NetApp Console 에서 시작하기

Cloud Volumes ONTAP

NetApp
February 17, 2026

목차

NetApp Console 에서 시작하기

Azure에서 Cloud Volumes ONTAP 대한 빠른 시작

몇 단계만 거치면 Azure용 Cloud Volumes ONTAP 시작할 수 있습니다.

1 콘솔 에이전트 만들기

만약 당신이 없다면 "콘솔 에이전트" 하지만, 하나는 만들어야 합니다. "Azure에서 콘솔 에이전트를 만드는 방법을 알아보세요."

인터넷 접속이 불가능한 서브넷에 Cloud Volumes ONTAP 배포하려면 콘솔 에이전트를 수동으로 설치하고 해당 콘솔 에이전트에서 실행 중인 NetApp Console 에 액세스해야 합니다. "인터넷 접속이 불가능한 위치에 콘솔 에이전트를 수동으로 설치하는 방법을 알아보세요."

2 구성을 계획하세요

콘솔은 사용자의 작업 부하 요구 사항에 맞는 미리 구성된 패키지를 제공하거나 사용자가 직접 구성을 만들 수도 있습니다. 원하는 구성을 선택하는 경우, 사용 가능한 옵션을 이해해야 합니다. 자세한 내용은 다음을 참조하세요. "Azure에서 Cloud Volumes ONTAP 구성 계획" .

3 네트워킹을 설정하세요

1. VNet과 서브넷이 콘솔 에이전트와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인하세요.
2. NetApp AutoSupport 에 대해 대상 VPC에서 아웃바운드 인터넷 액세스를 활성화합니다.

   인터넷 접속이 불가능한 위치에 Cloud Volumes ONTAP 배포하는 경우 이 단계는 필요하지 않습니다.

"네트워킹 요구 사항에 대해 자세히 알아보세요" .

4 Cloud Volumes ONTAP 출시

*시스템 추가*를 클릭하고 배포하려는 시스템 유형을 선택한 다음 마법사의 단계를 완료합니다. "단계별 지침을 읽어보세요" .

관련 링크

- "콘솔에서 콘솔 에이전트 만들기"
- "Azure Marketplace에서 콘솔 에이전트 만들기"
- "Linux 호스트에 콘솔 에이전트 소프트웨어 설치"
- "콘솔이 권한으로 수행하는 작업"

Azure에서 Cloud Volumes ONTAP 구성 계획

Azure에 Cloud Volumes ONTAP 배포할 때 워크로드 요구 사항에 맞는 미리 구성된 시스템을 선택하거나 고유한 구성을 만들 수 있습니다. 원하는 구성을 선택하는 경우, 사용 가능한 옵션을 이해해야 합니다.

Cloud Volumes ONTAP 라이선스를 선택하세요

Cloud Volumes ONTAP 에는 여러 가지 라이선싱 옵션이 제공됩니다. 각 옵션을 통해 귀하의 필요에 맞는 소비 모델을 선택할 수 있습니다.

- "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요"
- "라이선싱 설정 방법 알아보기"

지원되는 지역을 선택하세요

Cloud Volumes ONTAP 대부분의 Microsoft Azure 지역에서 지원됩니다. "지원되는 지역의 전체 목록 보기" .

지원되는 VM 유형을 선택하세요

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

"Azure의 Cloud Volumes ONTAP 에 지원되는 구성"

저장 한도 이해하기

Cloud Volumes ONTAP 시스템의 원시 용량 제한은 라이선스에 따라 결정됩니다. 추가적인 제한은 골재와 부피의 크기에 영향을 미칩니다. 구성을 계획할 때 이러한 제한 사항을 알고 있어야 합니다.

"Azure의 Cloud Volumes ONTAP 에 대한 저장소 한도"

Azure에서 시스템 크기 조정

Cloud Volumes ONTAP 시스템의 크기를 조정하면 성능 및 용량 요구 사항을 충족하는 데 도움이 될 수 있습니다. VM 유형, 디스크 유형 및 디스크 크기를 선택할 때 몇 가지 핵심 사항을 알아야 합니다.

가상 머신 유형

지원되는 가상 머신 유형을 살펴보세요. "Cloud Volumes ONTAP 릴리스 노트" 그런 다음 지원되는 각 VM 유형에 대한 세부 정보를 검토합니다. 각 VM 유형은 특정 수의 데이터 디스크를 지원한다는 점을 알아두세요.

- "Azure 설명서: 범용 가상 머신 크기"
- "Azure 설명서: 메모리 최적화된 가상 머신 크기"

단일 노드 시스템의 **Azure** 디스크 유형

Cloud Volumes ONTAP 에 대한 볼륨을 생성할 때 Cloud Volumes ONTAP 디스크로 사용하는 기본 클라우드 스토리지를 선택해야 합니다.

단일 노드 시스템에서는 다음과 같은 유형의 Azure 관리 디스크를 사용할 수 있습니다.

- _프리미엄 SSD 관리 디스크_는 비용이 더 많이 들더라도 I/O 집약적 워크로드에 대해 높은 성능을 제공합니다.
- _프리미엄 SSD v2 관리형 디스크_는 프리미엄 SSD 관리형 디스크에 비해 더 낮은 비용으로 더 높은 성능과 더 낮은 지연 시간을 제공합니다.
- _표준 SSD 관리 디스크_는 낮은 IOPS가 필요한 작업 부하에 대해 일관된 성능을 제공합니다.
- _표준 HDD 관리 디스크_는 높은 IOPS가 필요하지 않고 비용을 절감하고 싶은 경우에 좋은 선택입니다.

이러한 디스크의 사용 사례에 대한 추가 세부 정보는 다음을 참조하세요. "Microsoft Azure 설명서: Azure에서 사용할 수 있는 디스크 유형은 무엇인가요?" .

HA 쌍이 있는 **Azure** 디스크 유형

HA 시스템은 비용이 더 많이 들더라도 I/O 집약적 워크로드에 대해 높은 성능을 제공하는 프리미엄 SSD 공유 관리 디스크를 사용합니다. 9.12.1 릴리스 이전에 생성된 HA 배포는 프리미엄 페이지 Blob을 사용합니다.

Azure 디스크 크기

Cloud Volumes ONTAP 인스턴스를 시작할 때 집계에 대한 기본 디스크 크기를 선택해야 합니다. NetApp Console 초기 집계에 이 디스크 크기를 사용하고, 간단한 프로비저닝 옵션을 사용할 때 생성하는 추가 집계에도 이 디스크 크기를 사용합니다. 기본값과 다른 디스크 크기를 사용하는 집계를 생성할 수 있습니다."고급 할당 옵션 사용" .

집계된 모든 디스크의 크기는 동일해야 합니다.

디스크 크기를 선택할 때는 여러 가지 요소를 고려해야 합니다. 디스크 크기는 스토리지 비용, 집계하여 생성할 수 있는 볼륨 크기, Cloud Volumes ONTAP 에서 사용할 수 있는 총 용량, 스토리지 성능에 영향을 미칩니다.

Azure Premium Storage의 성능은 디스크 크기에 따라 달라집니다. 더 큰 디스크는 더 높은 IOPS와 처리량을 제공합니다. 예를 들어, 1TiB 디스크를 선택하면 500GiB 디스크보다 비용이 더 많이 들더라도 더 나은 성능을 제공할 수 있습니다.

표준 저장소의 디스크 크기에는 성능 차이가 없습니다. 필요한 용량에 따라 디스크 크기를 선택해야 합니다.

디스크 크기별 IOPS 및 처리량은 Azure를 참조하세요.

- "Microsoft Azure: 관리 디스크 가격"
- "Microsoft Azure: 페이지 Blob 가격 책정"

기본 시스템 디스크 보기

사용자 데이터 저장 외에도 콘솔은 Cloud Volumes ONTAP 시스템 데이터(부팅 데이터, 루트 데이터, 코어 데이터 및 NVRAM)를 위한 클라우드 스토리지도 구매합니다. 계획을 세우려면 Cloud Volumes ONTAP 배포하기 전에 이러한 세부 정보를 검토하는 것이 도움이 될 수 있습니다.

"Azure에서 Cloud Volumes ONTAP 시스템 데이터의 기본 디스크 보기" .

콘솔 에이전트에도 시스템 디스크가 필요합니다. "콘솔 에이전트의 기본 구성에 대한 세부 정보 보기" .

네트워킹 정보 수집

Azure에 Cloud Volumes ONTAP 배포하는 경우 가상 네트워크에 대한 세부 정보를 지정해야 합니다. 워크시트를 사용하여 관리자로부터 정보를 수집할 수 있습니다.

Azure 정보	당신의 가치
지역	
가상 네트워크(VNet)	
서브넷	
네트워크 보안 그룹(자체 그룹 사용 시)	

쓰기 속도를 선택하세요

콘솔을 사용하면 Cloud Volumes ONTAP 에 대한 쓰기 속도 설정을 선택할 수 있습니다. 쓰기 속도를 선택하기 전에 일반 설정과 높은 설정의 차이점, 높은 쓰기 속도를 사용할 때의 위험과 권장 사항을 이해해야 합니다. "쓰기 속도에 대해 자세히 알아보세요" .

볼륨 사용 프로필을 선택하세요

ONTAP 에는 필요한 총 저장 용량을 줄일 수 있는 여러 가지 저장 효율성 기능이 포함되어 있습니다. 콘솔에서 볼륨을 생성할 때 이러한 기능을 활성화하는 프로필이나 비활성화하는 프로필을 선택할 수 있습니다. 어떤 프로필을 사용할지 결정하는 데 도움이 되도록 이러한 기능에 대해 자세히 알아보세요.

NetApp 스토리지 효율성 기능은 다음과 같은 이점을 제공합니다.

씬 프로비저닝

실제 물리적 스토리지 풀에 있는 것보다 더 많은 논리적 스토리지를 호스트나 사용자에게 제공합니다. 저장 공간을 미리 할당하는 대신, 데이터가 기록됨에 따라 각 볼륨에 저장 공간이 동적으로 할당됩니다.

중복제거

동일한 데이터 블록을 찾아 단일 공유 블록에 대한 참조로 대체하여 효율성을 향상시킵니다. 이 기술은 동일한 볼륨에 있는 중복된 데이터 블록을 제거하여 저장 용량 요구 사항을 줄입니다.

압축

1차, 2차, 보관 저장소의 볼륨 내 데이터를 압축하여 데이터를 저장하는 데 필요한 물리적 용량을 줄입니다.

Cloud Volumes ONTAP 에 대한 Azure 네트워킹 설정

NetApp Console IP 주소, 넷마스크, 경로 등 Cloud Volumes ONTAP 의 네트워킹 구성 요소를 설정합니다. 아웃바운드 인터넷 접속이 가능한지, 충분한 개인 IP 주소가 사용 가능한지, 올바른 연결이 설정되어 있는지 등을 확인해야 합니다.

Cloud Volumes ONTAP 요구 사항

Azure에서는 다음과 같은 네트워킹 요구 사항을 충족해야 합니다.

아웃바운드 인터넷 접속

Cloud Volumes ONTAP 시스템은 다양한 기능을 위해 외부 엔드포인트에 액세스하기 위해 아웃바운드 인터넷 액세스가 필요합니다. 엄격한 보안 요구 사항이 있는 환경에서 이러한 엔드포인트가 차단되면 Cloud Volumes ONTAP 제대로 작동할 수 없습니다.

콘솔 에이전트는 일상 업무를 위해 여러 엔드포인트에 연결합니다. 엔드포인트에 대한 정보는 다음을 참조하세요. "콘솔 에이전트에서 연결된 엔드포인트 보기" 그리고 "콘솔 사용을 위한 네트워킹 준비" .

Cloud Volumes ONTAP 엔드포인트

Cloud Volumes ONTAP 이러한 엔드포인트를 사용하여 다양한 서비스와 통신합니다.

엔드포인트	적용 가능	목적	배포 모드	사용할 수 없는 경우 영향
\ https://netapp-cloud-account.auth0.com	입증	콘솔에서 인증에 사용됩니다.	표준 모드와 제한 모드.	사용자 인증에 실패하고 다음 서비스를 계속 사용할 수 없습니다. • Cloud Volumes ONTAP 서비스 • ONTAP 서비스 • 프로토콜 및 프록시 서비스
https://vault.azure.net	키 볼트	고객 관리 키(CMK)를 사용할 때 Azure Key Vault에서 클라이언트 비밀 키를 검색하는 데 사용됩니다.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP 서비스를 사용할 수 없습니다.
\ https://api.bluexp.netapp.com/tenancy	차용	콘솔에서 Cloud Volumes ONTAP 리소스를 검색하여 리소스와 사용자에게 권한을 부여하는 데 사용됩니다.	표준 모드와 제한 모드.	Cloud Volumes ONTAP 리소스와 사용자는 권한이 없습니다.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	AutoSupport 원격 측정 데이터를 NetApp 지원팀으로 전송하는 데 사용됩니다.	표준 모드와 제한 모드.	AutoSupport 정보가 전달되지 않았습니다.
\ https://management.azure.com \ https://login.microsoftonline.com \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://core.windows.net	공공 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.

엔드포인트	적용 가능	목적	배포 모드	사용할 수 없는 경우 영향
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	중국 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.
\ https://management.microsoftazure.de \ https://login.microsoftonline.de \ https://blob.core.cloudapi.de \ https://core.cloudapi.de	독일 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	정부 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.
\ https://management.azure.microsoft.scloud \ https://login.microsoftonline.microsoft.scloud \ https://blob.core.microsoft.scloud \ https://core.microsoft.scloud	정부 DoD 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.

NetApp Console 에이전트의 네트워크 프록시 구성

NetApp Console 에이전트의 프록시 서버 구성을 사용하여 Cloud Volumes ONTAP 에서 아웃바운드 인터넷 액세스를 활성화할 수 있습니다. 콘솔은 두 가지 유형의 프록시를 지원합니다.

- 명시적 프록시: Cloud Volumes ONTAP 의 아웃바운드 트래픽은 콘솔 에이전트의 프록시 구성 중에 지정된 프록시 서버의 HTTP 주소를 사용합니다. 관리자는 추가 인증을 위해 사용자 자격 증명과 루트 CA 인증서를 구성했을 수도 있습니다. 명시적 프록시에 대해 루트 CA 인증서를 사용할 수 있는 경우 다음을 사용하여 동일한 인증서를 Cloud Volumes ONTAP 시스템에 가져와 업로드해야 합니다. "ONTAP CLI: 보안 인증서 설치" 명령.
- 투명 프록시: 네트워크는 콘솔 에이전트의 프록시를 통해 Cloud Volumes ONTAP 에서 아웃바운드 트래픽을

자동으로 라우팅하도록 구성됩니다. 투명 프록시를 설정할 때 관리자는 프록시 서버의 HTTP 주소가 아닌 Cloud Volumes ONTAP 에서의 연결을 위한 루트 CA 인증서만 제공하면 됩니다. 다음을 사용하여 Cloud Volumes ONTAP 시스템에 동일한 루트 CA 인증서를 가져와 업로드해야 합니다. "ONTAP CLI: 보안 인증서 설치" 명령.

프록시 서버 구성에 대한 정보는 다음을 참조하세요. "프록시 서버를 사용하도록 콘솔 에이전트 구성" .

IP 주소

콘솔은 Azure의 Cloud Volumes ONTAP 에 필요한 수의 개인 IP 주소를 자동으로 할당합니다. 네트워크에 사용 가능한 개인 IP 주소가 충분한지 확인해야 합니다.

