Azure 관리

Cloud Volumes ONTAP

NetApp
April 23, 2024

목차

Azure 관리 1
Cloud Volumes ONTAP의 Azure VM 유형을 변경합니다 1
Azure의 Cloud Volumes ONTAP HA 쌍에 대한 CIFS 잠금 재정의 2
Azure Private Link 또는 서비스 끝점을 사용합니다 3
리소스 그룹 이동 중 7
Azure에서 SnapMirror 트래픽을 분리합니다 7

Azure 관리

Cloud Volumes ONTAP의 Azure VM 유형을 변경합니다

Microsoft Azure에서 Cloud Volumes ONTAP를 시작할 때 여러 VM 유형 중에서 선택할 수 있습니다. 필요에 따라 크기가 작거나 특대형 것으로 판단될 경우 언제든지 VM 유형을 변경할 수 있습니다.

이 작업에 대해

- Cloud Volumes ONTAP HA 쌍(기본 설정)에서 자동 반환이 활성화되어 있어야 합니다. 그렇지 않으면 작업이 실패합니다.

  "ONTAP 9 설명서: 자동 반환 구성을 위한 명령입니다"

- VM 유형을 변경하면 Microsoft Azure 서비스 요금에 영향을 줄 수 있습니다.
- Cloud Volumes ONTAP가 다시 시작됩니다.

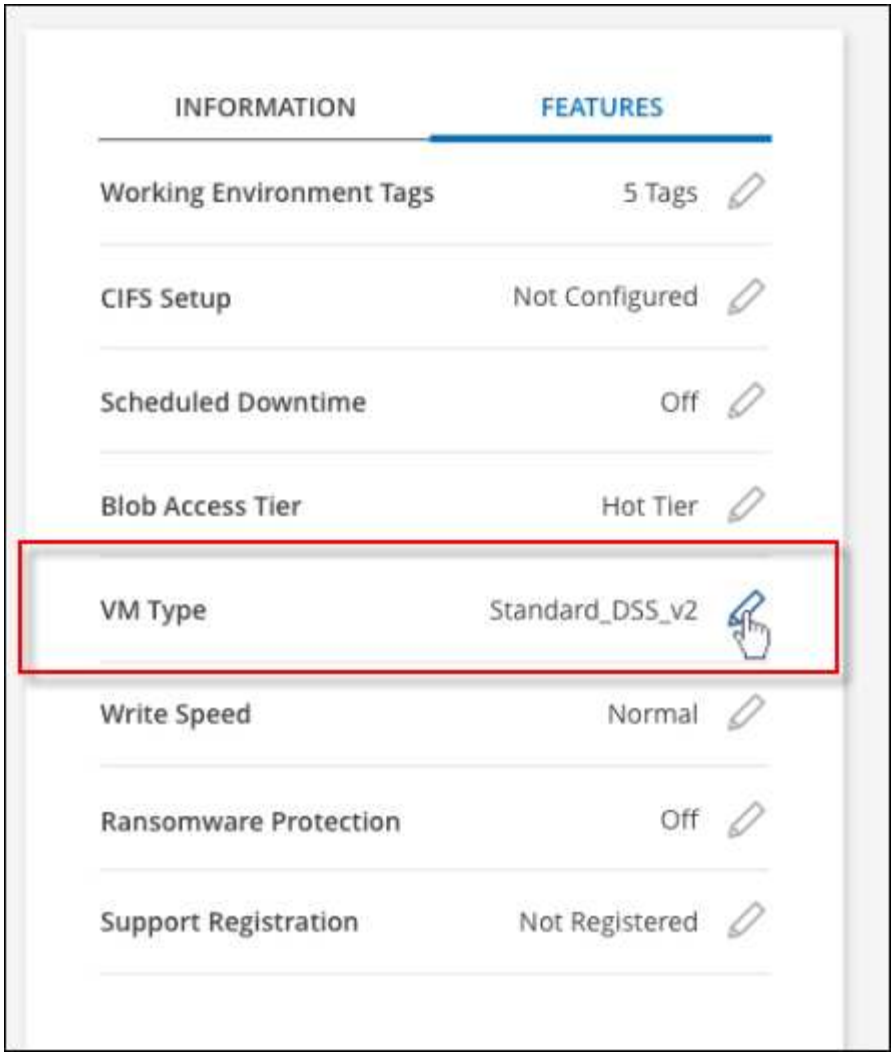
  단일 노드 시스템의 경우 입출력이 중단됩니다.

