Administração do Azure

Cloud Volumes ONTAP

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/pt-br/storage-management-cloud-volumes-ontap/task-change-azure-vm.html on February 13, 2026. Always check docs.netapp.com for the latest.

Índice

Administração do Azure

Alterar o tipo de VM do Azure para Cloud Volumes ONTAP

Você pode escolher entre vários tipos de VM ao iniciar o Cloud Volumes ONTAP no Microsoft Azure. Você pode alterar o tipo de VM a qualquer momento se determinar que ela é subdimensionada ou superdimensionada para suas necessidades.

Sobre esta tarefa

- O retorno automático deve ser habilitado em um par de Cloud Volumes ONTAP HA (esta é a configuração padrão). Caso contrário, a operação falhará.

  "Documentação do ONTAP 9: Comandos para configurar o retorno automático"

- Alterar o tipo de VM pode afetar as taxas de serviço do Microsoft Azure.
- A operação reinicia o Cloud Volumes ONTAP.

  Para sistemas de nó único, a entrada/saída é interrompida.

  Para pares HA, a mudança não é disruptiva. Os pares HA continuam a fornecer dados.

  O NetApp Console altera um nó por vez, iniciando a aquisição e aguardando o retorno. A equipe de Garantia de Qualidade da NetApp testou a gravação e a leitura de arquivos durante esse processo e não observou nenhum problema no lado do cliente. Conforme as conexões mudavam, algumas tentativas eram observadas no nível de E/S, mas a camada de aplicação superou a reconfiguração das conexões NFS/CIFS.

Passos

1. Na página **Sistemas**, selecione o sistema.
2. Na guia Visão geral, clique no painel Recursos e, em seguida, clique no ícone de lápis ao lado de **Tipo de VM**.

   Se você estiver usando uma licença de pagamento conforme o uso (PAYGO) baseada em nó, poderá escolher uma licença e um tipo de VM diferentes clicando no ícone de lápis ao lado de **Tipo de licença**.

3. Selecione um tipo de VM, marque a caixa de seleção para confirmar que você entende as implicações da alteração e clique em **Alterar**.

Resultado

O Cloud Volumes ONTAP é reinicializado com a nova configuração.

Substituir bloqueios CIFS para pares de alta disponibilidade do Cloud Volumes ONTAP no Azure

O administrador da organização ou da conta pode habilitar uma configuração no NetApp Console que evita problemas com o retorno do armazenamento Cloud Volumes ONTAP durante eventos de manutenção do Azure. Quando você habilita essa configuração, o Cloud Volumes ONTAP veta bloqueios CIFS e redefine sessões CIFS ativas.

Sobre esta tarefa

O Microsoft Azure agenda eventos de manutenção periódicos em suas máquinas virtuais. Quando ocorre um evento de manutenção em um par de HA do Cloud Volumes ONTAP , o par de HA inicia a aquisição do armazenamento. Se houver sessões CIFS ativas durante este evento de manutenção, os bloqueios nos arquivos CIFS podem impedir o retorno do armazenamento.

Se você habilitar essa configuração, o Cloud Volumes ONTAP vetará os bloqueios e redefinirá as sessões CIFS ativas. Como resultado, o par HA pode concluir a devolução do armazenamento durante esses eventos de manutenção.