Cloud Volumes ONTAP에 할당된 LIF 수는 단일 노드 시스템을 배포하는지 또는 HA 쌍을 배포하는지에 따라 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다. SVM 관리 LIF는 SnapCenter와 같은 관리 툴에 필요합니다.

iSCSI LIF는 iSCSI 프로토콜을 통해 클라이언트 액세스를 제공하며 시스템에서 다른 중요한 네트워킹 워크플로에 사용됩니다. 이러한 LIF는 필수이므로 삭제하면 안 됩니다.

단일 노드 시스템의 **IP** 주소

NetApp Console은 단일 노드 시스템에 5개 또는 6개의 IP 주소를 할당합니다.

- 클러스터 관리 IP
- 노드 관리 IP
- SnapMirror 용 클러스터 간 IP
- NFS/CIFS IP
- iSCSI IP

iSCSI IP는 iSCSI 프로토콜을 통해 클라이언트 액세스를 제공합니다. 또한 시스템에서 다른 중요한 네트워킹 워크플로에도 사용됩니다. 이 LIF는 필수이므로 삭제하면 안 됩니다.

- SVM 관리(선택 사항 - 기본적으로 구성되지 않음)

HA 쌍의 **IP** 주소

콘솔은 배포 중에 노드당 4개의 NIC에 IP 주소를 할당합니다.

참고로 Console은 HA 쌍에 대해서는 SVM 관리 LIF를 생성하지만, Azure의 단일 노드 시스템에 대해서는 생성하지 않습니다.

NIC0

- 노드 관리 IP
- 클러스터 간 IP
- iSCSI IP

iSCSI IP는 iSCSI 프로토콜을 통해 클라이언트 액세스를 제공합니다. 또한 시스템에서 다른 중요한 네트워킹 워크플로에도 사용됩니다. 이 LIF는 필수이므로 삭제하면 안 됩니다.

NIC1

- 클러스터 네트워크 IP

NIC2

- 클러스터 상호 연결 IP(HA IC)

NIC3

- Pageblob NIC IP(디스크 액세스)

NIC3는 페이지 Blob 스토리지를 사용하는 HA 배포에만 적용할 수 있습니다.

위의 IP 주소는 장애 조치 이벤트 시 마이그레이션되지 않습니다.

또한 4개의 프런트엔드 IP(FIP)가 장애 조치 이벤트 시 마이그레이션되도록 구성됩니다. 이러한 프런트엔드 IP는 로드 밸런서에 있습니다.

- 클러스터 관리 IP
- NodeA 데이터 IP(NFS/CIFS)
- NodeB 데이터 IP(NFS/CIFS)
- SVM 관리 IP

Azure 서비스에 대한 보안 연결

기본적으로 콘솔은 Cloud Volumes ONTAP 과 Azure 페이지 Blob 스토리지 계정 간의 연결을 위해 Azure Private Link를 활성화합니다.

대부분의 경우 사용자가 해야 할 일은 없습니다. 콘솔이 사용자를 대신하여 Azure Private Link를 관리해 줍니다. 하지만 Azure Private DNS를 사용하는 경우 구성 파일을 편집해야 합니다. Azure에서 콘솔 에이전트의 위치에 대한 요구 사항도 알고 있어야 합니다.

비즈니스 요구 사항에 따라 Private Link 연결을 비활성화할 수도 있습니다. 링크를 비활성화하면 콘솔은 Cloud Volumes ONTAP 대신 서비스 엔드포인트를 사용하도록 구성합니다.

"Cloud Volumes ONTAP 에서 Azure Private Links 또는 서비스 엔드포인트를 사용하는 방법에 대해 자세히 알아보세요." .

Azure VNet 암호화를 위한 네트워킹

Cloud Volumes ONTAP는 VNet 내부 또는 피어링된 VNet 간의 VM 간 트래픽 "Azure Virtual Network(VNet) 암호화"을 지원합니다. 이 기능은 Azure VNet 계층에서 구성되며 Cloud Volumes ONTAP 토폴로지(단일 노드 또는 HA)와는 무관합니다.

VM의 NIC에서 가속 네트워킹이 활성화되어 있는지 확인하고 Azure VNet 암호화 요구 사항 및 제한 사항을 검토한 후 해당 기능을 활성화하면 됩니다. NetApp 관리형 로드 밸런서 개체는 수정해서는 안 됩니다.

"Azure 설명서: VNet 암호화 및 가속 네트워킹".

다른 **ONTAP** 시스템에 대한 연결

Azure의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 Azure VNet과 다른 네트워크(예: 회사 네트워크) 간에 VPN 연결이 필요합니다.

지침은 다음을 참조하세요. "Microsoft Azure 설명서: Azure Portal에서 사이트 간 연결 만들기" .

HA 상호 연결을 위한 포트

Cloud Volumes ONTAP HA 쌍에는 HA 상호 연결이 포함되어 있어 각 노드가 파트너가 제대로 작동하는지 지속적으로 확인하고 다른 노드의 비휘발성 메모리에 대한 로그 데이터를 미러링할 수 있습니다. HA 상호 연결은 통신을 위해 TCP 포트 10006을 사용합니다.

기본적으로 HA 상호 연결 LIF 간 통신은 열려 있으며 이 포트에 대한 보안 그룹 규칙은 없습니다. 하지만 HA 상호 연결 LIF 사이에 방화벽을 만드는 경우 HA 쌍이 제대로 작동할 수 있도록 포트 10006에 대한 TCP 트래픽이 열려 있는지 확인해야 합니다.

Azure 리소스 그룹에는 **HA** 쌍이 하나만 있습니다**.**

Azure에 배포하는 각 Cloud Volumes ONTAP HA 쌍에 대해 전용 리소스 그룹을 사용해야 합니다. 리소스 그룹에서는 HA 쌍을 하나만 지원합니다.

Azure 리소스 그룹에 두 번째 Cloud Volumes ONTAP HA 쌍을 배포하려고 하면 콘솔에서 연결 문제가 발생합니다.

보안 그룹 규칙

콘솔은 Cloud Volumes ONTAP 성공적으로 작동할 수 있도록 인바운드 및 아웃바운드 규칙을 포함하는 Azure 보안 그룹을 만듭니다. "콘솔 에이전트에 대한 보안 그룹 규칙 보기" .

Cloud Volumes ONTAP 용 Azure 보안 그룹에는 노드 간 내부 통신을 위해 적절한 포트가 열려 있어야 합니다. "ONTAP 내부 포트에 대해 알아보세요" .

미리 정의된 보안 그룹을 수정하거나 사용자 지정 보안 그룹을 사용하는 것은 권장하지 않습니다. 하지만 반드시 그렇게 해야 하는 경우 배포 프로세스에서 Cloud Volumes ONTAP 시스템이 자체 서브넷 내에서 전체 액세스 권한을 가져야 한다는 점에 유의하세요. 배포가 완료된 후 네트워크 보안 그룹을 수정하기로 결정한 경우 클러스터 포트와 HA 네트워크 포트를 열어 두세요. 이를 통해 Cloud Volumes ONTAP 클러스터 내에서 원활한 통신(노드 간 모든 통신)이 보장됩니다.

단일 노드 시스템에 대한 인바운드 규칙

Cloud Volumes ONTAP 시스템을 추가하고 미리 정의된 보안 그룹을 선택하면 다음 중 하나 내에서 트래픽을 허용하도록 선택할 수 있습니다.

- 선택된 **VNet**만 해당: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템의 VNet 서브넷 범위와 콘솔 에이전트가 있는 VNet의 서브넷 범위입니다. 이것은 권장되는 옵션입니다.
- 모든 **VNet**: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
- 비활성화: 이 옵션은 스토리지 계정에 대한 공용 네트워크 액세스를 제한하고 Cloud Volumes ONTAP 시스템의 데이터 계층화를 비활성화합니다. 보안 규정 및 정책으로 인해 동일한 VNet 내에서도 개인 IP 주소가 노출되어서는 안 되는 경우 이 옵션을 사용하는 것이 좋습니다.

우선순위와 이름	포트 및 프로토콜	출발지와 목적지	설명
1000 인바운드_ssh	22 TCP	어떤 것으로든	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 대한 SSH 액세스
1001 인바운드_http	80 TCP	어떤 것으로든	클러스터 관리 LIF의 IP 주소를 사용하여 ONTAP System Manager 웹 콘솔에 대한 HTTP 액세스
1002 inbound_111_tcp	111 TCP	어떤 것으로든	NFS에 대한 원격 프로시저 호출
1003 inbound_111_udp	111 UDP	어떤 것으로든	NFS에 대한 원격 프로시저 호출
1004 inbound_139	139 TCP	어떤 것으로든	CIFS용 NetBIOS 서비스 세션
1005 인바운드_161-162_tcp	161-162 TCP	어떤 것으로든	간단한 네트워크 관리 프로토콜
1006 인바운드_161-162_udp	161-162 UDP	어떤 것으로든	간단한 네트워크 관리 프로토콜
1007 inbound_443	443 TCP	어떤 것으로든	클러스터 관리 LIF의 IP 주소를 사용하여 콘솔 에이전트와 ONTAP System Manager 웹 콘솔에 대한 HTTPS 액세스 연결
1008 inbound_445	445 TCP	어떤 것으로든	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
1009 inbound_635_tcp	635 TCP	어떤 것으로든	NFS 마운트
1010 inbound_635_udp	635 UDP	어떤 것으로든	NFS 마운트
1011 inbound_749	749 TCP	어떤 것으로든	케르베로스
1012 inbound_2049_tcp	2049 TCP	어떤 것으로든	NFS 서버 데몬
1013 inbound_2049_udp	2049 UDP	어떤 것으로든	NFS 서버 데몬
1014 inbound_3260	3260 TCP	어떤 것으로든	iSCSI 데이터 LIF를 통한 iSCSI 액세스
1015 인바운드_4045-4046_tcp	4045-4046 TCP	어떤 것으로든	NFS 잠금 데몬 및 네트워크 상태 모니터
1016 인바운드_4045-4046_udp	4045-4046 UDP	어떤 것으로든	NFS 잠금 데몬 및 네트워크 상태 모니터
1017 inbound_10000	10000 TCP	어떤 것으로든	NDMP를 사용한 백업
1018 인바운드_11104-11105	11104-11105 TCP	어떤 것으로든	SnapMirror 데이터 전송
3000 인바운드_거부_모든_tcp	모든 포트 TCP	어떤 것으로든	다른 모든 TCP 인바운드 트래픽 차단

우선순위와 이름	포트 및 프로토콜	출발지와 목적지	설명
3001 인바운드_거부_모든_udp	모든 포트 UDP	어떤 것으로든	다른 모든 UDP 인바운드 트래픽 차단
65000 AllowVnetInBound	모든 포트 모든 프로토콜	VirtualNetwork에서 VirtualNetwork로	VNet 내부에서 들어오는 트래픽
65001 AllowAzureLoad BalancerInBound	모든 포트 모든 프로토콜	AzureLoadBalancer를 Any로	Azure Standard Load Balancer의 데이터 트래픽
65500 DenyAllInBound	모든 포트 모든 프로토콜	어떤 것으로든	다른 모든 인바운드 트래픽 차단

HA 시스템에 대한 인바운드 규칙

Cloud Volumes ONTAP 시스템을 추가하고 미리 정의된 보안 그룹을 선택하면 다음 중 하나 내에서 트래픽을 허용하도록 선택할 수 있습니다.

- 선택된 **VNet**만 해당: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템의 VNet 서브넷 범위와 콘솔 에이전트가 있는 VNet의 서브넷 범위입니다. 이것은 권장되는 옵션입니다.
- 모든 **VNet**: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.

HA 시스템은 인바운드 데이터 트래픽이 Azure Standard Load Balancer를 통과하기 때문에 단일 노드 시스템보다 인바운드 규칙이 적습니다. 따라서 "AllowAzureLoadBalancerInBound" 규칙에 표시된 것처럼 Load Balancer에서 들어오는 트래픽은 허용되어야 합니다.

- 비활성화: 이 옵션은 스토리지 계정에 대한 공용 네트워크 액세스를 제한하고 Cloud Volumes ONTAP 시스템의 데이터 계층화를 비활성화합니다. 보안 규정 및 정책으로 인해 동일한 VNet 내에서도 개인 IP 주소가 노출되어서는 안 되는 경우 이 옵션을 사용하는 것이 좋습니다.

우선순위와 이름	포트 및 프로토콜	출발지와 목적지	설명
100 inbound_443	443 모든 프로토콜	어떤 것으로든	클러스터 관리 LIF의 IP 주소를 사용하여 콘솔 에이전트와 ONTAP System Manager 웹 콘솔에 대한 HTTPS 액세스 연결
101 inbound_111_tcp	111 모든 프로토콜	어떤 것으로든	NFS에 대한 원격 프로시저 호출
102 inbound_2049_tcp	2049 모든 프로토콜	어떤 것으로든	NFS 서버 데몬
111 인바운드_ssh	22 모든 프로토콜	어떤 것으로든	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 대한 SSH 액세스
121 inbound_53	53 모든 프로토콜	어떤 것으로든	DNS와 CIFS
65000 AllowVnetInBound	모든 포트 모든 프로토콜	VirtualNetwork에서 VirtualNetwork로	VNet 내부에서 들어오는 트래픽
65001 AllowAzureLoad BalancerInBound	모든 포트 모든 프로토콜	AzureLoadBalancer를 Any로	Azure Standard Load Balancer의 데이터 트래픽

우선순위와 이름	포트 및 프로토콜	출발지와 목적지	설명
65500 DenyAllInBound	모든 포트 모든 프로토콜	어떤 것으로든	다른 모든 인바운드 트래픽 차단

아웃바운드 규칙

Cloud Volumes ONTAP 의 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 개방합니다. 이것이 허용된다면, 기본적인 아웃바운드 규칙을 따르세요. 더욱 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용하세요.

기본 아웃바운드 규칙

Cloud Volumes ONTAP 의 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함되어 있습니다.

포트	규약	목적
모두	모든 TCP	모든 아웃바운드 트래픽
모두	모든 UDP	모든 아웃바운드 트래픽

고급 아웃바운드 규칙

아웃바운드 트래픽에 대한 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Cloud Volumes ONTAP 의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

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

서비스	포트	규약	원천	목적지	목적
액티브 디렉토리	88	TCP	노드 관리 LIF	Active Directory 포리스트	Kerberos V 인증
	137	UDP	노드 관리 LIF	Active Directory 포리스트	NetBIOS 이름 서비스
	138	UDP	노드 관리 LIF	Active Directory 포리스트	NetBIOS 데이터그램 서비스
	139	TCP	노드 관리 LIF	Active Directory 포리스트	NetBIOS 서비스 세션
	389	TCP 및 UDP	노드 관리 LIF	Active Directory 포리스트	LDAP
	445	TCP	노드 관리 LIF	Active Directory 포리스트	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
	464	TCP	노드 관리 LIF	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(SET_CHANGE)
	464	UDP	노드 관리 LIF	Active Directory 포리스트	Kerberos 키 관리
	749	TCP	노드 관리 LIF	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(RPCSEC_GSS)
	88	TCP	데이터 LIF(NFS, CIFS, iSCSI)	Active Directory 포리스트	Kerberos V 인증
	137	UDP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 이름 서비스
	138	UDP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 데이터그램 서비스
	139	TCP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 서비스 세션
	389	TCP 및 UDP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	LDAP
	445	TCP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
	464	TCP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(SET_CHANGE)
	464	UDP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos 키 관리
	749	TCP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(RPCSEC_GSS)

서비스	포트	규약	원천	목적지	목적
AutoSupport	HTTPS	443	노드 관리 LIF	mysupport.netapp.com	AutoSupport (HTTPS가 기본값)
	HTTP	80	노드 관리 LIF	mysupport.netapp.com	AutoSupport (전송 프로토콜이 HTTPS에서 HTTP로 변경된 경우에만)
	TCP	3128	노드 관리 LIF	콘솔 에이전트	아웃바운드 인터넷 연결이 불가능한 경우 콘솔 에이전트의 프록시 서버를 통해 AutoSupport 메시지 보내기
구성 백업	HTTP	80	노드 관리 LIF	http://<콘솔 에이전트 IP 주소>/occm/offboxconfig	구성 백업을 콘솔 에이전트로 보냅니다. "ONTAP 문서" .
DHCP	68	UDP	노드 관리 LIF	DHCP	최초 설정을 위한 DHCP 클라이언트
DHCPS	67	UDP	노드 관리 LIF	DHCP	DHCP 서버
DNS	53	UDP	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	18600년–18699년	TCP	노드 관리 LIF	대상 서버	NDMP 사본
SMTP	25	TCP	노드 관리 LIF	메일 서버	SMTP 알림은 AutoSupport 에 사용할 수 있습니다.
SNMP	161	TCP	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	161	UDP	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	162	TCP	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	162	UDP	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
SnapMirror	11104	TCP	클러스터 간 LIF	ONTAP 클러스터 간 LIF	SnapMirror 위한 클러스터 간 통신 세션 관리
	11105	TCP	클러스터 간 LIF	ONTAP 클러스터 간 LIF	SnapMirror 데이터 전송
시스템 로그	514	UDP	노드 관리 LIF	시스템 로그 서버	Syslog 전달 메시지

콘솔 에이전트에 대한 요구 사항

아직 콘솔 에이전트를 만들지 않았다면 콘솔 에이전트에 대한 네트워킹 요구 사항도 검토해야 합니다.

