Azure 管理

Cloud Volumes ONTAP

NetApp
February 13, 2026

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太小或太大，无法满足您的需求，您可以随时更改虚拟机类型。

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）。如果不是，则操作将失败。

  "ONTAP 9 文档：用于配置自动交还的命令"

- 更改 VM 类型可能会影响 Microsoft Azure 服务费用。
- 该操作重新启动Cloud Volumes ONTAP。

  对于单节点系统，I/O 被中断。

  对于 HA 对来说，这种变化是无中断的。 HA 对继续提供数据。

NetApp Console通过启动接管并等待返回来一次更改一个节点。 NetApp 的质量保证团队在此过程中对文件的写入和读取进行了测试，并且没有发现客户端的任何问题。随着连接的变化，在 I/O 级别观察到一些重试，但应用层克服了 NFS/CIFS 连接的重新连接。

步骤

1. 在*系统*页面上，选择系统。
2. 在“概述”选项卡上，单击“功能”面板，然后单击“**VM** 类型”旁边的铅笔图标。

   如果您使用的是基于节点的即用即付 (PAYGO) 许可证，则可以通过单击“许可证类型”旁边的铅笔图标来选择不同的许可证和 VM 类型。

3. 选择一种 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使用新配置重新启动。

覆盖 Azure 中Cloud Volumes ONTAP HA 对的 CIFS 锁

组织或帐户管理员可以在NetApp Console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 锁定并重置活动的 CIFS 会话。

关于此任务

Microsoft Azure 会安排其虚拟机的定期维护事件。当Cloud Volumes ONTAP HA 对上发生维护事件时，HA 对会启动存储接管。如果在此维护事件期间有活动的 CIFS 会话，则 CIFS 文件上的锁定可能会阻止存储恢复。

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。

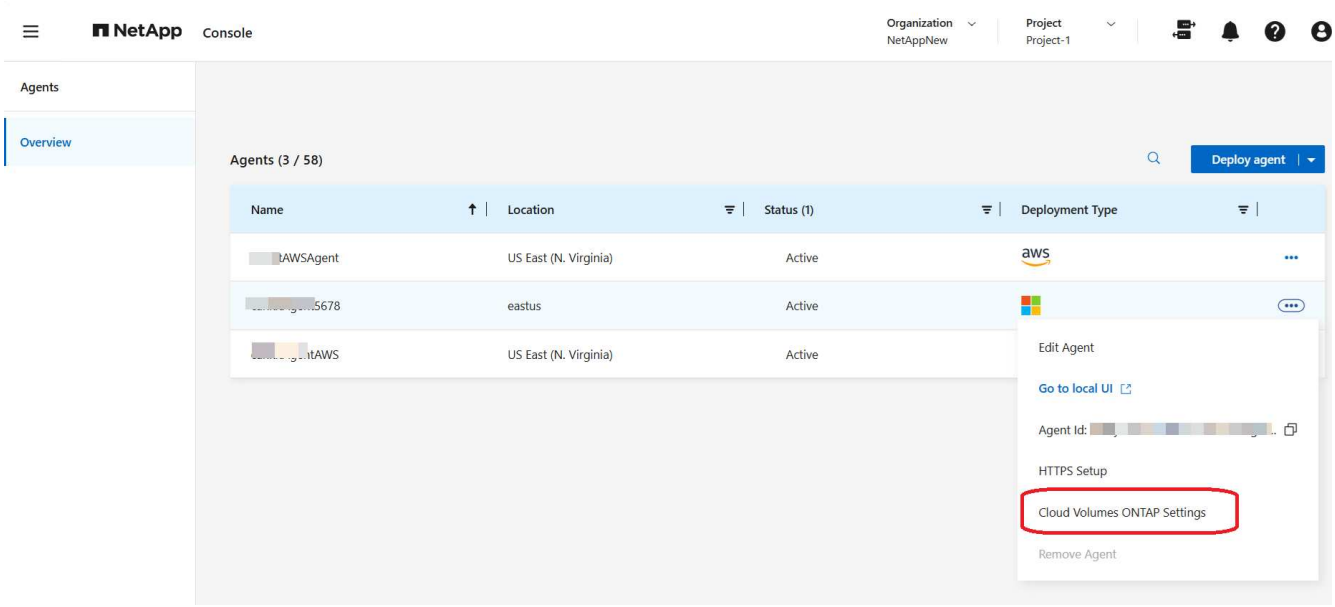
此过程可能会对 CIFS 客户端造成破坏。 CIFS 客户端未提交的数据可能会丢失。