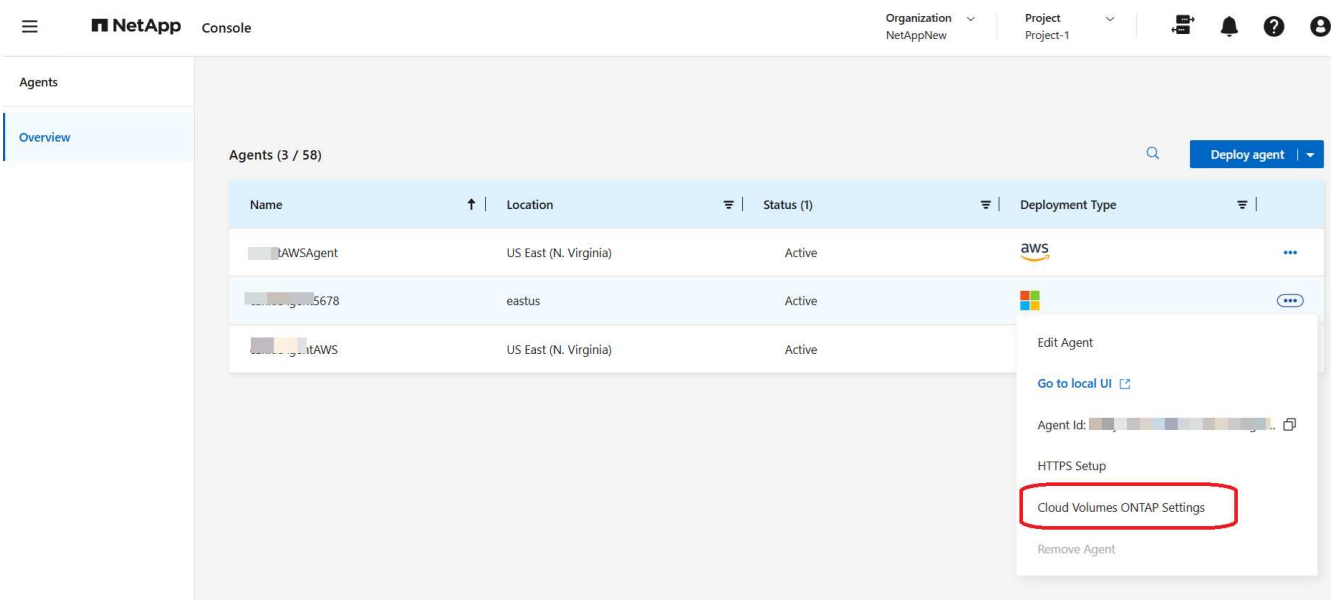
Esse processo pode ser prejudicial aos clientes do CIFS. Dados não confirmados de clientes CIFS podem ser perdidos.

Antes de começar

Você precisa criar um agente do Console antes de poder alterar as configurações do Console. "Aprenda como" .

Passos

1. No painel de navegação esquerdo, acesse **Administração > Agentes**.
2. Clique no ícone para o agente do Console que gerencia seu sistema Cloud Volumes ONTAP .
3. Selecione * Configurações do Cloud Volumes ONTAP *.



4. Em **Azure**, clique em **Bloqueios CIFS do Azure para sistemas HA do Azure**.
5. Clique na caixa de seleção para habilitar o recurso e depois clique em **Salvar**.

Use um Azure Private Link ou pontos de extremidade de serviço para sistemas Cloud Volumes ONTAP

O Cloud Volumes ONTAP usa um Azure Private Link para conexões com suas contas de armazenamento associadas. Se necessário, você pode desabilitar os Links Privados do Azure e usar pontos de extremidade de serviço.

Visão geral

Por padrão, o NetApp Console habilita um Azure Private Link para conexões entre o Cloud Volumes ONTAP e suas contas de armazenamento associadas. Um Link Privado do Azure protege conexões entre pontos de extremidade no Azure e oferece benefícios de desempenho.

Se necessário, você pode configurar o Cloud Volumes ONTAP para usar pontos de extremidade de serviço em vez de um Link Privado do Azure.

Com qualquer configuração, o Console sempre limita o acesso à rede para conexões entre o Cloud Volumes ONTAP e contas de armazenamento. O acesso à rede é limitado à VNet onde o Cloud Volumes ONTAP está implantado e à VNet onde o agente do Console está implantado.