- "콘솔 에이전트에 대한 네트워킹 요구 사항 보기"
- "Azure의 보안 그룹 규칙"

관련 주제

- "Cloud Volumes ONTAP 에 대한 AutoSupport 설정 확인"

- "ONTAP 내부 포트에 대해 알아보세요" .

Azure에서 고객 관리 키를 사용하도록 Cloud Volumes ONTAP 설정

Azure의 Cloud Volumes ONTAP 에서는 Microsoft에서 관리하는 키를 사용하여 Azure Storage Service Encryption을 사용하여 데이터가 자동으로 암호화됩니다. 하지만 이 페이지의 단계에 따라 자신의 암호화 키를 대신 사용할 수 있습니다.

데이터 암호화 개요

Cloud Volumes ONTAP 데이터는 Azure에서 자동으로 암호화됩니다. "Azure Storage 서비스 암호화" . 기본 구현에서는 Microsoft에서 관리하는 키를 사용합니다. 설정이 필요하지 않습니다.

Cloud Volumes ONTAP 에서 고객 관리 키를 사용하려면 다음 단계를 완료해야 합니다.

1. Azure에서 키 자격 증명 모음을 만든 다음 해당 자격 증명 모음에서 키를 생성합니다.
2. NetApp Console 에서 API를 사용하여 키를 사용하는 Cloud Volumes ONTAP 시스템을 만듭니다.

데이터 암호화 방법

콘솔은 디스크 암호화 세트를 사용하는데, 이를 통해 페이지 블롭이 아닌 관리형 디스크에서 암호화 키를 관리할 수 있습니다. 새로운 데이터 디스크도 동일한 디스크 암호화 세트를 사용합니다. 하위 버전에서는 고객 관리 키 대신 Microsoft 관리 키를 사용합니다.

고객 관리 키를 사용하도록 구성된 Cloud Volumes ONTAP 시스템을 생성한 후 Cloud Volumes ONTAP 데이터는 다음과 같이 암호화됩니다.

Cloud Volumes ONTAP 구성	키 암호화에 사용되는 시스템 디스크	키 암호화에 사용되는 데이터 디스크
단일 노드	• 부팅 • 핵심 • NVRAM	• 뿌리 • 데이터
페이지 Blob이 있는 Azure HA 단일 가용성 영역	• 부팅 • 핵심 • NVRAM	None
공유 관리 디스크가 있는 Azure HA 단일 가용성 영역	• 부팅 • 핵심 • NVRAM	• 뿌리 • 데이터

Cloud Volumes ONTAP 구성	키 암호화에 사용되는 시스템 디스크	키 암호화에 사용되는 데이터 디스크
공유 관리 디스크를 사용한 Azure HA 다중 가용성 영역	• 부팅 • 핵심 • NVRAM	• 뿌리 • 데이터

Cloud Volumes ONTAP 의 모든 Azure 스토리지 계정은 고객 관리 키를 사용하여 암호화됩니다. 스토리지 계정을 생성하는 동안 암호화하려면 Cloud Volumes ONTAP 생성 요청에서 리소스 ID를 생성하고 제공해야 합니다. 이는 모든 유형의 배포에 적용됩니다. 해당 정보를 제공하지 않으면 저장소 계정은 여전히 암호화되지만 콘솔은 먼저 Microsoft에서 관리하는 키 암호화를 사용하여 저장소 계정을 만든 다음, 저장소 계정을 업데이트하여 고객이 관리하는 키를 사용합니다.

Cloud Volumes ONTAP 의 키 회전

암호화 키를 구성할 때 Azure Portal을 사용하여 자동 키 순환을 설정하고 활성화해야 합니다. 암호화 키의 새로운 버전을 만들고 활성화하면 Cloud Volumes ONTAP 암호화에 최신 키 버전을 자동으로 감지하고 사용할 수 있으므로 수동 개입 없이도 데이터가 안전하게 유지됩니다.

키 구성 및 키 순환 설정에 대한 자세한 내용은 다음 Microsoft Azure 설명서 항목을 참조하세요.

- "Azure Key Vault에서 암호화 키 자동 순환 구성"
- "Azure PowerShell - 고객 관리 키 사용"

> 키를 구성한 후 다음을 선택했는지 확인하십시오. "자동 회전 활성화" 이를 통해 Cloud Volumes ONTAP 이전 키가 만료되면 새 키를 사용할 수 있습니다. Azure Portal에서 이 옵션을 활성화하지 않으면 Cloud Volumes ONTAP 새 키를 자동으로 감지하지 못하여 스토리지 프로비저닝에 문제가 발생할 수 있습니다.

사용자가 할당한 관리 ID 만들기

사용자 지정 관리 ID라는 리소스를 만들 수 있는 옵션이 있습니다. 이렇게 하면 Cloud Volumes ONTAP 시스템을 생성할 때 스토리지 계정을 암호화할 수 있습니다. 키 보관소를 만들고 키를 생성하기 전에 이 리소스를 만드는 것이 좋습니다.

리소스의 ID는 다음과 같습니다. `userassignedidentity` .

단계

1. Azure에서 Azure 서비스로 이동하여 *관리 ID*를 선택합니다.
2. *만들기*를 클릭하세요.
3. 다음 세부 정보를 제공하세요.
   - 구독: 구독을 선택하세요. 콘솔 에이전트 구독과 동일한 구독을 선택하는 것이 좋습니다.
   - 리소스 그룹: 기존 리소스 그룹을 사용하거나 새 리소스 그룹을 만듭니다.
   - 지역: 선택적으로 콘솔 에이전트와 동일한 지역을 선택합니다.
   - 이름: 리소스의 이름을 입력하세요.
4. 선택적으로 태그를 추가합니다.

5. *만들기*를 클릭하세요.

키 볼트를 생성하고 키를 생성합니다.

키 보관소는 Cloud Volumes ONTAP 시스템을 만들려는 동일한 Azure 구독 및 지역에 있어야 합니다.

만약 당신이라면사용자가 할당한 관리 ID를 생성했습니다. 키 보관소를 생성하는 동안 키 보관소에 대한 액세스 정책도 생성해야 합니다.

단계

1. "Azure 구독에서 키 자격 증명 모음 만들기" .

   키 보관소에 대한 다음 요구 사항을 참고하세요.

   - 키 볼트는 Cloud Volumes ONTAP 시스템과 동일한 지역에 있어야 합니다.
   - 다음 옵션을 활성화해야 합니다.
     - 소프트 삭제 (이 옵션은 기본적으로 활성화되어 있지만 비활성화해서는 안 됩니다)
     - 퍼지 보호
     - 볼륨 암호화를 위한 **Azure Disk Encryption** (단일 노드 시스템, 여러 영역의 HA 쌍 및 HA 단일 AZ 배포용)

       Azure 고객 관리 암호화 키를 사용하려면 키 자격 증명 모음에 Azure Disk 암호화가 활성화되어 있어야 합니다.
   - 사용자가 할당한 관리 ID를 생성한 경우 다음 옵션을 활성화해야 합니다.
     - 금고 접근 정책
2. Vault 액세스 정책을 선택한 경우 만들기를 클릭하여 키 볼트에 대한 액세스 정책을 만듭니다. 그렇지 않은 경우 3단계로 넘어가세요.
   a. 다음 권한을 선택하세요.
      - 얻다
      - 목록
      - 해독하다
      - 암호화하다
      - 열쇠를 풀다
      - 랩 키
      - 확인하다
      - 징후
   b. 사용자가 할당한 관리 ID(리소스)를 주체로 선택합니다.
   c. 액세스 정책을 검토하고 생성합니다.
3. "키 보관소에서 키 생성" .

   키에 대한 다음 요구 사항을 참고하세요.

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

암호화 키를 사용하는 시스템을 만듭니다.

키 볼트를 만들고 암호화 키를 생성한 후에는 해당 키를 사용하도록 구성된 새 Cloud Volumes ONTAP 시스템을 만들 수 있습니다. 이러한 단계는 API를 사용하여 지원됩니다.

필요한 권한

단일 노드 Cloud Volumes ONTAP 시스템에서 고객 관리 키를 사용하려면 콘솔 에이전트에 다음 권한이 있는지 확인하세요.

```
"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",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"최신 권한 목록 보기"

단계

1. 다음 API 호출을 사용하여 Azure 구독의 주요 자격 증명 모음 목록을 가져옵니다.

   HA 쌍의 경우: `GET /azure/ha/metadata/vaults`

   단일 노드의 경우: `GET /azure/vsa/metadata/vaults`

   *이름*과 *리소스그룹*을 기록해 두세요. 다음 단계에서 해당 값을 지정해야 합니다.

   "이 API 호출에 대해 자세히 알아보세요" .

2. 다음 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 두세요. 다음 단계에서는 해당 값(볼트 이름과 함께)을 지정해야 합니다.

   "이 API 호출에 대해 자세히 알아보세요" .

3. 다음 API 호출을 사용하여 Cloud Volumes ONTAP 시스템을 만듭니다.

   a. HA 쌍의 경우:

      `POST /azure/ha/working-environments`

요청 본문에는 다음 필드가 포함되어야 합니다.

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

포함하다 "userAssignedIdentity": " userAssignedIdentityId" 저장소 계정 암호화에 사용할 리소스를 만든 경우 필드입니다.

"이 API 호출에 대해 자세히 알아보세요" .

b. 단일 노드 시스템의 경우:

```
POST /azure/vsa/working-environments
```

요청 본문에는 다음 필드가 포함되어야 합니다.

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

포함하다 "userAssignedIdentity": " userAssignedIdentityId" 저장소 계정 암호화에 사용할 리소스를 만든 경우 필드입니다.

"이 API 호출에 대해 자세히 알아보세요" .

결과

데이터 암호화를 위해 고객 관리 키를 사용하도록 구성된 새로운 Cloud Volumes ONTAP 시스템이 있습니다.

Azure에서 Cloud Volumes ONTAP 에 대한 라이선싱 설정

Cloud Volumes ONTAP 에서 사용할 라이선싱 옵션을 결정한 후에는 새 시스템을 만들 때 해당 라이선싱 옵션을 선택하기 전에 몇 가지 단계를 거쳐야 합니다.

프리미엄

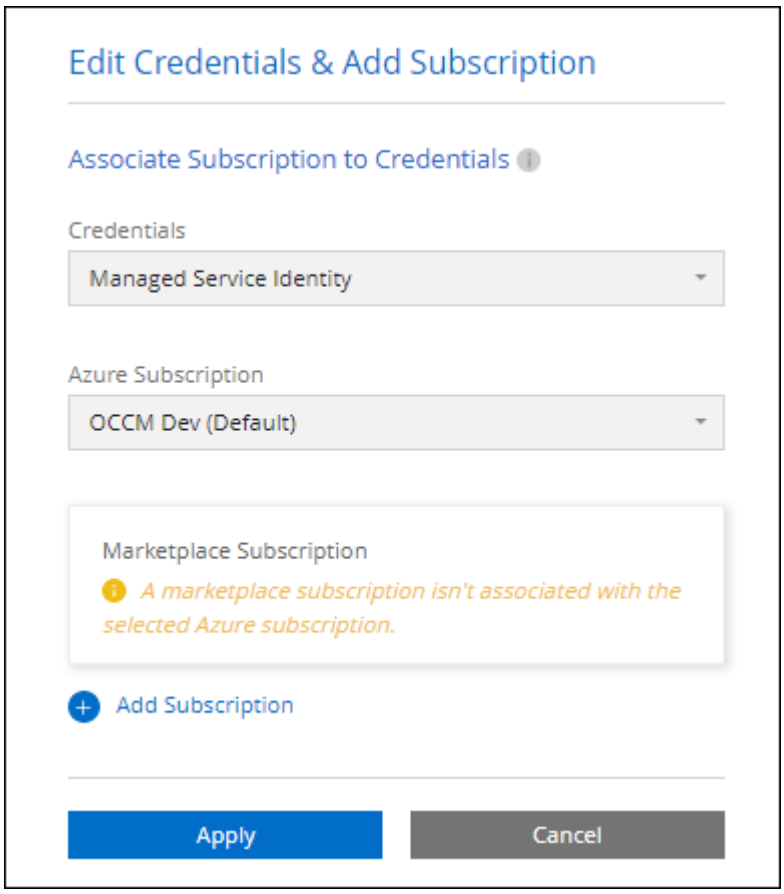
최대 500GiB의 프로비저닝 용량을 제공하는 Cloud Volumes ONTAP 무료로 사용하려면 Freemium 옵션을 선택하세요. "Freemium 제공에 대해 자세히 알아보세요" .

단계

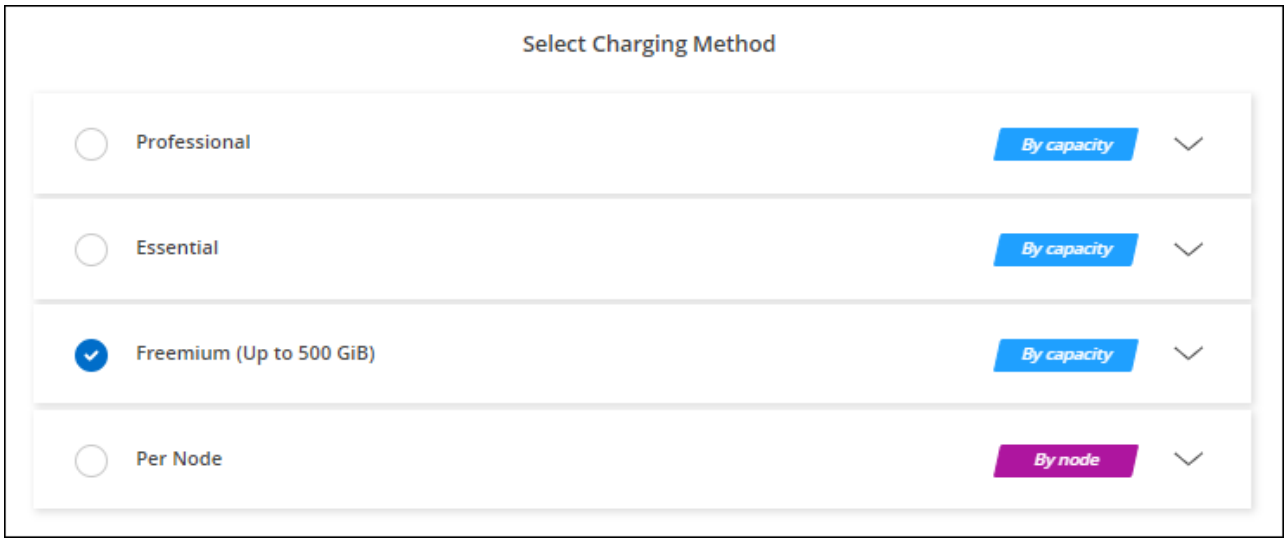
1. NetApp Console 의 왼쪽 탐색 메뉴에서 *스토리지 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 화면의 지시에 따라 Azure Marketplace에서 종량제 상품을 구독하세요.

   프로비저닝된 용량이 500GiB를 초과하지 않는 한 마켓플레이스 구독을 통해 요금이 청구되지 않습니다. 초과 시 시스템은 자동으로 다음 용량으로 변환됩니다."필수 패키지" .



a. 콘솔로 돌아와서 요금 청구 방법 페이지에서 *프리미엄*을 선택하세요.



"Azure에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

용량 기반 라이센스

용량 기반 라이선싱을 사용하면 TiB 용량당 Cloud Volumes ONTAP 비용을 지불할 수 있습니다. 용량 기반 라이선싱은 패키지 형태로 제공됩니다. 패키지에는 Essentials 패키지와 Professional 패키지가 있습니다.

Essentials 및 Professional 패키지는 다음과 같은 소비 모델 또는 구매 옵션으로 이용 가능합니다.

- NetApp 에서 구매한 라이선스(BYOL(Bring Your Own License))
- Azure Marketplace의 시간당, 사용량에 따라 지불(PAYGO) 구독
- 연간 계약

"용량 기반 라이선싱에 대해 자세히 알아보세요" .

다음 섹션에서는 각 소비 모델을 시작하는 방법을 설명합니다.

바이올

NetApp 에서 라이선스(BYOL)를 구매하여 선불로 지불하면 모든 클라우드 공급자에 Cloud Volumes ONTAP 시스템을 배포할 수 있습니다.

NetApp BYOL 라이선스 구매, 연장 및 갱신을 제한하고 있습니다. 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAP 에 대한 BYOL 라이선싱의 제한된 가용성" .

단계

1. "라이센스를 얻으려면 NetApp Sales에 문의하세요."
2. "콘솔에 NetApp 지원 사이트 계정 추가"

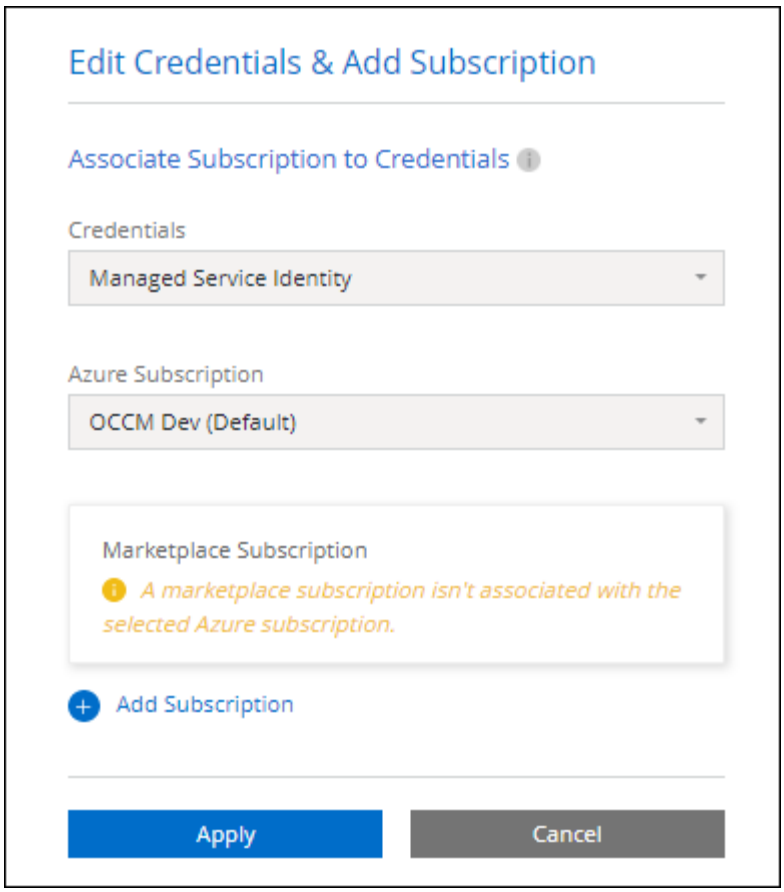
   콘솔은 NetApp 지원 사이트 계정과 연결된 라이선스에 대한 세부 정보를 얻기 위해 NetApp 라이선스 서비스에 자동으로 쿼리를 보냅니다. 오류가 없으면 콘솔이 자동으로 라이선스를 콘솔에 추가합니다.

   Cloud Volumes ONTAP 에서 라이선스를 사용하려면 먼저 콘솔에서 라이선스를 사용할 수 있어야 합니다. 필요한 경우 다음을 수행할 수 있습니다."콘솔에 라이센스를 수동으로 추가합니다." .

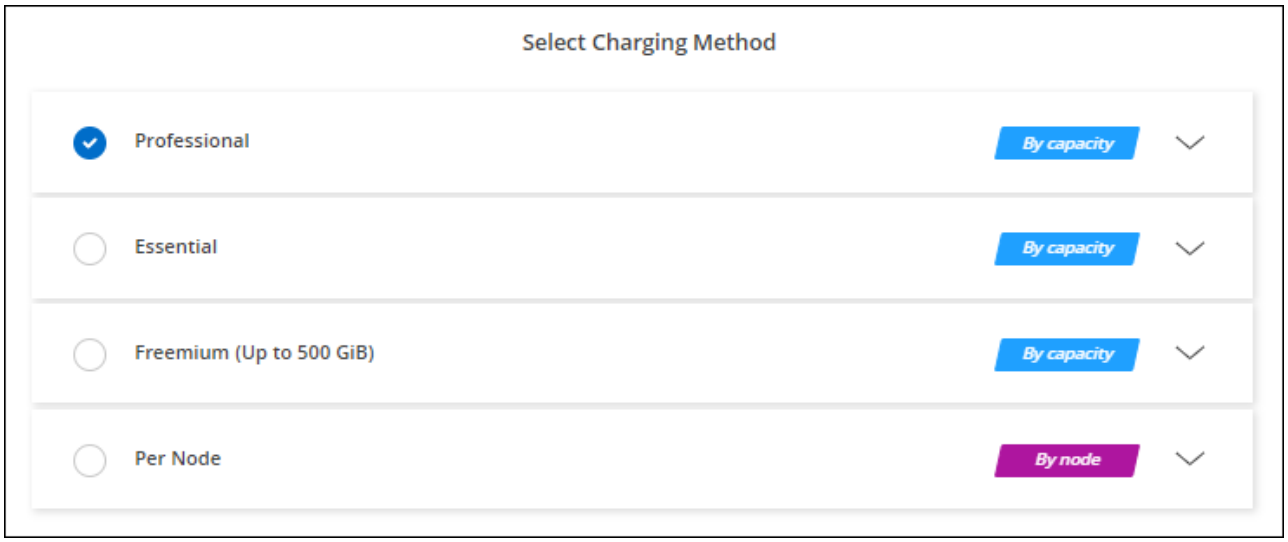
3. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 화면의 지시에 따라 Azure Marketplace에서 종량제 상품을 구독하세요.

      NetApp 에서 구매한 라이선스는 항상 먼저 청구되지만, 라이선스 용량을 초과하거나 라이선스 기간이 만료되면 마켓플레이스의 시간당 요금으로 청구됩니다.



a. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"Azure에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

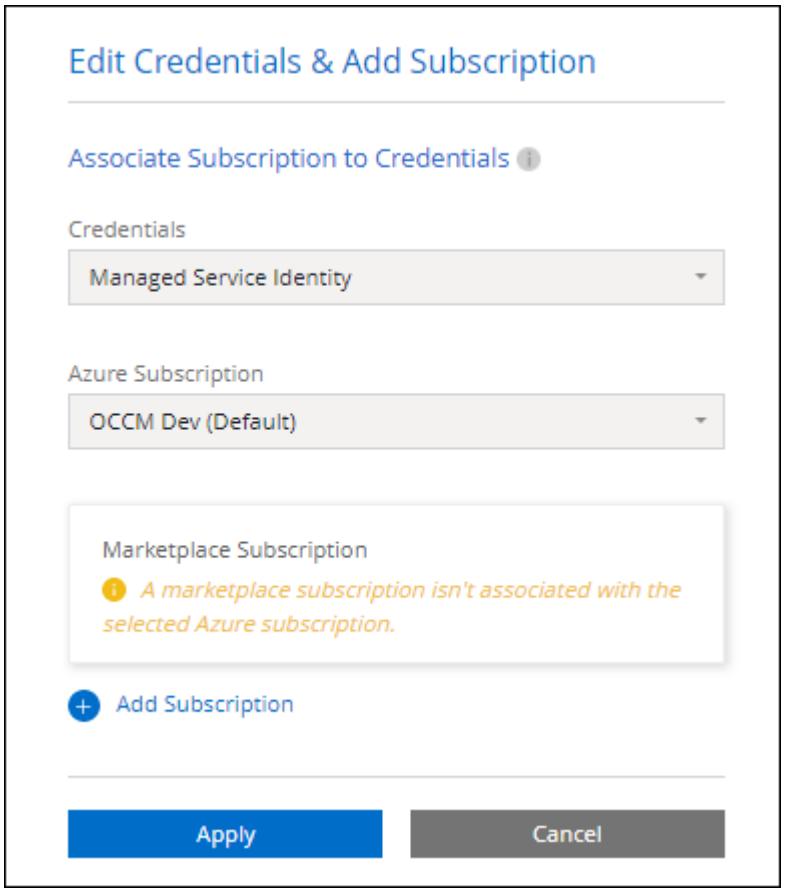
PAYGO 구독

클라우드 공급업체의 마켓플레이스에서 제공하는 혜택을 구독하여 시간당 요금을 지불하세요.

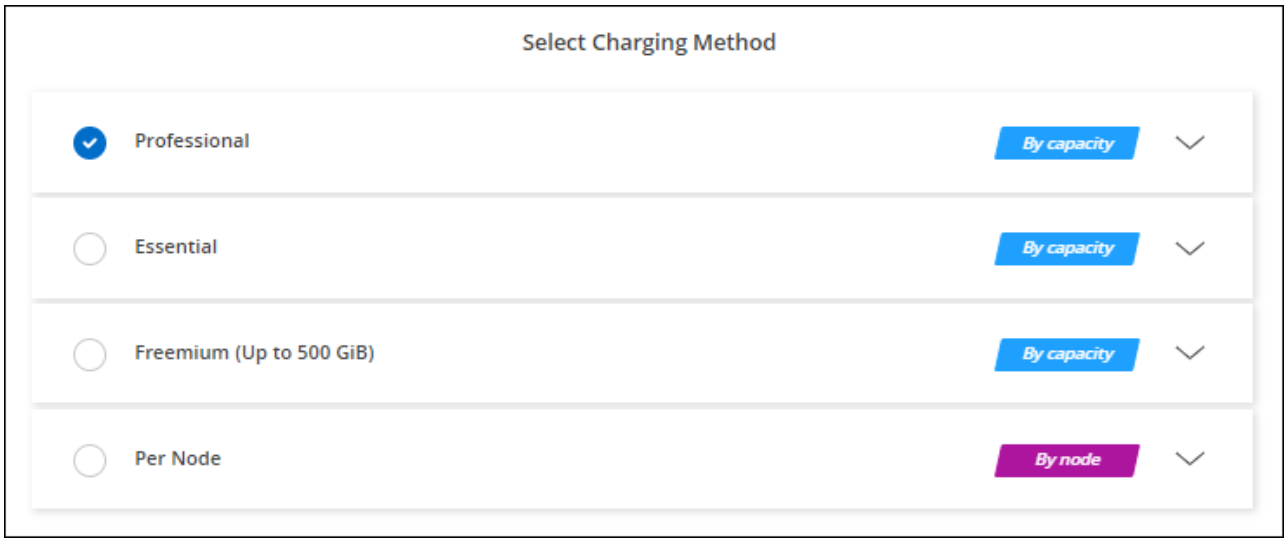
Cloud Volumes ONTAP 시스템을 만들면 콘솔에서 Azure Marketplace에서 제공되는 계약에 가입하라는 메시지가 표시됩니다. 해당 구독은 요금 청구를 위해 시스템에 연결됩니다. 동일한 구독을 추가 시스템에도 사용할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.
   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 화면의 지시에 따라 Azure Marketplace에서 종량제 상품을 구독하세요.



   b. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"Azure에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

설정 > 자격 증명 페이지에서 Azure 계정과 연결된 Azure Marketplace 구독을 관리할 수 있습니다. "Azure 계정 및 구독을 관리하는 방법을 알아보세요."

연간 계약

연간 계약을 구매하여 매년 Cloud Volumes ONTAP 에 대한 비용을 지불하세요.

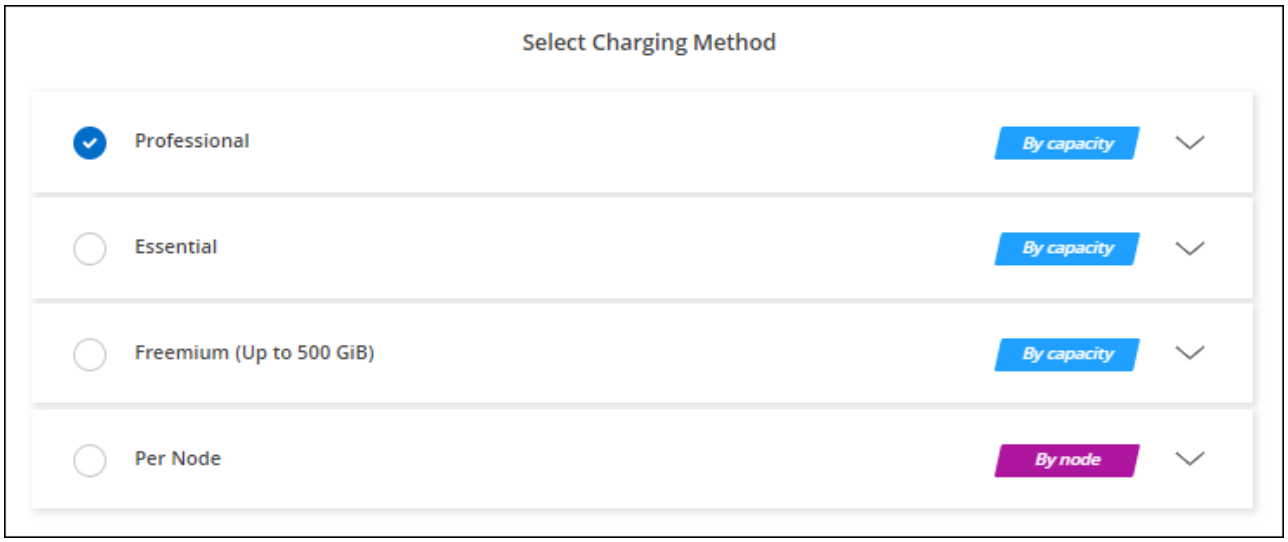
단계

1. 연간 계약을 구매하려면 NetApp 영업 담당자에게 문의하세요.

   해당 계약은 Azure Marketplace에서 비공개 제안으로 제공됩니다.

   NetApp 에서 비공개 제안을 공유한 후, 시스템을 만드는 동안 Azure Marketplace에서 구독할 때 연간 요금제를 선택할 수 있습니다.

2. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.
   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가 > 계속*을 클릭합니다.
   b. Azure Portal에서 Azure 계정과 공유된 연간 플랜을 선택한 다음 *구독*을 클릭합니다.
   c. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"Azure에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

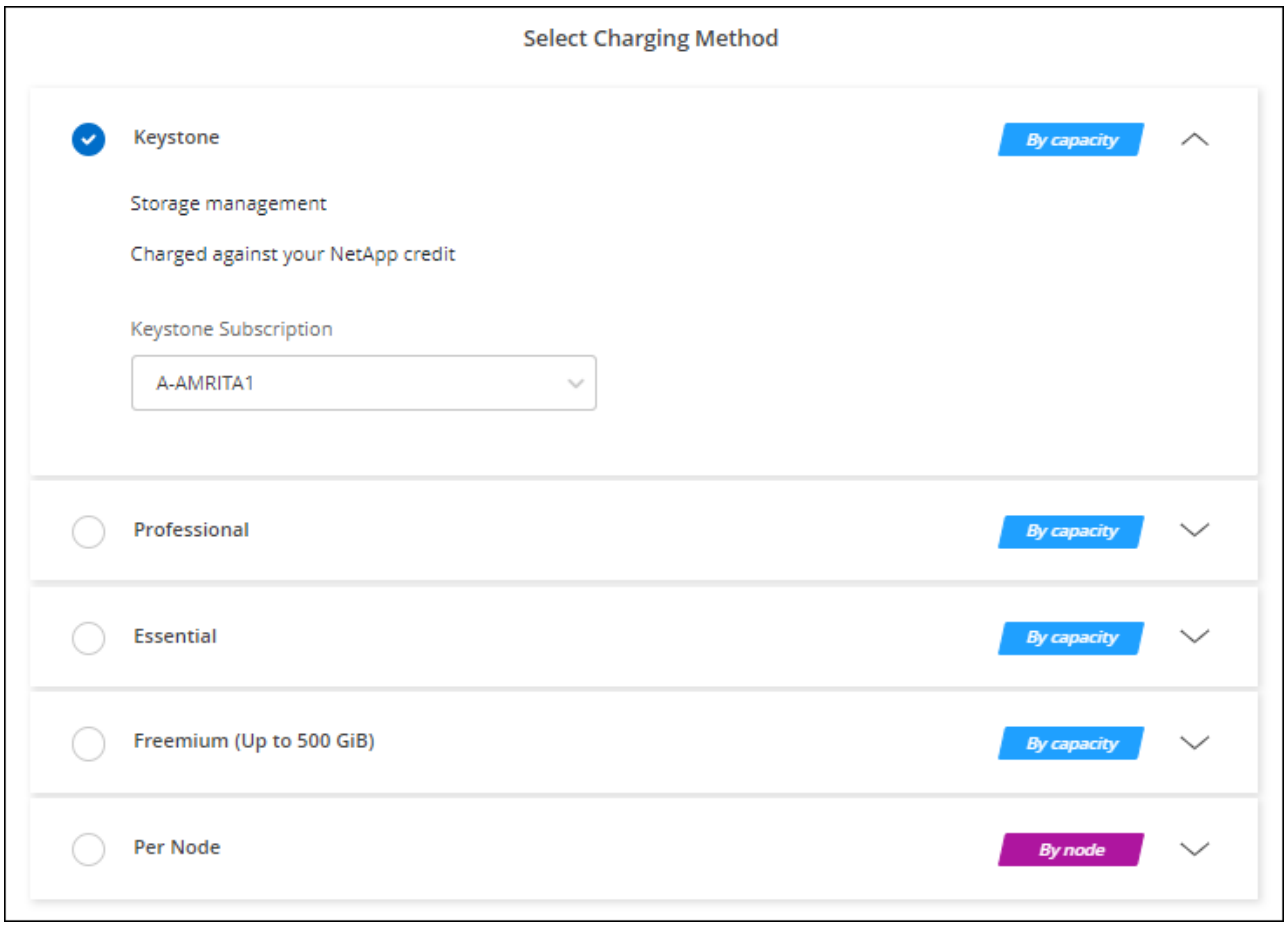
Keystone 구독

Keystone 구독은 사용량에 따라 비용을 지불하는 구독 기반 서비스입니다. "NetApp Keystone 구독에 대해 자세히 알아보세요" .

단계

1. 아직 구독이 없으신 경우, "NetApp 에 문의하세요"
2. 콘솔에서 하나 이상의 Keystone 구독으로 사용자 계정을 인증하려면 NetApp 에 문의으로 이메일을 보내주세요.
3. NetApp 귀하의 계정을 승인한 후,"Cloud Volumes ONTAP 과 함께 사용할 구독을 연결하세요" .

4. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.
   a. 청구 방법을 선택하라는 메시지가 표시되면 Keystone 구독 청구 방법을 선택하세요.



"Azure에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

노드 기반 라이센스

노드 기반 라이선스는 Cloud Volumes ONTAP 의 이전 세대 라이선스입니다. 노드 기반 라이선스는 NetApp (BYOL)에서 구매할 수 있으며, 특정 경우에만 라이선스를 갱신할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- "노드 기반 라이선스의 가용성 종료"
- "노드 기반 라이선스 제공 종료"
- "노드 기반 라이선스를 용량 기반 라이선스로 변환"

Azure에서 Cloud Volumes ONTAP 에 대해 고가용성 모드 활성화

예기치 않은 장애 조치 시간을 줄이고 Cloud Volumes ONTAP에 대한 NFSv4 지원을 활성화하려면 Microsoft Azure의 고가용성(HA) 모드를 활성화해야 합니다. 이 모드를 활성화하면 Cloud Volumes ONTAP HA 노드는 CIFS 및 NFSv4 클라이언트에 대한 예기치 않은 장애 조치 시 낮은(60초) 복구 시간 목표(RTO)를 달성할 수 있습니다.

Cloud Volumes ONTAP 9.10.1부터 Microsoft Azure에서 실행되는 Cloud Volumes ONTAP HA 쌍에 대한 계획되지

않은 장애 조치 시간을 줄이고 NFSv4에 대한 지원을 추가했습니다. 이러한 향상된 기능을 Cloud Volumes ONTAP 에 적용하려면 Azure 구독에서 고가용성 기능을 활성화해야 합니다.

이 작업에 관하여

NetApp Console은 Azure 구독에서 해당 기능을 활성화해야 할 때 다음과 같은 세부 정보를 표시합니다. 다음 사항에 유의하십시오.

- Cloud Volumes ONTAP HA 쌍의 고가용성에는 문제가 없습니다. 이 Azure 기능은 ONTAP 과 함께 작동하여 계획되지 않은 장애 조치 이벤트로 인해 NFS 프로토콜에 대한 클라이언트 관찰 애플리케이션 중단 시간을 줄입니다.
- 이 기능을 활성화해도 Cloud Volumes ONTAP HA 쌍은 중단되지 않습니다.
- Azure 구독에서 이 기능을 활성화해도 다른 VM에는 문제가 발생하지 않습니다.
- Cloud Volumes ONTAP CIFS 및 NFS 클라이언트에서 클러스터 및 SVM 관리 LIF의 장애 조치 중에 내부 Azure Load Balancer를 사용합니다.
- HA 모드가 활성화되면 콘솔은 12시간마다 시스템을 검사하여 내부 Azure Load Balancer 규칙을 업데이트합니다.

단계

소유자 권한이 있는 Azure 사용자는 Azure CLI에서 해당 기능을 활성화할 수 있습니다.

1. "Azure Portal에서 Azure Cloud Shell에 액세스"
2. 고가용성 모드 기능을 등록하세요:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. 선택적으로 해당 기능이 등록되었는지 확인하세요.

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Azure CLI는 다음과 유사한 결과를 반환해야 합니다.

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

관련 링크

1. "Microsoft Azure 설명서: 고가용성 포트 개요"
2. "Microsoft Azure 설명서: Azure CLI 시작하기"

Azure에서 Cloud Volumes ONTAP 에 VMOrchestratorZonalMultiFD 사용

로컬 중복 스토리지(LRS) 단일 가용성 영역(AZ)에 VM 인스턴스를 배포하려면 Microsoft를 활성화해야 합니다. `Microsoft.Compute/VMOrchestratorZonalMultiFD` 귀하의 구독에 대한 기능입니다. 고가용성(HA) 모드에서 이 기능은 동일한 가용성 영역 내의 별도의 장애 도메인에 노드를 배포하는 것을 용이하게 합니다.

이 기능을 활성화하지 않으면 영역별 배포가 발생하지 않으며, 이전 LRS 비영역별 배포가 적용됩니다.

단일 가용성 영역에 VM을 배포하는 방법에 대한 자세한 내용은 다음을 참조하세요."Azure의 고가용성 쌍" .

"소유자" 권한이 있는 사용자로 다음 단계를 수행하세요.

단계

1. Azure Portal에서 Azure Cloud Shell에 액세스합니다. 자세한 내용은 다음을 참조하세요. "Microsoft Azure 설명서: Azure Cloud Shell 시작하기" .
2. 등록하세요 `Microsoft.Compute/VMOrchestratorZonalMultiFD` 다음 명령을 실행하여 기능을 추가하세요.

   az 계정 설정 -s <*Azure_subscription_name_or_ID*> az 기능 등록 --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute

3. 등록 상태와 출력 샘플을 확인하세요.

az 기능 표시 -n VMOrchestratorZonalMultiFD --네임스페이스 Microsoft.Compute { "id": "/subscriptions/<*ID*>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiFD", "name": "Microsoft.Compute/VMOrchestratorZonalMultiFD", "properties": { "state": "등록됨" }, "type": "Microsoft.Features/providers/features" }

Azure에서 Cloud Volumes ONTAP 실행

NetApp Console에서 Cloud Volumes ONTAP 시스템을 생성하여 Azure에서 단일 노드 시스템 또는 HA 쌍을 시작할 수 있습니다.

시작하기 전에

시작하기 전에 다음 사항이 필요합니다.

- 이미 실행 중인 콘솔 에이전트입니다.
  - 당신은 ~을 가져야합니다 "시스템과 연결된 콘솔 에이전트" .
  - "항상 콘솔 에이전트를 실행 상태로 두어야 합니다." .
- 사용하려는 구성에 대한 이해.

  구성을 계획해야 하며, 관리자로부터 필요한 Azure 네트워킹 세부 정보를 받아야 합니다. 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAP 구성 계획" .

- Cloud Volumes ONTAP 에 대한 라이선싱을 설정하는 데 필요한 사항에 대한 이해.

  "라이선싱 설정 방법 알아보기" .

이 작업에 관하여

콘솔이 Azure에 Cloud Volumes ONTAP 시스템을 만들면 리소스 그룹, 네트워크 인터페이스, 스토리지 계정 등 여러 Azure 개체가 만들어집니다. 마법사가 끝나면 리소스 요약을 검토할 수 있습니다.

데이터 손실 가능성

가장 좋은 방법은 각 Cloud Volumes ONTAP 시스템에 대해 새로운 전용 리소스 그룹을 사용하는 것입니다.

데이터 손실 위험 때문에 기존의 공유 리소스 그룹에 Cloud Volumes ONTAP 배포하는 것은 권장되지 않습니다. 배포 실패 또는 삭제 시 콘솔에서 공유 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거할 수 있지만, Azure 사용자가 실수로 공유 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 삭제할 수도 있습니다.

Azure에서 단일 노드 Cloud Volumes ONTAP 시스템 실행

Azure에서 단일 노드 Cloud Volumes ONTAP 시스템을 시작하려면 Console에서 단일 노드 시스템을 생성해야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.

2. 시스템 페이지에서 *시스템 추가*를 클릭하고 안내를 따르세요.
3. 위치 선택: *Microsoft Azure*와 * Cloud Volumes ONTAP 단일 노드*를 선택하세요.
4. 메시지가 표시되면 "콘솔 에이전트 생성" .
5. 세부 정보 및 자격 증명: 필요에 따라 Azure 자격 증명과 구독을 변경하고, 클러스터 이름을 지정하고, 필요한 경우 태그를 추가한 다음 자격 증명을 지정합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
시스템 이름	콘솔은 시스템 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Azure 가상 머신의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
리소스 그룹 태그	태그는 Azure 리소스에 대한 메타데이터입니다. 이 필드에 태그를 입력하면 콘솔이 Cloud Volumes ONTAP 시스템과 연결된 리소스 그룹에 태그를 추가합니다. 시스템을 생성할 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 시스템을 생성한 후에 태그를 더 추가할 수 있습니다. API는 시스템을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 정보는 다음을 참조하세요. "Microsoft Azure 설명서: 태그를 사용하여 Azure 리소스 구성" .
사용자 이름과 비밀번호	이는 Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하면 ONTAP System Manager나 ONTAP CLI를 통해 Cloud Volumes ONTAP 에 연결할 수 있습니다. 기본 *admin* 사용자 이름을 유지하거나 사용자 지정 사용자 이름으로 변경하세요.
자격 증명 편집	이 Cloud Volumes ONTAP 시스템에서는 다양한 Azure 자격 증명과 Azure 구독을 선택하여 사용할 수 있습니다. 사용량에 따라 지불하는 Cloud Volumes ONTAP 시스템을 배포하려면 선택한 Azure 구독과 Azure Marketplace 구독을 연결해야 합니다. "자격 증명을 추가하는 방법을 알아보세요" .

6. 서비스: Cloud Volumes ONTAP 과 함께 사용하거나 사용하지 않을 개별 서비스를 활성화하거나 비활성화합니다.
   - "NetApp Data Classification 에 대해 자세히 알아보세요"
   - "NetApp Backup and Recovery 에 대해 자세히 알아보세요"

   WORM 및 데이터 계층화를 활용하려면 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 시스템을 배포해야 합니다.

7. 위치: 지역, 가용성 영역, VNet 및 서브넷을 선택한 다음 확인란을 선택하여 콘솔 에이전트와 대상 위치 간의 네트워크 연결을 확인합니다.

   중국 지역의 경우 단일 노드 배포는 Cloud Volumes ONTAP 9.12.1 GA 및 9.13.0 GA에서만 지원됩니다. 이러한 버전을 Cloud Volumes ONTAP 의 최신 패치 및 릴리스로 업그레이드할 수 있습니다."Azure에서 지원됨" . 중국 지역에 이후 Cloud Volumes ONTAP 버전을 배포하려면 NetApp 지원팀에 문의하세요. 중국 지역에서는 NetApp 에서 직접 구매한 라이선스만 지원되며, 마켓플레이스 구독은 이용할 수 없습니다.

