Microsoft Azure에서 시작하십시오

Cloud Volumes ONTAP

NetApp
June 27, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/test/task-getting-started-azure.html on June 27, 2024. Always check docs.netapp.com for the latest.

목차

Microsoft Azure에서 시작하십시오

Azure에서 Cloud Volumes ONTAP를 빠르게 시작합니다

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"

인터넷에 액세스할 수 없는 서브넷에 Cloud Volumes ONTAP를 배포하려는 경우 수동으로 커넥터를 설치하고 해당 커넥터에서 실행 중인 BlueXP 사용자 인터페이스에 액세스해야 합니다. "인터넷에 액세스하지 않고 커넥터에 수동으로 설치하는 방법에 대해 알아봅니다"

2 구성을 계획합니다

BlueXP는 워크로드 요구 사항에 맞는 사전 구성된 패키지를 제공하거나 사용자가 직접 구성할 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. NetApp AutoSupport용 VPC 타겟으로부터 아웃바운드 인터넷 액세스 지원

   인터넷에 액세스할 수 없는 위치에 Cloud Volumes ONTAP를 배포하는 경우에는 이 단계가 필요하지 않습니다.

"네트워킹 요구 사항에 대해 자세히 알아보십시오".

4 **BlueXP**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

- "BlueXP에서 커넥터 만들기"
- "Azure Marketplace에서 커넥터 만들기"
- "Linux 호스트에 Connector 소프트웨어 설치"
- "권한을 가진 BlueXP의 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.

Cloud Volumes ONTAP 라이센스를 선택합니다

Cloud Volumes ONTAP에는 몇 가지 라이센스 옵션이 있습니다. 각 옵션을 사용하여 요구사항에 맞는 소비 모델을 선택할 수 있습니다.

- "Cloud Volumes ONTAP의 라이센스 옵션에 대해 자세히 알아보십시오"
- "라이센스 설정 방법에 대해 알아보십시오"

지원되는 지역을 선택하십시오

Cloud Volumes ONTAP는 대부분의 Microsoft Azure 지역에서 지원됩니다. "지원되는 영역의 전체 목록을 봅니다".

지원되는 VM 유형을 선택합니다

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

"Azure에서 Cloud Volumes ONTAP에 대해 지원되는 구성입니다"

스토리지 제한사항을 파악합니다

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.

"Azure의 Cloud Volumes ONTAP에 대한 스토리지 제한"

Azure에서 시스템 크기 조정

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"

단일 노드 시스템이 있는 **Azure** 디스크 유형입니다

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

단일 노드 시스템에서는 세 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?".

HA 쌍을 지원하는 **Azure** 디스크 유형

HA 시스템은 프리미엄 SSD 공유 관리 디스크를 사용합니다. 이 두 디스크는 모두 I/O 집약적인 워크로드를 더 높은 비용으로 처리합니다. 9.12.1 릴리즈 이전에 생성된 HA 배포에서는 프리미엄 페이지 Blob을 사용합니다.

Azure 디스크 크기입니다

Cloud Volumes ONTAP 인스턴스를 시작할 때 Aggregate의 기본 디스크 크기를 선택해야 합니다. BlueXP에서는 이 디스크 크기를 초기 집계와 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, 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"

기본 시스템 디스크를 봅니다

BlueXP는 사용자 데이터를 위한 스토리지 외에도 Cloud Volumes ONTAP 시스템 데이터(부팅 데이터, 루트 데이터, 핵심 데이터 및 NVRAM)를 위한 클라우드 스토리지를 구입합니다. 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".

네트워킹 정보를 수집합니다

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)	

Azure 정보	귀사의 가치
서브넷	
네트워크 보안 그룹(자체 사용 시)	

쓰기 속도를 선택합니다

BlueXP에서는 Cloud Volumes ONTAP에 대한 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 프로필을 선택합니다

ONTAP에는 필요한 총 스토리지 양을 줄일 수 있는 몇 가지 스토리지 효율성 기능이 포함되어 있습니다. BlueXP에서 볼륨을 생성할 때 이러한 기능을 활성화하는 프로필이나 해당 기능을 비활성화하는 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.

Azure의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항

Cloud Volumes ONTAP 시스템이 올바르게 작동할 수 있도록 Azure 네트워킹을 설정합니다.

Cloud Volumes ONTAP에 대한 요구사항

Azure에서 다음 네트워킹 요구사항을 충족해야 합니다.

아웃바운드 인터넷 액세스

Cloud Volumes ONTAP 노드를 사용하려면 NetApp AutoSupport에 대한 아웃바운드 인터넷 액세스가 필요합니다. 사전 예방적으로 시스템의 상태를 모니터링하고 메시지를 NetApp 기술 지원으로 보냅니다.

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
- https://support.netapp.com/asupprod/post/1.0/postAsup

AutoSupport 메시지를 보내는 데 아웃바운드 인터넷 연결을 사용할 수 없는 경우 BlueXP는 자동으로 Cloud Volumes ONTAP 시스템에서 커넥터를 프록시 서버로 사용하도록 구성합니다. 유일한 요구 사항은 커넥터의 보안 그룹이 포트 3128을 통한 _IN인바운드_연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

Cloud Volumes ONTAP에 대해 엄격한 아웃바운드 규칙을 정의한 경우 Cloud Volumes ONTAP 보안 그룹이 포트 3128을 통한 _outbound_connection을 허용하는지 확인해야 합니다.

