Azure 관리

Cloud Volumes ONTAP

NetApp
February 13, 2026

목차

Azure 관리

Cloud Volumes ONTAP 에 대한 Azure VM 유형 변경

Microsoft Azure에서 Cloud Volumes ONTAP 시작하면 여러 VM 유형 중에서 선택할 수 있습니다. 필요에 따라 VM 유형이 너무 크거나 작다고 판단되면 언제든지 VM 유형을 변경할 수 있습니다.

이 작업에 관하여

- Cloud Volumes ONTAP HA 쌍에서 자동 반환 기능을 활성화해야 합니다(이는 기본 설정입니다). 그렇지 않으면 작업이 실패합니다.

  "ONTAP 9 설명서: 자동 반환 구성을 위한 명령"

- VM 유형을 변경하면 Microsoft Azure 서비스 요금에 영향을 미칠 수 있습니다.
- 이 작업은 Cloud Volumes ONTAP 다시 시작합니다.

  단일 노드 시스템의 경우 I/O가 중단됩니다.

  HA 쌍의 경우 변경은 중단되지 않습니다. HA 쌍은 계속해서 데이터를 제공합니다.

NetApp Console 인수를 시작하고 반환을 기다리는 방식으로 한 번에 한 노드씩 변경합니다. NetApp의 품질 보증 팀은 이 프로세스 동안 파일 쓰기와 읽기를 모두 테스트했으며 클라이언트 측에서 아무런 문제도 발견하지 못했습니다. 연결이 변경됨에 따라 I/O 수준에서 일부 재시도가 관찰되었지만 애플리케이션 계층은 NFS/CIFS 연결의 재배선을 극복했습니다.

단계

1. 시스템 페이지에서 시스템을 선택하세요.
2. 개요 탭에서 기능 패널을 클릭한 다음 **VM** 유형 옆에 있는 연필 아이콘을 클릭합니다.

   노드 기반 사용량 기반(PAYGO) 라이선스를 사용하는 경우, 라이선스 유형 옆에 있는 연필 아이콘을 클릭하여 다른 라이선스와 VM 유형을 선택할 수 있습니다.

3. VM 유형을 선택하고, 변경 사항의 의미를 이해했음을 확인하는 확인란을 선택한 다음 *변경*을 클릭합니다.

결과

Cloud Volumes ONTAP 새로운 구성으로 재부팅됩니다.

Azure에서 Cloud Volumes ONTAP HA 쌍에 대한 CIFS 잠금 재정의

조직 또는 계정 관리자는 NetApp Console 에서 Azure 유지 관리 이벤트 중에 Cloud Volumes ONTAP 저장소 반환 문제를 방지하는 설정을 활성화할 수 있습니다. 이 설정을 활성화하면 Cloud Volumes ONTAP CIFS 잠금을 거부하고 활성 CIFS 세션을 재설정합니다.

이 작업에 관하여

Microsoft Azure는 가상 머신에 대한 정기적인 유지 관리 이벤트를 예약합니다. Cloud Volumes ONTAP HA 쌍에서 유지 관리 이벤트가 발생하면 HA 쌍이 스토리지 인수를 시작합니다. 이 유지 관리 이벤트 중에 활성 CIFS 세션이 있는 경우 CIFS 파일에 대한 잠금으로 인해 저장소 반환이 방해받을 수 있습니다.

이 설정을 활성화하면 Cloud Volumes ONTAP 이 잠금을 거부하고 활성 CIFS 세션을 재설정합니다. 결과적으로 HA 쌍은 이러한 유지 관리 이벤트 중에 스토리지 반환을 완료할 수 있습니다.