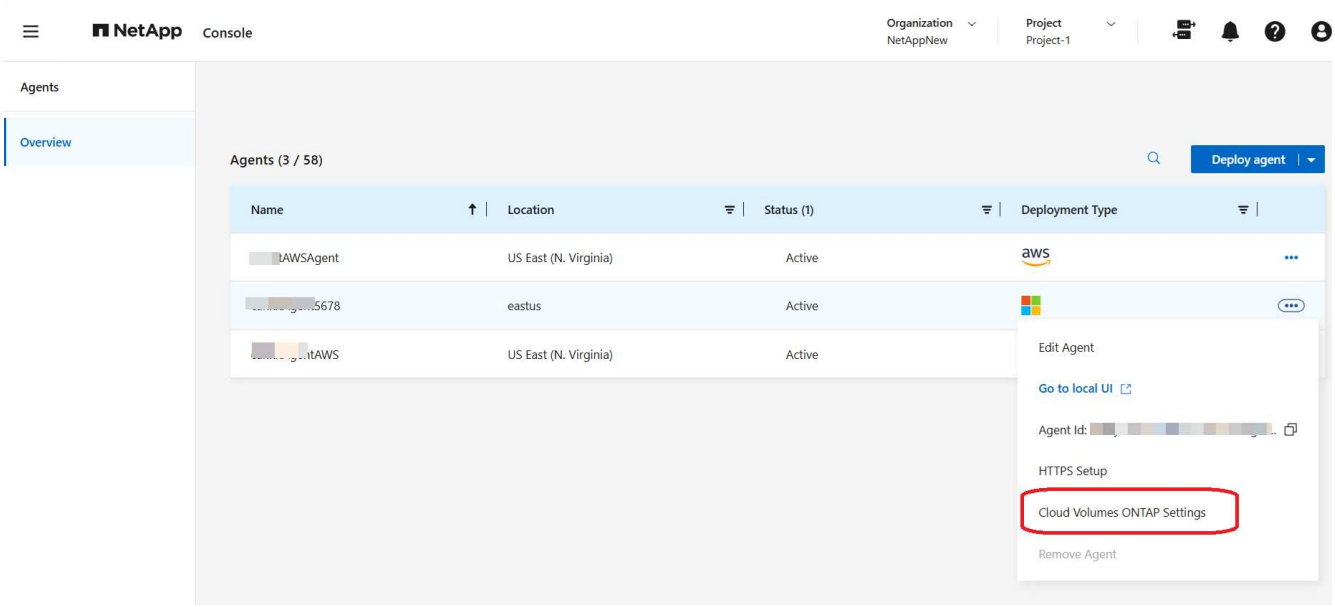
Desabilite os Links Privados do Azure e use pontos de extremidade de serviço em vez deles

Se necessário para sua empresa, você pode alterar uma configuração no Console para que ele configure o Cloud Volumes ONTAP para usar pontos de extremidade de serviço em vez de um Link Privado do Azure. A alteração desta configuração se aplica aos novos sistemas Cloud Volumes ONTAP que você criar. Os pontos de extremidade de serviço são suportados apenas em"Pares de regiões do Azure" entre o agente do Console e as VNets Cloud Volumes ONTAP .

O agente do Console deve ser implantado na mesma região do Azure que os sistemas Cloud Volumes ONTAP que ele gerencia ou no "Par de regiões do Azure" para os sistemas Cloud Volumes ONTAP .

Passos

1. No painel de navegação esquerdo, acesse **Administração > Agentes**.
2. Clique no ••• ícone para o agente do Console que gerencia seu sistema Cloud Volumes ONTAP .
3. Selecione * Configurações do Cloud Volumes ONTAP *.



4. Em **Azure**, clique em **Usar link privado do Azure**.
5. Desmarque **Conexão de link privado entre o Cloud Volumes ONTAP e contas de armazenamento**.
6. Clique em **Salvar**.

Depois que você terminar

Se você desabilitou os Links Privados do Azure e o agente do Console usa um servidor proxy, você deve habilitar o tráfego direto da API.

