Azure에서 시작하십시오

Cloud Manager 3.8

NetApp
March 25, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/occm38/task_getting_started_azure.html on March 25, 2024. Always check docs.netapp.com for the latest.

목차

Azure에서 시작하십시오 1
Azure용 Cloud Volumes ONTAP 시작하기 1
Azure에서 Cloud Volumes ONTAP 구성 계획 2
Azure에서 Cloud Volumes ONTAP를 구축 및 관리하기 위한 네트워킹 요구 사항 4
Azure에서 Cloud Volumes ONTAP 실행 14

Azure에서 시작하십시오

Azure용 Cloud Volumes ONTAP 시작하기

몇 가지 단계를 통해 Azure용 Cloud Volumes ONTAP를 시작하십시오.

1 커넥터를 작성합니다

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

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

2 구성을 계획합니다

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".

3 네트워크 설정

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".

4 **Cloud Manager**를 사용하여 **Cloud Volumes ONTAP**를 실행합니다

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

관련 링크

- "평가 중"
- "Cloud Manager에서 커넥터 생성"
- "Azure Marketplace에서 커넥터 만들기"
- "Linux 호스트에 Connector 소프트웨어 설치"
- "Cloud Manager가 Azure 권한으로 수행하는 기능"

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.

라이센스 유형을 선택합니다

Cloud Volumes ONTAP는 사용한 만큼만 지불하는 BYOL(Bring Your Own License)이라는 두 가지 가격 옵션으로 제공됩니다. 선불 종량제 의 경우 Explore, Standard 또는 Premium의 세 가지 라이센스 중에서 선택할 수 있습니다. 각 라이센스는 용량과 컴퓨팅 옵션을 다르게 제공합니다.

"Azure에서 Cloud Volumes ONTAP 9.7 구성 지원"

스토리지 제한 이해

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

"Azure에서 Cloud Volumes ONTAP 9.7의 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. 에서는 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 1TB 디스크를 선택하면 500GB 디스크보다 더 높은 성능을 얻을 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".

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 단일 노드 Cloud Volumes ONTAP 시스템에 대해 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.

일반 쓰기 속도와 높은 쓰기 속도 간의 차이

정상적인 쓰기 속도를 선택하면 데이터가 디스크에 직접 기록되므로 계획되지 않은 시스템 중단 시 데이터 손실 가능성이 줄어듭니다.

빠른 쓰기 속도를 선택하면 데이터가 디스크에 쓰기 전에 메모리에 버퍼링되어 쓰기 성능이 향상됩니다. 이 캐싱으로 인해 계획되지 않은 시스템 중단이 발생할 경우 데이터 손실이 발생할 수 있습니다.

계획되지 않은 시스템 중단 시 손실될 수 있는 데이터 양은 마지막 두 정합성 보장 지점의 스팬입니다. 정합성 보장 지점은 버퍼링된 데이터를 디스크에 쓰는 작업을 가리킵니다. 정합성 보장 지점은 쓰기 로그가 꽉 찼거나 10초 후에(둘 중 먼저 도래하는 시점)에 발생합니다. 그러나 AWS EBS 볼륨 성능은 정합성 보장 지점 처리 시간에 영향을 미칠 수 있습니다.

빠른 쓰기 속도 사용 시기

워크로드에 빠른 쓰기 성능이 필요하고 계획되지 않은 시스템 운영 중단 시 데이터 손실 위험을 감수할 수 있는 경우 빠른 쓰기 속도가 가장 좋습니다.

빠른 쓰기 속도 사용 시 권장 사항

빠른 쓰기 속도를 설정하는 경우 애플리케이션 계층에서 쓰기 보호가 보장되어야 합니다.

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.

씬 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.

Azure에서 Cloud Volumes ONTAP를 구축 및 관리하기 위한 네트워킹 요구 사항

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.

Cloud Volumes ONTAP에 대한 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 구성 방법을 알아보십시오".

보안 그룹

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

IP 주소 수입니다

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.

데이터 계층화를 위해 **Cloud Volumes ONTAP**에서 **Azure Blob** 저장소로 연결

콜드 데이터를 Azure Blob 저장소에 계층화하려는 경우 Cloud Manager에 필요한 권한이 있는 경우 성능 계층과 용량 계층 간의 연결을 설정할 필요가 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".