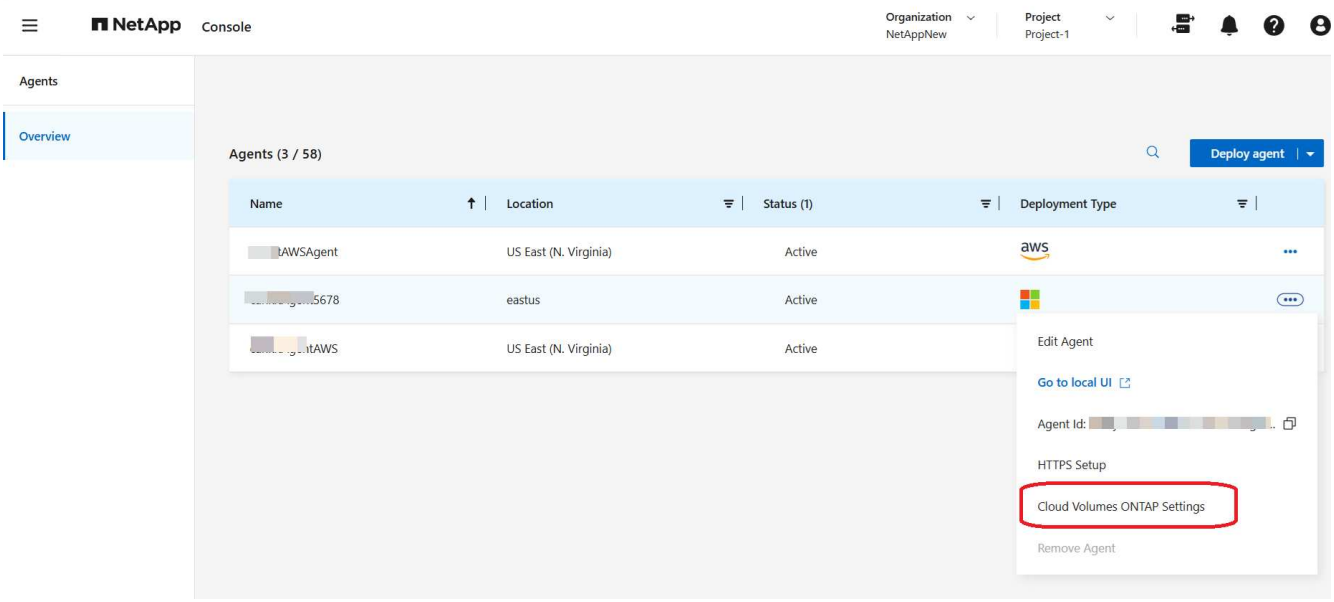
> 이 프로세스는 CIFS 클라이언트에 방해가 될 수 있습니다. CIFS 클라이언트에서 커밋되지 않은 데이터는 손실될 수 있습니다.

시작하기 전에

콘솔 설정을 변경하려면 먼저 콘솔 에이전트를 만들어야 합니다. "방법을 알아보세요" .

단계

1. 왼쪽 탐색 창에서 *관리 > 에이전트*로 이동합니다.
2. 클릭 ••• Cloud Volumes ONTAP 시스템을 관리하는 콘솔 에이전트의 아이콘입니다.
3. * Cloud Volumes ONTAP 설정*을 선택합니다.



4. *Azure*에서 *Azure HA 시스템에 대한 Azure CIFS 잠금*을 클릭합니다.
5. 해당 기능을 활성화하려면 확인란을 클릭한 다음 *저장*을 클릭하세요.

Cloud Volumes ONTAP 시스템에 Azure Private Link 또는 서비스 엔드포인트 사용

Cloud Volumes ONTAP 연결된 스토리지 계정에 연결하기 위해 Azure Private Link를 사용합니다. 필요한 경우 Azure Private Links를 비활성화하고 대신 서비스 엔드포인트를 사용할 수 있습니다.

개요

기본적으로 NetApp Console Cloud Volumes ONTAP 과 연결된 스토리지 계정 간의 연결을 위해 Azure Private Link를 활성화합니다. Azure Private Link는 Azure의 엔드포인트 간 연결을 보호하고 성능 이점을 제공합니다.

필요한 경우 Azure Private Link 대신 서비스 엔드포인트를 사용하도록 Cloud Volumes ONTAP 구성할 수 있습니다.

두 구성 모두에서 콘솔은 항상 Cloud Volumes ONTAP 과 스토리지 계정 간 연결에 대한 네트워크 액세스를 제한합니다. 네트워크 액세스는 Cloud Volumes ONTAP 배포된 VNet과 콘솔 에이전트가 배포된 VNet으로 제한됩니다.