8. 연결성: 새 리소스 그룹이나 기존 리소스 그룹을 선택한 다음, 미리 정의된 보안 그룹을 사용할지 아니면 사용자 고유의 보안 그룹을 사용할지 선택합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
리소스 그룹	Cloud Volumes ONTAP 에 대한 새 리소스 그룹을 만들거나 기존 리소스 그룹을 사용하세요. 가장 좋은 방법은 Cloud Volumes ONTAP 에 대해 새로운 전용 리소스 그룹을 사용하는 것입니다. 기존의 공유 리소스 그룹에 Cloud Volumes ONTAP 배포하는 것은 가능하지만 데이터 손실 위험 때문에 권장하지는 않습니다. 자세한 내용은 위의 경고를 참조하세요. 사용 중인 Azure 계정에 다음이 있는 경우 "필요한 권한" 배포 실패 또는 삭제 시 콘솔은 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거합니다.
생성된 보안 그룹	콘솔에서 보안 그룹을 생성하도록 허용하는 경우 트래픽 허용 방법을 선택해야 합니다. • *선택한 VNet만*을 선택하는 경우 인바운드 트래픽의 소스는 선택한 VNet의 서브넷 범위와 콘솔 에이전트가 있는 VNet의 서브넷 범위입니다. 이것은 권장되는 옵션입니다. • *모든 VNet*을 선택하면 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
기존 사용	기존 보안 그룹을 선택하는 경우 Cloud Volumes ONTAP 요구 사항을 충족해야 합니다. "기본 보안 그룹 보기" .

9. 청구 방법 및 **NSS** 계정: 이 시스템에서 사용할 청구 옵션을 지정한 다음 NetApp 지원 사이트 계정을 지정하세요.
   - "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요" .
   - "라이선싱 설정 방법 알아보기" .
10. 사전 구성된 패키지: Cloud Volumes ONTAP 시스템을 빠르게 배포하려면 패키지 중 하나를 선택하거나 *내 구성 만들기*를 클릭하세요.

    패키지 중 하나를 선택하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.
11. 라이선스: 필요한 경우 Cloud Volumes ONTAP 버전을 변경하고 가상 머신 유형을 선택합니다.

    선택한 버전에 대해 최신 릴리스 후보, 일반 출시 버전 또는 패치 릴리스가 제공되는 경우 BlueXP 작업 환경을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.16.1 P3를 선택하고 9.16.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리스에서 다른 릴리스로 전달되지 않습니다(예: 9.15에서 9.16로 전달).
12. **Azure Marketplace**에서 구독: 콘솔에서 Cloud Volumes ONTAP 의 프로그래밍 방식 배포를 활성화할 수 없는 경우 이 페이지가 표시됩니다. 화면에 나열된 단계를 따르세요. "마켓플레이스 제품의 프로그래밍 방식 배포" 자세한 내용은.
13. 기본 스토리지 리소스: 초기 집계에 대한 설정을 선택합니다. 디스크 유형, 각 디스크의 크기, Blob 스토리지에 대한 데이터 계층화를 활성화할지 여부입니다.

    다음 사항에 유의하세요.
    - VNet 내에서 스토리지 계정에 대한 공용 액세스가 비활성화된 경우 Cloud Volumes ONTAP 시스템에서 데이터 계층화를 활성화할 수 없습니다. 자세한 내용은 다음을 참조하세요."보안 그룹 규칙" .

- 디스크 유형은 초기 볼륨을 위한 것입니다. 이후 볼륨에는 다른 디스크 유형을 선택할 수 있습니다.
- 디스크 크기는 초기 집계의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 콘솔이 생성하는 모든 추가 집계에 적용됩니다. 고급 할당 옵션을 사용하면 다른 디스크 크기를 사용하는 집계를 만들 수 있습니다.

  디스크 유형 및 크기 선택에 대한 도움말은 다음을 참조하세요."Azure에서 시스템 크기 조정" .

- 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
- 데이터 계층화를 비활성화하면 이후 집계에서 활성화할 수 있습니다.

  "데이터 계층화에 대해 자세히 알아보세요" .

14. 쓰기 속도 및 **WORM**:

    a. 원하는 경우 보통 또는 높음 쓰기 속도를 선택하세요.

       "쓰기 속도에 대해 자세히 알아보세요" .

    b. 원하는 경우 WORM(한 번 쓰고 여러 번 읽기) 저장소를 활성화합니다.

       이 옵션은 특정 VM 유형에만 사용할 수 있습니다. 지원되는 VM 유형을 알아보려면 다음을 참조하세요."HA 쌍에 대한 라이선스별 지원 구성" .

       Cloud Volumes ONTAP 버전 9.7 이하에서 데이터 계층화가 활성화된 경우 WORM을 활성화할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로 되돌리거나 다운그레이드하는 것이 차단됩니다.

    "WORM 스토리지에 대해 자세히 알아보세요" .

    a. WORM 저장소를 활성화하는 경우 보존 기간을 선택하세요.

15. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

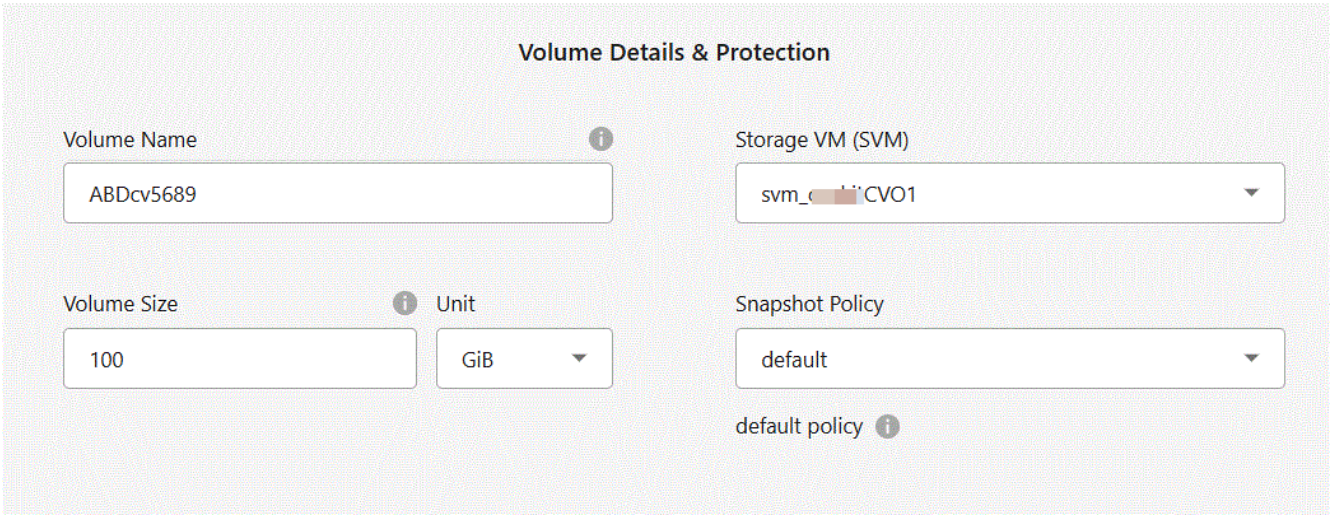
    "지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요" .

    이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝을 활성화하는지 여부에 따라 크게 달라집니다. 씬 프로비저닝을 활성화하면 현재 사용 가능한 물리적 저장소보다 큰 볼륨을 만들 수 있습니다.
액세스 제어(NFS에만 해당)	내보내기 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 콘솔은 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS에만 해당)	이러한 필드를 사용하면 사용자 및 그룹의 공유 액세스 수준(액세스 제어 목록 또는 ACL이라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자나 그룹, 또는 UNIX 사용자나 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자 도메인을 포함해야 합니다.

필드	설명
스냅샷 정책	스냅샷 복사 정책은 NetApp 스냅샷 복사본이 자동으로 생성되는 빈도와 수를 지정합니다. NetApp 스냅샷 복사본은 성능에 영향을 미치지 않고 최소한의 저장 공간만 필요한 특정 시점의 파일 시스템 이미지입니다. 기본 정책을 선택하거나 아무것도 선택하지 않을 수 있습니다. 일시적인 데이터의 경우 '없음'을 선택할 수 있습니다. 예를 들어 Microsoft SQL Server의 경우 tempdb를 선택합니다.
고급 옵션(NFS에만 해당)	볼륨에 대한 NFS 버전을 선택합니다: NFSv3 또는 NFSv4.
이니시에이터 그룹 및 IQN(iSCSI에만 해당)	iSCSI 스토리지 대상은 LUN(논리 단위)이라고 하며 호스트에 표준 블록 장치로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름 테이블이며, 어떤 이니시에이터가 어떤 LUN에 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 컨버지드 네트워크 어댑터(CNA) 또는 전용 호스트 버스 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 정규화된 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성하면 콘솔이 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후, "IQN을 사용하여 호스트에서 LUN에 연결합니다." .

다음 이미지는 볼륨 생성 마법사의 첫 번째 페이지를 보여줍니다.



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

필드	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 가입할 도메인의 Active Directory LDAP 서버와 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
가입할 Active Directory 도메인	CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.
도메인에 가입할 수 있는 권한이 있는 자격 증명	AD 도메인 내의 지정된 조직 단위(OU)에 컴퓨터를 추가할 수 있는 권한이 있는 Windows 계정의 이름과 비밀번호입니다.
CIFS 서버 NetBIOS 이름	AD 도메인에서 고유한 CIFS 서버 이름입니다.

필드	설명
조직 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. Cloud Volumes ONTAP 의 AD 서버로 Azure AD Domain Services를 구성하려면 이 필드에 **OU=AADDC Computers** 또는 *OU=AADDC Users*를 입력해야 합니다.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 설명서: Azure AD Domain Services 관리 도메인에서 OU(조직 단위) 만들기"^]
DNS 도메인	Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 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 참조하세요 "NetApp Console 자동화 문서" 자세한 내용은. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 만든 후에는 구성할 수 없습니다.

17. 사용 프로필, 디스크 유형 및 계층화 정책: 필요한 경우 스토리지 효율성 기능을 활성화할지 여부를 선택하고 볼륨 계층화 정책을 변경합니다.

    자세한 내용은 다음을 참조하세요."볼륨 사용 프로필 이해" 그리고"데이터 계층화 개요" .

18. 검토 및 승인: 선택 사항을 검토하고 확인합니다.

    a. 구성에 대한 세부 정보를 검토하세요.

    b. *자세한 정보*를 클릭하여 콘솔에서 구매할 지원 및 Azure 리소스에 대한 세부 정보를 검토하세요.

    c. 이해합니다... 확인란을 선택하세요.

    d. *이동*을 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP 시스템을 배포합니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템 배포 중 문제가 발생하면 실패 메시지를 검토하세요. 시스템을 선택하고 *환경 다시 만들기*를 클릭할 수도 있습니다.

추가 도움말을 보려면 다음으로 이동하세요. "NetApp Cloud Volumes ONTAP 지원" .

배포 프로세스가 완료된 후에는 Azure Portal에서 시스템 생성 Cloud Volumes ONTAP 구성, 특히 시스템 태그를 수정하지 마세요. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

당신이 완료한 후

- CIFS 공유를 프로비저닝한 경우 사용자 또는 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 ONTAP 시스템 관리자나 ONTAP CLI를 사용하세요.

  할당량을 사용하면 사용자, 그룹 또는 Qtree에서 사용하는 디스크 공간과 파일 수를 제한하거나 추적할 수 있습니다.

Azure에서 Cloud Volumes ONTAP HA 쌍 시작

Azure에서 Cloud Volumes ONTAP HA 쌍을 시작하려면 콘솔에서 HA 시스템을 만들어야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 안내를 따르세요.
3. 메시지가 표시되면 "콘솔 에이전트 생성" .
4. 세부 정보 및 자격 증명: 필요에 따라 Azure 자격 증명과 구독을 변경하고, 클러스터 이름을 지정하고, 필요한 경우 태그를 추가한 다음 자격 증명을 지정합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
시스템 이름	콘솔은 시스템 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Azure 가상 머신의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
리소스 그룹 태그	태그는 Azure 리소스에 대한 메타데이터입니다. 이 필드에 태그를 입력하면 콘솔이 Cloud Volumes ONTAP 시스템과 연결된 리소스 그룹에 태그를 추가합니다. 시스템을 생성할 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 시스템을 생성한 후에 태그를 더 추가할 수 있습니다. API는 시스템을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 정보는 다음을 참조하세요. "Microsoft Azure 설명서: 태그를 사용하여 Azure 리소스 구성" .
사용자 이름과 비밀번호	이는 Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하면 ONTAP System Manager나 ONTAP CLI를 통해 Cloud Volumes ONTAP 에 연결할 수 있습니다. 기본 *admin* 사용자 이름을 유지하거나 사용자 지정 사용자 이름으로 변경하세요.
자격 증명 편집	이 Cloud Volumes ONTAP 시스템에서는 다양한 Azure 자격 증명과 Azure 구독을 선택하여 사용할 수 있습니다. 사용량에 따라 지불하는 Cloud Volumes ONTAP 시스템을 배포하려면 선택한 Azure 구독과 Azure Marketplace 구독을 연결해야 합니다. "자격 증명을 추가하는 방법을 알아보세요" .

5. 서비스: Cloud Volumes ONTAP 과 함께 사용할지 여부에 따라 개별 서비스를 활성화하거나 비활성화합니다.
   - "NetApp Data Classification 에 대해 자세히 알아보세요"
   - "NetApp Backup and Recovery 에 대해 자세히 알아보세요"

   WORM 및 데이터 계층화를 활용하려면 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 시스템을 배포해야 합니다.

6. **HA** 배포 모델:
   a. 단일 가용 영역 또는 *다중 가용 영역*을 선택하세요.
      - 단일 가용성 영역의 경우 Azure 지역, 가용성 영역, VNet 및 서브넷을 선택합니다.

        Cloud Volumes ONTAP 9.15.1부터 Azure의 단일 가용성 영역(AZ)에 HA 모드로 가상 머신(VM) 인스턴스를 배포할 수 있습니다. 이 배포를 지원하는 영역과 지역을 선택해야 합니다. 해당 영역이나 지역이 영역별 배포를 지원하지 않는 경우 LRS에 대한 이전 비영역별 배포 모드가 따릅니다. 공유 관리 디스크에

대해 지원되는 구성을 이해하려면 다음을 참조하세요."공유 관리 디스크를 사용한 HA 단일 가용성 영역 구성" .

- 여러 가용성 영역의 경우 노드 1에 대한 지역, VNet, 서브넷, 영역, 노드 2에 대한 영역을 선택합니다.

b. 네트워크 연결을 확인했습니다... 확인란을 선택하세요.

7. 연결성: 새 리소스 그룹이나 기존 리소스 그룹을 선택한 다음, 미리 정의된 보안 그룹을 사용할지 아니면 사용자 고유의 보안 그룹을 사용할지 선택합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
리소스 그룹	Cloud Volumes ONTAP 에 대한 새 리소스 그룹을 만들거나 기존 리소스 그룹을 사용하세요. 가장 좋은 방법은 Cloud Volumes ONTAP 에 대해 새로운 전용 리소스 그룹을 사용하는 것입니다. 기존의 공유 리소스 그룹에 Cloud Volumes ONTAP 배포하는 것은 가능하지만 데이터 손실 위험 때문에 권장하지는 않습니다. 자세한 내용은 위의 경고를 참조하세요. Azure에 배포하는 각 Cloud Volumes ONTAP HA 쌍에 대해 전용 리소스 그룹을 사용해야 합니다. 리소스 그룹에서는 HA 쌍을 하나만 지원합니다. Azure 리소스 그룹에서 두 번째 Cloud Volumes ONTAP HA 쌍을 배포하려고 하면 콘솔에서 연결 문제가 발생합니다. 사용 중인 Azure 계정에 다음이 있는 경우 "필요한 권한" 배포 실패 또는 삭제 시 콘솔은 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거합니다.
생성된 보안 그룹	콘솔에서 보안 그룹을 생성하도록 허용하는 경우 트래픽 허용 방법을 선택해야 합니다. • *선택한 VNet만*을 선택하는 경우 인바운드 트래픽의 소스는 선택한 VNet의 서브넷 범위와 콘솔 에이전트가 있는 VNet의 서브넷 범위입니다. 이것은 권장되는 옵션입니다. • *모든 VNet*을 선택하면 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
기존 사용	기존 보안 그룹을 선택하는 경우 Cloud Volumes ONTAP 요구 사항을 충족해야 합니다. "기본 보안 그룹 보기" .

8. 청구 방법 및 **NSS** 계정: 이 시스템에서 사용할 청구 옵션을 지정한 다음 NetApp 지원 사이트 계정을 지정하세요.
   - "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요" .
   - "라이선싱 설정 방법 알아보기" .
9. 사전 구성된 패키지: Cloud Volumes ONTAP 시스템을 빠르게 배포하려면 패키지 중 하나를 선택하거나 *구성 변경*을 클릭하세요.

   패키지 중 하나를 선택하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.

10. 라이선스: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 가상 머신 유형을 선택합니다.

선택한 버전에 대해 최신 릴리스 후보, 일반 공급 또는 패치 릴리스가 제공되는 경우 콘솔은 버전을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.13.1을 선택하고 9.13.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리스에서 다른 릴리스로 전달되지 않습니다. 예를 들어, 9.13에서 9.14로 전달되지 않습니다.

