



시작하십시오 Cloud Volumes ONTAP

NetApp
May 11, 2022

목차

| | |
|--|---|
| 시작하십시오 | 1 |
| Cloud Volumes ONTAP에 대해 자세히 알아보십시오 | 1 |
| Microsoft Azure에서 시작하십시오 | 2 |

시작하십시오

Cloud Volumes ONTAP에 대해 자세히 알아보십시오

Cloud Volumes ONTAP를 사용하면 클라우드 스토리지 비용과 성능을 최적화하는 동시에 데이터 보호, 보안 및 규정 준수를 향상할 수 있습니다.

Cloud Volumes ONTAP은 클라우드에서 ONTAP 데이터 관리 소프트웨어를 실행하는 소프트웨어 전용 스토리지 어플라이언스입니다. 엔터프라이즈급 스토리지에서 제공하는 주요 기능은 다음과 같습니다.

- 스토리지 효율성

내장된 데이터 중복제거, 데이터 압축, 씬 프로비저닝 및 복제를 활용하여 스토리지 비용을 최소화합니다.

- 고가용성

클라우드 환경에서 장애가 발생할 경우 엔터프라이즈급 안정성과 지속적인 운영을 보장합니다.

- 데이터 보호

Cloud Volumes ONTAP는 업계 최고 수준의 NetApp 복제 기술인 SnapMirror를 활용하여 사내 데이터를 클라우드로 복제하므로 여러 사용 사례에서 2차 복사본을 쉽게 사용할 수 있습니다.

Cloud Volumes ONTAP은 또한 클라우드 백업과 통합되어 클라우드 데이터를 보호하는 백업 및 복원 기능 및 장기간 아카이브할 수 있는 기능을 제공합니다.

["Cloud Backup에 대해 자세히 알아보십시오"](#)

- 데이터 계층화

애플리케이션을 오프라인으로 전환하지 않고도 필요에 따라 고성능 및 고성능 스토리지 풀 간에 전환할 수 있습니다.

- 애플리케이션 정합성

NetApp SnapCenter를 사용하여 NetApp Snapshot 복사본의 일관성을 보장합니다.

["SnapCenter에 대해 자세히 알아보십시오"](#)

- 데이터 보안

Cloud Volumes ONTAP는 데이터 암호화를 지원하고 바이러스 및 랜섬웨어에 대한 보호를 제공합니다.

- 개인 정보 보호 규정 준수 관리

클라우드 데이터 센스와 통합되어 데이터 컨텍스트를 이해하고 중요한 데이터를 식별할 수 있습니다.

["클라우드 데이터 센스에 대해 자세히 알아보십시오"](#)



ONTAP 기능에 대한 라이선스는 Cloud Volumes ONTAP에 포함되어 있습니다.

"지원되는 Cloud Volumes ONTAP 구성을 봅니다"

"Cloud Volumes ONTAP에 대해 자세히 알아보십시오"

Microsoft Azure에서 시작하십시오

Azure에서 Cloud Volumes ONTAP를 빠르게 시작합니다

몇 가지 단계를 통해 Azure용 Cloud Volumes ONTAP를 시작하십시오.

가 없는 경우 "커넥터" 그러나 계정 관리자는 계정을 만들어야 합니다. "Azure에서 커넥터를 만드는 방법에 대해 알아보십시오".

첫 번째 Cloud Volumes ONTAP 작업 환경을 생성할 때 아직 커넥터가 없는 경우 Cloud Manager에서 커넥터를 배포할지 묻는 메시지를 표시합니다.

Cloud Manager는 워크로드 요구사항에 맞게 사전 구성된 패키지를 제공하거나 자체 구성을 생성할 수 있습니다. 자신의 구성을 선택하는 경우 사용 가능한 옵션을 이해해야 합니다. "자세한 정보".

1. VNET와 서브넷이 커넥터와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인합니다.
2. 커넥터 및 Cloud Volumes ONTAP가 여러 엔드포인트에 연결할 수 있도록 대상 VNET에서 아웃바운드 인터넷 액세스를 활성화합니다.

이 단계는 커넥터가 아웃바운드 인터넷 액세스 없이 Cloud Volumes ONTAP를 관리할 수 없기 때문에 중요합니다. 아웃바운드 연결을 제한해야 하는 경우 의 끝점 목록을 참조하십시오 "커넥터 및 Cloud Volumes ONTAP".

"네트워킹 요구 사항에 대해 자세히 알아보십시오".

작업 환경 추가 * 를 클릭하고 배포할 시스템 유형을 선택한 다음 마법사의 단계를 완료합니다. "단계별 지침을 읽습니다".

관련 링크

- "Cloud Manager에서 커넥터 생성"
- "Azure Marketplace에서 커넥터 만들기"
- "Linux 호스트에 Connector 소프트웨어 설치"
- "Cloud Manager가 권한을 가지고 하는 일"

Azure에서 Cloud Volumes ONTAP 구성 계획

Azure에서 Cloud Volumes ONTAP를 구축할 때 워크로드 요구사항에 맞게 사전 구성된 시스템을 선택하거나 고유한 구성을 생성할 수 있습니다. 자신의 구성을 선택하는 경우 사용 가능한 옵션을 이해해야 합니다.

지원되는 영역 보기

Cloud Volumes ONTAP는 대부분의 Microsoft Azure 지역에서 지원됩니다. ["지원되는 영역의 전체 목록을 봅니다"](#).

라이선스 선택

Cloud Volumes ONTAP에는 몇 가지 라이선스 옵션이 있습니다. 각 옵션을 사용하여 요구사항에 맞는 소비 모델을 선택할 수 있습니다. ["Cloud Volumes ONTAP의 라이선스 옵션에 대해 자세히 알아보십시오"](#).

지원되는 VM 유형입니다

Cloud Volumes ONTAP는 선택한 라이선스 유형에 따라 여러 VM 유형을 지원합니다.

["Azure에서 Cloud Volumes ONTAP에 대해 지원되는 구성입니다"](#)

스토리지 제한 이해

Cloud Volumes ONTAP 시스템의 물리적 용량 제한은 라이선스에 연결되어 있습니다. 추가 제한은 애그리게이트 및 볼륨 크기에 영향을 줍니다. 구성을 계획할 때 이러한 제한 사항을 숙지해야 합니다.

["Azure의 Cloud Volumes ONTAP에 대한 스토리지 제한"](#)

Azure에서 시스템 사이징

Cloud Volumes ONTAP 시스템을 사이징하면 성능 및 용량 요구사항을 충족하는 데 도움이 될 수 있습니다. VM 유형, 디스크 유형 및 디스크 크기를 선택할 때 고려해야 할 몇 가지 주요 사항은 다음과 같습니다.

가상 머신 유형입니다

에서 지원되는 가상 머신 유형을 확인합니다 ["Cloud Volumes ONTAP 릴리즈 노트"](#) 지원되는 각 VM 유형에 대한 세부 정보를 검토합니다. 각 VM 유형은 특정 수의 데이터 디스크를 지원합니다.