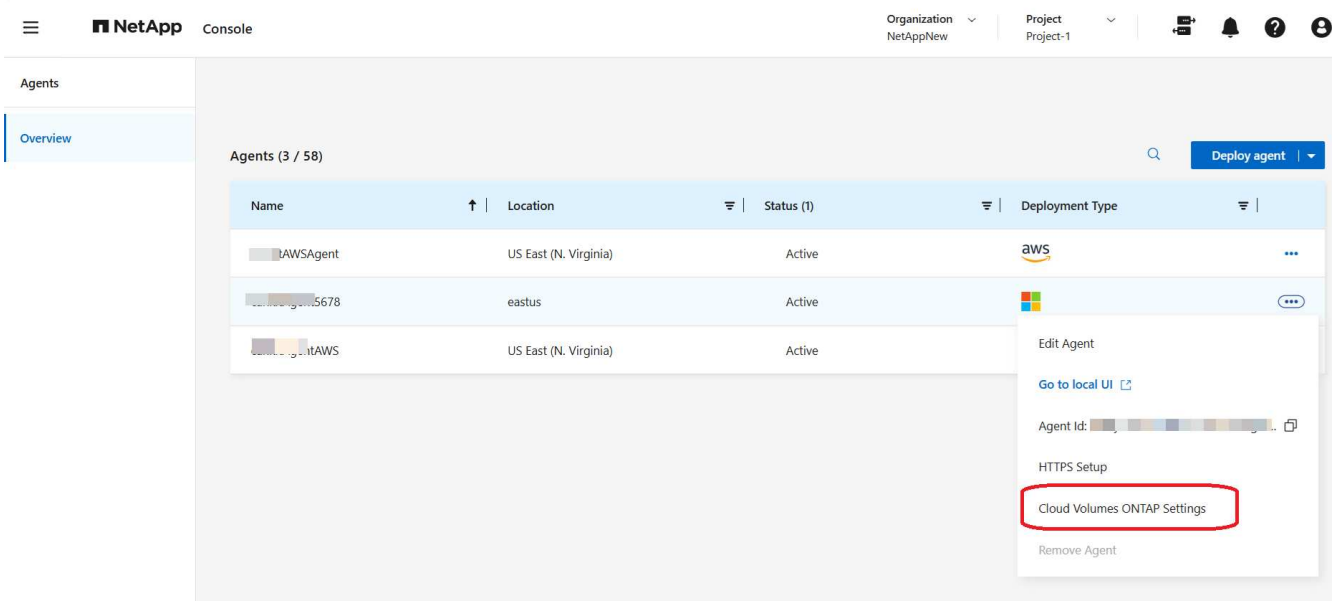
Azure Private Links를 비활성화하고 대신 서비스 엔드포인트를 사용하세요.

비즈니스에 필요한 경우 콘솔에서 설정을 변경하여 Azure Private Link 대신 서비스 엔드포인트를 사용하도록 Cloud Volumes ONTAP 구성할 수 있습니다. 이 설정을 변경하면 새로 만든 Cloud Volumes ONTAP 시스템에 적용됩니다. 서비스 엔드포인트는 다음에서만 지원됩니다."Azure 지역 쌍" 콘솔 에이전트와 Cloud Volumes ONTAP VNet 사이.

콘솔 에이전트는 관리하는 Cloud Volumes ONTAP 시스템과 동일한 Azure 지역이나 "Azure 지역 쌍" Cloud Volumes ONTAP 시스템용.

단계

1. 왼쪽 탐색 창에서 *관리 > 에이전트*로 이동합니다.
2. 클릭 ••• Cloud Volumes ONTAP 시스템을 관리하는 콘솔 에이전트의 아이콘입니다.
3. * Cloud Volumes ONTAP 설정*을 선택합니다.



4. *Azure*에서 *Azure Private Link 사용*을 클릭합니다.
5. Cloud Volumes ONTAP 과 스토리지 계정 간의 개인 링크 연결을 선택 해제합니다.
6. *저장*을 클릭하세요.

당신이 완료한 후

Azure Private Links를 비활성화하고 콘솔 에이전트가 프록시 서버를 사용하는 경우 직접 API 트래픽을 활성화해야 합니다.

"콘솔 에이전트에서 직접 API 트래픽을 활성화하는 방법을 알아보세요."

Azure Private Links로 작업

대부분의 경우 Cloud Volumes ONTAP 사용하여 Azure Private Link를 설정하는 데 필요한 작업은 없습니다. 콘솔은 Azure Private Links를 관리합니다. 하지만 기존 Azure Private DNS 영역을 사용하는 경우 구성 파일을 편집해야 합니다.