开始之前

您需要先创建控制台代理，然后才能更改控制台设置。 "了解详情" 。

步骤

1. 从左侧导航窗格转到*管理>代理*。
2. 点击 ••• 管理Cloud Volumes ONTAP系统的控制台代理的图标。
3. 选择* Cloud Volumes ONTAP设置*。



4. 在“Azure”下，单击“Azure HA 系统的 Azure CIFS 锁”。
5. 单击复选框以启用该功能，然后单击“保存”。

为Cloud Volumes ONTAP系统使用 Azure Private Link 或服务端点

Cloud Volumes ONTAP使用 Azure Private Link 连接到其关联的存储帐户。如果需要，您可以禁用 Azure Private Links 并改用服务端点。

概述

默认情况下， NetApp Console启用 Azure Private Link 来建立Cloud Volumes ONTAP与其关联存储帐户之间的连接。 Azure 专用链接可保护 Azure 中端点之间的连接并提供性能优势。

如果需要，您可以将Cloud Volumes ONTAP配置为使用服务端点而不是 Azure Private Link。

无论采用哪种配置，控制台始终限制Cloud Volumes ONTAP和存储帐户之间的连接的网络访问。网络访问仅限

于部署Cloud Volumes ONTAP 的VNet 和部署控制台代理的 VNet。

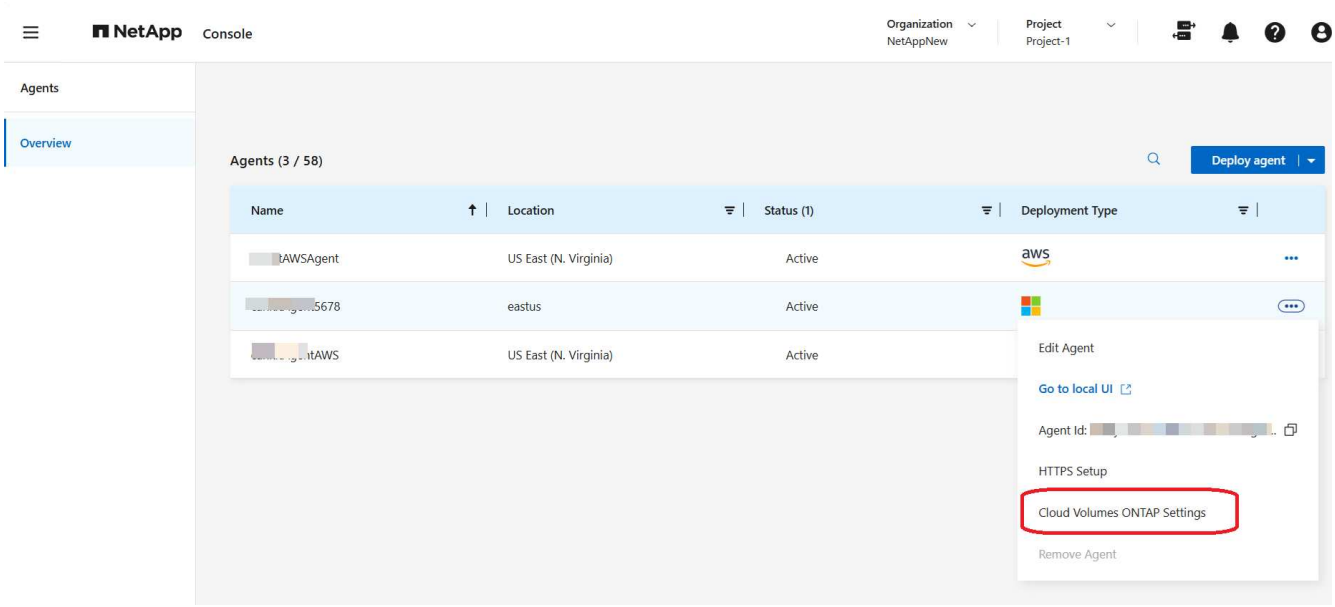
禁用 **Azure Private Links** 并改用服务终结点

如果您的业务需要，您可以在控制台中更改设置，以便将Cloud Volumes ONTAP配置为使用服务端点而不是 Azure Private Link。更改此设置适用于您创建的新Cloud Volumes ONTAP系统。服务端点仅支持"Azure 区域对"控制台代理和Cloud Volumes ONTAP VNet 之间。