- ["Azure 설명서: 범용 가상 머신 크기"](#)
- ["Azure 설명서: 메모리에 최적화된 가상 머신 크기"](#)

Azure 디스크 유형입니다

Cloud Volumes ONTAP용 볼륨을 생성할 때 Cloud Volumes ONTAP가 디스크로 사용하는 기본 클라우드 스토리지를 선택해야 합니다.

HA 시스템은 프리미엄 페이지 Blob을 사용합니다. 한편, 단일 노드 시스템에서는 두 가지 유형의 Azure 관리 디스크를 사용할 수 있습니다.

- *Premium SSD* 관리 디스크 높은 비용으로 I/O 집약적인 작업 부하에 높은 성능을 제공합니다.
- *_Standard SSD Managed Disks_*는 낮은 IOPS가 필요한 워크로드에 일관된 성능을 제공합니다.
- *_표준 HDD 관리 디스크_*는 높은 IOPS가 필요하지 않고 비용을 절감하려는 경우에 적합합니다.

이러한 디스크의 사용 사례에 대한 자세한 내용은 를 참조하십시오 ["Microsoft Azure 설명서: Azure에서 사용할 수 있는 디스크 유형은 무엇입니까?"](#).

Azure 디스크 크기입니다

Cloud Volumes ONTAP 인스턴스를 시작할 때 Aggregate의 기본 디스크 크기를 선택해야 합니다. Cloud Manager에서는 이 디스크 크기를 초기 aggregate와 단순 프로비저닝 옵션을 사용할 때 생성되는 추가 애그리게이트에 사용합니다. 예서는 기본적으로 와는 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다 ["고급 할당 옵션을 사용합니다"](#).



Aggregate의 모든 디스크는 동일한 크기여야 합니다.

디스크 크기를 선택할 때는 몇 가지 요소를 고려해야 합니다. 디스크 크기는 스토리지에 대한 비용 지불, 애그리게이트에서 생성할 수 있는 볼륨 크기, Cloud Volumes ONTAP에 사용할 수 있는 총 용량 및 스토리지 성능에 영향을 줍니다.

Azure 프리미엄 스토리지의 성능은 디스크 크기와 관련이 있습니다. 디스크가 클수록 IOPS와 처리량이 높아집니다. 예를 들어, 1TiB 디스크를 선택하면 더 높은 비용으로 500GiB 디스크보다 뛰어난 성능을 제공할 수 있습니다.

표준 스토리지의 디스크 크기 간에는 성능 차이가 없습니다. 필요한 용량에 따라 디스크 크기를 선택해야 합니다.

IOPS 및 디스크 크기별 처리량은 Azure를 참조하십시오.

- ["Microsoft Azure: 관리형 디스크 가격"](#)
- ["Microsoft Azure: 페이지 Blob 가격 책정"](#)

Flash Cache를 지원하는 구성 선택

Azure의 Cloud Volumes ONTAP 구성에는 Cloud Volumes ONTAP이 성능 향상을 위해 _ Flash Cache _ 로 사용하는 로컬 NVMe 스토리지가 포함됩니다. ["Flash Cache에 대해 자세히 알아보십시오"](#).

기본 시스템 디스크를 봅니다

사용자 데이터를 위한 스토리지 외에, Cloud Manager는 Cloud Volumes ONTAP 시스템 데이터(부팅 데이터, 루트 데이터, 코어 데이터, NVRAM)를 위한 클라우드 스토리지도 구매합니다. 계획을 위해 Cloud Volumes ONTAP를 배포하기 전에 이러한 세부 정보를 검토하는 것이 도움이 될 수 있습니다.

["Azure에서 Cloud Volumes ONTAP 시스템 데이터에 대한 기본 디스크를 봅니다"](#).



커넥터에는 시스템 디스크도 필요합니다. ["커넥터의 기본 설정에 대한 세부 정보를 봅니다"](#).

Azure 네트워크 정보 워크시트

Azure에서 Cloud Volumes ONTAP를 구축할 때는 가상 네트워크에 대한 세부 정보를 지정해야 합니다. 워크시트를 사용하여 관리자로부터 정보를 수집할 수 있습니다.

| Azure 정보 | 귀사의 가치 |
|---------------------|--------|
| 지역 | |
| VNet(가상 네트워크) | |
| 서브넷 | |
| 네트워크 보안 그룹(자체 사용 시) | |

쓰기 속도 선택

Cloud Manager를 사용하면 Cloud Volumes ONTAP의 쓰기 속도 설정을 선택할 수 있습니다. 쓰기 속도를 선택하기 전에 고속 쓰기 속도를 사용할 때 정상 및 높음 설정의 차이점과 위험 및 권장 사항을 이해해야 합니다. "[쓰기 속도에 대해 자세히 알아보십시오](#)".

볼륨 사용 프로필 선택

ONTAP에는 필요한 총 스토리지 양을 줄일 수 있는 몇 가지 스토리지 효율성 기능이 포함되어 있습니다. Cloud Manager에서 볼륨을 생성할 때 이러한 기능을 사용하도록 설정하는 프로필이나 기능을 사용하지 않도록 설정하는 프로필을 선택할 수 있습니다. 사용할 프로파일을 결정하는 데 도움이 되도록 이러한 기능에 대해 자세히 알아 두어야 합니다.

NetApp 스토리지 효율성 기능은 다음과 같은 이점을 제공합니다.

스핀 프로비저닝

에서는 실제 스토리지 풀에 있는 것보다 더 많은 논리적 스토리지를 호스트 또는 사용자에게 제공합니다. 스토리지 공간을 사전에 할당하는 대신 데이터가 기록될 때 스토리지 공간을 각 볼륨에 동적으로 할당합니다.

중복 제거

동일한 데이터 블록을 찾아 단일 공유 블록에 대한 참조로 대체하여 효율성을 향상시킵니다. 이 기술은 동일한 볼륨에 상주하는 중복된 데이터 블록을 제거하여 스토리지 용량 요구 사항을 줄여줍니다.

압축

1차, 2차 및 아카이브 스토리지의 볼륨 내에서 데이터를 압축하여 데이터를 저장하는 데 필요한 물리적 용량을 줄입니다.

Azure의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항

Cloud Volumes ONTAP 시스템이 올바르게 작동할 수 있도록 Azure 네트워킹을 설정합니다. 여기에는 커넥터 및 Cloud Volumes ONTAP에 대한 네트워킹이 포함됩니다.

Cloud Volumes ONTAP에 대한 요구사항

Azure에서 다음 네트워킹 요구사항을 충족해야 합니다.

아웃바운드 인터넷 액세스

Cloud Volumes ONTAP에서 스토리지 상태를 능동적으로 모니터링하는 NetApp AutoSupport에 메시지를 보내려면 아웃바운드 인터넷 액세스가 필요합니다.

라우팅 및 방화벽 정책은 Cloud Volumes ONTAP가 AutoSupport 메시지를 보낼 수 있도록 다음 엔드포인트에 대한 HTTP/HTTPS 트래픽을 허용해야 합니다.

- <https://support.netapp.com/aods/asupmessage> 으로 문의하십시오
- <https://support.netapp.com/asupprod/post/1.0/postAsup> 으로 문의하십시오

"[AutoSupport 확인 방법을 알아보십시오](#)".

IP 주소

Cloud Manager는 Azure의 Cloud Volumes ONTAP에 다음과 같은 수의 IP 주소를 할당합니다.