사용자 정의 **DNS**에 대한 요구 사항

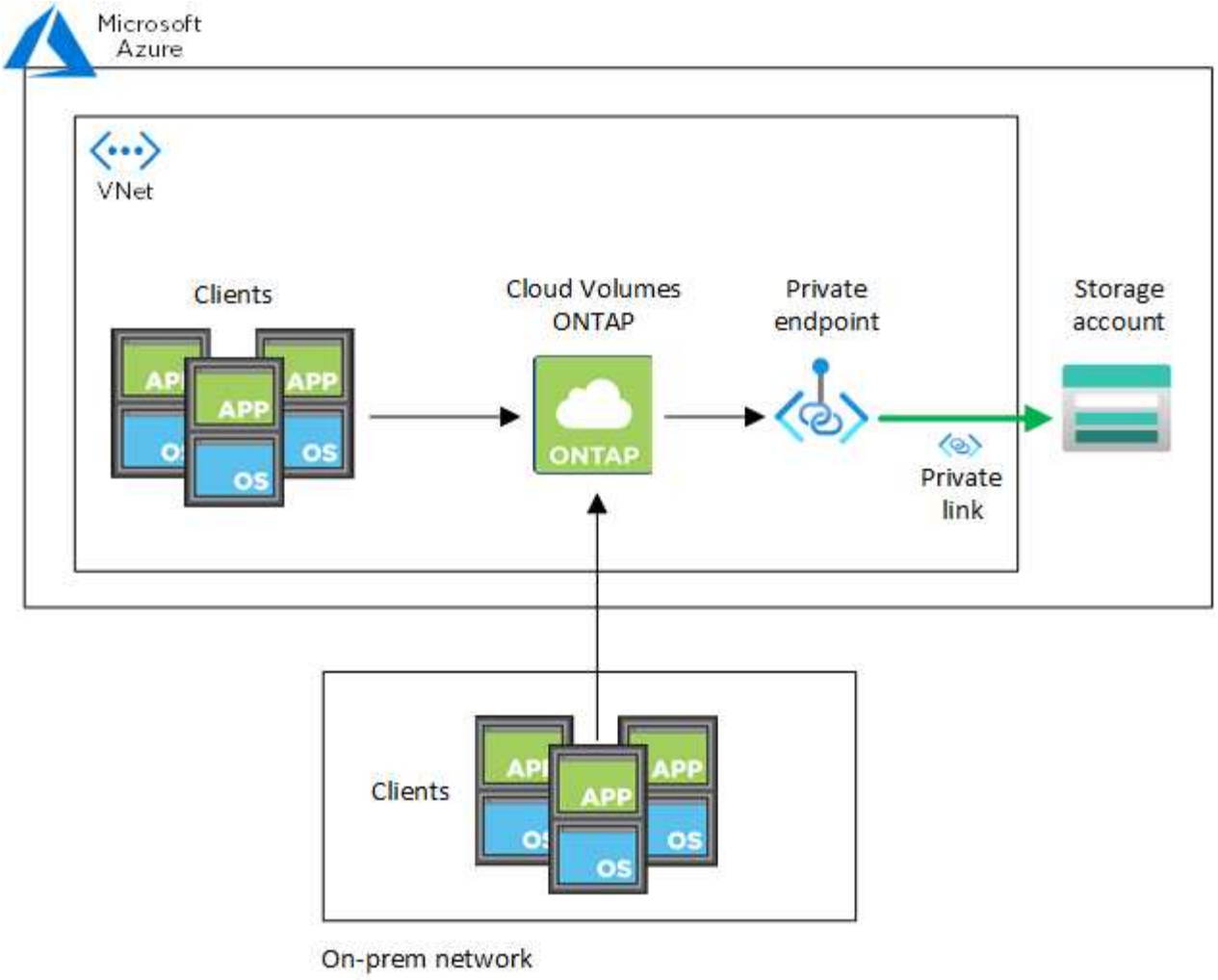
선택적으로 사용자 지정 DNS를 사용하는 경우 사용자 지정 DNS 서버에서 Azure 개인 DNS 영역에 대한 조건부 전달자를 만들어야 합니다. 자세한 내용은 다음을 참조하세요."DNS 전달자 사용에 대한 Azure 설명서" .