아웃바운드 인터넷 액세스가 가능한지 확인한 후 AutoSupport를 테스트하여 메시지를 보낼 수 있는지 확인할 수 있습니다. 자세한 지침은 을 참조하십시오 "ONTAP 문서: AutoSupport 설정".

BlueXP에서 AutoSupport 메시지를 보낼 수 없다고 알리는 경우 "AutoSupport 구성 문제를 해결합니다".

IP 주소

BlueXP는 Azure의 Cloud Volumes ONTAP에 필요한 수의 전용 IP 주소를 자동으로 할당합니다. 네트워킹에 사용 가능한 개인 IP 주소가 충분한지 확인해야 합니다.

BlueXP에서 Cloud Volumes ONTAP에 할당하는 LIF 수는 단일 노드 시스템을 배포할지 HA 쌍을 구축하는지에 따라 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다. SnapCenter와 같은 관리 툴을 사용하려면 SVM 관리 LIF가 필요합니다.

iSCSI LIF는 iSCSI 프로토콜을 통해 클라이언트에 액세스할 수 있도록 지원하며 시스템에서 다른 중요한 네트워킹 워크플로우에 사용됩니다. 이러한 LIF는 필수 항목이므로 삭제할 수 없습니다.

단일 노드 시스템의 **IP** 주소입니다

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

- 클러스터 관리 IP
- 노드 관리 IP
- SnapMirror에 대한 인터클러스터 IP
- NFS/CIFS IP입니다
- iSCSI IP입니다

iSCSI IP는 iSCSI 프로토콜을 통한 클라이언트 액세스를 제공합니다. 또한 시스템에서 다른 중요한 네트워킹 워크플로우에 사용됩니다. 이 LIF는 필수 항목이므로 삭제할 수 없습니다.

- SVM 관리(선택 사항 - 기본적으로 구성되지 않음)

HA 쌍의 **IP** 주소

BlueXP는 구축하는 동안 노드당 4개의 NIC에 IP 주소를 할당합니다.

BlueXP는 HA 쌍에서 SVM 관리 LIF를 생성하지만 Azure의 단일 노드 시스템에서는 생성한 것이 아닙니다.

- NIC0 *
- 노드 관리 IP
- 인터클러스터 IP

- iSCSI IP입니다

> iSCSI IP는 iSCSI 프로토콜을 통한 클라이언트 액세스를 제공합니다. 또한 시스템에서 다른 중요한 네트워킹 워크플로우에 사용됩니다. 이 LIF는 필수 항목이므로 삭제할 수 없습니다.

- NIC1 *
- 클러스터 네트워크 IP
- NIC2 *
- 클러스터 인터커넥트 IP(HA IC)
- NIC3 *
- Pageblob NIC IP(디스크 액세스)

> NIC3는 페이지 BLOB 스토리지를 사용하는 HA 구축에만 적용됩니다.

위의 IP 주소는 페일오버 이벤트에서 마이그레이션되지 않습니다.

또한 페일오버 이벤트에 마이그레이션하도록 4개의 프런트엔드 IP(FIPS)가 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 BlueXP는 Cloud Volumes ONTAP 및 Azure 페이지 blob 저장소 계정 간의 연결에 Azure 프라이빗 링크를 활성화합니다.

대부분의 경우 BlueXP는 Azure Private Link를 관리합니다. 그러나 Azure Private DNS를 사용하는 경우에는 구성 파일을 편집해야 합니다. Azure의 커넥터 위치에 대한 요구 사항도 알고 있어야 합니다.

비즈니스 요구 사항에 따라 필요한 경우 비공개 링크 연결을 비활성화할 수도 있습니다. 링크를 사용하지 않도록 설정하면 BlueXP는 서비스 끝점을 사용하도록 Cloud Volumes ONTAP를 구성합니다.

"Cloud Volumes ONTAP에서 Azure 프라이빗 링크 또는 서비스 엔드포인트를 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 배포하려고 하면 BlueXP에서 연결 문제가 발생합니다.

보안 그룹 규칙

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

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

커넥터에 대한 정보를 찾고 계십니까? "Connector에 대한 보안 그룹 규칙을 봅니다"

단일 노드 시스템에 대한 인바운드 규칙입니다

작업 환경을 만들고 미리 정의된 보안 그룹을 선택할 때 다음 중 한 가지 내에서 트래픽을 허용하도록 선택할 수 있습니다.

- * 선택한 VNET만 해당 *: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템에 대한 VNET의 서브넷 범위와 커넥터가 상주하는 VNET의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다.
- * All VNets *: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.

우선 순위 및 이름	포트 및 프로토콜	소스 및 대상	설명
1000입니다 inbound_ssh입니다	22 TCP	모두 해당	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다
1001 inbound_http(인바운드_http	80 TCP	모두 해당	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTP 액세스
1002 인바운드_111_TCP	111 TCP	모두 해당	NFS에 대한 원격 프로시저 호출
1003 인바운드_111_UDP	111 UDP입니다	모두 해당	NFS에 대한 원격 프로시저 호출