"Aprenda como habilitar o tráfego direto da API no agente do Console"

Trabalhar com Links Privados do Azure

Na maioria dos casos, não há nada que você precise fazer para configurar links privados do Azure com o Cloud Volumes ONTAP. O Console gerencia os Links Privados do Azure para você. Mas se você usar uma zona DNS privada do Azure existente, precisará editar um arquivo de configuração.

Requisito para DNS personalizado

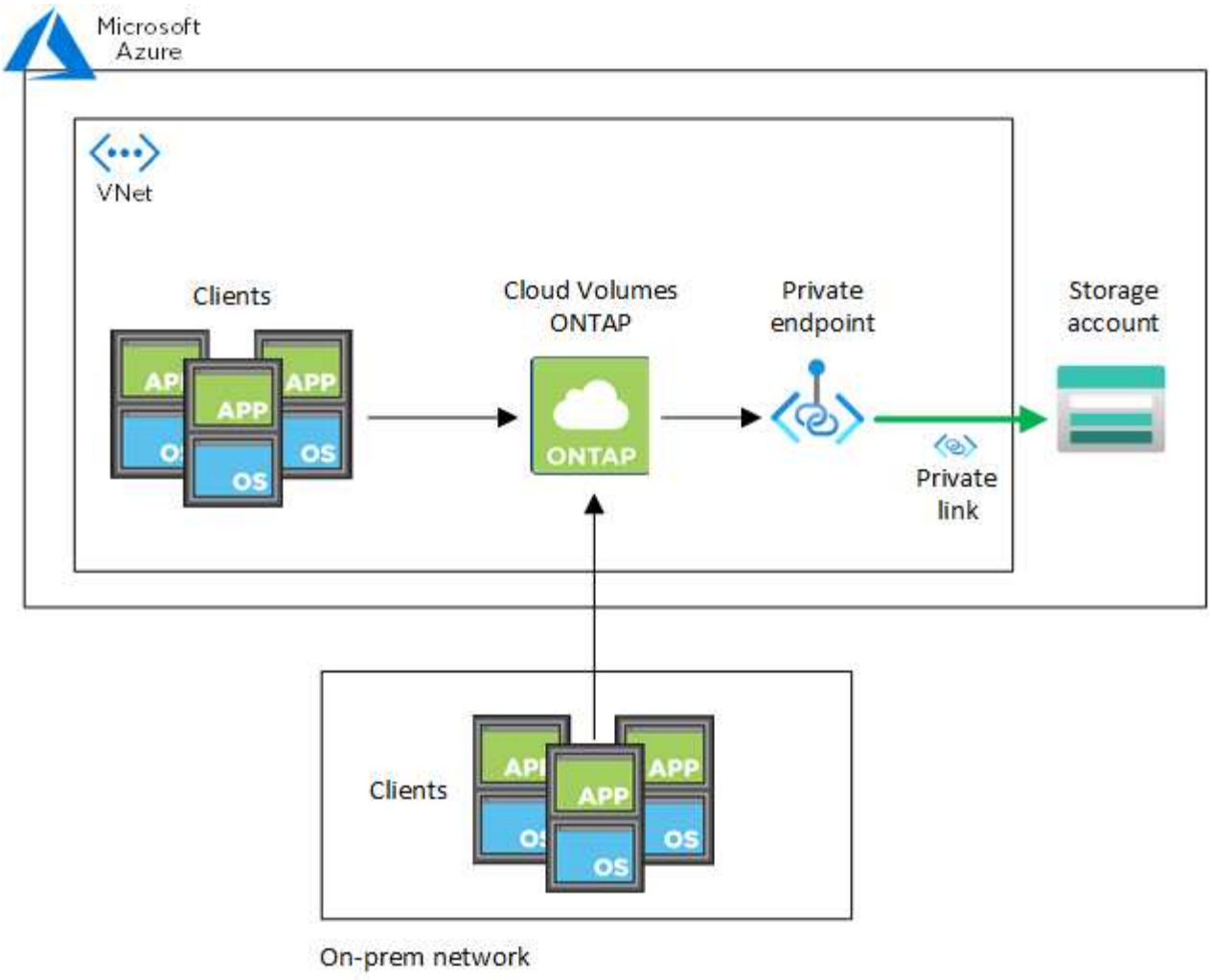
Opcionalmente, se você trabalhar com DNS personalizado, precisará criar um encaminhador condicional para a zona DNS privada do Azure a partir dos seus servidores DNS personalizados. Para saber mais, consulte"Documentação do Azure sobre o uso de um encaminhador DNS" .