Private Link 연결 작동 방식

콘솔이 Azure에 Cloud Volumes ONTAP 배포하면 리소스 그룹에 개인 엔드포인트가 생성됩니다. 개인 엔드포인트는 Cloud Volumes ONTAP 의 스토리지 계정과 연결됩니다. 결과적으로 Cloud Volumes ONTAP 스토리지에 대한 액세스는 Microsoft 백본 네트워크를 통해 이루어집니다.

클라이언트가 Cloud Volumes ONTAP 과 동일한 VNet에 있거나, 피어링된 VNet에 있거나, VNet에 대한 개인 VPN이나 ExpressRoute 연결을 사용할 때 온프레미스 네트워크에 있는 경우 클라이언트 액세스는 개인 링크를 통해 이루어집니다.

다음은 동일한 VNet 내부와 개인 VPN 또는 ExpressRoute 연결이 있는 온프레미스 네트워크에서 개인 링크를 통해 클라이언트 액세스를 보여주는 예입니다.



콘솔 에이전트와 Cloud Volumes ONTAP 시스템이 서로 다른 VNet에 배포된 경우 콘솔 에이전트가 배포된 VNet과 Cloud Volumes ONTAP 시스템이 배포된 VNet 간에 VNet 피어링을 설정해야 합니다.

Azure Private DNS에 대한 세부 정보를 제공하세요**.**

당신이 사용하는 경우 "Azure 프라이빗 DNS" 그러면 각 콘솔 에이전트에서 구성 파일을 수정해야 합니다. 그렇지 않으면 콘솔은 Cloud Volumes ONTAP 과 연결된 스토리지 계정 간에 Azure Private Link 연결을 설정할 수 없습니다.

DNS 이름은 Azure DNS 명명 요구 사항과 일치해야 합니다. "Azure 설명서에 표시된 대로" .

단계

1. 콘솔 에이전트 호스트에 SSH를 실행하고 로그인합니다.
2. 로 이동합니다 `/opt/application/netapp/cloudmanager/docker_occm/data` 예배 규칙서.
3. 편집하다 `app.conf` 추가하여 `user-private-dns-zone-settings` 다음 키워드-값 쌍을 포함하는 매개변수:

```
"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
}
```

그만큼 `subscription` 키워드는 개인 DNS 영역이 콘솔 에이전트와 다른 구독에 있는 경우에만 필요합니다.

4. 파일을 저장하고 콘솔 에이전트에서 로그오프합니다.

   재부팅이 필요하지 않습니다.

실패 시 롤백 활성화

콘솔이 특정 작업의 일부로 Azure Private Link를 만들지 못하면 Azure Private Link 연결 없이 작업을 완료합니다. 이는 새로운 시스템(단일 노드 또는 HA 쌍)을 생성할 때 또는 HA 쌍에서 다음 작업이 발생할 때 발생할 수 있습니다. 새로운 집계 생성, 기존 집계에 디스크 추가 또는 32TiB를 초과할 때 새로운 스토리지 계정 생성.

콘솔에서 Azure Private Link를 만들지 못하는 경우 롤백을 활성화하여 이 기본 동작을 변경할 수 있습니다. 이를 통해 회사의 보안 규정을 완벽하게 준수하는 데 도움이 될 수 있습니다.

롤백을 활성화하면 콘솔에서 작업이 중지되고 작업의 일부로 생성된 모든 리소스가 롤백됩니다.

API를 통해 롤백을 활성화하거나 app.conf 파일을 업데이트할 수 있습니다.

API를 통한 롤백 활성화

단계

1. 사용하다 `PUT /occm/config` 다음 요청 본문을 포함하는 API 호출:

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

app.conf를 업데이트하여 롤백을 활성화합니다

단계

1. 콘솔 에이전트 호스트에 SSH를 실행하고 로그인합니다.
2. 다음 디렉토리로 이동합니다: /opt/application/netapp/cloudmanager/docker_occm/data
3. 다음 매개변수와 값을 추가하여 app.conf를 편집합니다.

```
 "rollback-on-private-link-failure": true
. 파일을 저장하고 콘솔 에이전트에서 로그오프합니다.
```

재부팅이 필요하지 않습니다.

Azure 콘솔에서 Cloud Volumes ONTAP 대한 Azure 리소스 그룹 이동

Cloud Volumes ONTAP Azure 리소스 그룹 이동을 지원하지만 워크플로는 Azure 콘솔에서만 발생합니다.