우선 순위 및 이름	포트 및 프로토콜	소스 및 대상	설명
1004 인바운드_139	139 TCP	모두 해당	CIFS에 대한 NetBIOS 서비스 세션입니다
1005 인바운드_161-162_TCP	161-162 TCP	모두 해당	단순한 네트워크 관리 프로토콜
1006 인바운드_161-162_UDP	161-162 UDP입니다	모두 해당	단순한 네트워크 관리 프로토콜
1007 인바운드_443	443 TCP	모두 해당	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 커넥터 및 HTTPS 액세스와의 연결
1008년 IN인바운드_445	445 TCP	모두 해당	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
1009입니다 인바운드_635_TCP	635 TCP	모두 해당	NFS 마운트
1010 인바운드_635_UDP	635 UDP입니다	모두 해당	NFS 마운트
1011 인바운드_749	749 TCP	모두 해당	Kerberos
1012입니다 인바운드_2049_TCP	2049년 TCP	모두 해당	NFS 서버 데몬
1013 인바운드_2049_UDP	2049년 UDP입니다	모두 해당	NFS 서버 데몬
1014 인바운드_3260	3260입니다 TCP	모두 해당	iSCSI 데이터 LIF를 통한 iSCSI 액세스
1015 인바운드_4045-4046_TCP	4045-4046 을 참조하십시오 TCP	모두 해당	NFS 잠금 데몬 및 네트워크 상태 모니터
1016 인바운드_4045-4046_UDP	4045-4046 을 참조하십시오 UDP입니다	모두 해당	NFS 잠금 데몬 및 네트워크 상태 모니터
1017 인바운드 _ 10000	10000 TCP	모두 해당	NDMP를 사용한 백업
1018세 IN인바운드_11104-11105	11104-11105 를 참조하십시오 TCP	모두 해당	SnapMirror 데이터 전송
3000입니다 inbound_deny_all_tcp입니다	모든 포트 TCP	모두 해당	다른 모든 TCP 인바운드 트래픽을 차단합니다
3001입니다 inbound_deny_all_udp입니다	모든 포트 UDP입니다	모두 해당	다른 모든 UDP 인바운드 트래픽을 차단합니다

우선 순위 및 이름	포트 및 프로토콜	소스 및 대상	설명
65000입니다 AllowVnetInBound 를 참조하십시오	모든 포트 모든 프로토콜	VirtualNetwork - VirtualNetwork	VNET 내에서 들어오는 인바운드 트래픽입니다
65001 AllowAzureLoad BalancerInBound 를 참조하십시오	모든 포트 모든 프로토콜	어느 것이든 AzureLoadBalancer를 사용합니다	Azure 표준 로드 밸런서의 데이터 트래픽
6,5005 DenyAllInBound를 참조하십시오	모든 포트 모든 프로토콜	모두 해당	다른 모든 인바운드 트래픽을 차단합니다

HA 시스템에 대한 인바운드 규칙

작업 환경을 만들고 미리 정의된 보안 그룹을 선택할 때 다음 중 한 가지 내에서 트래픽을 허용하도록 선택할 수 있습니다.

- * 선택한 VNET만 해당 *: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템에 대한 VNET의 서브넷 범위와 커넥터가 상주하는 VNET의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다.
- * All VNets *: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.

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 인바운드_443	443 모든 프로토콜	모두 해당	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 커넥터 및 HTTPS 액세스와의 연결
101 인바운드_111_TCP	111 모든 프로토콜	모두 해당	NFS에 대한 원격 프로시저 호출
102 인바운드_2049_TCP	2049년 모든 프로토콜	모두 해당	NFS 서버 데몬
111 inbound_ssh입니다	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
65000입니다 AllowVnetInBound 를 참조하십시오	모든 포트 모든 프로토콜	VirtualNetwork - VirtualNetwork	VNET 내에서 들어오는 인바운드 트래픽입니다

우선 순위 및 이름	포트 및 프로토콜	소스 및 대상	설명
65001 AllowAzureLoad BalancerInBound 를 참조하십시오	모든 포트 모든 프로토콜	어느 것이든 AzureLoadBalancer를 사용합니다	Azure 표준 로드 밸런서의 데이터 트래픽
6,5005 DenyAllInBound를 참조하십시오	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					

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)
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)
	TCP	3128	노드 관리 LIF	커넥터	아웃바운드 인터넷 연결을 사용할 수 없는 경우 커넥터의 프록시 서버를 통해 AutoSupport 메시지 보내기
구성 백업	HTTP	80	노드 관리 LIF	http://<connector-IP-address>/occm/offboxconfig입니다	Connector로 구성 백업을 보냅니다. "구성 백업 파일에 대해 자세히 알아보십시오".
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	11104를 참조하십시오	TCP	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror에 대한 인터클러스터 통신 세션의 관리
	11105를 참조하십시오	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

아직 Connector를 만들지 않은 경우 Connector에 대한 네트워킹 요구 사항도 검토해야 합니다.

- "커넥터에 대한 네트워킹 요구 사항을 봅니다"
- "Azure의 보안 그룹 규칙"

Azure에서 고객이 관리하는 키를 사용하도록 Cloud Volumes ONTAP를 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. BlueXP에서 API를 사용하여 키를 사용하는 Cloud Volumes ONTAP 작업 환경을 만듭니다

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.

Azure HA 다중 가용성 영역

- Cloud Volumes ONTAP의 모든 Azure 저장소 계정은 고객이 관리하는 키를 사용하여 암호화됩니다.[1]
- 루트, 부팅, NVRAM, 코어 및 데이터 디스크의 경우 BlueXP는 디스크 암호화 세트를 사용하여 관리되는 디스크로 암호화 키를 관리할 수 있습니다.
- 새 데이터 디스크도 동일한 디스크 암호화 세트를 사용합니다.