  HA 쌍의 경우 변경은 무중단 것입니다. HA 쌍이 계속해서 데이터를 제공합니다.

> BlueXP는 테이크오버를 시작하고 Giveback을 기다리면서 한 번에 하나의 노드를 정상적으로 변경합니다. NetApp의 QA 팀은 이 프로세스 중에 파일 쓰기와 읽기를 모두 테스트했지만 클라이언트 측에서는 문제가 발생하지 않았습니다. 접속이 변경됨에 따라 입출력 레벨에서 재시도 횟수가 확인되었지만 애플리케이션 계층은 NFS/CIFS 연결의 이러한 짧은 "재연결"을 극복했습니다.

단계

1. Canvas 페이지에서 작업 환경을 선택합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 * VM 유형 * 옆에 있는 연필 아이콘을 클릭합니다.



a. 노드 기반 PAYGO 라이센스를 사용하는 경우 * 라이센스 유형 * 옆에 있는 연필 아이콘을 클릭하여 다른 라이센스 및 VM 유형을 선택할 수 있습니다.

3. VM 유형을 선택하고 확인란을 선택하여 변경의 영향을 이해했는지 확인한 다음 * 변경 * 을 클릭합니다.

결과

Cloud Volumes ONTAP가 새 구성으로 재부팅됩니다.

Azure의 Cloud Volumes ONTAP HA 쌍에 대한 CIFS 잠금 재정의

계정 관리자는 BlueXP에서 Azure 유지 관리 이벤트 중에 Cloud Volumes ONTAP 스토리지 반환과 관련된 문제를 방지하는 설정을 활성화할 수 있습니다. 이 설정을 활성화하면 Cloud Volumes ONTAP가 CIFS 잠금을 확인하고 활성 CIFS 세션을 재설정합니다.

이 작업에 대해

Microsoft Azure는 가상 시스템에서 정기적인 유지 관리 이벤트를 예약합니다. Cloud Volumes ONTAP HA 쌍에서 유지보수 이벤트가 발생하면 HA 쌍이 스토리지 테이크오버 시작됩니다. 이 유지 관리 이벤트 중에 활성 CIFS 세션이 있는 경우 CIFS 파일의 잠금이 스토리지 반환을 방지할 수 있습니다.

이 설정을 활성화하면 Cloud Volumes ONTAP가 잠금을 거부하여 활성 CIFS 세션을 재설정합니다. 따라서 HA 쌍이 이러한 유지보수 이벤트 중에 스토리지 반환을 완료할 수 있습니다.

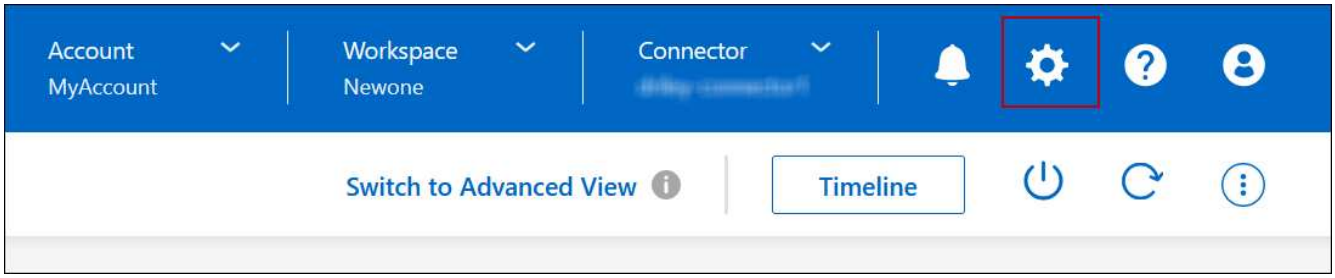
이 프로세스는 CIFS 클라이언트에 영향을 줄 수 있습니다. CIFS 클라이언트에서 커밋되지 않은 데이터는 손실될 수 있습니다.