控制台代理应部署在与其管理的Cloud Volumes ONTAP系统相同的 Azure 区域中，或者部署在 "Azure 区域对"适用于Cloud Volumes ONTAP系统。

步骤

1. 从左侧导航窗格转到*管理>代理*。
2. 点击 ••• 管理Cloud Volumes ONTAP系统的控制台代理的图标。
3. 选择* Cloud Volumes ONTAP设置*。



4. 在“**Azure**”下，单击“使用 **Azure** 专用链接”。
5. 取消选择* Cloud Volumes ONTAP和存储帐户之间的专用链接连接*。
6. 单击“保存”。

完成后

如果您禁用了 Azure Private Links 并且控制台代理使用代理服务器，则必须启用直接 API 流量。

"了解如何在控制台代理上启用直接 API 流量"

使用 **Azure Private Links**

在大多数情况下，您无需执行任何操作即可设置与Cloud Volumes ONTAP 的Azure Private 链接。控制台为您管理 Azure 专用链接。但是如果您使用现有的 Azure 私有 DNS 区域，则需要编辑配置文件。

自定义 **DNS** 的要求

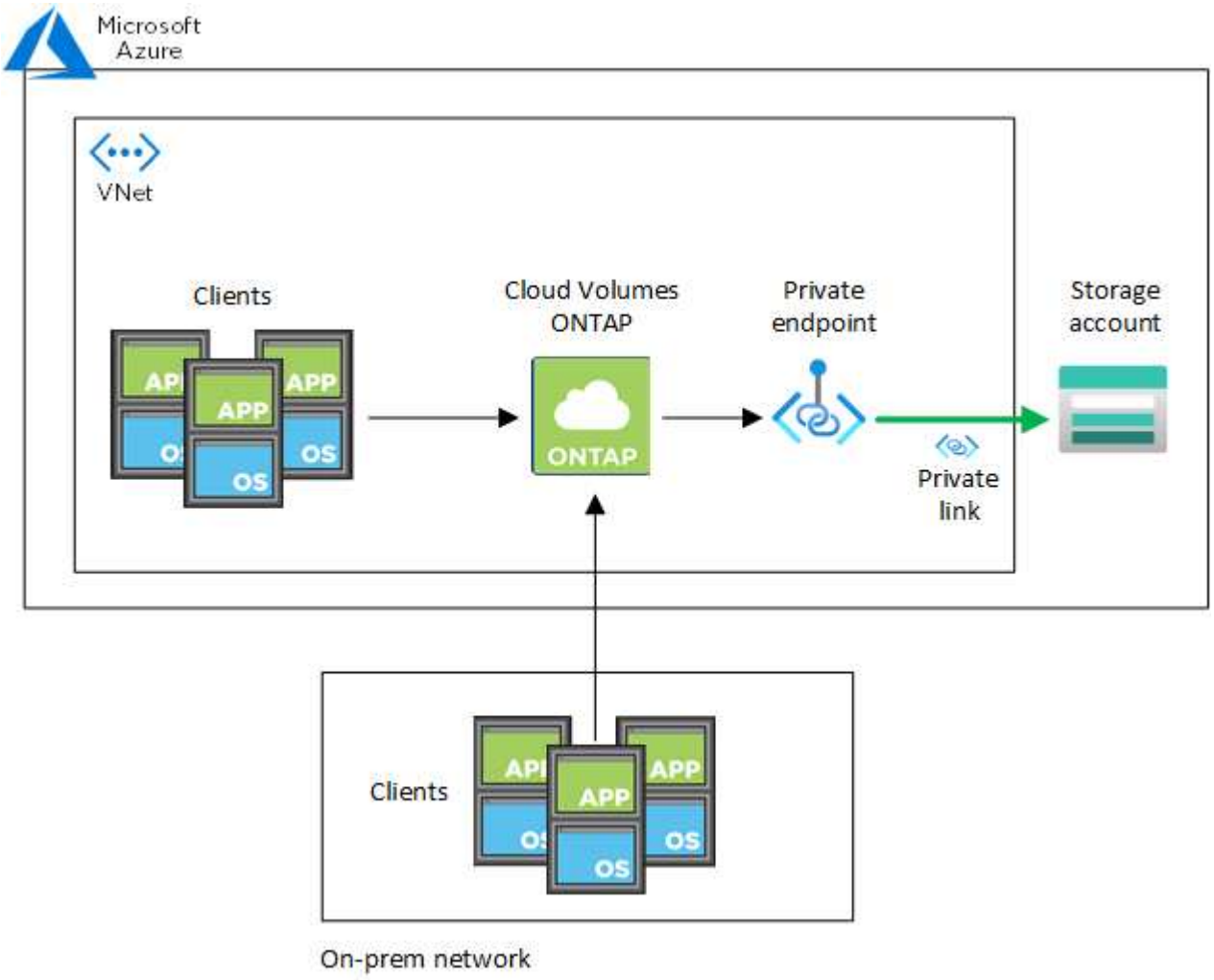
或者，如果您使用自定义 DNS，则需要从自定义 DNS 服务器创建到 Azure 私有 DNS 区域的条件转发器。要了解更多信息，请参阅"Azure 关于使用 DNS 转发器的文档"。