다른 네트워크의 **ONTAP** 시스템에 대한 연결

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

자세한 지침은 을 참조하십시오 "Microsoft Azure 문서: Azure 포털에서 사이트 간 연결을 만듭니다".

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. Connector는 Azure에서 리소스를 관리할 때 다음 끝점에 연결합니다.

엔드포인트	목적
https://management.azure.com https://login.microsoftonline.com 으로 문의하십시오	Cloud Manager를 사용하면 대부분의 Azure 지역에서 Cloud Volumes ONTAP를 구축 및 관리할 수 있습니다.
https://management.microsoftazure.de https://login.microsoftonline.de 으로 문의하십시오	Cloud Manager를 사용하여 Azure 독일 지역에서 Cloud Volumes ONTAP를 구축 및 관리할 수 있습니다.
https://management.usgovcloudapi.net https://login.microsoftonline.com 으로 문의하십시오	Cloud Manager를 사용하여 Azure US Gov 지역에 Cloud Volumes ONTAP를 배포하고 관리할 수 있습니다.
https://api.services.cloud.netapp.com:443 으로 문의하십시오	NetApp Cloud Central에 API 요청
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com 으로 문의하십시오	소프트웨어 이미지, 매니페스트 및 템플릿에 대한 액세스를 제공합니다.
https://repo.cloud.support.netapp.com 으로 문의하십시오	Cloud Manager 종속성을 다운로드하는 데 사용됩니다.
http://repo.mysql.com/ 으로 문의하십시오	MySQL 다운로드에 사용됩니다.
https://cognito-idp.us-east-1.amazonaws.com\https://cognito-identity.us-east-1.amazonaws.com\https://sts.amazonaws.com\https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Cloud Manager에서 매니페스트, 템플릿 및 Cloud Volumes ONTAP 업그레이드 이미지에 액세스하고 다운로드할 수 있습니다.
https://cloudmanagerinfraprod.azurecr.io 으로 문의하십시오	Docker를 실행하는 인프라에 대한 컨테이너 구성 요소의 소프트웨어 이미지에 액세스하고 Cloud Manager와의 서비스 통합을 위한 솔루션을 제공합니다.
https://kinesis.us-east-1.amazonaws.com 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.

엔드포인트	목적
https://cloudmanager.cloud.netapp.com 으로 문의하십시오	Cloud Central 계정을 포함한 Cloud Manager 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com 으로 문의하십시오	NetApp Cloud Central과 통신하여 중앙 집중식 사용자 인증 제공
https://mysupport.netapp.com 으로 문의하십시오	NetApp AutoSupport과 커뮤니케이션:
https://support.netapp.com/svcgw\https://support.netapp.com/ServiceGW/entitlement\https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com\https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	시스템 라이센스 및 지원 등록을 위해 NetApp과 커뮤니케이션
https://ipa-signer.cloudmanager.netapp.com 으로 문의하십시오	Cloud Manager에서 라이센스 생성(예: Cloud Volumes ONTAP용 FlexCache 라이센스)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/ 으로 문의하십시오	Cloud Volumes ONTAP 시스템을 Kubernetes 클러스터에 연결하는 데 필요합니다. 엔드포인트를 통해 NetApp Trident를 설치할 수 있습니다.
.blob.core.windows.net 으로 문의하십시오	프록시를 사용할 때 HA 쌍에 필요합니다.
다음과 같은 다양한 타사 위치: • https://repo1.maven.org/maven2 으로 문의하십시오 • https://oss.sonatype.org/content/repositories 으로 문의하십시오 • https://repo.typesafe.org 으로 문의하십시오 타사 위치는 변경될 수 있습니다.	업그레이드하는 동안 Cloud Manager는 타사 종속성을 위한 최신 패키지를 다운로드합니다.

SaaS 사용자 인터페이스에서 거의 모든 작업을 수행해야 하지만 로컬 사용자 인터페이스는 Connector에서 계속 사용할 수 있습니다. 웹 브라우저를 실행하는 컴퓨터는 다음 끝점에 연결되어 있어야 합니다.