- 단일 노드: 5개의 IP 주소
- HA 쌍: 16개의 IP 주소

Cloud Manager는 HA 쌍에서 SVM 관리 LIF를 생성하지만 Azure의 단일 노드 시스템에는 없습니다.



LIF는 물리적 포트와 연결된 IP 주소입니다. SnapCenter와 같은 관리 툴을 사용하려면 SVM 관리 LIF가 필요합니다.

Azure 서비스에 대한 보안 연결

클라우드 관리자는 Cloud Volumes ONTAP가 Azure 서비스에 개인적으로 연결할 수 있도록 VNET 서비스 끝점과 Azure 프라이빗 링크 끝점을 설정합니다.

서비스 엔드포인트

Cloud Manager를 사용하면 VNET 서비스 엔드포인트를 통해 Cloud Volumes ONTAP에서 데이터 계층화를 위한 Azure Blob 스토리지로 보안 연결을 생성할 수 있습니다. Cloud Volumes ONTAP에서 Azure 서비스로 지원되는 추가 서비스 엔드포인트는 없습니다.

Cloud Manager 정책에 다음과 같은 권한이 있는 경우 Cloud Manager를 통해 VNET 서비스 엔드포인트를 사용할 수 있습니다.

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

이러한 권한은 최신 에 포함되어 있습니다 ["Cloud Manager 정책"](#).

데이터 계층화 설정에 대한 자세한 내용은 을 참조하십시오 ["콜드 데이터를 저비용 오브젝트 스토리지로 계층화"](#).

개인 엔드포인트

기본적으로 Cloud Manager는 Cloud Volumes ONTAP과 관련 스토리지 계정 간의 Azure 프라이빗 링크 연결을 지원합니다. 프라이빗 링크는 Azure의 엔드포인트 간 연결을 보호하고 성능상의 이점을 제공합니다. 대부분의 경우 Cloud Manager는 Azure Private Link를 관리합니다. 그러나 Azure Private DNS를 사용하는 경우에는 구성 파일을 편집해야 합니다. 필요한 경우 비공개 링크 연결을 비활성화할 수도 있습니다.

["Cloud Volumes ONTAP에서 Azure 프라이빗 링크를 사용하는 방법에 대해 자세히 알아보십시오"](#).

다른 ONTAP 시스템에 대한 연결

Azure의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 Azure VNET와 다른 네트워크(예: 기업 네트워크) 간에 VPN 연결이 있어야 합니다.

자세한 지침은 을 참조하십시오 ["Microsoft Azure 문서: Azure 포털에서 사이트 간 연결을 만듭니다"](#).

HA 인터커넥트용 포트입니다

Cloud Volumes ONTAP HA 쌍에는 HA 인터커넥트가 포함되어 있어 각 노드가 해당 파트너의 작동 여부를 지속적으로 확인하고 다른 노드의 비휘발성 메모리에 대한 로그 데이터를 미러링할 수 있습니다. HA 인터커넥트에서는 통신에 TCP 포트 10006을 사용합니다.

기본적으로 HA 인터커넥트 LIF 간 통신은 열려 있으며 이 포트에 대한 보안 그룹 규칙이 없습니다. 하지만 HA 인터커넥트 LIF 간에 방화벽을 생성하는 경우, HA 쌍이 제대로 작동할 수 있도록 TCP 트래픽이 포트 10006에 대해 열려 있는지 확인해야 합니다.

Azure 리소스 그룹에서는 하나의 **HA** 쌍만 제공됩니다

Azure에 구축하는 각 Cloud Volumes ONTAP HA 쌍에 대해 `_Dedicated_resource` 그룹을 사용해야 합니다. 리소스 그룹에서는 하나의 HA 쌍만 지원됩니다.

Azure 리소스 그룹에 두 번째 Cloud Volumes ONTAP HA 쌍을 구축하려고 하면 Cloud Manager에서 연결 문제가 발생합니다.

보안 그룹

Cloud Manager가 보안 그룹을 생성할 필요가 없습니다. 직접 사용해야 하는 경우 아래 나열된 보안 그룹 규칙을 참조하십시오.

보안 그룹 규칙

Cloud Manager는 Cloud Volumes ONTAP가 성공적으로 운영하는 데 필요한 인바운드 및 아웃바운드 규칙을 포함하는 Azure 보안 그룹을 생성합니다. 테스트 목적으로 또는 자체 보안 그룹을 사용하려는 경우 포트를 참조할 수 있습니다.

Cloud Volumes ONTAP의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

단일 노드 시스템에 대한 인바운드 규칙입니다

아래 나열된 규칙은 특정 인바운드 트래픽을 차단한다는 설명이 없는 한 트래픽을 허용합니다.

| 우선 순위 및 이름 | 포트 및 프로토콜 | 소스 및 대상 | 설명 |
|----------------------|------------------|---------|---|
| 1000 inbound_ssh | 22 TCP | 모두 해당 | 클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다 |
| 1001 인바운드_http | TCP 80개 | 모두 해당 | 클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTP 액세스 |
| 1002 inbound_111_tcp | 111 TCP | 모두 해당 | NFS에 대한 원격 프로시저 호출 |
| 1003 인바운드_111_UDP | 111 UDP | 모두 해당 | NFS에 대한 원격 프로시저 호출 |
| 1004 인바운드_139 | 139 TCP 를 참조하십시오 | 모두 해당 | CIFS에 대한 NetBIOS 서비스 세션입니다 |

| 우선 순위 및 이름 | 포트 및 프로토콜 | 소스 및 대상 | 설명 |
|--------------------------------------|-----------------|---------------------------------|--|
| 1005 inbound_161-162_tcp | 161-162 TCP | 모두 해당 | 단순한 네트워크 관리 프로토콜 |
| 1006 inbound_161-162_udp | 161-162 UDP | 모두 해당 | 단순한 네트워크 관리 프로토콜 |
| 1007 인바운드_443 | 443 TCP | 모두 해당 | 클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTPS 액세스 |
| 1008 인바운드_445 | 445 TCP | 모두 해당 | Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임 |
| 1009 인바운드_635_TCP | 635 TCP | 모두 해당 | NFS 마운트 |
| 1010 inbound_635_udp | 635 UDP | 모두 해당 | NFS 마운트 |
| 1011 인바운드_749 | 749 TCP | 모두 해당 | Kerberos |
| 1012 인바운드_2049_TCP | 2049 TCP | 모두 해당 | NFS 서버 데몬 |
| 1013 인바운드_2049_UDP | 2049 UDP | 모두 해당 | NFS 서버 데몬 |
| 1014 인바운드_3260 | 3260 TCP | 모두 해당 | iSCSI 데이터 LIF를 통한 iSCSI 액세스 |
| 1015 인바운드_4045-4046_TCP | 4045-4046 TCP | 모두 해당 | NFS 잠금 데몬 및 네트워크 상태 모니터 |
| 1016 인바운드_4045-4046_UDP | 4045-4046 UDP | 모두 해당 | NFS 잠금 데몬 및 네트워크 상태 모니터 |
| 1017 inbound_10000 | 10000 TCP | 모두 해당 | NDMP를 사용한 백업 |
| 1018 인바운드_11104-11105 | 11104-11105 TCP | 모두 해당 | SnapMirror 데이터 전송 |
| 3000 inbound_deny_all_tcp입니다 | 모든 포트 TCP | 모두 해당 | 다른 모든 TCP 인바운드 트래픽을 차단합니다 |
| 3001 inbound_deny_all_udp | 모든 포트 UDP | 모두 해당 | 다른 모든 UDP 인바운드 트래픽을 차단합니다 |
| 65000 AllowVnetInBound | 모든 포트 모든 프로토콜 | VirtualNetwork - VirtualNetwork | VNET 내에서 들어오는 인바운드 트래픽입니다 |
| 65001 AllowAzureLoad BalancerInBound | 모든 포트 모든 프로토콜 | 어느 것이든 AzureLoadBalancer를 사용합니다 | Azure 표준 로드 밸런서의 데이터 트래픽 |
| 65500 DenyAllInBound | 모든 포트 모든 프로토콜 | 모두 해당 | 다른 모든 인바운드 트래픽을 차단합니다 |