专用链接连接的工作原理

当控制台在 Azure 中部署Cloud Volumes ONTAP时，它会在资源组中创建一个私有端点。私有端点与Cloud Volumes ONTAP 的存储帐户相关联。因此，对Cloud Volumes ONTAP存储的访问需要通过 Microsoft 主干网络。

当客户端与Cloud Volumes ONTAP位于同一 VNet 内、位于对等 VNet 内或位于本地网络中时，客户端访问将通过专用链接进行。

以下示例展示了客户端如何通过专用链接从同一 VNet 内部以及从具有专用 VPN 或 ExpressRoute 连接的本地网络进行访问。



如果控制台代理和Cloud Volumes ONTAP系统部署在不同的 VNet 中，则必须在部署控制台代理的 VNet 和部署Cloud Volumes ONTAP系统的 VNet 之间设置 VNet 对等连接。

提供有关 **Azure** 专用 **DNS** 的详细信息

如果你使用 "Azure 专用 DNS"，那么就需要在每个Console代理上修改一个配置文件。否则，控制台无法设置Cloud Volumes ONTAP与其关联存储帐户之间的 Azure Private Link 连接。

请注意，DNS 名称必须符合 Azure DNS 命名要求 "如 Azure 文档所示"。

步骤

1. 通过 SSH 连接到控制台代理主机并登录。
2. 导航至 `/opt/application/netapp/cloudmanager/docker_occm/data`目录。
3. 编辑 `app.conf`通过添加 `user-private-dns-zone-settings`具有以下关键字-值对的参数：

```
"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
}
```

这 `subscription`仅当私有 DNS 区域与控制台代理的订阅不同时才需要关键字。

4. 保存文件并注销控制台代理。

不需要重新启动。

启用故障回滚

如果控制台无法在特定操作中创建 Azure 专用链接，它将在没有 Azure 专用链接连接的情况下完成该操作。创建新系统（单个节点或 HA 对）时，或者在 HA 对上执行以下操作时，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 时创建新的存储帐户。

如果控制台无法创建 Azure 专用链接，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遵守公司的安全规定。

如果启用回滚，控制台将停止该操作并回滚作为该操作的一部分创建的所有资源。

您可以通过 API 或更新 app.conf 文件来启用回滚。

通过 **API** 启用回滚

步骤

1. 使用 `PUT /occm/config`具有以下请求主体的 API 调用：

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

通过更新 **app.conf** 启用回滚

步骤

1. 通过 SSH 连接到控制台代理的主机并登录。
2. 导航到以下目录：/opt/application/netapp/cloudmanager/docker_occm/data
3. 编辑 app.conf，添加以下参数和值：

```
 "rollback-on-private-link-failure": true
. 保存文件并注销控制台代理。
```