Como funcionam as conexões do Private Link

Quando o Console implanta o Cloud Volumes ONTAP no Azure, ele cria um ponto de extremidade privado no grupo de recursos. O ponto de extremidade privado está associado às contas de armazenamento do Cloud Volumes ONTAP. Como resultado, o acesso ao armazenamento do Cloud Volumes ONTAP passa pela rede de backbone da Microsoft.

O acesso do cliente ocorre por meio do link privado quando os clientes estão na mesma VNet que o Cloud Volumes ONTAP, em VNets pareadas ou na sua rede local ao usar uma VPN privada ou conexão ExpressRoute com a VNet.

Aqui está um exemplo que mostra o acesso do cliente por meio de um link privado de dentro da mesma VNet e de uma rede local que tem uma VPN privada ou uma conexão ExpressRoute.



Se o agente do Console e os sistemas Cloud Volumes ONTAP forem implantados em VNets diferentes, você deverá configurar o peering de VNet entre a VNet onde o agente do Console está implantado e a VNet onde os sistemas Cloud Volumes ONTAP estão implantados.

Forneça detalhes sobre seu DNS privado do Azure

Se você usar "DNS privado do Azure" , então você precisa modificar um arquivo de configuração em cada agente do Console. Caso contrário, o Console não poderá definir a conexão do Azure Private Link entre o Cloud Volumes ONTAP e suas contas de armazenamento associadas.

Observe que o nome DNS deve corresponder aos requisitos de nomenclatura DNS do Azure "conforme mostrado na documentação do Azure" .

Passos

1. Conecte-se via SSH ao host do agente do Console e efetue login.
2. Navegue até o `/opt/application/netapp/cloudmanager/docker_occm/data` diretório.
3. Editar `app.conf` adicionando o `user-private-dns-zone-settings` parâmetro com os seguintes pares de palavra-chave-valor:

```
"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
}
```

O `subscription` A palavra-chave é necessária somente se a zona DNS privada estiver em uma assinatura diferente daquela do agente do Console.

4. Salve o arquivo e faça logoff do agente do Console.

   Não é necessário reinicializar.

Habilitar reversão em caso de falhas

Se o Console não conseguir criar um Link Privado do Azure como parte de ações específicas, ele concluirá a ação sem a conexão do Link Privado do Azure. Isso pode acontecer ao criar um novo sistema (nó único ou par HA) ou quando as seguintes ações ocorrem em um par HA: criar um novo agregado, adicionar discos a um agregado existente ou criar uma nova conta de armazenamento ao ultrapassar 32 TiB.

Você pode alterar esse comportamento padrão habilitando a reversão caso o Console não consiga criar o Link Privado do Azure. Isso pode ajudar a garantir que você esteja em total conformidade com os regulamentos de segurança da sua empresa.

Se você habilitar a reversão, o Console interromperá a ação e reverterá todos os recursos que foram criados como parte da ação.

Você pode habilitar a reversão por meio da API ou atualizando o arquivo app.conf.

Habilitar rollback através da API

Etapa

1. Use o `PUT /occm/config` Chamada de API com o seguinte corpo de solicitação:

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

Habilite a reversão atualizando app.conf

Passos

1. Conecte-se via SSH ao host do agente do Console e efetue login.
2. Navegue até o seguinte diretório: /opt/application/netapp/cloudmanager/docker_occm/data
3. Edite app.conf adicionando o seguinte parâmetro e valor:

```
 "rollback-on-private-link-failure": true
. Salve o arquivo e faça logoff do agente do Console.
```

Não é necessário reinicializar.