HA 시스템에 대한 인바운드 규칙

아래 나열된 규칙은 특정 인바운드 트래픽을 차단한다는 설명이 없는 한 트래픽을 허용합니다.



인바운드 데이터 트래픽이 Azure 표준 로드 밸런서를 통과하기 때문에 HA 시스템은 단일 노드 시스템보다 인바운드 규칙이 적습니다. 따라서 "AllowAzureLoadBalancerInBound" 규칙에 나와 있는 것처럼 로드 밸런서의 트래픽이 열려 있어야 합니다.

| 우선 순위 및 이름 | 포트 및 프로토콜 | 소스 및 대상 | 설명 |
|--------------------------------------|---------------|---------------------------------|--|
| 100 inbound_443 | 443 모든 프로토콜 | 모두 해당 | 클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTPS 액세스 |
| 101 inbound_111_tcp | 111 모든 프로토콜 | 모두 해당 | NFS에 대한 원격 프로시저 호출 |
| 102 inbound_2049_tcp | 2049 모든 프로토콜 | 모두 해당 | NFS 서버 데몬 |
| 111 inbound_ssh | 22 모든 프로토콜 | 모두 해당 | 클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다 |
| 121 인바운드_53 | 53 모든 프로토콜 | 모두 해당 | DNS 및 CIFS를 지원합니다 |
| 65000 AllowVnetInBound | 모든 포트 모든 프로토콜 | VirtualNetwork - VirtualNetwork | VNET 내에서 들어오는 인바운드 트래픽입니다 |
| 65001 AllowAzureLoad BalancerInBound | 모든 포트 모든 프로토콜 | 어느 것이든 AzureLoadBalancer를 사용합니다 | Azure 표준 로드 밸런서의 데이터 트래픽 |
| 65500 DenyAllInBound | 모든 포트 모든 프로토콜 | 모두 해당 | 다른 모든 인바운드 트래픽을 차단합니다 |

아웃바운드 규칙

Cloud Volumes ONTAP에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

Cloud Volumes ONTAP에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

| 포트 | 프로토콜 | 목적 |
|----|--------|--------------|
| 모두 | 모든 TCP | 모든 아웃바운드 트래픽 |
| 모두 | 모든 UDP | 모든 아웃바운드 트래픽 |

고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Cloud Volumes ONTAP의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.



소스는 Cloud Volumes ONTAP 시스템의 인터페이스(IP 주소)입니다.

| 서비스 | 포트 | 프로 토콜 | 출처 | 목적지 | 목적 |
|---------------------------------------|----|----------|----|-----|----|
| Active Directory 를 클릭합니 다 | | | | | |

| | | | | | |
|--------------------|-------------|-------------|--------------------------------|--------------------------|---|
| | 404 | TCP | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | Kerberos V 변경 및 암호 설정(set_change) |
| 서비스 | 464 포트 | UDP 프로토콜 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | Kerberos 키 관리 목적 |
| | 749 | TCP | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | Kerberos V 변경 및 암호 설정(RPCSEC_GSS) |
| AutoSupport | HTTPS | 443 | 노드 관리 LIF | support.netapp.com | AutoSupport(기본값은 HTTPS) |
| | HTTP | 80 | 노드 관리 LIF | support.netapp.com | AutoSupport(전송 프로토콜이 HTTPS에서 HTTP로 변경된 경우에만 해당) |
| DHCP를 선택합니다 | 68 | UDP 입니다 | 노드 관리 LIF | DHCP를 선택합니다 | 처음으로 설정하는 DHCP 클라이언트 |
| DHCPs | 67 | UDP 입니다 | 노드 관리 LIF | DHCP를 선택합니다 | DHCP 서버 |
| DNS | 53 | UDP 입니다 | 노드 관리 LIF 및 데이터 LIF(NFS, CIFS) | DNS | DNS |
| NDMP | 18600–18699 | TCP | 노드 관리 LIF | 대상 서버 | NDMP 복제 |
| SMTP | 25 | TCP | 노드 관리 LIF | 메일 서버 | AutoSupport에 사용할 수 있는 SMTP 경고 |
| SNMP를 선택합니다 | 161 | TCP | 노드 관리 LIF | 서버 모니터링 | SNMP 트랩으로 모니터링 |
| | 161 | UDP 입니다 | 노드 관리 LIF | 서버 모니터링 | SNMP 트랩으로 모니터링 |
| | 162 | TCP | 노드 관리 LIF | 서버 모니터링 | SNMP 트랩으로 모니터링 |
| | 162 | UDP 입니다 | 노드 관리 LIF | 서버 모니터링 | SNMP 트랩으로 모니터링 |
| SnapMirror를 참조하십시오 | 11104 | TCP | 인터클러스터 LIF | ONTAP 인터클러스터 LIF | SnapMirror에 대한 인터클러스터 통신 세션의 관리 |
| | 11105 | TCP | 인터클러스터 LIF | ONTAP 인터클러스터 LIF | SnapMirror 데이터 전송 |
| Syslog를 클릭합니다 | 514 | UDP 입니다 | 노드 관리 LIF | Syslog 서버 | Syslog 메시지를 전달합니다 |

커넥터 요구 사항

Connector가 공용 클라우드 환경 내에서 리소스와 프로세스를 관리할 수 있도록 네트워킹을 설정합니다. 가장 중요한 단계는 다양한 엔드포인트에 대한 아웃바운드 인터넷 액세스를 보장하는 것입니다.



네트워크에서 인터넷에 대한 모든 통신에 프록시 서버를 사용하는 경우 설정 페이지에서 프록시 서버를 지정할 수 있습니다. 을 참조하십시오 ["프록시 서버를 사용하도록 Connector 구성"](#).

대상 네트워크에 대한 연결

커넥터를 사용하려면 Cloud Volumes ONTAP를 배포할 VPC 및 VNets에 대한 네트워크 연결이 필요합니다.

예를 들어 회사 네트워크에 커넥터를 설치하는 경우 Cloud Volumes ONTAP를 실행하는 VPC 또는 VNET에 대한 VPN 연결을 설정해야 합니다.