동일한 Azure 구독 내에서 Azure의 한 리소스 그룹에서 다른 리소스 그룹으로 Cloud Volumes ONTAP 시스템을 이동할 수 있습니다. 서로 다른 Azure 구독 간에 리소스 그룹을 이동하는 것은 지원되지 않습니다.

단계

1. Cloud Volumes ONTAP 시스템을 제거합니다. "Cloud Volumes ONTAP 시스템 제거" .
2. Azure 콘솔에서 리소스 그룹 이동을 실행합니다.

   이동을 완료하려면 다음을 참조하세요."Microsoft Azure 설명서에서 리소스를 새 리소스 그룹 또는 구독으로 이동" .
3. 시스템 페이지에서 시스템을 알아보세요.
4. 시스템 정보에서 새로운 리소스 그룹을 찾으세요.

결과

시스템과 해당 리소스(VM, 디스크, 스토리지 계정, 네트워크 인터페이스, 스냅샷)는 새 리소스 그룹에 있습니다.

Azure에서 SnapMirror 트래픽 분리

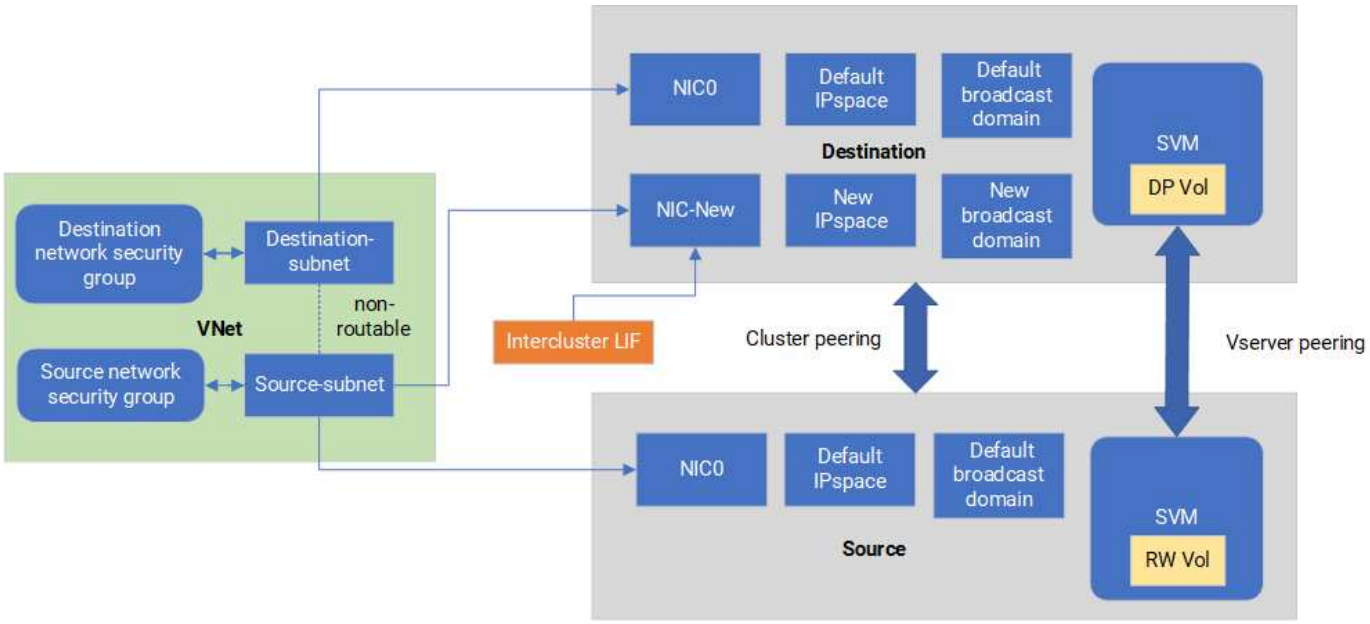
Azure의 Cloud Volumes ONTAP 사용하면 SnapMirror 복제 트래픽을 데이터 및 관리 트래픽에서 분리할 수 있습니다. SnapMirror 복제 트래픽을 데이터 트래픽에서 분리하려면 새 네트워크 인터페이스 카드(NIC), 연관된 클러스터 간 LIF 및 라우팅이 불가능한 서브넷을 추가합니다.