Mover um grupo de recursos do Azure para o Cloud Volumes ONTAP no console do Azure

O Cloud Volumes ONTAP oferece suporte a movimentações de grupos de recursos do Azure, mas o fluxo de trabalho ocorre somente no console do Azure.

Você pode mover um sistema Cloud Volumes ONTAP de um grupo de recursos para um grupo de recursos diferente no Azure dentro da mesma assinatura do Azure. Não há suporte para mover grupos de recursos entre diferentes assinaturas do Azure.

Passos

1. Remova o sistema Cloud Volumes ONTAP . Consulte "Removendo sistemas Cloud Volumes ONTAP" .
2. Execute a movimentação do grupo de recursos no console do Azure.

   Para concluir a mudança, consulte"Mover recursos para um novo grupo de recursos ou assinatura na documentação do Microsoft Azure" .

3. Na página **Sistemas**, descubra o sistema.
4. Procure o novo grupo de recursos nas informações do sistema.

Resultado

O sistema e seus recursos (VMs, discos, contas de armazenamento, interfaces de rede, snapshots) estão no novo grupo de recursos.

Segregar o tráfego do SnapMirror no Azure

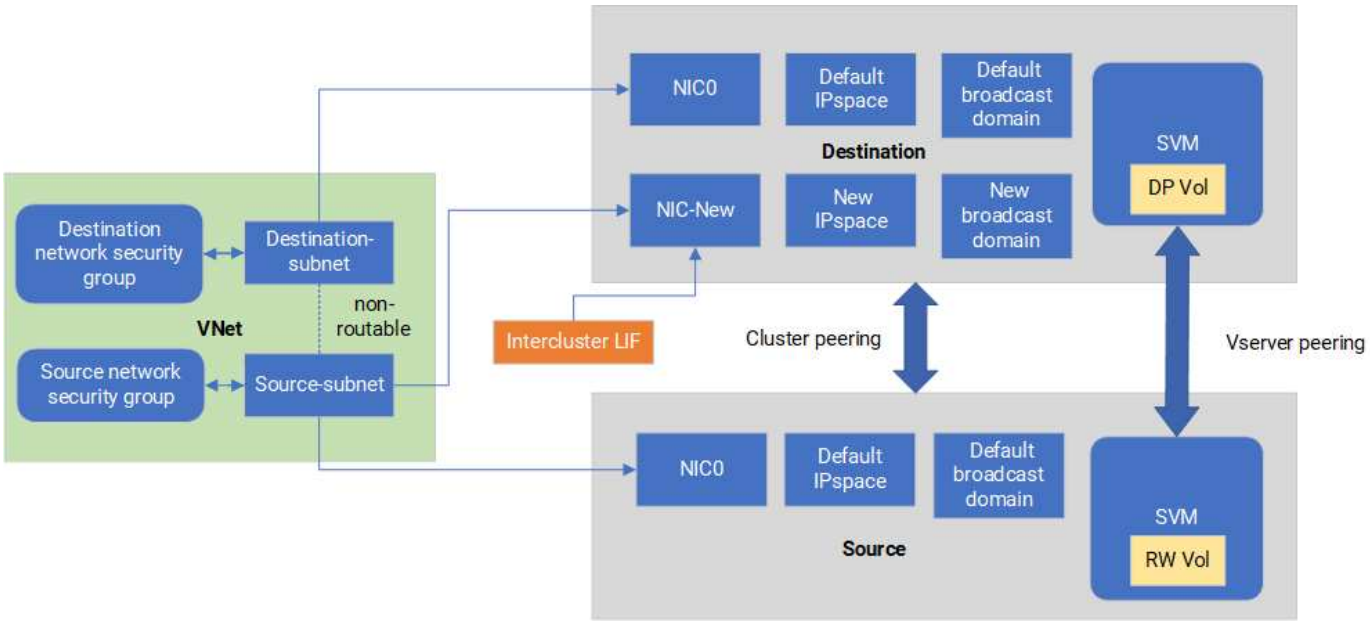
Com o Cloud Volumes ONTAP no Azure, você pode segregar o tráfego de replicação do SnapMirror do tráfego de dados e gerenciamento. Para segregar o tráfego de replicação do SnapMirror do seu tráfego de dados, você adicionará uma nova placa de interface de rede (NIC), um LIF intercluster associado e uma sub-rede não roteável.