아웃바운드 인터넷 액세스

Connector를 사용하려면 공용 클라우드 환경 내의 리소스와 프로세스를 관리하기 위한 아웃바운드 인터넷 액세스가 필요합니다.

| 엔드포인트 | 목적 |
|--|--|
| https://support.netapp.com 으로 문의하십시오 | 라이선스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다. |
| https://*.cloudmanager.cloud.netapp.com 으로 문의하십시오 | Cloud Manager 내에서 SaaS 기능 및 서비스를 제공합니다. |
| https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net 으로 문의하십시오 | Connector 및 해당 Docker 구성 요소를 업그레이드합니다. |

보안 그룹 규칙

Connector의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

인바운드 규칙

| 포트 | 프로토콜 | 목적 |
|-----|------------|---|
| 22 | SSH를 클릭합니다 | 커넥터 호스트에 대한 SSH 액세스를 제공합니다 |
| 80 | HTTP | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다 |
| 443 | HTTPS | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTPS 액세스를 제공합니다 |

아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

| 포트 | 프로토콜 | 목적 |
|----|--------|--------------|
| 모두 | 모든 TCP | 모든 아웃바운드 트래픽 |
| 모두 | 모든 UDP | 모든 아웃바운드 트래픽 |

고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Connector의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.



소스 IP 주소는 커넥터 호스트입니다.

| 서비스 | 포트 | 프로토콜 | 목적지 | 목적 |
|----------------------|-----|--------|-------------------------------|--|
| API 호출 및 AutoSupport | 443 | HTTPS | 아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF | API는 Azure 및 ONTAP, 클라우드 데이터 감지, 랜섬웨어 서비스 요청, AutoSupport 메시지를 NetApp에 전송합니다 |
| DNS | 53 | UDP입니다 | DNS | Cloud Manager에서 DNS Resolve에 사용됩니다 |

Azure에서 고객이 관리하는 키를 사용하도록 **Cloud Volumes ONTAP**를 설정합니다

Azure의 Cloud Volumes ONTAP에서 를 사용하여 데이터가 자동으로 암호화됩니다 "[Azure 스토리지 서비스 암호화](#)" Microsoft 관리 키를 사용합니다. 그러나 이 페이지의 단계를 따르면 사용자 고유의 암호화 키를 사용할 수 있습니다.

데이터 암호화 개요

Cloud Volumes ONTAP 데이터는 를 사용하여 Azure에서 자동으로 암호화됩니다 "[Azure 스토리지 서비스 암호화](#)". 기본 구현에는 Microsoft 관리 키가 사용됩니다. 설정이 필요하지 않습니다.

Cloud Volumes ONTAP에서 고객 관리 키를 사용하려면 다음 단계를 완료해야 합니다.

1. Azure에서 키 볼트를 작성한 다음 해당 볼트에 키를 생성합니다
2. Cloud Manager에서 API를 사용하여 키를 사용하는 Cloud Volumes ONTAP 작업 환경을 생성합니다

키 회전

새 버전의 키를 만들면 Cloud Volumes ONTAP에서 자동으로 최신 키 버전을 사용합니다.

데이터 암호화 방법

고객이 관리하는 키를 사용하도록 구성된 Cloud Volumes ONTAP 작업 환경을 생성한 후 Cloud Volumes ONTAP 데이터는 다음과 같이 암호화됩니다.

HA 쌍

- Cloud Volumes ONTAP의 모든 Azure 저장소 계정은 고객이 관리하는 키를 사용하여 암호화됩니다.
- 디스크 또는 애그리게이트를 추가하는 경우와 같이 새로운 스토리지 계정에서도 동일한 키를 사용합니다.

단일 노드

- Cloud Volumes ONTAP의 모든 Azure 저장소 계정은 고객이 관리하는 키를 사용하여 암호화됩니다.
- 루트, 부팅 및 데이터 디스크의 경우 Cloud Manager는 를 사용합니다 ["디스크 암호화가 설정되었습니다"](#)관리 디스크를 사용하여 암호화 키를 관리할 수 있습니다.
- 새 데이터 디스크도 동일한 디스크 암호화 세트를 사용합니다.
- NVRAM과 코어 디스크는 고객이 관리하는 키 대신 Microsoft 관리 키를 사용하여 암호화됩니다.

키 볼트를 작성하고 키를 생성합니다

키 볼트는 Cloud Volumes ONTAP 시스템을 생성하려는 Azure 가입 및 지역에 있어야 합니다.

단계

1. ["Azure 구독에서 키 볼트를 작성합니다"](#).

키 볼트에 대한 다음 요구 사항을 확인합니다.

- 키 볼트는 Cloud Volumes ONTAP 시스템과 동일한 영역에 있어야 합니다.
- 다음 옵션을 활성화해야 합니다.
 - * soft-delete * (이 옵션은 기본적으로 활성화되어 있지만 반드시 _not_ 사용하지 않아야 함)
 - * 퍼지 보호 *
 - * 볼륨 암호화를 위한 Azure 디스크 암호화 * (단일 노드 Cloud Volumes ONTAP 시스템에만 해당)

2. ["키 볼트에 키를 생성합니다"](#).

키에 대한 다음 요구 사항을 확인합니다.

- 키 유형은 * rsa * 여야 합니다.
- 권장되는 RSA 키 크기는 * 2048 * 이지만 다른 크기가 지원됩니다.

암호화 키를 사용하는 작업 환경을 만듭니다

키 볼트를 작성하고 암호화 키를 생성한 후 키를 사용하도록 구성된 새 Cloud Volumes ONTAP 시스템을 작성할 수 있습니다. 이러한 단계는 Cloud Manager API를 사용하여 지원됩니다.

단일 노드 Cloud Volumes ONTAP 시스템에서 고객 관리 키를 사용하려면 Cloud Manager Connector에 다음 권한이 있는지 확인합니다.

```
"Microsoft.Compute/diskEncryptionSets/read"  
"Microsoft.Compute/diskEncryptionSets/write",  
"Microsoft.Compute/diskEncryptionSets/delete"  
"Microsoft.KeyVault/vaults/deploy/action",  
"Microsoft.KeyVault/vaults/read",  
"Microsoft.KeyVault/vaults/accessPolicies/write"
```

에서 최신 사용 권한 목록을 찾을 수 있습니다 ["Cloud Manager 정책 페이지"](#).

HA 쌍에는 이러한 권한이 필요하지 않습니다.

단계

1. 다음 Cloud Manager API 호출을 사용하여 Azure 구독의 키 볼트 목록을 가져옵니다.

HA 쌍의 경우: 'get/Azure/ha/metadata/vaults'

단일 노드의 경우: 'get/Azure/VSA/metadata/vaults'

이름 * 과 * resourceGroup * 을 기록해 둡니다. 다음 단계에서 이러한 값을 지정해야 합니다.

["이 API 호출에 대해 자세히 알아보십시오"](#).

2. 다음 Cloud Manager API 호출을 사용하여 볼트 내의 키 목록을 가져옵니다.

HA 쌍의 경우: 'get/Azure/ha/metadata/keys-vault'

단일 노드의 경우: 'get/Azure/VSA/metadata/keys-vault'

keyName * 을 기록해 두십시오. 다음 단계에서 해당 값을 볼트 이름과 함께 지정해야 합니다.