不需要重新启动。

在 Azure 控制台中移动Cloud Volumes ONTAP的 Azure 资源组

Cloud Volumes ONTAP支持 Azure 资源组移动，但工作流程仅在 Azure 控制台中进行。

您可以将Cloud Volumes ONTAP系统从同一 Azure 订阅内的一个资源组移动到 Azure 中的另一个资源组。不支持在不同的 Azure 订阅之间移动资源组。

步骤

1. 删除Cloud Volumes ONTAP系统。请参阅"删除Cloud Volumes ONTAP系统" 。
2. 在 Azure 控制台中执行资源组移动。

   要完成移动，请参阅"Microsoft Azure 文档中的“将资源移动到新的资源组或订阅”"。

3. 在*系统*页面上，发现系统。
4. 在系统信息中查找新的资源组。

结果

系统及其资源（虚拟机、磁盘、存储帐户、网络接口、快照）位于新的资源组中。

在 Azure 中隔离SnapMirror流量

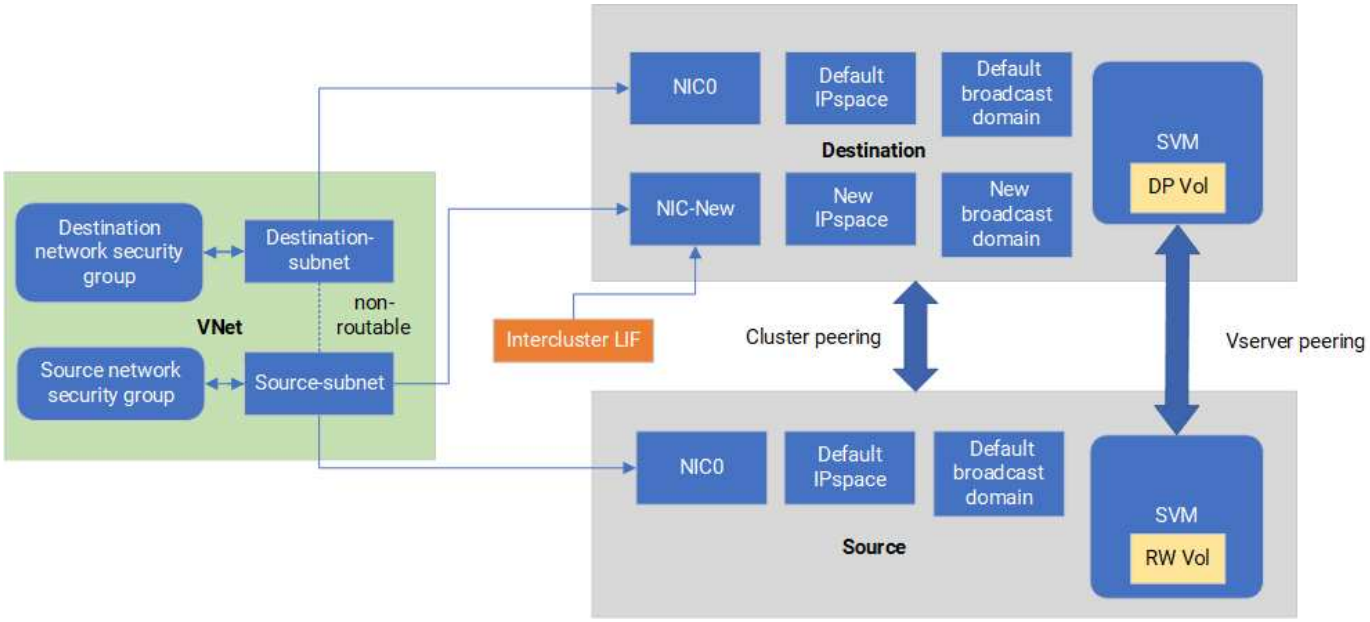
使用 Azure 中的Cloud Volumes ONTAP ，您可以将SnapMirror复制流量与数据和管理流量分离。为了将SnapMirror复制流量与数据流量隔离，您需要添加一个新的网络接口卡 (NIC)、一个相关的集群间 LIF 和一个不可路由的子网。

关于 Azure 中的SnapMirror流量隔离

默认情况下， NetApp Console会在同一子网上配置Cloud Volumes ONTAP部署中的所有 NIC 和 LIF。在这样的配置中， SnapMirror复制流量和数据和管理流量使用相同的子网。隔离SnapMirror流量利用了无法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 和不可路由子网对SnapMirror复制流量进行隔离。HA 对部署略有不同。