Sobre a segregação de tráfego do SnapMirror no Azure

Por padrão, o NetApp Console configura todas as NICs e LIFs em uma implantação do Cloud Volumes ONTAP na mesma sub-rede. Nessas configurações, o tráfego de replicação do SnapMirror e o tráfego de dados e gerenciamento usam a mesma sub-rede. A segregação do tráfego do SnapMirror aproveita uma sub-rede adicional que não é roteável para a sub-rede existente usada para tráfego de dados e gerenciamento.

Figura 1

Os diagramas a seguir mostram a segregação do tráfego de replicação do SnapMirror com uma NIC adicional, um LIF intercluster associado e uma sub-rede não roteável em uma única implantação de nó. Uma implantação de par HA é um pouco diferente.



Antes de começar

Revise as seguintes considerações:

- Você só pode adicionar uma única NIC a uma implantação de nó único ou par HA do Cloud Volumes ONTAP (instância de VM) para segregação de tráfego do SnapMirror .
- Para adicionar uma nova NIC, o tipo de instância de VM que você implanta deve ter uma NIC não utilizada.
- Os clusters de origem e destino devem ter acesso à mesma Rede Virtual (VNet). O cluster de destino é um sistema Cloud Volumes ONTAP no Azure. O cluster de origem pode ser um sistema Cloud Volumes ONTAP no Azure ou um sistema ONTAP .

Etapa 1: crie uma NIC adicional e anexe-a à VM de destino

Esta seção fornece instruções sobre como criar uma NIC adicional e anexá-la à VM de destino. A VM de destino é o nó único ou sistema de par HA no Cloud Volumes ONTAP no Azure onde você deseja configurar sua NIC adicional.

Passos

1. Na CLI do ONTAP , pare o nó.

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

2. No portal do Azure, verifique se o status da VM (nó) está parado.

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

3. Use o ambiente Bash no Azure Cloud Shell para parar o nó.
   a. Pare o nó.

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

b. Desaloque o nó.

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

4. Configure regras de grupo de segurança de rede para tornar as duas sub-redes (sub-rede do cluster de origem e sub-rede do cluster de destino) não roteáveis entre si.
   a. Crie a nova NIC na VM de destino.
   b. Procure o ID da sub-rede do cluster de origem.

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

   c. Crie a nova NIC na VM de destino com o ID de sub-rede da sub-rede do cluster de origem. Aqui você insere o nome da nova NIC.

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

   d. Salve o endereço IP privado. Este endereço IP, <new_added_nic_primary_addr>, é usado para criar um LIF intercluster emdomínio de transmissão, LIF intercluster para o novo NIC .

5. Anexe a nova NIC à VM.

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

6. Inicie a VM (nó).

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

7. No portal do Azure, acesse **Rede** e confirme se a nova NIC, por exemplo, nic-new, existe e se a rede acelerada está habilitada.

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

Para implantações de par HA, repita as etapas para o nó parceiro.

Etapa 2: Crie um novo IPspace, domínio de transmissão e LIF intercluster para o novo NIC

Um IPspace separado para LIFs interclusters fornece separação lógica entre a funcionalidade de rede para replicação entre clusters.

Use o ONTAP CLI para as etapas a seguir.