["이 API 호출에 대해 자세히 알아보십시오"](#).

3. 다음 Cloud Manager API 호출을 사용하여 Cloud Volumes ONTAP 시스템을 생성합니다.

a. HA 쌍:

'POST/Azure/ha/Working-Environments(POST/Azure/ha/Working-Environments

요청 본문에는 다음 필드가 포함되어야 합니다.

```
"azureEncryptionParameters": {  
  "key": "keyName",  
  "vaultName": "vaultName"  
}
```

["이 API 호출에 대해 자세히 알아보십시오"](#).

b. 단일 노드 시스템의 경우:

'POST/Azure/VSA/Working-Environments(POST/Azure/VSA/작업 환경)

요청 본문에는 다음 필드가 포함되어야 합니다.

```
"azureEncryptionParameters": {  
  "key": "keyName",  
  "vaultName": "vaultName"  
}
```

+

"이 API 호출에 대해 자세히 알아보십시오".

데이터 암호화에 고객 관리 키를 사용하도록 구성된 새 Cloud Volumes ONTAP 시스템이 있습니다.

Azure에서 Cloud Volumes ONTAP 실행

Cloud Manager에서 Cloud Volumes ONTAP 작업 환경을 생성하여 Azure에서 단일 노드 시스템 또는 HA 쌍을 시작할 수 있습니다.

작업 환경을 만들려면 다음이 필요합니다.

- 실행 중인 커넥터입니다.
 - 가 있어야 합니다 "작업 영역과 연결된 커넥터입니다".
 - "항상 Connector를 실행 상태로 둘 준비가 되어 있어야 합니다".
- 사용하려는 구성에 대한 이해.

구성을 선택하고 관리자로부터 Azure 네트워킹 정보를 받아야 합니다. 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP 구성 계획".

- 작업 환경 추가 마법사에서 특정 라이선스 옵션을 선택하는 데 필요한 사항을 이해합니다. "Cloud Volumes ONTAP 라이선스에 대해 자세히 알아보십시오".

| 라이선스 옵션 | 요구 사항 | 요구 사항을 충족하는 방법 |
|-------------------------------|---|--|
| 프리모늄 | 마켓플레이스 구독 또는 NSS(NetApp Support Site) 계정이 필요합니다. | 세부 정보 및 자격 증명 * 페이지에서 클라우드 공급자의 마켓플레이스를 구독할 수 있습니다. 충전 방법 및 NSS 계정 * 페이지에서 NSS 계정을 입력할 수 있습니다. |
| Professional 또는 Essential 패키지 | BYOL(Marketplace Subscription 또는 용량 기반 라이선스)이 필요합니다. 계정에 유효한 용량 기반 라이선스가 없거나 프로비저닝된 용량이 라이선스 용량을 초과하는 경우 용량 기반 충전을 위해 Marketplace 구독을 사용하는 것이 좋습니다. | 세부 정보 및 자격 증명 * 페이지에서 클라우드 공급자의 마켓플레이스를 구독할 수 있습니다. NetApp에서 구매한 용량 기반 라이선스(BYOL)를 사용하려면 먼저 * Digital Wallet * 에 추가해야 합니다. "용량 기반 BYOL 라이선스를 추가하는 방법에 대해 알아보십시오". |
| 유연한 Keystone 구독 | 계정이 인증되어야 하며 Cloud Volumes ONTAP에서 사용할 수 있도록 구독을 활성화해야 합니다. | a. mailto:ng-keystone-success@netapp.com [Contact NetApp]: 하나 이상의 Keystone Flex 구독으로 Cloud Manager 사용자 계정을 인증하십시오. b. NetApp이 사용자 계정을 승인한 후 "Cloud Volumes ONTAP에서 사용할 수 있도록 구독을 연결합니다". c. Cloud Volumes ONTAP HA 쌍을 생성할 때 Keystone 유연한 구독 충전 방법을 선택하십시오. |

| 라이선스 옵션 | 요구 사항 | 요구 사항을 충족하는 방법 |
|----------|--|---|
| 노드당 라이선스 | Marketplace 구독이 필요하거나 BYOL(Bring Your Own License)을 사용해야 합니다. 이 옵션은 기존 구독 또는 기존 라이선스를 보유한 고객에게 제공됩니다. 신규 고객은 사용할 수 없습니다. | NetApp에서 구매한 노드 기반 라이선스(BYOL)를 사용하려면 먼저 * Digital Wallet * 에 추가해야 합니다. "노드 기반 BYOL 라이선스를 추가하는 방법에 대해 알아보십시오" . 충전 방법 및 NSS 계정 * 페이지에서 NSS 계정을 입력할 수 있습니다. |

Cloud Manager는 Azure에서 Cloud Volumes ONTAP 시스템을 생성할 때 리소스 그룹, 네트워크 인터페이스, 스토리지 계정 등과 같은 여러 Azure 개체를 생성합니다. 마법사 마지막에서 리소스 요약을 검토할 수 있습니다.



데이터 손실 가능성

모범 사례는 각 Cloud Volumes ONTAP 시스템에 새로운 전용 리소스 그룹을 사용하는 것입니다.

기존 공유 리소스 그룹에 Cloud Volumes ONTAP를 배포하는 것은 데이터 손실 위험이 있기 때문에 권장되지 않습니다. Cloud Manager는 배포 실패 또는 삭제 시 공유 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거할 수 있지만 Azure 사용자는 실수로 공유 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 삭제할 수 있습니다.

단계

1. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 화면의 지시를 따릅니다.
2. * 위치 선택 *: * Microsoft Azure * 및 * Cloud Volumes ONTAP 단일 노드 * 또는 * Cloud Volumes ONTAP 고가용성 * 을 선택합니다.
3. 메시지가 표시되면 ["커넥터를 작성합니다"](#).
4. * 세부 정보 및 자격 증명 *: 필요에 따라 Azure 자격 증명 및 구독을 변경하고, 클러스터 이름을 지정하고, 필요한 경우 태그를 추가한 다음 자격 증명을 지정합니다.

다음 표에서는 지침이 필요한 필드를 설명합니다.

| 필드에 입력합니다 | 설명 |
|-------------|--|
| 작업 환경 이름 | Cloud Manager에서는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Azure 가상 머신 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다. |
| 리소스 그룹 태그 | 태그는 Azure 리소스에 대한 메타데이터입니다. 이 필드에 태그를 입력하면 Cloud Manager가 Cloud Volumes ONTAP 시스템과 연결된 리소스 그룹에 태그를 추가합니다. 작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 생성된 후에는 더 많은 태그를 추가할 수 있습니다. API는 작업 환경을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 자세한 내용은 "Microsoft Azure 문서: 태그를 사용하여 Azure 리소스를 구성합니다" 를 참조하십시오. |
| 사용자 이름 및 암호 | Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하여 System Manager 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다. default_admin_user 이름을 유지하거나 사용자 지정 사용자 이름으로 변경합니다. |


| 필드에 입력합니다 | 설명 |
|-----------|--|
| 자격 증명 편집 | 이 Cloud Volumes ONTAP 시스템에서 사용할 다른 Azure 자격 증명과 다른 Azure 구독을 선택할 수 있습니다. 선불 종량제 Cloud Volumes ONTAP 시스템을 배포하려면 Azure 마켓플레이스 구독을 선택한 Azure 구독과 연결해야 합니다. " 자격 증명을 추가하는 방법에 대해 알아보십시오 ". |

다음 비디오에서는 마켓플레이스 구독을 Azure 구독에 연결하는 방법을 보여 줍니다.