11. **Azure Marketplace**에서 구독: 콘솔에서 Cloud Volumes ONTAP 의 프로그래밍 방식 배포를 활성화할 수 없는 경우 다음 단계를 따르세요.
12. 기본 스토리지 리소스: 초기 집계에 대한 설정을 선택합니다. 디스크 유형, 각 디스크의 크기, Blob 스토리지에 대한 데이터 계층화를 활성화할지 여부입니다.

    다음 사항에 유의하세요.

    - 디스크 크기는 초기 집계의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 콘솔이 생성하는 모든 추가 집계에 적용됩니다. 고급 할당 옵션을 사용하면 다른 디스크 크기를 사용하는 집계를 만들 수 있습니다.

      디스크 크기 선택에 대한 도움말은 다음을 참조하세요."Azure에서 시스템 크기 조정" .

    - VNet 내에서 스토리지 계정에 대한 공용 액세스가 비활성화된 경우 Cloud Volumes ONTAP 시스템에서 데이터 계층화를 활성화할 수 없습니다. 자세한 내용은 다음을 참조하세요."보안 그룹 규칙" .
    - 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
    - 데이터 계층화를 비활성화하면 이후 집계에서 활성화할 수 있습니다.

      "데이터 계층화에 대해 자세히 알아보세요" .

    - Cloud Volumes ONTAP 9.15.0P1부터 새로운 고가용성 쌍 배포에 대해 Azure 페이지 Blob이 더 이상 지원되지 않습니다. 현재 기존 고가용성 쌍 배포에서 Azure 페이지 Blob을 사용하는 경우 Edsv4 시리즈 VM 및 Edsv5 시리즈 VM에서 최신 VM 인스턴스 유형으로 마이그레이션할 수 있습니다.

      "Azure에서 지원되는 구성에 대해 자세히 알아보세요." .

13. 쓰기 속도 및 **WORM**:

    a. 원하는 경우 보통 또는 높음 쓰기 속도를 선택하세요.

       "쓰기 속도에 대해 자세히 알아보세요" .

    b. 원하는 경우 WORM(한 번 쓰고 여러 번 읽기) 저장소를 활성화합니다.

       이 옵션은 특정 VM 유형에만 사용할 수 있습니다. 지원되는 VM 유형을 알아보려면 다음을 참조하세요."HA 쌍에 대한 라이선스별 지원 구성" .

       Cloud Volumes ONTAP 버전 9.7 이하에서 데이터 계층화가 활성화된 경우 WORM을 활성화할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로 되돌리거나 다운그레이드하는 것이 차단됩니다.

    "WORM 스토리지에 대해 자세히 알아보세요" .

    a. WORM 저장소를 활성화하는 경우 보존 기간을 선택하세요.

14. 저장소 및 **WORM**에 대한 보안 통신: Azure 저장소 계정에 HTTPS 연결을 사용할지 여부를 선택하고, 필요한 경우 WORM(한 번 쓰고 여러 번 읽기) 저장소를 활성화합니다.

HTTPS 연결은 Cloud Volumes ONTAP 9.7 HA 쌍에서 Azure 페이지 Blob 스토리지 계정으로 이루어집니다. 이 옵션을 활성화하면 쓰기 성능에 영향을 줄 수 있습니다. 시스템을 만든 후에는 설정을 변경할 수 없습니다.

"WORM 스토리지에 대해 자세히 알아보세요" .

데이터 계층화가 활성화된 경우 WORM을 활성화할 수 없습니다.

"WORM 스토리지에 대해 자세히 알아보세요" .

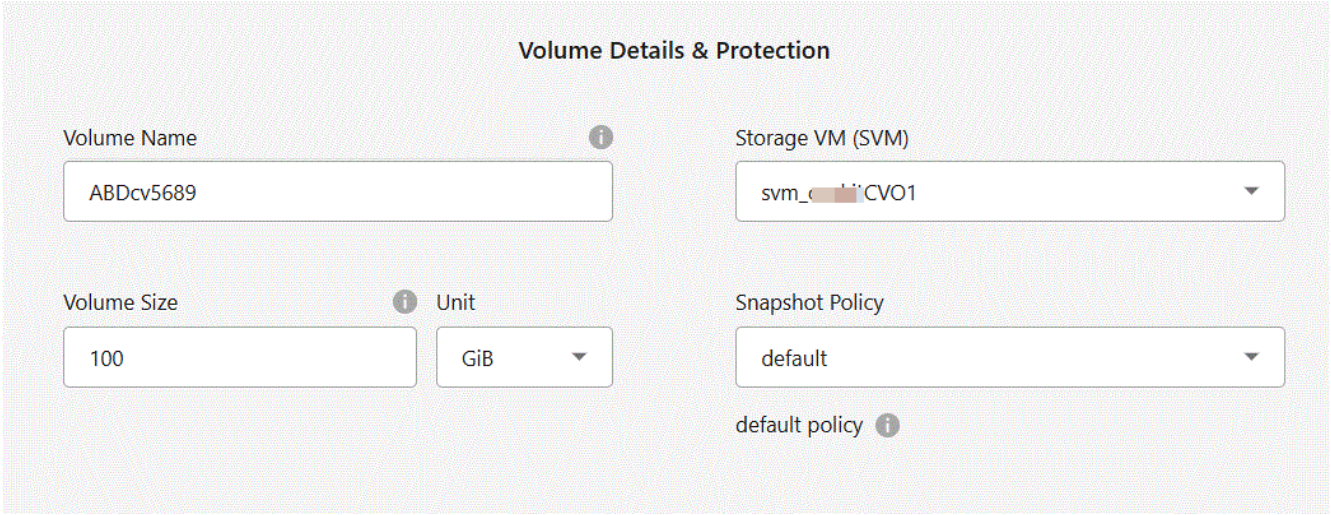
15. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

"지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요" .

이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝을 활성화하는지 여부에 따라 크게 달라집니다. 씬 프로비저닝을 활성화하면 현재 사용 가능한 물리적 저장소보다 큰 볼륨을 만들 수 있습니다.
액세스 제어(NFS에만 해당)	내보내기 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 콘솔은 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS에만 해당)	이러한 필드를 사용하면 사용자 및 그룹의 공유 액세스 수준(액세스 제어 목록 또는 ACL이라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자나 그룹, 또는 UNIX 사용자나 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사 정책은 NetApp 스냅샷 복사본이 자동으로 생성되는 빈도와 수를 지정합니다. NetApp 스냅샷 복사본은 성능에 영향을 미치지 않고 최소한의 저장 공간만 필요한 특정 시점의 파일 시스템 이미지입니다. 기본 정책을 선택하거나 아무것도 선택하지 않을 수 있습니다. 일시적인 데이터의 경우 '없음'을 선택할 수 있습니다. 예를 들어 Microsoft SQL Server의 경우 tempdb를 선택합니다.
고급 옵션(NFS에만 해당)	볼륨에 대한 NFS 버전을 선택합니다: NFSv3 또는 NFSv4.
이니시에이터 그룹 및 IQN(iSCSI에만 해당)	iSCSI 스토리지 대상은 LUN(논리 단위)이라고 하며 호스트에 표준 블록 장치로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름 테이블이며, 어떤 이니시에이터가 어떤 LUN에 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 컨버지드 네트워크 어댑터(CNA) 또는 전용 호스트 버스 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 정규화된 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성하면 콘솔이 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후, "IQN을 사용하여 호스트에서 LUN에 연결합니다." .

다음 이미지는 볼륨 생성 마법사의 첫 번째 페이지를 보여줍니다.



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

필드	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 가입할 도메인의 Active Directory LDAP 서버와 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
가입할 Active Directory 도메인	CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.
도메인에 가입할 수 있는 권한이 있는 자격 증명	AD 도메인 내의 지정된 조직 단위(OU)에 컴퓨터를 추가할 수 있는 권한이 있는 Windows 계정의 이름과 비밀번호입니다.
CIFS 서버 NetBIOS 이름	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. Cloud Volumes ONTAP 의 AD 서버로 Azure AD Domain Services를 구성하려면 이 필드에 **OU=AADDC Computers** 또는 *OU=AADDC Users*를 입력해야 합니다.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 설명서: Azure AD Domain Services 관리 도메인에서 OU(조직 단위) 만들기"^]
DNS 도메인	Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 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 참조하세요 "NetApp Console 자동화 문서" 자세한 내용은. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 만든 후에는 구성할 수 없습니다.

17. 사용 프로필, 디스크 유형 및 계층화 정책: 필요한 경우 스토리지 효율성 기능을 활성화할지 여부를 선택하고 볼륨 계층화 정책을 변경합니다.

    자세한 내용은 다음을 참조하세요."볼륨 사용 프로필을 선택하세요" ,"데이터 계층화 개요" , 그리고 "KB: CVO에서는 어떤 인라인 스토리지 효율성 기능이 지원되나요?"

18. 검토 및 승인: 선택 사항을 검토하고 확인합니다.

    a. 구성에 대한 세부 정보를 검토하세요.

b. *자세한 정보*를 클릭하여 콘솔에서 구매할 지원 및 Azure 리소스에 대한 세부 정보를 검토하세요.

c. 이해합니다... 확인란을 선택하세요.

d. *이동*을 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP 시스템을 배포합니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템 배포 중 문제가 발생하면 실패 메시지를 검토하세요. 시스템을 선택하고 *환경 다시 만들기*를 클릭할 수도 있습니다.

추가 도움말을 보려면 다음으로 이동하세요. "NetApp Cloud Volumes ONTAP 지원" .

당신이 완료한 후

- CIFS 공유를 프로비저닝한 경우 사용자 또는 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 ONTAP 시스템 관리자나 ONTAP CLI를 사용하세요.

  할당량을 사용하면 사용자, 그룹 또는 Qtree에서 사용하는 디스크 공간과 파일 수를 제한하거나 추적할 수 있습니다.

배포 프로세스가 완료된 후에는 Azure Portal에서 시스템 생성 Cloud Volumes ONTAP 구성, 특히 시스템 태그를 수정하지 마세요. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

관련 링크

*"Azure에서 Cloud Volumes ONTAP 구성 계획" *"Azure Marketplace에서 Azure에 Cloud Volumes ONTAP 배포"

Azure 플랫폼 이미지 확인

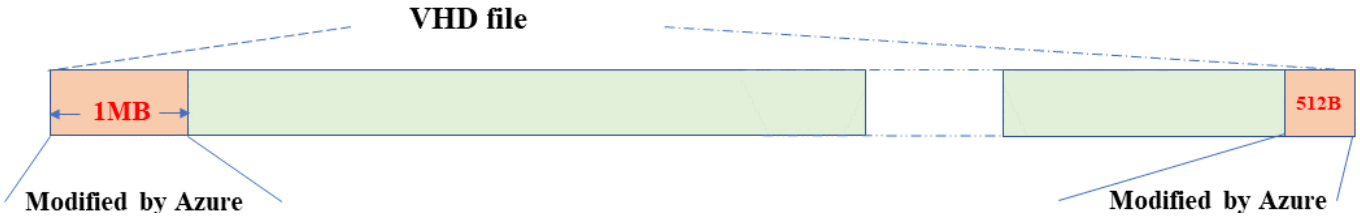
Cloud Volumes ONTAP 에 대한 Azure 마켓플레이스 이미지 검증

Azure 이미지 검증은 향상된 NetApp 보안 요구 사항을 준수합니다. 이미지 파일을 검증하는 것은 간단한 과정입니다. 그러나 Azure 이미지 서명 검증에는 Azure VHD 이미지 파일에 대한 특정 고려 사항이 필요합니다. Azure VHD 이미지 파일은 Azure Marketplace에서 변경되기 때문입니다.

Azure 이미지 검증은 Cloud Volumes ONTAP 9.15.0 이상에서 지원됩니다.

Azure에서 게시된 **VHD** 파일 변경

VHD 파일의 시작 부분인 1MB(1048576바이트)와 끝 부분인 512바이트는 Azure에 의해 수정됩니다. NetApp 나머지 VHD 파일에 서명합니다.



이 예에서 VHD 파일의 크기는 10GB입니다. NetApp 에서 서명한 부분은 녹색으로 표시되어 있습니다(10GB - 1MB - 512바이트).

관련 링크

- "페이지 폴트 블로그: OpenSSL을 사용하여 서명하고 확인하는 방법"
- "Azure Marketplace 이미지를 사용하여 Azure Stack Edge Pro GPU용 VM 이미지 만들기 | Microsoft Learn"
- "Azure CLI를 사용하여 관리 디스크를 저장소 계정으로 내보내기/복사 | Microsoft Learn"
- "Azure Cloud Shell 빠른 시작 - Bash | Microsoft Learn"
- "Azure CLI 설치 방법 | Microsoft Learn"
- "az 스토리지 BLOB 복사 | Microsoft Learn"
- "Azure CLI로 Sign in - 로그인 및 인증 | Microsoft Learn"

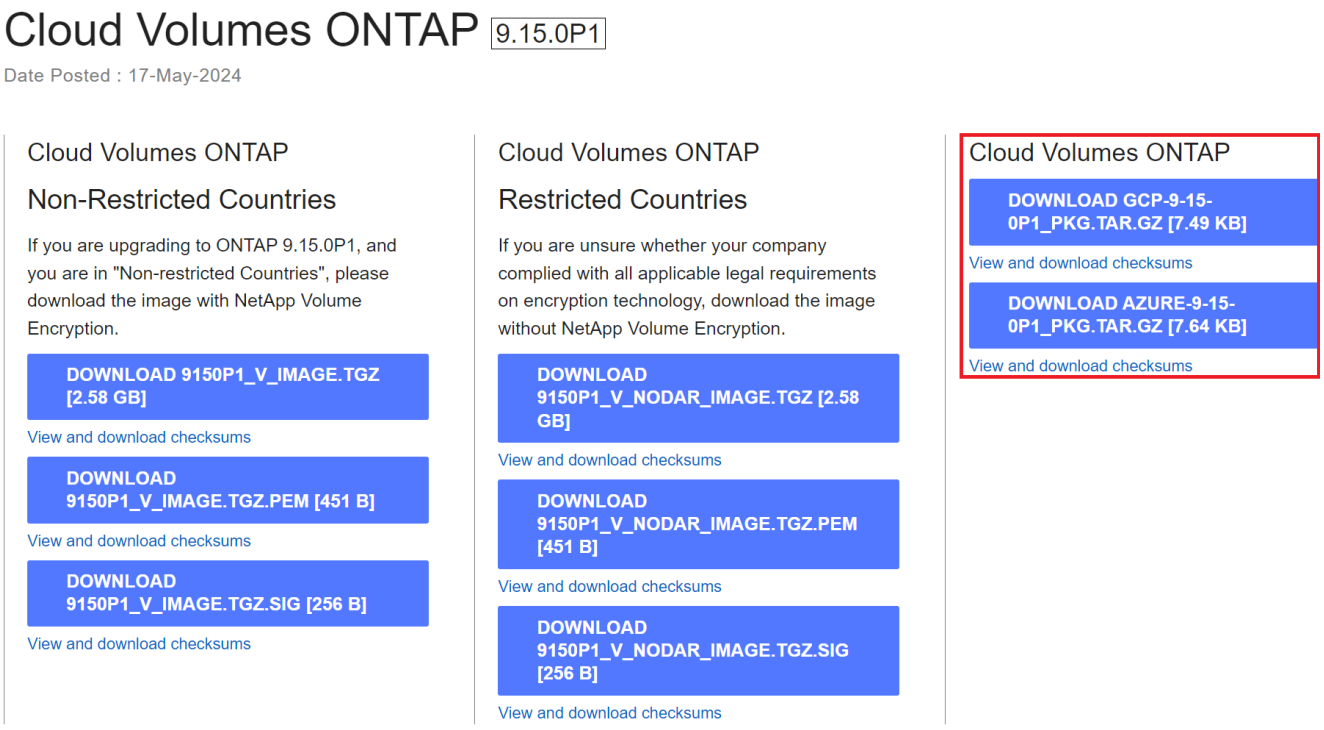
Cloud Volumes ONTAP 용 Azure 이미지 파일 다운로드

Azure 이미지 파일은 다음에서 다운로드할 수 있습니다. "NetApp 지원 사이트" .

tar.gz 파일에는 이미지 서명 검증에 필요한 파일이 포함되어 있습니다. *tar.gz* 파일과 함께 이미지에 대한 *checksum* 파일도 다운로드해야 합니다. 체크섬 파일에는 다음이 포함됩니다. `md5` 그리고 `sha256` *tar.gz* 파일의 체크섬.

단계

1. 로 가다 "NetApp 지원 사이트의 Cloud Volumes ONTAP 제품 페이지" 다운로드 섹션에서 필요한 소프트웨어 버전을 다운로드하세요.
2. Cloud Volumes ONTAP 다운로드 페이지에서 Azure 이미지에 대한 다운로드 가능한 파일을 클릭하고 *tar.gz* 파일을 다운로드합니다.



3. Linux에서 실행 `md5sum AZURE-<version>_PKG.TAR.GZ` .

   macOS에서는 다음을 실행합니다. `sha256sum AZURE-<version>_PKG.TAR.GZ` .

4. 다음을 확인하십시오. `md5sum` 그리고 `sha256sum` 값이 다운로드한 Azure 이미지의 값과 일치합니다.

5. Linux 및 macOS에서는 다음을 사용하여 *tar.gz* 파일을 추출합니다. `tar -xzf` 명령.

   추출된 *tar.gz* 파일에는 다이제스트(*.sig*) 파일, 공개 키 인증서(*.pem*) 파일, 체인 인증서(*.pem*) 파일이 포함되어 있습니다.

   tar.gz 파일을 추출한 후의 출력 예**:**

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

Azure Marketplace에서 Cloud Volumes ONTAP 용 VHD 이미지 내보내기

VHD 이미지가 Azure 클라우드에 게시되면 더 이상 NetApp 에서 관리되지 않습니다. 대신, 게시된 이미지는 Azure Marketplace에 배치됩니다. 이미지가 Azure 마켓플레이스에 스테이징되어 게시되면 Azure는 VHD의 시작 부분에서 1MB, 끝 부분에서 512바이트를 수정합니다. VHD 파일의 서명을 확인하려면 Azure 마켓플레이스에서 Azure가 수정한 VHD

이미지를 내보내야 합니다.

시작하기 전에

시스템에 Azure CLI가 설치되어 있는지, 아니면 Azure Portal을 통해 Azure Cloud Shell을 사용할 수 있는지 확인하세요. Azure CLI를 설치하는 방법에 대한 자세한 내용은 다음을 참조하세요. "Microsoft 설명서: Azure CLI 설치 방법" .

단계

1. *version_readme* 파일의 내용을 사용하여 시스템의 Cloud Volumes ONTAP 버전을 Azure Marketplace 이미지 버전에 매핑합니다. Cloud Volumes ONTAP 버전은 다음과 같이 표현됩니다. `buildname` Azure Marketplace 이미지 버전은 다음과 같이 표현됩니다. `version` 버전 매핑에서.

   다음 예에서는 Cloud Volumes ONTAP 버전 `9.15.0P1` Azure Marketplace 이미지 버전에 매핑됨 `9150.01000024.05090105` . 이 Azure 마켓플레이스 이미지 버전은 나중에 이미지 URN을 설정하는 데 사용됩니다.

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. VM을 만들려는 지역을 식별합니다. 지역 이름은 값으로 사용됩니다. `locName` 마켓플레이스 이미지의 URN을 설정할 때 변수입니다. 사용 가능한 지역을 나열하려면 다음 명령을 실행하세요.

   ```
   az account list-locations -o table
   ```

   이 표에서는 지역 이름이 다음과 같이 나타납니다. `Name` 필드.

   ```
   $ az account list-locations -o table
   DisplayName               Name                 RegionalDisplayName
   ------------------------  -------------------
   ------------------------------------
   East US                   eastus               (US) East US
   East US 2                 eastus2              (US) East US 2
   South Central US          southcentralus       (US) South Central US
   ...
   ```

3. 아래 표에서 해당 Cloud Volumes ONTAP 버전과 VM 배포 유형에 대한 SKU 이름을 검토하세요. SKU 이름은 값으로 사용됩니다. `skuName` 마켓플레이스 이미지의 URN을 설정할 때 변수입니다.

   예를 들어, Cloud Volumes ONTAP 9.15.0을 사용한 모든 단일 노드 배포는 다음을 사용해야 합니다. `ontap_cloud_byol` SKU 이름으로.

* Cloud Volumes ONTAP 버전*	**VM** 배포를 통해	**SKU** 이름
9.17.1 이상	Azure 마켓플레이스	ontap_cloud_direct_gen2
9.17.1 이상	NetApp Console	ontap_cloud_gen2
9.16.1	Azure 마켓플레이스	온탭_클라우드_다이렉트
9.16.1	콘솔	온탭_클라우드
9.15.1	콘솔	온탭_클라우드
9.15.0	콘솔, 단일 노드 배포	온탭_클라우드_바이올
9.15.0	콘솔, 고가용성(HA) 배포	온탑_클라우드_비올_하

4. ONTAP 버전과 Azure 마켓플레이스 이미지를 매핑한 후 Azure Cloud Shell 또는 Azure CLI를 사용하여 Azure 마켓플레이스에서 VHD 파일을 내보냅니다.

Linux에서 **Azure Cloud Shell**을 사용하여 **VHD** 파일 내보내기

Azure Cloud Shell에서 마켓플레이스 이미지를 VHD 파일(예: *9150.01000024.05090105.vhd*)로 내보내고 로컬 Linux 시스템에 다운로드합니다. Azure Marketplace에서 VHD 이미지를 가져오려면 다음 단계를 수행하세요.

단계

1. 마켓플레이스 이미지의 URN 및 기타 매개변수를 설정합니다. URN 형식은 다음과 같습니다. `<publisher>:<offer>:<sku>:<version>` . 선택적으로 NetApp 마켓플레이스 이미지를 나열하여 올바른 이미지 버전을 확인할 수 있습니다.

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. 일치하는 이미지 버전으로 마켓플레이스 이미지에서 새 관리 디스크를 만듭니다.