엔드포인트	목적
커넥터 호스트입니다	Cloud Manager 콘솔을 로드하려면 웹 브라우저에서 호스트의 IP 주소를 입력해야 합니다. 클라우드 공급자에 대한 연결에 따라 호스트에 할당된 프라이빗 IP 또는 공용 IP를 사용할 수 있습니다. • 개인 IP는 VPN이 있고 가상 네트워크에 직접 연결할 수 있는 경우 작동합니다 • 공용 IP는 모든 네트워킹 시나리오에서 작동합니다 어떤 경우든 보안 그룹 규칙이 승인된 IP 또는 서브넷에서의 액세스만 허용하도록 하여 네트워크 액세스를 보호해야 합니다.

엔드포인트	목적
https://auth0.com\https://cdn.auth0.com\https://netapp-cloud-account.auth0.com\https://services.cloud.netapp.com	웹 브라우저는 NetApp Cloud Central을 통해 중앙 집중식 사용자 인증을 위해 이러한 엔드포인트에 연결됩니다.
https://widget.intercom.io 으로 문의하십시오	제품 내에서 NetApp 클라우드 전문가와 상담할 수 있는 채팅을 제공합니다.

Cloud Volumes ONTAP의 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
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

우선 순위 및 이름	포트 및 프로토콜	소스 및 대상	설명
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

우선 순위 및 이름	포트 및 프로토콜	소스 및 대상	설명
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	프로토콜	출처	목적지	목적
Active Directory를 클릭합니다					

	464	TCP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
서비스	464 포트	UDP 입니다	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)
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

Connector에 대한 보안 그룹 규칙입니다

Connector의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

인바운드 규칙

미리 정의된 보안 그룹의 인바운드 규칙 소스는 0.0.0.0/0입니다.

포트	프로토콜	목적
22	SSH를 클릭합니다	커넥터 호스트에 대한 SSH 액세스를 제공합니다

포트	프로토콜	목적
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
Active Directory를 클릭합니다	88	TCP	Active Directory 포리스트입니다	Kerberos V 인증
	139	TCP	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	389	TCP	Active Directory 포리스트입니다	LDAP를 지원합니다
	445	TCP	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	464	TCP	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	749	TCP	Active Directory 포리스트입니다	Active Directory Kerberos V 변경 및 암호 설정(RPCSEC_GSS)
	137	UDP입니다	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	138	UDP입니다	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	464	UDP입니다	Active Directory 포리스트입니다	Kerberos 키 관리
API 호출 및 AutoSupport	443	HTTPS	아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF	API는 AWS 및 ONTAP를 호출하고 AutoSupport 메시지를 NetApp에 보냅니다
API 호출	3000입니다	TCP	ONTAP 클러스터 관리 LIF	ONTAP에 대한 API 호출
DNS	53	UDP입니다	DNS	Cloud Manager에서 DNS Resolve에 사용됩니다

Azure에서 Cloud Volumes ONTAP 실행

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

시작하기 전에

- 가 있어야 합니다 "작업 영역과 연결된 커넥터입니다".

> 커넥터를 생성하려면 계정 관리자여야 합니다. 첫 번째 Cloud Volumes ONTAP 작업 환경을 만들 때 아직 커넥터가 없는 경우 커넥터를 생성하라는 메시지가 Cloud Manager에 표시됩니다.

- "항상 Connector를 실행 상태로 둘 준비가 되어 있어야 합니다".

- 구성을 선택하고 관리자로부터 Azure 네트워킹 정보를 받아야 합니다. 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP 구성 계획".
- BYOL 시스템을 구축하려면 각 노드에 대해 20자리의 일련 번호(라이센스 키)가 필요합니다.

이 작업에 대해

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
>
> 기존 공유 리소스 그룹에 Cloud Volumes ONTAP를 배포하는 것은 데이터 손실 위험이 있기 때문에 권장되지 않습니다. API를 사용하여 기존 리소스 그룹에 배포할 때 롤백이 기본적으로 해제되어 있지만 Cloud Volumes ONTAP를 삭제하면 해당 공유 그룹에서 다른 리소스가 삭제될 수 있습니다.
>
> 모범 사례는 Cloud Volumes ONTAP에 대한 새로운 전용 리소스 그룹을 사용하는 것입니다. 이 옵션은 Cloud Manager에서 Azure에 Cloud Volumes ONTAP를 구축할 때 기본적으로 권장되는 옵션입니다.