开始之前

回顾以下注意事项：

- 您只能向Cloud Volumes ONTAP单节点或 HA 对部署（VM 实例）添加单个 NIC 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该可以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系统或ONTAP系统。

步骤 1：创建额外的 NIC 并连接到目标 VM

本节提供有关如何创建附加 NIC 并将其附加到目标 VM 的说明。目标 VM 是 Azure 中Cloud Volumes ONTAP中的单节点或 HA 对系统，您要在其中设置额外的 NIC。

步骤

1. 在ONTAP CLI 中，停止节点。

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

2. 在 Azure 门户中，检查 VM（节点）状态是否已停止。

```
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 环境停止节点。
   a. 停止节点。

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

b. 解除分配节点。

```
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）互不可达。
   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. 使用源集群子网的子网 ID 在目标虚拟机上创建新的 NIC。在这里输入新 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. 保存私有IP地址。此 IP 地址 <new_added_nic_primary_addr> 用于在广播域，新 NIC 的集群间 LIF。
5. 将新的 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. 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，转到 网络 并确认新的 NIC（例如 nic-new）存在并且加速网络已启用。

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

对于 HA 对部署，请对合作伙伴节点重复这些步骤。

步骤 2：为新 NIC 创建新的 IP 空间、广播域和集群间 LIF

集群间 LIF 的单独 IP 空间为集群间复制的网络功能提供了逻辑分离。

使用ONTAP CLI 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. 在新的 IP 空间（new_ipspace）上创建一个广播域并添加 nic-new 端口。

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

3. 对于单节点系统，新添加的端口为 *e0b*。对于具有托管磁盘的 HA 对部署，新添加的端口为 *e0d*。对于具有页面 blob 的 HA 对部署，新添加的端口为 *e0e*。使用节点名称而不是 VM 名称。通过运行 `node show`查找节点名称。

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

4. 在新的广播域 (new_bd) 和新的 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. 验证新的集群间 LIF 的创建。

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

对于 HA 对部署，请对合作伙伴节点重复这些步骤。

步骤 3：验证源系统和目标系统之间的集群对等连接

本节提供有关如何验证源系统和目标系统之间的对等关系的说明。

使用ONTAP CLI 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 ping 通目标集群的集群间 LIF。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，请对合作伙伴节点重复这些步骤。

步骤 4：在源系统和目标系统之间创建 SVM 对等连接

本节提供有关如何在源系统和目标系统之间创建 SVM 对等的说明。

使用ONTAP CLI 执行以下步骤。

步骤

1. 使用源集群间 LIF IP 地址作为目标在目标上创建集群对等 `-peer-addrs`。对于 HA 对，列出两个节点的源集群间 LIF IP 地址作为 `-peer-addrs`。

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

2. 输入并确认密码。
3. 使用目标集群 LIF IP 地址作为源集群的 IP 地址，在源上创建集群对等连接 `peer-addrs`。对于 HA 对，列出两个节点的目标集群间 LIF IP 地址作为 `-peer-addrs`。

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

4. 输入并确认密码。
5. 检查集群是否对等。

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

成功的对等连接在可用性字段中显示 可用。

6. 在目标上创建 SVM 对等连接。源 SVM 和目标 SVM 都应该是数据 SVM。

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

7. 接受 SVM 对等连接。

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

8. 检查 SVM 是否已对等。

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

同行国家显示*peered* 和对等应用程序显示*snapmirror*.

步骤 5：在源系统和目标系统之间创建SnapMirror复制关系

本节提供有关如何在源系统和目标系统之间创建SnapMirror复制关系的说明。

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

使用ONTAP CLI 执行以下步骤。

步骤

1. 在目标 SVM 上创建数据保护卷。

```
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. 在目标上初始化SnapMirror复制关系。

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

4. 在ONTAP CLI 中，通过运行以下命令验证SnapMirror关系状态：

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

关系状态是 `Snapmirrored`关系的健康是 `true`。

5. 可选：在ONTAP CLI 中，运行以下命令查看SnapMirror关系的操作历史记录。

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

或者，您可以挂载源卷和目标卷，将文件写入源卷，并验证卷是否复制到目标卷。

版权信息

商标信息