필요한 것

BlueXP 설정을 변경하려면 먼저 커넥터를 만들어야 합니다. "자세히 알아보기".

단계

1. BlueXP 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 * Cloud Volumes ONTAP Settings * 를 선택합니다.



2. Azure * 에서 * Azure HA 작업 환경에 대한 * Azure CIFS 잠금을 클릭합니다.
3. 확인란을 클릭하여 기능을 활성화한 다음 * 저장 * 을 클릭합니다.

Azure Private Link 또는 서비스 끝점을 사용합니다

Cloud Volumes ONTAP는 Azure 프라이빗 링크를 사용하여 연결된 저장소 계정에 연결합니다. 필요한 경우 Azure Private Links를 비활성화하고 서비스 끝점을 대신 사용할 수 있습니다.

개요

기본적으로 BlueXP는 Cloud Volumes ONTAP과 관련 저장소 계정 간의 연결을 위해 Azure 개인 링크를 활성화합니다. Azure Private Link는 Azure의 엔드포인트 간 연결을 보호하고 성능상의 이점을 제공합니다.

필요한 경우 Azure 프라이빗 링크 대신 서비스 끝점을 사용하도록 Cloud Volumes ONTAP를 구성할 수 있습니다.

BlueXP는 두 가지 구성 모두 Cloud Volumes ONTAP 및 스토리지 계정 간의 연결을 위해 항상 네트워크 액세스를 제한합니다. 네트워크 액세스는 Cloud Volumes ONTAP가 배포된 VNET와 커넥터가 배포된 VNET로 제한됩니다.

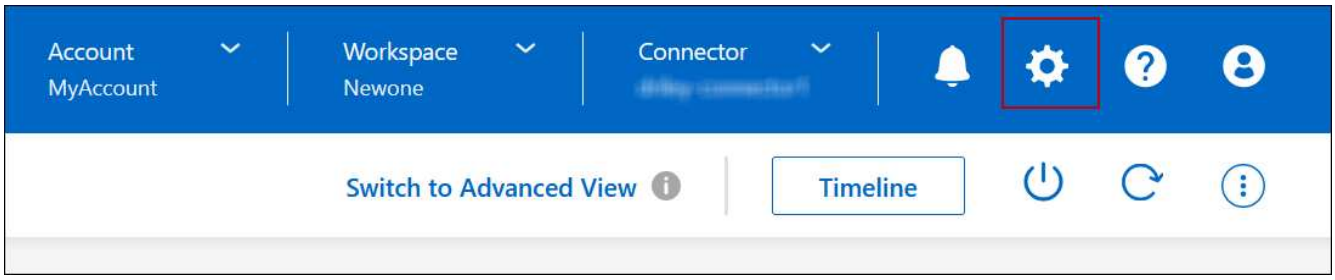
대신 Azure 전용 링크를 비활성화하고 서비스 끝점을 사용합니다

회사에서 요구하는 경우, BlueXP에서 Azure Private Link 대신 서비스 끝점을 사용하도록 Cloud Volumes ONTAP를 구성하도록 설정을 변경할 수 있습니다. 이 설정을 변경하면 새로 만든 Cloud Volumes ONTAP 시스템에 적용됩니다. 서비스 끝점은 에서만 지원됩니다 "Azure 지역 쌍" 커넥터와 Cloud Volumes ONTAP VNets 사이.

커넥터는 해당 커넥터가 관리하는 Cloud Volumes ONTAP 시스템과 동일한 Azure 영역에 배포하거나 에 배포되어야 합니다 "Azure 지역 쌍" Cloud Volumes ONTAP 시스템의 경우

단계

1. BlueXP 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 * Cloud Volumes ONTAP Settings * 를 선택합니다.



2. Azure * 에서 * Azure Private Link * 를 클릭합니다.
3. Cloud Volumes ONTAP 및 스토리지 계정 간 * 프라이빗 링크 연결을 선택 취소합니다.
4. 저장 * 을 클릭합니다.

