建SnapMirror复制关系、其中包括用于复制的SnapMirror策略和计划。

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

3. 初始化目标上的SnapMirror复制关系。

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

4. 在ONTAP命令行界面中、运行以下命令以验证SnapMirror关系状态：

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

关系状态为 `Snapmirrored` 关系的运行状况为 `true`。

5. 可选：在ONTAP命令行界面中、运行以下命令以查看SnapMirror关系的操作历史记录。

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

您也可以挂载源卷和目标卷、向源写入文件、并验证卷是否正在复制到目标。