▶ <https://docs.netapp.com/ko-kr/cloud-manager-cloud-volumes->

5. * 서비스 *: Cloud Volumes ONTAP에서 사용하지 않을 개별 서비스를 활성화 또는 비활성화합니다.
 - ["클라우드 데이터 센스에 대해 자세히 알아보십시오"](#).
 - ["Cloud Backup에 대해 자세히 알아보십시오"](#).
 - ["모니터링 서비스에 대해 자세히 알아보십시오"](#).
6. * 위치 및 연결 *: 위치, 리소스 그룹, 보안 그룹을 선택한 다음 확인란을 선택하여 커넥터와 대상 위치 사이의 네트워크 연결을 확인합니다.

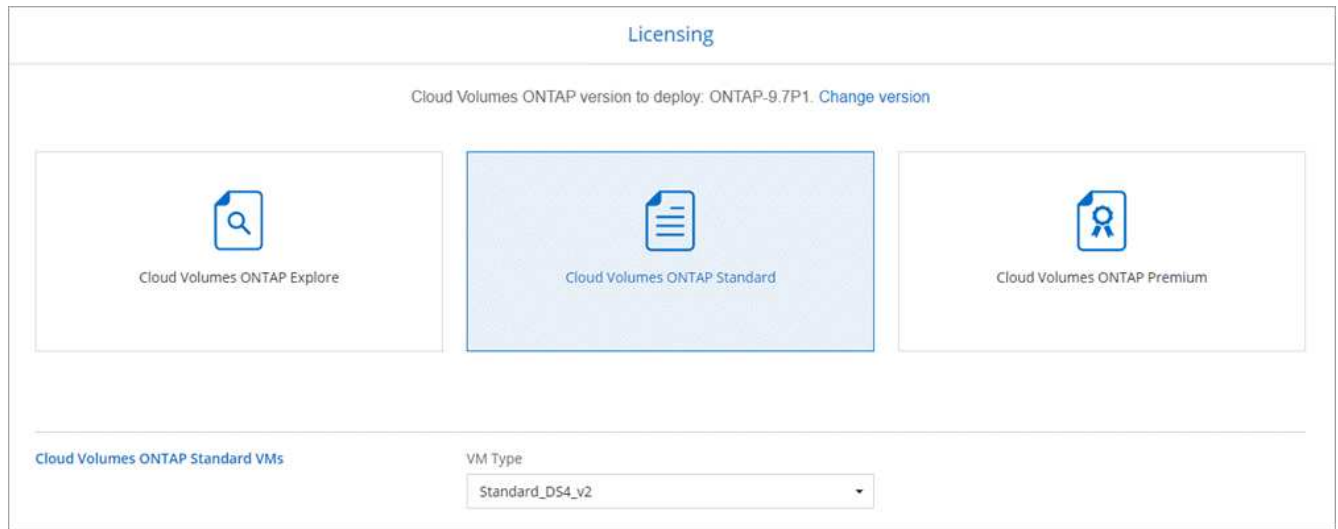
다음 표에서는 지침이 필요한 필드를 설명합니다.

| 필드에 입력합니다 | 설명 |
|-----------|---|
| 위치 | 단일 노드 시스템의 경우 Cloud Volumes ONTAP를 구축할 가용성 영역을 선택할 수 있습니다. AZ를 선택하지 않으면 Cloud Manager에서 자동으로 AZ를 선택합니다. |
| 리소스 그룹 | <p>Cloud Volumes ONTAP에 대한 새 리소스 그룹을 만들거나 기존 리소스 그룹을 사용합니다. 모범 사례는 Cloud Volumes ONTAP에 대한 새로운 전용 리소스 그룹을 사용하는 것입니다. 기존 공유 리소스 그룹에 Cloud Volumes ONTAP를 배포할 수는 있지만 데이터 손실 위험 때문에 권장되지 않습니다. 자세한 내용은 위의 경고를 참조하십시오.</p> <p>Azure에 구축하는 각 Cloud Volumes ONTAP HA 쌍에 대해 전용 리소스 그룹을 사용해야 합니다. 리소스 그룹에서는 하나의 HA 쌍만 지원됩니다. Azure 리소스 그룹에 두 번째 Cloud Volumes ONTAP HA 쌍을 구축하려고 하면 Cloud Manager에서 연결 문제가 발생합니다.</p> <div style="display: flex; align-items: center;">  <div> <p>사용 중인 Azure 계정에 가 있는 경우 "필수 권한", Cloud Manager는 배포 실패 또는 삭제 시 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거합니다.</p> </div> </div> |
| 보안 그룹 | 기존 보안 그룹을 선택하는 경우 Cloud Volumes ONTAP 요구 사항을 충족해야 합니다. "기본 보안 그룹을 봅니다" . |

7. * 충전 방법 및 NSS 계정 *: 이 시스템에서 사용할 충전 옵션을 지정한 다음 NetApp Support 사이트 계정을 지정합니다.
 - ["이러한 충전 방법에 대해 자세히 알아보십시오"](#).
 - ["마법사에서 사용하려는 라이선스 방법에 필요한 사항을 알아봅니다"](#).
8. * 사전 구성된 패키지 *: 패키지 중 하나를 선택하여 Cloud Volumes ONTAP 시스템을 신속하게 배포하거나 * 고유한 구성 만들기 * 를 클릭합니다.

패키지 중 하나를 선택하는 경우 볼륨을 지정한 다음 구성을 검토 및 승인하기만 하면 됩니다.

9. * 라이선스 *: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 라이선스를 선택한 다음 가상 머신 유형을 선택합니다.



시스템을 시작한 후 요구 사항이 변경되는 경우 나중에 라이선스 또는 가상 시스템 유형을 수정할 수 있습니다.



선택한 버전에 대해 새로운 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우, Cloud Manager는 작업 환경을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.6 RC1 및 9.6 GA를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리즈에서 다른 릴리즈로 발생하지 않습니다(예: 9.6에서 9.7로).

10. * Azure Marketplace * 구독: Cloud Manager가 Cloud Volumes ONTAP의 프로그래밍 방식 배포를 활성화할 수 없는 경우 다음 단계를 따르십시오.
11. * 기본 스토리지 리소스 *: 초기 애그리게이트의 설정(디스크 유형, 각 디스크의 크기, Blob 스토리지까지 데이터 계층화 활성화 여부)을 선택합니다.

다음 사항에 유의하십시오.

- 디스크 유형은 초기 볼륨입니다. 이후 볼륨에 대해 다른 디스크 유형을 선택할 수 있습니다.
- 디스크 크기는 초기 애그리게이트의 모든 디스크와 단순 프로비저닝 옵션을 사용할 때 Cloud Manager가 생성하는 추가 애그리게이트의 경우 모두 사용됩니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.

디스크 유형과 크기를 선택하는 방법은 을 참조하십시오 ["Azure에서 시스템 사이징"](#).