Azure HA 단일 가용성 영역

- Cloud Volumes ONTAP의 모든 Azure 저장소 계정은 고객이 관리하는 키를 사용하여 암호화됩니다.[1]
- 디스크 또는 애그리게이트를 추가하는 경우와 같이 새로운 스토리지 계정에서도 동일한 키를 사용합니다.[1]
- ONTAP 9.10.1P3에서 NVRAM 및 코어 디스크의 경우 BlueXP는 을 사용합니다 "디스크 암호화가 설정되었습니다"관리 디스크를 사용하여 암호화 키를 관리할 수 있습니다. 하위 버전은 고객 관리 키 대신 Microsoft 관리 키를 사용합니다.

단일 노드

- Cloud Volumes ONTAP의 모든 Azure 저장소 계정은 고객이 관리하는 키를 사용하여 암호화됩니다. [1]
- 루트, 부팅 및 데이터 디스크의 경우 BlueXP는 을 사용합니다 "디스크 암호화가 설정되었습니다"관리 디스크를 사용하여 암호화 키를 관리할 수 있습니다.
- 새 데이터 디스크도 동일한 디스크 암호화 세트를 사용합니다.
- ONTAP 9.9.1P7에서 NVRAM 및 코어 디스크의 경우 BlueXP는 디스크 암호화 세트를 사용하여 관리되는 디스크로 암호화 키를 관리할 수 있습니다. 하위 버전은 고객 관리 키 대신 Microsoft 관리 키를 사용합니다.

각주

1. 생성 중에 스토리지 계정을 암호화하려면 CVO 생성 요청에서 리소스 ID를 생성하고 제공해야 합니다. 이는 모든 유형의 배포에 적용됩니다. 제공하지 않으면 저장소 계정은 여전히 암호화되지만 BlueXP는 먼저 Microsoft 관리 키 암호화를 사용하여 저장소 계정을 만든 다음 고객이 관리하는 키를 사용하도록 저장소 계정을 업데이트합니다.

사용자가 할당한 관리 ID를 만듭니다

사용자가 할당한 관리 ID라는 리소스를 만들 수 있습니다. 이렇게 하면 Cloud Volumes ONTAP 작업 환경을 생성할 때 스토리지 계정을 암호화할 수 있습니다. 키 볼트를 작성하고 키를 생성하기 전에 이 리소스를 생성하는 것이 좋습니다.

리소스의 ID는 다음과 같습니다. `userassignedidentity`.

단계

1. Azure에서 Azure 서비스로 이동하여 * Managed Identities * 를 선택합니다.
2. Create * 를 클릭합니다.
3. 다음 세부 정보를 제공합니다.
   - * 구독 *: 구독을 선택합니다. Connector 가입과 동일한 구독을 선택하는 것이 좋습니다.
   - * 리소스 그룹 *: 기존 리소스 그룹을 사용하거나 새 리소스 그룹을 생성합니다.
   - * Region * (영역 *): 선택적으로 Connector (커넥터)와 동일한 영역을 선택합니다.
   - * 이름 *: 리소스 이름을 입력합니다.
4. 필요에 따라 태그를 추가합니다.
5. Create * 를 클릭합니다.

키 볼트를 작성하고 키를 생성합니다

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

있다면 사용자가 할당한 관리 ID를 만들었습니다키 볼트를 작성하는 동안 키 볼트에 대한 액세스 정책도 작성해야 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 시스템 또는 여러 존의 HA 쌍)
- 사용자 지정 관리 ID를 만든 경우 다음 옵션을 활성화해야 합니다.
  - * 볼트 액세스 정책 *

2. 볼트 액세스 정책을 선택한 경우, 작성 을 클릭하여 키 볼트에 대한 액세스 정책을 작성합니다. 그렇지 않은 경우 3단계로 건너뜁니다.
   a. 다음 권한을 선택합니다.
      - 가져오기
      - 목록
      - 암호를 해독합니다
      - 암호화
      - 줄 바꿈 해제 키
      - 랩 키
      - 확인합니다
      - 서명
   b. 사용자가 할당한 관리 ID(리소스)를 보안 주체에 선택합니다.
   c. 액세스 정책을 검토하고 생성합니다.
3. "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 BlueXP API를 사용하여 지원됩니다.