작업을 마친 후

Azure Private Links를 사용하지 않도록 설정하고 Connector가 프록시 서버를 사용하는 경우 직접 API 트래픽을 활성화해야 합니다.

"Connector에서 직접 API 트래픽을 활성화하는 방법에 대해 알아봅니다"

Azure 개인 링크 사용

대부분의 경우 Cloud Volumes ONTAP로 Azure Private 링크를 설정할 필요가 없습니다. BlueXP는 Azure 프라이빗 링크를 관리합니다. 그러나 기존 Azure Private DNS 영역을 사용하는 경우에는 구성 파일을 편집해야 합니다.

사용자 지정 **DNS** 요구 사항

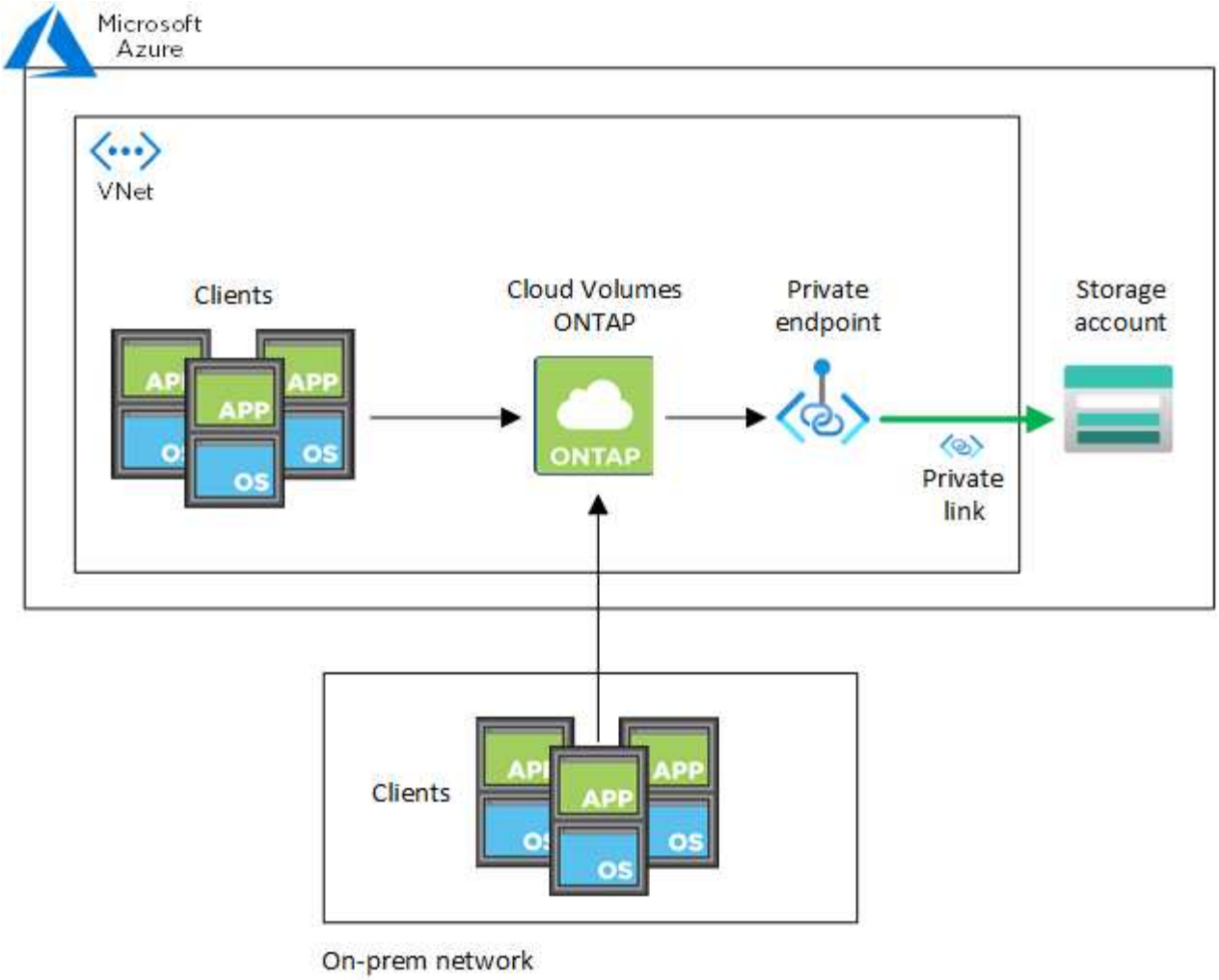
필요에 따라 사용자 지정 DNS로 작업하는 경우 사용자 지정 DNS 서버에서 Azure 개인 DNS 영역에 조건부 전달자를 만들어야 합니다. 자세한 내용은 을 참조하십시오 "DNS 전달자 사용에 대한 Azure의 설명서".