단계

1. 작업 환경 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. * 세부 정보 및 자격 증명 *: 필요에 따라 Azure 자격 증명 및 구독을 변경하고, 클러스터 이름과 리소스 그룹 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 이름	새 자원 그룹의 기본 이름을 유지하거나 * 기본값 사용 * 의 선택을 취소하고 새 자원 그룹에 대한 사용자 이름을 입력합니다. 모범 사례는 Cloud Volumes ONTAP에 대한 새로운 전용 리소스 그룹을 사용하는 것입니다. API를 사용하여 기존 공유 리소스 그룹에 Cloud Volumes ONTAP를 배포할 수는 있지만 데이터 손실 위험 때문에 권장되지 않습니다. 자세한 내용은 위의 경고를 참조하십시오.
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 을 참조하십시오 "Microsoft Azure 문서: 태그를 사용하여 Azure 리소스를 구성합니다".
사용자 이름 및 암호	Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하여 OnCommand 시스템 관리자 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다.
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 알아봅니다".

다음 비디오에서는 마켓플레이스 구독을 Azure 구독에 연결하는 방법을 보여 줍니다.

► https://docs.netapp.com/ko-kr/occm38//media/video_subscribing_azure.mp4 *(video)*

4. * 서비스 *: Cloud Volumes ONTAP에서 사용하지 않을 개별 서비스를 활성화 또는 비활성화합니다.
   - "클라우드 규정 준수 에 대해 자세히 알아보십시오".
   - "클라우드 백업에 대해 자세히 알아보십시오".
5. * 위치 및 연결 *: 위치 및 보안 그룹을 선택하고 확인란을 선택하여 Cloud Manager와 타겟 위치 간의 네트워크 연결을 확인합니다.
6. * 라이센스 및 지원 사이트 계정 *: 용량제 또는 BYOL 중 무엇을 사용할지 지정한 다음 NetApp Support 사이트 계정을 지정합니다.

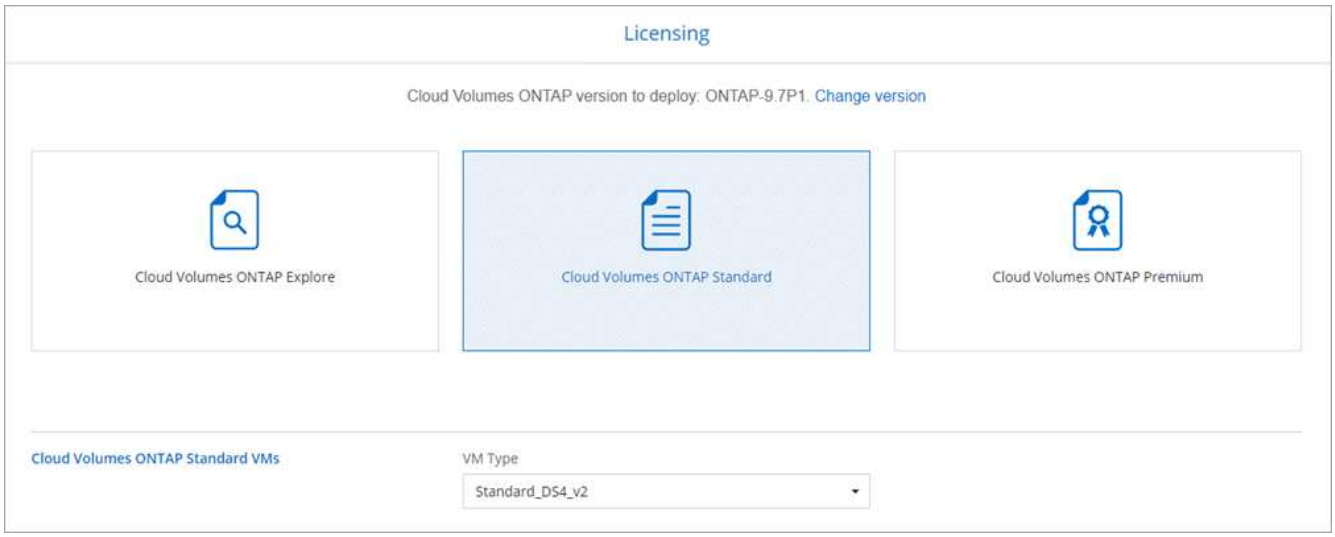
   라이센스 작동 방식을 이해하려면 를 참조하십시오 "라이센싱".