필수 권한

단일 노드 Cloud Volumes ONTAP 시스템에서 고객 관리 키를 사용하려면 BlueXP 커넥터에 다음과 같은 권한이 있는지 확인하십시오.

```
"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 사용 권한 목록을 봅니다"

단계

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

   HA 쌍: `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 BlueXP API 호출을 사용하여 볼트 내의 키 목록을 가져옵니다.

   HA 쌍: `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 BlueXP API 호출을 사용하여 Cloud Volumes ONTAP 시스템을 생성합니다.

   a. HA 쌍:

      `POST /azure/ha/working-environments`

      요청 본문에는 다음 필드가 포함되어야 합니다.

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

      을 포함합니다 `"userAssignedIdentity": " userAssignedIdentityId"` 스토리지 계정 암호화에 사용할 이 리소스를 생성한 경우 필드입니다.

"이 API 호출에 대해 자세히 알아보십시오".

b. 단일 노드 시스템의 경우:

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

요청 본문에는 다음 필드가 포함되어야 합니다.

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

을 포함합니다 `"userAssignedIdentity": " userAssignedIdentityId"` 스토리지 계정 암호화에 사용할 이 리소스를 생성한 경우 필드입니다.

"이 API 호출에 대해 자세히 알아보십시오".

결과

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

Azure에서 Cloud Volumes ONTAP에 대한 라이센스를 설정합니다