Passos

1. Crie o novo IPspace (new_ipspace).

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

2. Crie um domínio de transmissão no novo IPspace (new_ipspace) e adicione a porta nic-new.

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

3. Para sistemas de nó único, a porta recém-adicionada é *e0b*. Para implantações de par de HA com discos gerenciados, a porta recém-adicionada é *e0d*. Para implantações de par de HA com blobs de página, a porta recém-adicionada é *e0e*. Use o nome do nó, não o nome da VM. Encontre o nome do nó executando `node show`.

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

4. Crie um LIF intercluster no novo domínio de transmissão (new_bd) e no novo NIC (nic-new).

```
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. Verifique a criação do novo LIF intercluster.

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

Para implantações de par HA, repita as etapas para o nó parceiro.

Etapa 3: verificar o peering do cluster entre os sistemas de origem e destino

Esta seção fornece instruções sobre como verificar o peering entre os sistemas de origem e destino.

Use o ONTAP CLI para as etapas a seguir.

Passos

1. Verifique se o LIF intercluster do cluster de destino pode executar ping no LIF intercluster do cluster de origem. Como o cluster de destino executa esse comando, o endereço IP de destino é o endereço IP do LIF intercluster na origem.

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

2. Verifique se o LIF intercluster do cluster de origem pode executar ping no LIF intercluster do cluster de destino. O destino é o endereço IP da nova NIC criada no destino.

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

Para implantações de par HA, repita as etapas para o nó parceiro.

Etapa 4: criar peering SVM entre os sistemas de origem e destino

Esta seção fornece instruções sobre como criar o peering SVM entre os sistemas de origem e de destino.

Use o ONTAP CLI para as etapas a seguir.

Passos

1. Crie o peering de cluster no destino usando o endereço IP do LIF intercluster de origem como `-peer-addrs` . Para pares HA, liste o endereço IP do LIF intercluster de origem para ambos os nós como `-peer-addrs` .

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

2. Digite e confirme a senha.
3. Crie um peering de cluster na origem usando o endereço IP do LIF do cluster de destino como `peer-addrs` . Para pares HA, liste o endereço IP do LIF intercluster de destino para ambos os nós como `-peer-addrs` .

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

4. Digite e confirme a senha.
5. Verifique se o cluster está pareado.

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

O peering bem-sucedido mostra **Disponível** no campo de disponibilidade.

6. Crie um peering SVM no destino. Tanto os SVMs de origem quanto os de destino devem ser SVMs de dados.

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

7. Aceitar peering SVM.

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

8. Verifique se o SVM está pareado.

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

Mostra de estado de pares*`peered` * e aplicações de peering mostram*`snapmirror` *.

Etapa 5: Crie um relacionamento de replicação SnapMirror entre o sistema de origem e o de destino

Esta seção fornece instruções sobre como criar um relacionamento de replicação do SnapMirror entre o sistema de origem e o de destino.

Para mover um relacionamento de replicação SnapMirror existente, você deve primeiro quebrar o relacionamento de replicação SnapMirror existente antes de criar um novo relacionamento de replicação SnapMirror .

Use o ONTAP CLI para as etapas a seguir.

Passos

1. Crie um volume de dados protegido no SVM de destino.

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

2. Crie o relacionamento de replicação do SnapMirror no destino, que inclui a política do SnapMirror e o agendamento para a replicação.

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

3. Inicialize o relacionamento de replicação do SnapMirror no destino.

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

4. Na CLI do ONTAP , valide o status do relacionamento do SnapMirror executando o seguinte comando:

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

   O status do relacionamento é `Snapmirrored` e a saúde do relacionamento é `true` .

5. Opcional: Na CLI do ONTAP , execute o seguinte comando para visualizar o histórico de ações do relacionamento SnapMirror .

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

Opcionalmente, você pode montar os volumes de origem e destino, gravar um arquivo na origem e verificar se o volume está sendo replicado para o destino.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em http://www.netapp.com/TM são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.