개별 링크 연결의 작동 방식

BlueXP는 Azure에 Cloud Volumes ONTAP를 배포할 때 리소스 그룹에 개인 끝점을 만듭니다. 프라이빗 엔드포인트는 Cloud Volumes ONTAP의 스토리지 계정과 연결되어 있습니다. 따라서 Cloud Volumes ONTAP 스토리지에 대한 액세스는 Microsoft 백본 네트워크를 통해 이루어집니다.

클라이언트가 Cloud Volumes ONTAP와 동일한 VNET 내에 있거나, 피어링된 VNets 내에 있거나, VNET에 대한 전용 VPN 또는 ExpressRoute 연결을 사용할 때 사내 네트워크에 있는 경우 클라이언트 액세스는 개인 링크를 통해 이루어집니다.

이 예에서는 동일한 VNET 내의 전용 링크와 전용 VPN 또는 ExpressRoute 연결이 있는 온프레미스 네트워크에서 클라이언트 액세스를 보여 줍니다.



> 커넥터 및 Cloud Volumes ONTAP 시스템이 다른 VNets에 구축된 경우 커넥터가 배포된 VNET와 Cloud Volumes ONTAP 시스템이 배포된 VNET 간에 VNET 피어링을 설정해야 합니다.

Azure 프라이빗 **DNS**에 대한 자세한 내용은 **BlueXP**를 참조하십시오

를 사용하는 경우 "Azure 프라이빗 DNS"그런 다음 각 Connector에서 설정 파일을 수정해야 합니다. 그렇지 않으면 BlueXP에서 Cloud Volumes ONTAP 및 관련 저장소 계정 간에 Azure Private Link 연결을 활성화할 수 없습니다.

DNS 이름은 Azure DNS 명명 요구 사항과 일치해야 합니다 "Azure 설명서에 나와 있는 대로 적용됩니다".

단계

1. 커넥터 호스트에 SSH로 접속하고 로그인합니다.
2. /opt/application/netapp/cloudmanager/docker_occm/data 디렉토리로 이동합니다
3. "user-private-dns-zone-settings" 매개 변수를 다음 키워드 값 쌍으로 추가하여 app.conf를 편집합니다.

```
"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
}
```

아래와 같이 "system-id"와 동일한 수준으로 매개 변수를 입력해야 합니다.

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

전용 DNS 영역이 Connector와 다른 구독에 있는 경우에만 subscription 키워드가 필요합니다.

4. 파일을 저장하고 Connector를 로그오프합니다.

   재부팅할 필요는 없습니다.

장애 시 롤백 사용

BlueXP가 특정 작업의 일부로 Azure Private Link를 생성하지 못할 경우 Azure Private Link 연결이 없어도 작업이 완료됩니다. 이는 새 작업 환경(단일 노드 또는 HA 쌍)을 생성하거나 HA 쌍에서 다음 작업이 발생하는 경우, 즉 새 애그리게이트 생성, 기존 애그리게이트에 디스크 추가, 32TiB 이상으로 진행할 때 발생할 수 있습니다.

BlueXP에서 Azure Private Link를 생성하지 못할 경우 롤백을 활성화하여 이 기본 동작을 변경할 수 있습니다. 이를 통해 회사의 보안 규정을 완벽하게 준수할 수 있습니다.