- 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
- 데이터 계층화를 사용하지 않는 경우, 후속 애그리게이트에서 이 기능을 사용하도록 설정할 수 있습니다.

["데이터 계층화에 대해 자세히 알아보십시오"](#).

12. * 쓰기 속도 및 WORM * (단일 노드 시스템만 해당): * 일반 * 또는 * 고속 * 쓰기 속도를 선택하고 원하는 경우 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

["쓰기 속도에 대해 자세히 알아보십시오"](#).

Cloud Backup이 활성화되었거나 데이터 계층화가 활성화된 경우 WORM을 설정할 수 없습니다.

["WORM 스토리지에 대해 자세히 알아보십시오"](#).

13. * 스토리지와 WORM * (HA만 해당) 보안 통신: Azure 스토리지 계정에 대한 HTTPS 연결을 사용하도록 설정하고 원하는 경우 WORM(Write Once, Read Many) 스토리지를 활성화할지 여부를 선택합니다.

HTTPS 연결은 Cloud Volumes ONTAP 9.7 HA 쌍에서 Azure 스토리지 계정에 연결됩니다. 이 옵션을 설정하면 쓰기 성능에 영향을 줄 수 있습니다. 작업 환경을 만든 후에는 설정을 변경할 수 없습니다.

["WORM 스토리지에 대해 자세히 알아보십시오"](#).

14. * 볼륨 생성 *: 새 볼륨에 대한 세부 정보를 입력하거나 * 건너뛰기 * 를 클릭합니다.

["지원되는 클라이언트 프로토콜 및 버전에 대해 알아보십시오"](#).

이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요한 필드를 설명합니다.

| 필드에 입력합니다 | 설명 |
|---------------------------|--|
| 크기 | 입력할 수 있는 최대 크기는 씬 프로비저닝의 사용 여부에 따라 크게 달라집니다. 이를 통해 현재 사용 가능한 물리적 스토리지보다 더 큰 볼륨을 생성할 수 있습니다. |
| 액세스 제어(NFS에만 해당) | 엑스포트 정책은 볼륨에 액세스할 수 있는 서버넷의 클라이언트를 정의합니다. 기본적으로 Cloud Manager는 서버넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다. |
| 권한 및 사용자/그룹(CIFS 전용) | 이러한 필드를 사용하면 사용자 및 그룹의 공유에 대한 액세스 수준(액세스 제어 목록 또는 ACL라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자 또는 그룹, UNIX 사용자 또는 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자의 도메인을 포함해야 합니다. |
| 스냅샷 정책 | 스냅샷 복사본 정책은 자동으로 생성되는 NetApp 스냅샷 복사본의 수와 빈도를 지정합니다. NetApp 스냅샷 복사본은 성능 영향이 없고 최소한의 스토리지가 필요한 시점 파일 시스템 이미지입니다. 기본 정책을 선택하거나 선택하지 않을 수 있습니다. Microsoft SQL Server의 tempdb와 같이 임시 데이터에 대해 없음을 선택할 수 있습니다. |
| 고급 옵션(NFS에만 해당) | 볼륨의 NFS 버전 선택: NFSv3 또는 NFSv4 |
| 이니시에이터 그룹 및 IQN(iSCSI 전용) | iSCSI 스토리지 타겟을 LUN(논리 유닛)이라고 하며 호스트에 표준 블록 디바이스로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름의 테이블이며 어떤 이니시에이터가 어떤 LUN을 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 통합 네트워크 어댑터(CNA) 또는 전용 호스트 파스트 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 공인 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성할 때 Cloud Manager에서 자동으로 LUN을 생성합니다. 볼륨 당 하나의 LUN만 생성하므로 관리가 필요 없습니다. 볼륨을 생성한 후 "IQN을 사용하여 호스트에서 LUN에 연결합니다" . |

다음 이미지는 CIFS 프로토콜에 대해 작성된 볼륨 페이지를 보여 줍니다.

Volume Details, Protection & Protocol

Details & Protection

Volume Name: Size (GB):

Snapshot Policy:

default

Default Policy

Protocol

NFS
CIFS
iSCSI

Share name: Permissions:

Full Control

Users / Groups:

Valid users and groups separated by a semicolon

15. * CIFS 설정 *: CIFS 프로토콜을 선택한 경우 CIFS 서버를 설정합니다.

| 필드에 입력합니다 | 설명 |
|-----------------------------|--|
| DNS 기본 및 보조 IP 주소 | CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다. |
| 연결할 Active Directory 도메인입니다 | CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다. |
| 도메인에 가입하도록 승인된 자격 증명입니다 | AD 도메인 내의 지정된 OU(조직 구성 단위)에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름 및 암호입니다. |
| CIFS 서버 NetBIOS 이름입니다 | AD 도메인에서 고유한 CIFS 서버 이름입니다. |
| 조직 구성 단위 | CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. Azure AD 도메인 서비스를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 * OU=ADDC 컴퓨터 * 또는 * OU=ADDC 사용자 * 를 입력해야 합니다. https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou ["Azure 설명서: Azure AD 도메인 서비스 관리 도메인에 OU(조직 구성 단위)를 만듭니다"] |
| DNS 도메인 | SVM(Cloud Volumes ONTAP 스토리지 가상 머신)용 DNS 도메인 대부분의 경우 도메인은 AD 도메인과 동일합니다. |
| NTP 서버 | Active Directory DNS를 사용하여 NTP 서버를 구성하려면 * Active Directory 도메인 사용 * 을 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 를 참조하십시오 "Cloud Manager 자동화 문서" 를 참조하십시오. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 생성한 후에는 구성할 수 없습니다. |

16. * Usage Profile, Disk Type, Tiering Policy *: 스토리지 효율성 기능을 사용하도록 설정하고 필요한 경우 볼륨 계층화 정책을 변경할 것인지 선택합니다.

자세한 내용은 을 참조하십시오 ["볼륨 사용 프로파일 이해"](#) 및 ["데이터 계층화 개요"](#).

17. * 검토 및 승인 *: 선택 사항을 검토 및 확인합니다.

- a. 구성에 대한 세부 정보를 검토합니다.
- b. Cloud Manager가 구매할 지원 및 Azure 리소스에 대한 세부 정보를 검토하려면 * 추가 정보 * 를 클릭합니다.
- c. 이해함... * 확인란을 선택합니다.
- d. Go * 를 클릭합니다.

Cloud Manager는 Cloud Volumes ONTAP 시스템을 구축합니다. 타임라인에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템을 배포하는 데 문제가 있으면 오류 메시지를 검토합니다. 작업 환경을 선택하고 * 환경 다시 작성 * 을 클릭할 수도 있습니다.

자세한 내용은 를 참조하십시오 ["NetApp Cloud Volumes ONTAP 지원"](#).

작업을 마친 후

- CIFS 공유를 프로비저닝한 경우 파일 및 폴더에 대한 사용자 또는 그룹 권한을 제공하고 해당 사용자가 공유를 액세스하고 파일을 생성할 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 System Manager 또는 CLI를 사용하십시오.

할당량을 사용하면 사용자, 그룹 또는 qtree가 사용하는 파일 수와 디스크 공간을 제한하거나 추적할 수 있습니다.

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.