   NetApp Support 사이트 계정은 사용한 만큼만 지불하는 데 선택 사항이지만 BYOL 시스템에는 필요합니다. "NetApp Support 사이트 계정을 추가하는 방법을 알아보십시오".

7. 사전 구성된 패키지 *: 패키지 중 하나를 선택하여 Cloud Volumes ONTAP 시스템을 신속하게 배포하거나 * 나만의 구성 만들기 * 를 클릭합니다.

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

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



   시스템을 시작한 후 요구 사항이 변경되는 경우 나중에 라이센스 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).

9. * Azure Marketplace * 구독: Cloud Manager가 Cloud Volumes ONTAP의 프로그래밍 방식 배포를 활성화할 수 없는 경우 다음 단계를 따르십시오.

10. * 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".

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

    쓰기 속도 선택은 단일 노드 시스템에서만 지원됩니다.

    "쓰기 속도에 대해 자세히 알아보십시오".

    데이터 계층화가 설정된 경우 WORM을 설정할 수 없습니다.

    "WORM 스토리지에 대해 자세히 알아보십시오".

12. * 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".

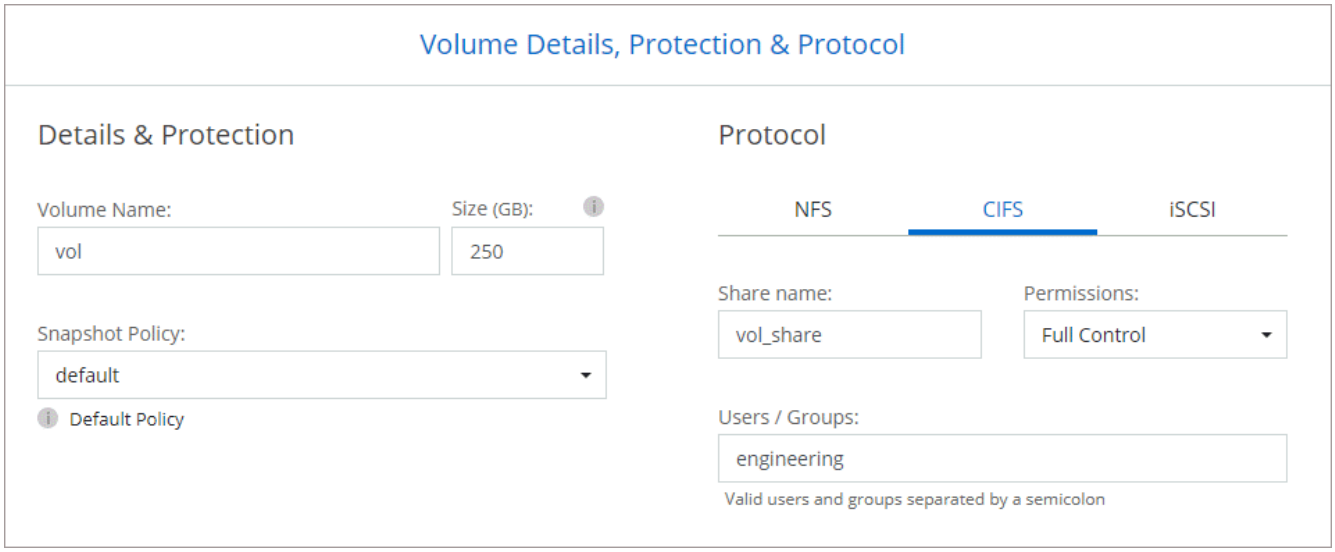
13. * 볼륨 생성 *: 새 볼륨에 대한 세부 정보를 입력하거나 * 건너뛰기 * 를 클릭합니다.

    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 서브넷의 클라이언트를 정의합니다. 기본적으로 Cloud Manager는 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.

필드에 입력합니다	설명
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.



14. * 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.

필드에 입력합니다	설명
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 API 개발자 가이드 를 참조하십시오" 를 참조하십시오.

15. * 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 프로필 이해" 및 "데이터 계층화 개요".

16. * 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.

결과

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.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.