Cloud Volumes ONTAP에서 사용할 라이센스 옵션을 결정한 후에는 몇 가지 단계를 거쳐 새 작업 환경을 만들 때 해당 라이센스 옵션을 선택해야 합니다.

프리모늄

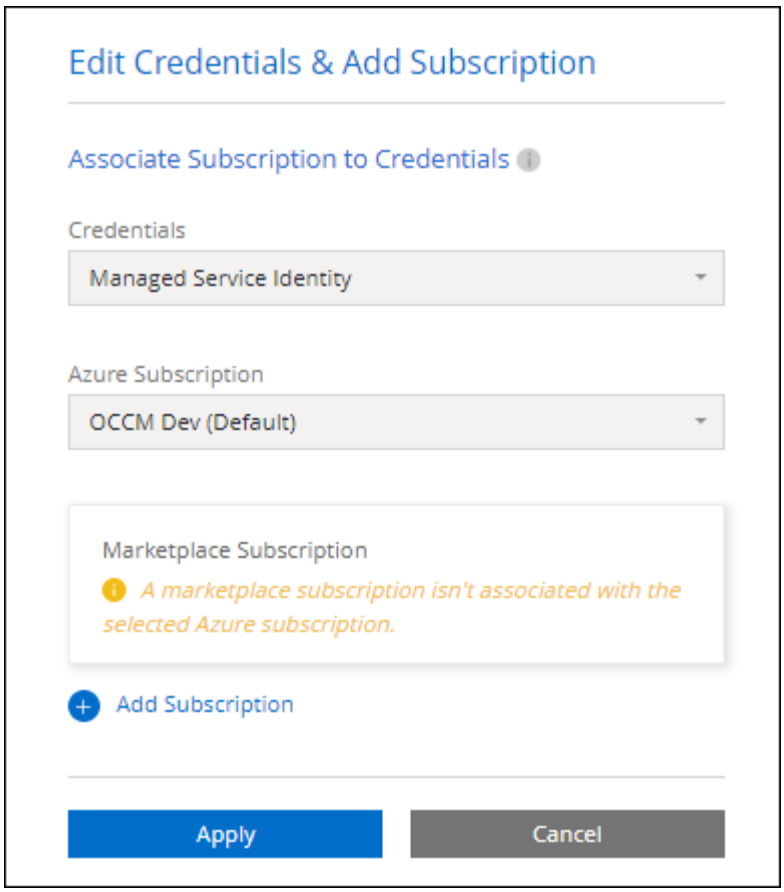
최대 500GiB의 용량을 제공하는 Cloud Volumes ONTAP를 무료로 사용할 수 있는 Freemium 오퍼링을 선택하십시오. "Freemium 제품에 대해 자세히 알아보십시오".

단계

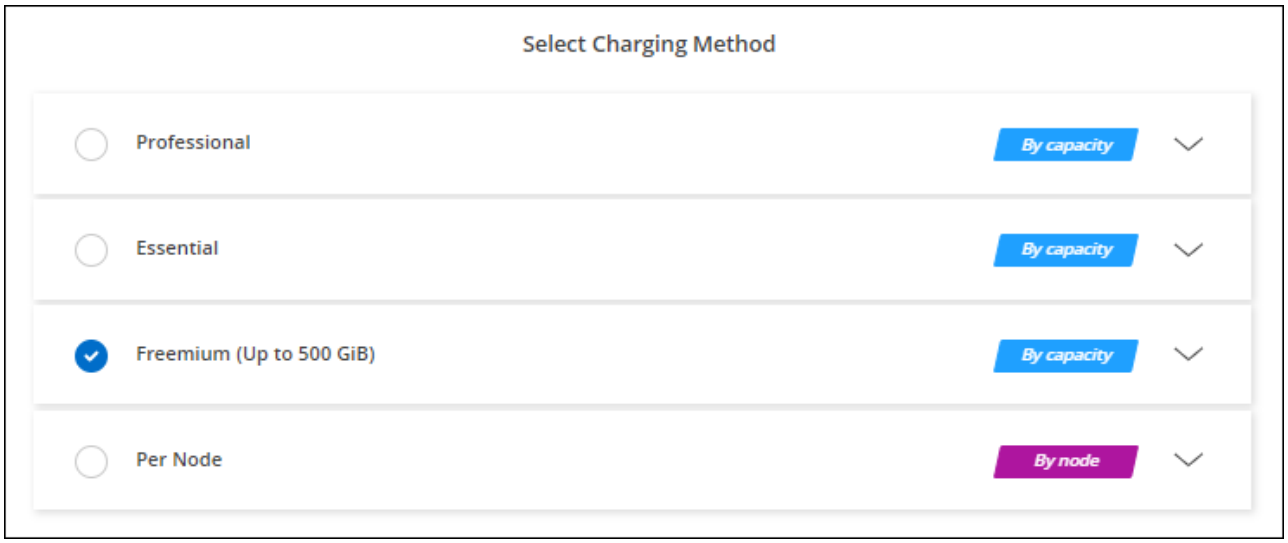
1. 왼쪽 탐색 메뉴에서 * Storage > Canvas * 를 선택합니다.
2. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 BlueXP의 단계를 따릅니다.

   a. 세부 정보 및 자격 증명 * 페이지에서 * 자격 증명 편집 > 구독 추가 * 를 클릭한 다음 화면의 지시에 따라 Azure Marketplace에서 선불 종량제 서비스를 구독합니다.

   프로비저닝된 용량 500GiB를 초과하지 않는 한, 마켓플레이스 구독을 통해 비용이 청구되지 않으며, 이 경우 시스템이 으로 자동으로 변환됩니다 "Essentials 패키지를 선택합니다".



a. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 * Freemium * 을 선택합니다.



"Azure에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".

용량 기반 라이센스

용량 기반 라이센스를 통해 Cloud Volumes ONTAP 1TiB 용량 단위로 비용을 지불할 수 있습니다. 용량 기반 라이센스는 Essentials 패키지 또는 Professional 패키지 형태로 제공됩니다.

Essentials 및 Professional 패키지는 다음 소비 모델과 함께 제공됩니다.

- NetApp에서 구입한 라이센스(BYOL
- Azure Marketplace에서 PAYGO(Pay-as-you-Go) 구독을 통해 시간 단위로 비용을 지불하는 것이 좋습니다
- 연간 계약입니다

"용량 기반 라이센스에 대해 자세히 알아보십시오".

다음 섹션에서는 이러한 각 소비 모델을 시작하는 방법을 설명합니다.

BYOL