Azure의 SnapMirror 트래픽 분리에 관하여

기본적으로 NetApp Console 동일한 서브넷의 Cloud Volumes ONTAP 배포에 있는 모든 NIC와 LIF를 구성합니다. 이러한 구성에서는 SnapMirror 복제 트래픽과 데이터 및 관리 트래픽이 동일한 서브넷을 사용합니다. SnapMirror 트래픽을 분리하면 데이터 및 관리 트래픽에 사용되는 기존 서브넷으로 라우팅할 수 없는 추가 서브넷을 활용할 수 있습니다.

그림 **1**

다음 다이어그램은 단일 노드 배포에서 추가 NIC, 연관된 클러스터 간 LIF 및 라우팅 불가능한 서브넷을 사용하여 SnapMirror 복제 트래픽을 분리하는 방식을 보여줍니다. HA 쌍 배포는 약간 다릅니다.



시작하기 전에

다음 고려 사항을 검토하세요.

- SnapMirror 트래픽 분리를 위해 Cloud Volumes ONTAP 단일 노드 또는 HA 쌍 배포(VM 인스턴스)에 단일 NIC만 추가할 수 있습니다.
- 새로운 NIC를 추가하려면 배포하는 VM 인스턴스 유형에 사용되지 않는 NIC가 있어야 합니다.
- 소스 및 대상 클러스터는 동일한 가상 네트워크(VNet)에 액세스할 수 있어야 합니다. 대상 클러스터는 Azure의 Cloud Volumes ONTAP 시스템입니다. 소스 클러스터는 Azure의 Cloud Volumes ONTAP 시스템이나 ONTAP 시스템이 될 수 있습니다.

1단계: 추가 NIC를 생성하고 대상 VM에 연결합니다.

이 섹션에서는 추가 NIC를 생성하고 대상 VM에 연결하는 방법에 대한 지침을 제공합니다. 대상 VM은 Azure의 Cloud Volumes ONTAP 에 있는 단일 노드 또는 HA 쌍 시스템으로, 여기에 추가 NIC를 설정하려는 것입니다.

단계

1. ONTAP CLI에서 노드를 중지합니다.

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

2. Azure Portal에서 VM(노드) 상태가 중지되었는지 확인하세요.

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

3. Azure Cloud Shell의 Bash 환경을 사용하여 노드를 중지합니다.
   a. 노드를 중지합니다.

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

b. 노드의 할당을 해제합니다.

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

4. 두 서브넷(소스 클러스터 서브넷과 대상 클러스터 서브넷)이 서로 라우팅되지 않도록 네트워크 보안 그룹 규칙을 구성합니다.

a. 대상 VM에 새 NIC를 만듭니다.

b. 소스 클러스터 서브넷의 서브넷 ID를 찾습니다.

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

c. 소스 클러스터 서브넷의 서브넷 ID를 사용하여 대상 VM에 새 NIC를 만듭니다. 여기에 새 NIC의 이름을 입력합니다.

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

d. 개인IP주소를 저장합니다. 이 IP 주소 <new_added_nic_primary_addr>는 클러스터 간 LIF를 생성하는 데 사용됩니다.브로드캐스트 도메인, 새 NIC에 대한 클러스터 간 LIF .

5. 새 NIC를 VM에 연결합니다.

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

6. VM(노드)을 시작합니다.

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

7. Azure Portal에서 *네트워킹*으로 이동하여 새 NIC(예: nic-new)가 있는지, 가속 네트워킹이 활성화되어 있는지 확인합니다.

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

HA 쌍 배포의 경우 파트너 노드에 대해 단계를 반복합니다.

2단계: 새 NIC에 대한 새 IP 공간, 브로드캐스트 도메인 및 클러스터 간 LIF 만들기

클러스터 간 LIF를 위한 별도의 IP 공간은 클러스터 간 복제를 위한 네트워킹 기능 간의 논리적 분리를 제공합니다.

다음 단계에서는 ONTAP CLI를 사용하세요.

단계

1. 새로운 IPspace(new_ipspace)를 생성합니다.

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

2. 새로운 IPspace(new_ipspace)에 브로드캐스트 도메인을 만들고 nic-new 포트를 추가합니다.

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

3. 단일 노드 시스템의 경우 새로 추가된 포트는 _e0b_입니다. 관리형 디스크를 사용하는 HA 페어 배포의 경우 새로 추가된 포트는 _e0d_입니다. 페이지 블롭을 사용하는 HA 페어 배포의 경우 새로 추가된 포트는 _e0e_입니다. VM 이름이 아닌 노드 이름을 사용하십시오. `node show`을 실행하여 노드 이름을 확인할 수 있습니다.