롤백을 활성화하면 BlueXP는 작업을 중지하고 작업의 일부로 생성된 모든 리소스를 롤백합니다.

API를 통해 또는 app.conf 파일을 업데이트하여 롤백을 활성화할 수 있습니다.

- API를 통한 롤백 활성화 *

단계

1. 다음 요청 본문과 함께 'Put/occm/config' API 호출 사용:

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

   - app.conf * 를 업데이트하여 롤백 기능을 활성화합니다

단계

1. 커넥터 호스트에 SSH로 접속하고 로그인합니다.
2. /opt/application/netapp/cloudmanager/docker_occm/data 디렉토리로 이동합니다
3. 다음 매개 변수와 값을 추가하여 app.conf를 편집합니다.

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

재부팅할 필요는 없습니다.

리소스 그룹 이동 중

Cloud Volumes ONTAP는 Azure 리소스 그룹 이동을 지원하지만 워크플로는 Azure 콘솔에서만 실행됩니다.

동일한 Azure 가입 내에서 하나의 리소스 그룹에서 Azure의 다른 리소스 그룹으로 작업 환경을 이동할 수 있습니다. 서로 다른 Azure 구독 간에 리소스 그룹을 이동하는 것은 지원되지 않습니다.

단계

1. Canvas * 에서 작업 환경을 제거합니다.

   작업 환경을 제거하는 방법에 대한 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP 작업 환경 제거".

2. Azure 콘솔에서 리소스 그룹 이동을 실행합니다.

   이동을 완료하려면 을 참조하십시오 "리소스를 새 리소스 그룹 또는 Microsoft Azure 설명서에 있는 구독으로 이동합니다".

3. Canvas * 에서 작업 환경을 검색합니다.
4. 작업 환경에 대한 정보에서 새 리소스 그룹을 찾습니다.

결과

작업 환경 및 해당 리소스(VM, 디스크, 스토리지 계정, 네트워크 인터페이스, 스냅샷)가 새 리소스 그룹에 있습니다.

Azure에서 SnapMirror 트래픽을 분리합니다

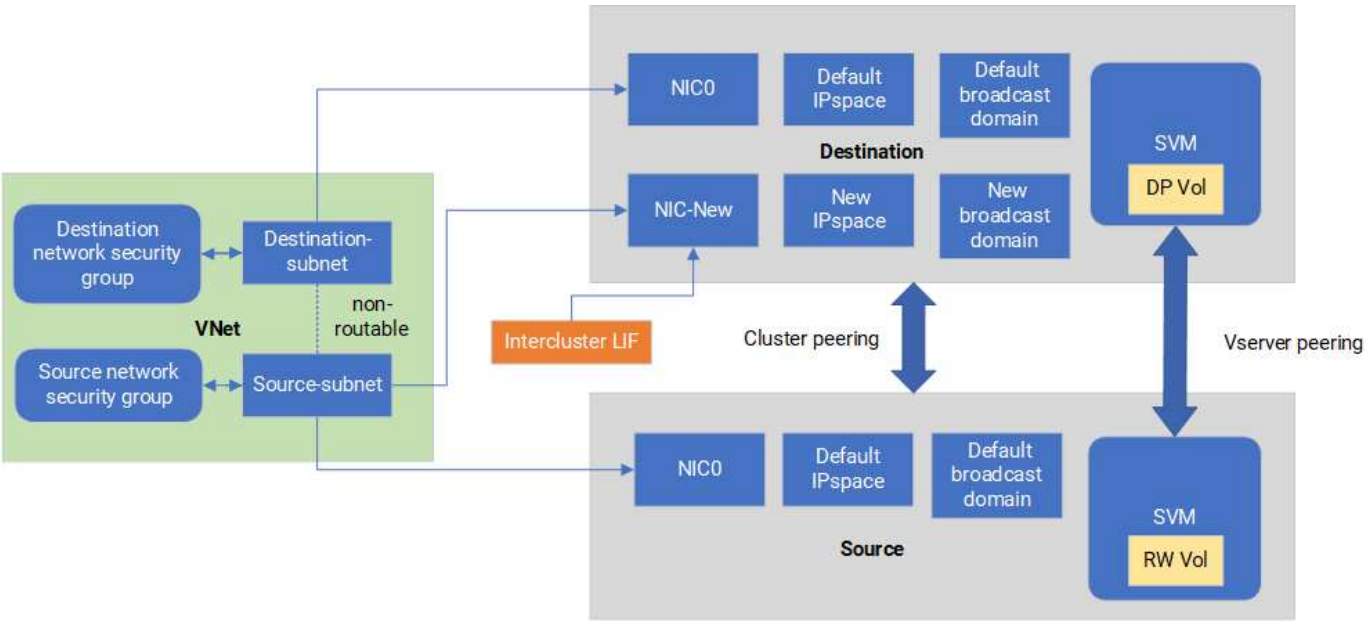
Azure의 Cloud Volumes ONTAP를 사용하면 SnapMirror 복제 트래픽을 데이터와 관리 트래픽에서 분리할 수 있습니다. SnapMirror 복제 트래픽을 데이터 트래픽에서 분리하려면 새 네트워크 인터페이스 카드(NIC), 관련 인터클러스터 LIF 및 라우팅할 수 없는 서브넷을 추가합니다.