```
PS /home/user1> $diskName = “9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = “fnf1”
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. 관리 디스크에서 Azure Storage로 VHD 파일을 내보냅니다. 적절한 액세스 수준으로 컨테이너를 만듭니다. 이 예에서 우리는 다음과 같은 이름의 컨테이너를 사용했습니다. `vm-images` ~와 함께 `Container` 접근 수준. Azure Portal에서 저장소 계정 액세스 키를 가져옵니다. 저장소 계정 **> *examplesaname* >** 액세스 키 **> *key1* > *key* >** 표시 **> <복사>**

```
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. 생성된 이미지를 Linux 시스템에 다운로드합니다. 사용하다 `wget` VHD 파일을 다운로드하는 명령:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

URL은 표준 형식을 따릅니다. 자동화를 위해 아래와 같이 URL 문자열을 파생시킬 수 있습니다. 또는 Azure CLI를 사용할 수 있습니다. `az` URL을 가져오는 명령입니다. URL 예시:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. 관리되는 디스크 정리

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Linux에서 Azure CLI를 사용하여 VHD 파일 내보내기

로컬 Linux 시스템에서 Azure CLI를 사용하여 마켓플레이스 이미지를 VHD 파일로 내보냅니다.

단계

1. Azure CLI에 로그인하고 마켓플레이스 이미지를 나열합니다.