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

4. 새로운 브로드캐스트 도메인(new_bd)과 새로운 NIC(nic-new)에 클러스터 간 LIF를 만듭니다.

```
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. 새로운 클러스터 간 LIF 생성을 확인합니다.

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

HA 쌍 배포의 경우 파트너 노드에 대해 단계를 반복합니다.

3단계: 소스 시스템과 대상 시스템 간 클러스터 피어링 확인

이 섹션에서는 소스 시스템과 대상 시스템 간의 피어링을 확인하는 방법에 대한 지침을 제공합니다.

다음 단계에서는 ONTAP CLI를 사용하세요.

단계

1. 대상 클러스터의 클러스터 간 LIF가 소스 클러스터의 클러스터 간 LIF를 ping할 수 있는지 확인합니다. 대상 클러스터가 이 명령을 실행하므로 대상 IP 주소는 소스의 클러스터 간 LIF IP 주소입니다.

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

2. 소스 클러스터의 클러스터 간 LIF가 대상 클러스터의 클러스터 간 LIF를 ping할 수 있는지 확인합니다. 목적지는 목적지에 생성된 새로운 NIC의 IP 주소입니다.

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

HA 쌍 배포의 경우 파트너 노드에 대해 단계를 반복합니다.

4단계: 소스 시스템과 대상 시스템 간 SVM 피어링 생성

이 섹션에서는 소스 시스템과 대상 시스템 간에 SVM 피어링을 생성하는 방법에 대한 지침을 제공합니다.

다음 단계에서는 ONTAP CLI를 사용하세요.

단계

1. 소스 클러스터 간 LIF IP 주소를 사용하여 대상에서 클러스터 피어링을 생성합니다. `-peer-addrs` . HA 쌍의 경우 두 노드의 소스 클러스터 간 LIF IP 주소를 다음과 같이 나열합니다. `-peer-addrs` .

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

2. 암호를 입력하고 확인하세요.
3. 대상 클러스터 LIF IP 주소를 사용하여 소스에서 클러스터 피어링을 생성합니다. `peer-addrs` . HA 쌍의 경우 두 노드 모두에 대한 대상 클러스터 간 LIF IP 주소를 다음과 같이 나열합니다. `-peer-addrs` .

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

4. 암호를 입력하고 확인하세요.
5. 클러스터가 피어링되었는지 확인하세요.

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

피어링이 성공하면 가용성 필드에 *사용 가능*이 표시됩니다.

6. 목적지에 SVM 피어링을 생성합니다. 소스 SVM과 대상 SVM은 모두 데이터 SVM이어야 합니다.

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

7. SVM 피어링을 허용합니다.

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

8. SVM이 피어링되었는지 확인하세요.

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

피어 스테이트 쇼*`peered` * 및 피어링 애플리케이션이 표시됩니다.*`snapmirror` *.

5단계: 소스 시스템과 대상 시스템 간에 **SnapMirror** 복제 관계 생성

이 섹션에서는 소스 시스템과 대상 시스템 간에 SnapMirror 복제 관계를 만드는 방법에 대한 지침을 제공합니다.

기존 SnapMirror 복제 관계를 이동하려면 새 SnapMirror 복제 관계를 만들기 전에 먼저 기존 SnapMirror 복제 관계를 해제해야 합니다.

다음 단계에서는 ONTAP CLI를 사용하세요.

단계

1. 대상 SVM에 데이터 보호 볼륨을 만듭니다.

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

2. SnapMirror 정책과 복제 일정을 포함하는 대상에 SnapMirror 복제 관계를 만듭니다.

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

3. 대상에서 SnapMirror 복제 관계를 초기화합니다.

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

4. ONTAP CLI에서 다음 명령을 실행하여 SnapMirror 관계 상태를 확인합니다.

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

관계 상태는 다음과 같습니다. `Snapmirrored` 그리고 관계의 건강은 `true` .

5. 선택 사항: ONTAP CLI에서 다음 명령을 실행하여 SnapMirror 관계에 대한 작업 기록을 확인합니다.

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

선택적으로 소스 및 대상 볼륨을 마운트하고, 소스에 파일을 쓰고, 볼륨이 대상에 복제되는지 확인할 수 있습니다.