Azure에서 SnapMirror 트래픽 분리 에 대해 자세히 알아보십시오

기본적으로 BlueXP는 동일한 서브넷에 있는 Cloud Volumes ONTAP 구축의 모든 NIC 및 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 활용합니다.

그림 **1**

다음 다이어그램은 단일 노드 배포에서 추가 NIC, 관련 인터클러스터 LIF 및 라우팅할 수 없는 서브넷과 SnapMirror 복제 트래픽의 분리 과정을 보여줍니다. HA 쌍 구축이 약간 다릅니다.



시작하기 전에

다음 고려 사항을 검토하십시오.

- SnapMirror 트래픽 분리를 위해 단일 NIC를 Cloud Volumes ONTAP 단일 노드 또는 HA 쌍 구축(VM 인스턴스)에 추가할 수 있습니다.
- 새 NIC를 추가하려면 배포하는 VM 인스턴스 유형에 미사용 NIC가 있어야 합니다.
- 소스 및 대상 클러스터는 동일한 VNet(Virtual Network)에 액세스할 수 있어야 합니다. 대상 클러스터는 Azure의 Cloud Volumes ONTAP 시스템입니다. 소스 클러스터는 Azure의 Cloud Volumes ONTAP 시스템 또는 ONTAP 시스템이 될 수 있습니다.

1단계: 추가 NIC를 생성하고 대상 VM에 연결합니다

이 섹션에서는 추가 NIC를 생성하여 대상 VM에 연결하는 방법에 대한 지침을 제공합니다. 대상 VM은 Cloud Volumes ONTAP의 Azure에서 추가 NIC를 설정하려는 단일 노드 또는 HA 쌍 시스템입니다.

단계

1. ONTAP CLI에서 노드를 중지합니다.

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

2. Azure 포털에서 VM(노드) 상태가 Stopped인지 확인합니다.

```
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. 노드 할당 해제

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

4. 두 서브넷(소스 클러스터 서브넷 및 대상 클러스터 서브넷)을 서로 라우팅할 수 없도록 네트워크 보안 그룹 규칙을 구성합니다.

   a. 대상 VM에 새 NIC를 생성합니다.

   b. 소스 클러스터 서브넷의 서브넷 ID를 조회합니다.

```
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 생성합니다. 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. privateIPAddress를 저장합니다. 이 IP 주소인 <new_added_nic_primary_addr>는 에서 인터클러스터 LIF를 생성하는 데 사용됩니다 새 NIC의 브로드캐스트 도메인, 인터클러스터 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 포털에서 * Networking * 으로 이동하여 새 NIC(예: NIC-NEW)가 존재하고 가속 네트워킹이 활성화되었는지 확인합니다.

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

HA 쌍 구축의 경우 파트너 노드에 대해 단계를 반복합니다.