```
% az login --use-device-code
```

2. 로그인하려면 웹 브라우저를 사용하여 페이지를 엽니다. https://microsoft.com/devicelogin 인증코드를 입력하세요.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. 마켓플레이스 이미지에서 일치하는 이미지 버전으로 새로운 관리 디스크를 만듭니다.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
```

프로세스를 자동화하려면 표준 출력에서 SAS를 추출해야 합니다. 자세한 내용은 해당 문서를 참조하세요.

4. 관리 디스크에서 VHD 파일을 내보냅니다.

   a. 적절한 액세스 수준으로 컨테이너를 만듭니다. 이 예에서는 컨테이너라는 이름이 있습니다. `vm-images` ~와 함께 `Container` 접근 수준이 사용됩니다.

   b. Azure Portal에서 저장소 계정 액세스 키를 가져옵니다. 저장소 계정 **> *examplesaname* >** 액세스 키 **> *key1* > *key* >** 표시 **> <복사>**

      또한 다음을 사용할 수도 있습니다. `az` 이 단계에 대한 명령입니다.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Blob 복사본의 상태를 확인하세요.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. 생성된 이미지를 Linux 서버로 다운로드합니다.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

URL은 표준 형식을 따릅니다. 자동화를 위해 아래와 같이 URL 문자열을 파생시킬 수 있습니다. 또는 Azure CLI를 사용할 수 있습니다. `az` URL을 가져오는 명령입니다. URL 예시:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. 관리되는 디스크 정리

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

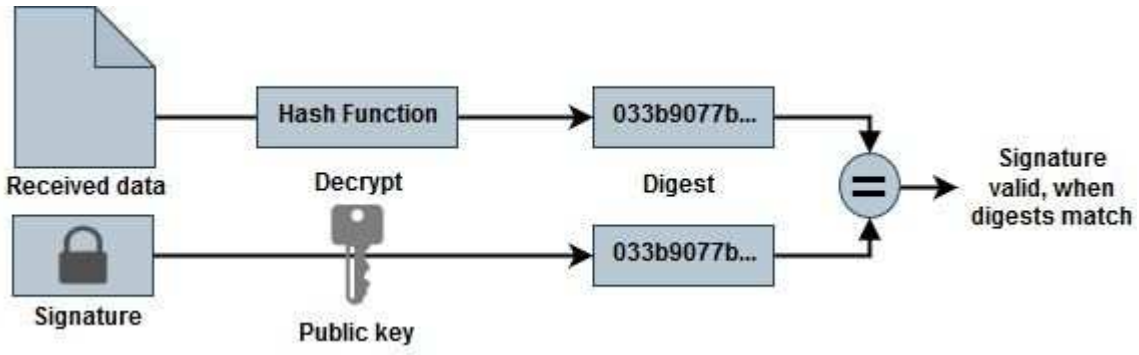
파일 서명 확인

Cloud Volumes ONTAP 에 대한 **Azure** 마켓플레이스 이미지 서명 확인

Azure 이미지 검증 프로세스는 VHD 파일의 시작 부분에서 1MB, 끝 부분에서 512바이트를 제거한 다음 해시 함수를 적용하여 다이제스트 파일을 생성합니다. 서명 절차를 일치시키기 위해 해싱에는 _sha256_이 사용됩니다.

파일 서명 검증 워크플로 요약

다음은 파일 서명 검증 워크플로 프로세스에 대한 개요입니다.



- Azure 이미지를 다운로드합니다. "NetApp 지원 사이트" 그리고 다이제스트(.sig) 파일, 공개 키 인증서(.pem) 파일, 체인 인증서(.pem) 파일을 추출합니다. . "Azure 이미지 다이제스트 파일 다운로드" 자세한 내용은.
- 신뢰 사슬의 검증.
- 공개 키 인증서(.pem)에서 공개 키(.pub)를 추출합니다.
- 추출된 공개 키를 사용하여 다이제스트 파일을 해독합니다.
- 이미지 파일에서 시작 부분 1MB와 끝 부분 512바이트를 제거한 후 생성된 임시 파일의 새로 생성된 다이제스트와 결과를 비교합니다. 이 단계는 OpenSSL 명령줄 도구를 사용하여 수행됩니다. OpenSSL CLI 도구는 파일 일치에 성공하거나 실패할 경우 적절한 메시지를 표시합니다.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

Linux에서 **Cloud Volumes ONTAP** 에 대한 **Azure** 마켓플레이스 이미지 서명 확인

Linux에서 내보낸 VHD 파일 서명을 검증하는 작업에는 신뢰 체인 검증, 파일 편집, 서명 검증이 포함됩니다.

단계

1. Azure 이미지 파일을 다운로드하세요. "NetApp 지원 사이트" 그리고 다이제스트(.sig) 파일, 공개 키 인증서(.pem) 파일, 체인 인증서(.pem) 파일을 추출합니다.

   참조하다 "Azure 이미지 다이제스트 파일 다운로드" 자세한 내용은.

2. 신뢰 사슬을 확인하세요.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. VHD 파일의 시작 부분에서 1MB(1,048,576바이트)를 제거하고 끝 부분에서 512바이트를 제거합니다. 사용시 `tail` , 그 `-c +K` 이 옵션은 파일의 K번째 바이트에서 바이트를 생성합니다. 따라서 1048577을 전달합니다.

tail -c .

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. OpenSSL을 사용하여 인증서에서 공개 키를 추출하고, 스트립된 파일(sign.tmp)을 서명 파일과 공개 키로 검증합니다.

   명령 프롬프트는 검증 결과에 따라 성공 또는 실패를 나타내는 메시지를 표시합니다.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 작업 공간을 정리하세요.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

macOS에서 **Cloud Volumes ONTAP** 대한 **Azure** 마켓플레이스 이미지 서명 확인

Linux에서 내보낸 VHD 파일 서명을 검증하는 작업에는 신뢰 체인 검증, 파일 편집, 서명 검증이 포함됩니다.

단계

1. Azure 이미지 파일을 다운로드하세요. "NetApp 지원 사이트" 그리고 다이제스트(.sig) 파일, 공개 키 인증서(.pem) 파일, 체인 인증서(.pem) 파일을 추출합니다.

   참조하다 "Azure 이미지 다이제스트 파일 다운로드" 자세한 내용은.

2. 신뢰 사슬을 확인하세요.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. VHD 파일의 시작 부분에서 1MB(1,048,576바이트)를 제거하고 끝 부분에서 512바이트를 제거합니다. 사용시 `tail` , 그 `-c +K` 이 옵션은 파일의 K번째 바이트에서 바이트를 생성합니다. 따라서 1048577을 전달합니다. `tail -c` . macOS에서는 tail 명령을 완료하는 데 약 10분이 걸릴 수 있습니다.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. OpenSSL을 사용하여 인증서에서 공개 키를 추출하고, 스트립된 파일(sign.tmp)을 서명 파일과 공개 키로 검증합니다. 명령 프롬프트는 검증 결과에 따라 성공 또는 실패를 나타내는 메시지를 표시합니다.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 작업 공간을 정리하세요.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```