NetApp에서 BYOL(License)을 구매하여 모든 클라우드 공급자를 통해 Cloud Volumes ONTAP 시스템 구축

단계

1. "라이센스를 획득하려면 NetApp 세일즈 팀에 문의하십시오"
2. "NetApp Support 사이트 계정을 BlueXP에 추가합니다"

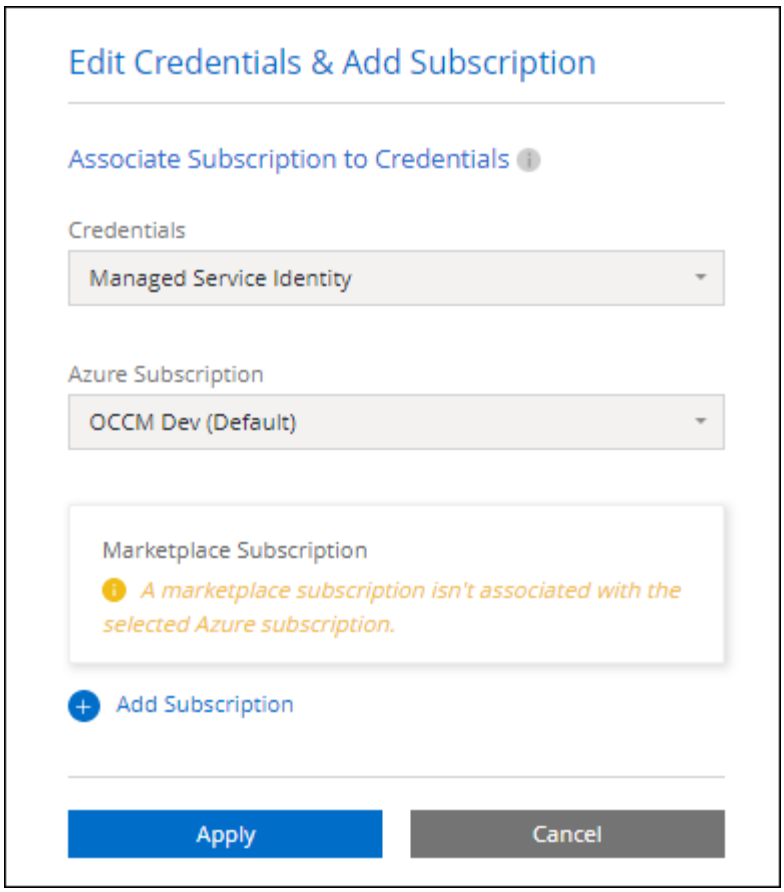
   BlueXP는 NetApp의 라이센스 서비스에 자동으로 쿼리하여 NetApp Support 사이트 계정과 관련된 라이센스에 대한 자세한 정보를 확인합니다. 오류가 없으면 BlueXP는 자동으로 디지털 지갑에 라이센스를 추가합니다.

   Cloud Volumes ONTAP와 함께 사용하기 전에 BlueXP 디지털 지갑에서 라이센스를 사용할 수 있어야 합니다. 필요한 경우, 할 수 있습니다 "BlueXP 디지털 지갑에 라이센스를 수동으로 추가합니다".

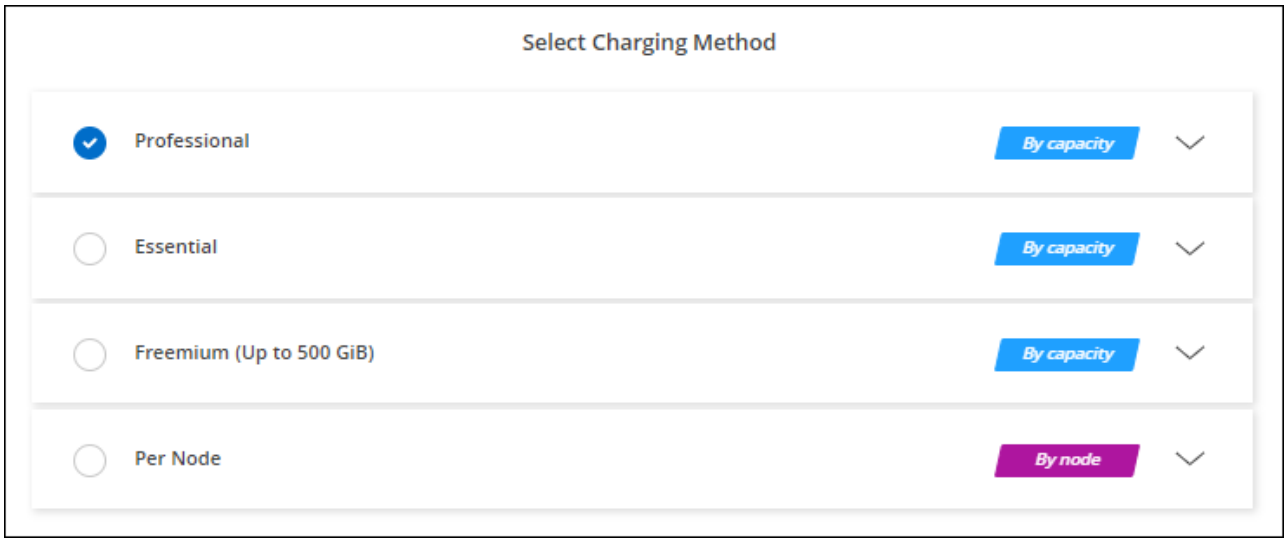
3. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 BlueXP의 단계를 따릅니다.

   a. 세부 정보 및 자격 증명 * 페이지에서 * 자격 증명 편집 > 구독 추가 * 를 클릭한 다음 화면의 지시에 따라 Azure Marketplace에서 선불 종량제 서비스를 구독합니다.

      NetApp에서 구매한 라이센스는 항상 먼저 부과되지만, 라이센스 용량을 초과하거나 라이센스 기간이 만료되면 마켓플레이스의 시간당 요율로 비용이 청구됩니다.



a. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 용량 기반 패키지를 선택합니다.



"Azure에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".

PAYGO 구독

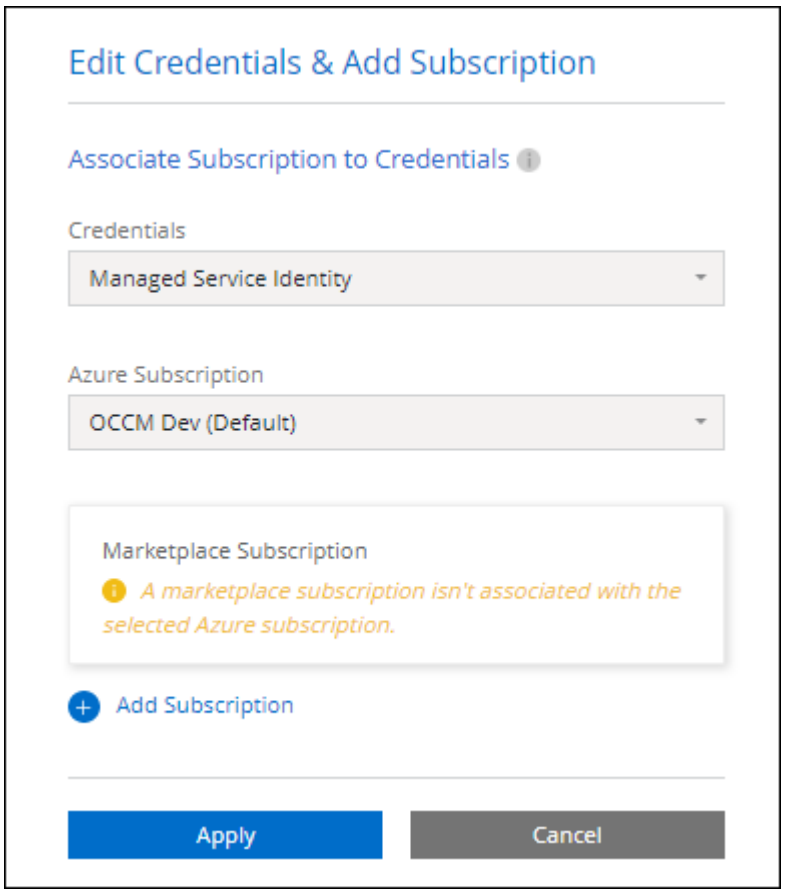
클라우드 공급자 마켓플레이스의 서비스에 가입하여 시간별 비용 지불

Cloud Volumes ONTAP 작업 환경을 만들 때 BlueXP는 Azure 마켓플레이스에서 사용 가능한 계약을 구독하라는 메시지를 표시합니다. 그러면 해당 구독이 충전을 위한 작업 환경과 연결됩니다. 추가 작업 환경에 동일한

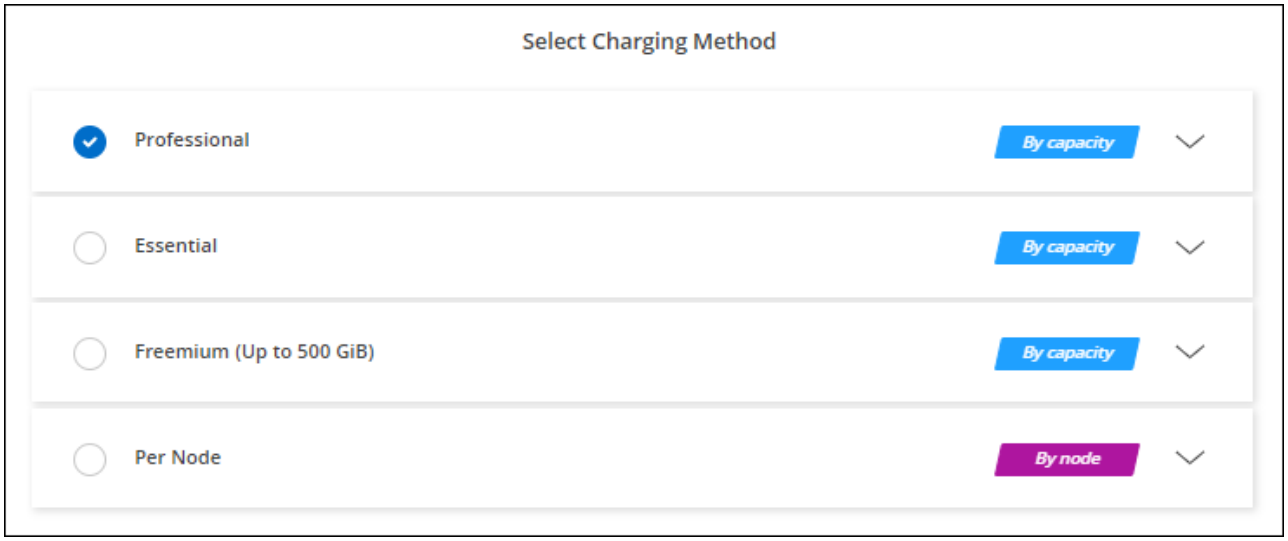