2단계: 새 NIC에 대한 새 IPspace, 브로드캐스트 도메인 및 인터클러스터 LIF를 생성합니다

인터클러스터 LIF에 대한 별도의 IPspace를 통해 클러스터 간 복제를 위해 네트워킹 기능 간에 논리적으로 분리할 수 있습니다.

다음 단계에서는 ONTAP CLI를 사용합니다.

단계

1. 새 IPspace(new_IPspace)를 생성합니다.

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

2. 새 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 디스크가 있는 HA Pair 배포의 경우 새로 추가된 포트는_e0d_입니다. 페이지 Blob이 있는 HA 쌍 구축의 경우 새로 추가된 포트는_e0e_입니다. VM 이름이 아닌 노드 이름을 사용합니다. 를 실행하여 노드 이름을 찾습니다 `node show`.

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

4. 새 브로드캐스트 도메인(new_BD) 및 새 NIC(NIC-NEW)에 인터클러스터 LIF를 생성합니다.

```
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. 새 인터클러스터 LIF가 생성되었는지 확인합니다.

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

HA 쌍 구축의 경우 파트너 노드에 대해 단계를 반복합니다.

3단계: 소스 시스템과 타겟 시스템 간 클러스터 피어링을 확인합니다

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

다음 단계에서는 ONTAP CLI를 사용합니다.

단계

1. 대상 클러스터의 인터클러스터 LIF가 소스 클러스터의 인터클러스터 LIF를 ping할 수 있는지 확인합니다. 대상 클러스터가 이 명령을 실행하므로 대상 IP 주소가 소스에서 인터클러스터 LIF IP 주소가 됩니다.

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

2. 소스 클러스터의 인터클러스터 LIF가 대상 클러스터의 인터클러스터 LIF를 ping할 수 있는지 확인합니다. 대상은 대상에 생성된 새 NIC의 IP 주소입니다.

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

HA 쌍 구축의 경우 파트너 노드에 대해 단계를 반복합니다.

4단계: 소스 시스템과 타겟 시스템 간에 SVM 피어링을 생성합니다

이 섹션은 소스 시스템과 타겟 시스템 간에 SVM 피어링을 생성하는 방법에 대한 지침을 제공합니다.

다음 단계에서는 ONTAP CLI를 사용합니다.

단계

1. 소스 인터클러스터 LIF IP 주소를 로 사용하여 대상에서 클러스터 피어링을 생성합니다 `-peer-addrs`. HA 페어의 경우 두 노드에 대한 소스 인터클러스터 LIF IP 주소를 로 나열합니다 `-peer-addrs`.

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

2. 암호를 입력하고 확인합니다.
3. 타겟 클러스터 LIF IP 주소를 로 사용하여 소스에서 클러스터 피어링을 생성합니다 `peer-addrs`. HA 쌍의 경우, 두 노드의 대상 인터클러스터 LIF IP 주소를 로 나열합니다 `-peer-addrs`.

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

4. 암호를 입력하고 확인합니다.
5. 클러스터가 피어링되었는지 확인합니다.

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

성공적인 피어링은 가용성 필드에 * 사용 가능 * 을 표시합니다.

6. 타겟에서 SVM 피어링을 생성합니다. 소스 및 대상 SVM 모두 데이터 SVM이어야 합니다.

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

7. SVM 피어링을 수락합니다.

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

8. SVM이 피어링되었는지 확인합니다.

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

피어 상태가 표시됩니다 **`peered`**와 피어링 응용 프로그램이 표시됩니다 **`*`snapmirror`**.

5단계: 소스 시스템과 대상 시스템 사이에 SnapMirror 복제 관계를 생성합니다

이 섹션에서는 소스 시스템과 대상 시스템 간에 SnapMirror 복제 관계를 생성하는 방법에 대해 설명합니다.

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

다음 단계에서는 ONTAP CLI를 사용합니다.

단계

1. 대상 SVM에 데이터로 보호된 볼륨을 생성합니다.

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

2. 복제 일정 및 SnapMirror 정책을 포함하는 대상에서 SnapMirror 복제 관계를 생성합니다.

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

3. 타겟에서 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 입니다 `Snapmirrored` 그리고 관계의 상태는 이다 `true`.

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

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

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