서브스크립션을 사용할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 * Storage > Canvas * 를 선택합니다.
2. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 BlueXP의 단계를 따릅니다.
   a. 세부 정보 및 자격 증명 * 페이지에서 * 자격 증명 편집 > 구독 추가 * 를 클릭한 다음 화면의 지시에 따라 Azure Marketplace에서 선불 종량제 서비스를 구독합니다.



   b. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 용량 기반 패키지를 선택합니다.



"Azure에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".

설정 > 자격 증명 페이지에서 Azure 계정과 연결된 Azure 마켓플레이스 구독을 관리할 수 있습니다. "Azure 계정 및 구독을 관리하는 방법에 대해 알아보십시오"

연간 계약

연간 계약을 구매하여 매년 Cloud Volumes ONTAP에 대한 비용을 지불합니다.

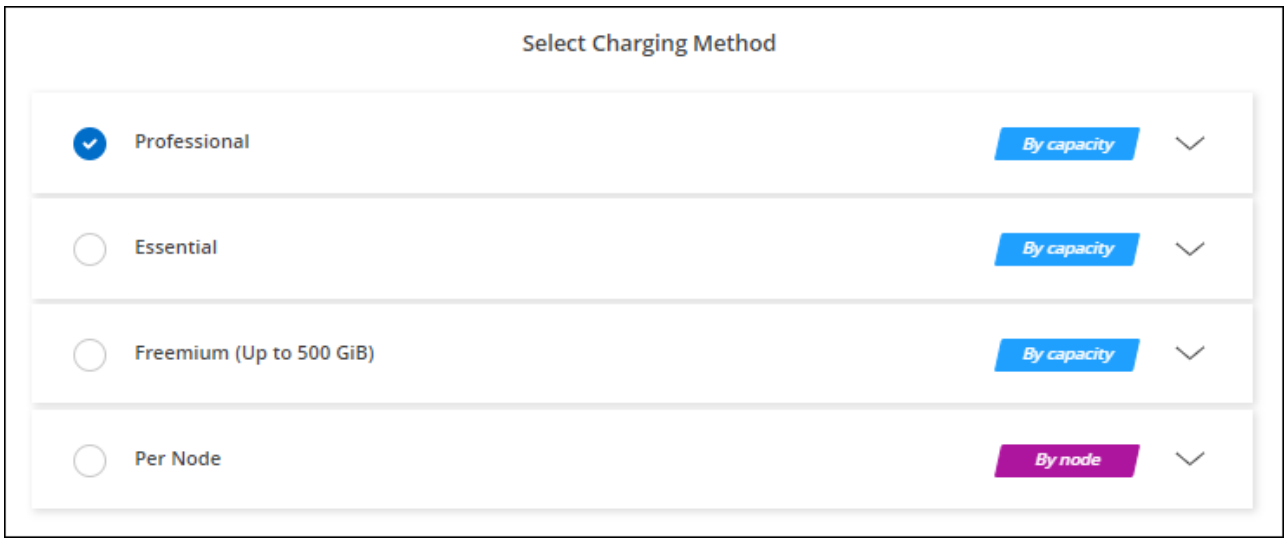
단계

1. 연간 계약을 구입하려면 NetApp 세일즈 담당자에게 문의하십시오.

   이 계약은 Azure 마켓플레이스에서 _private_Offer로 제공됩니다.

   NetApp이 프라이빗 오퍼를 공유하면 작업 환경을 생성하는 동안 Azure 마켓플레이스에서 구독할 때 연간 계획을 선택할 수 있습니다.

2. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 BlueXP의 단계를 따릅니다.
   a. 세부 정보 및 자격 증명 * 페이지에서 * 자격 증명 편집 > 구독 추가 > 계속 * 을 클릭합니다.
   b. Azure 포털에서 Azure 계정과 공유된 연간 계획을 선택한 다음 * 구독 * 을 클릭합니다.
   c. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 용량 기반 패키지를 선택합니다.



"Azure에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".

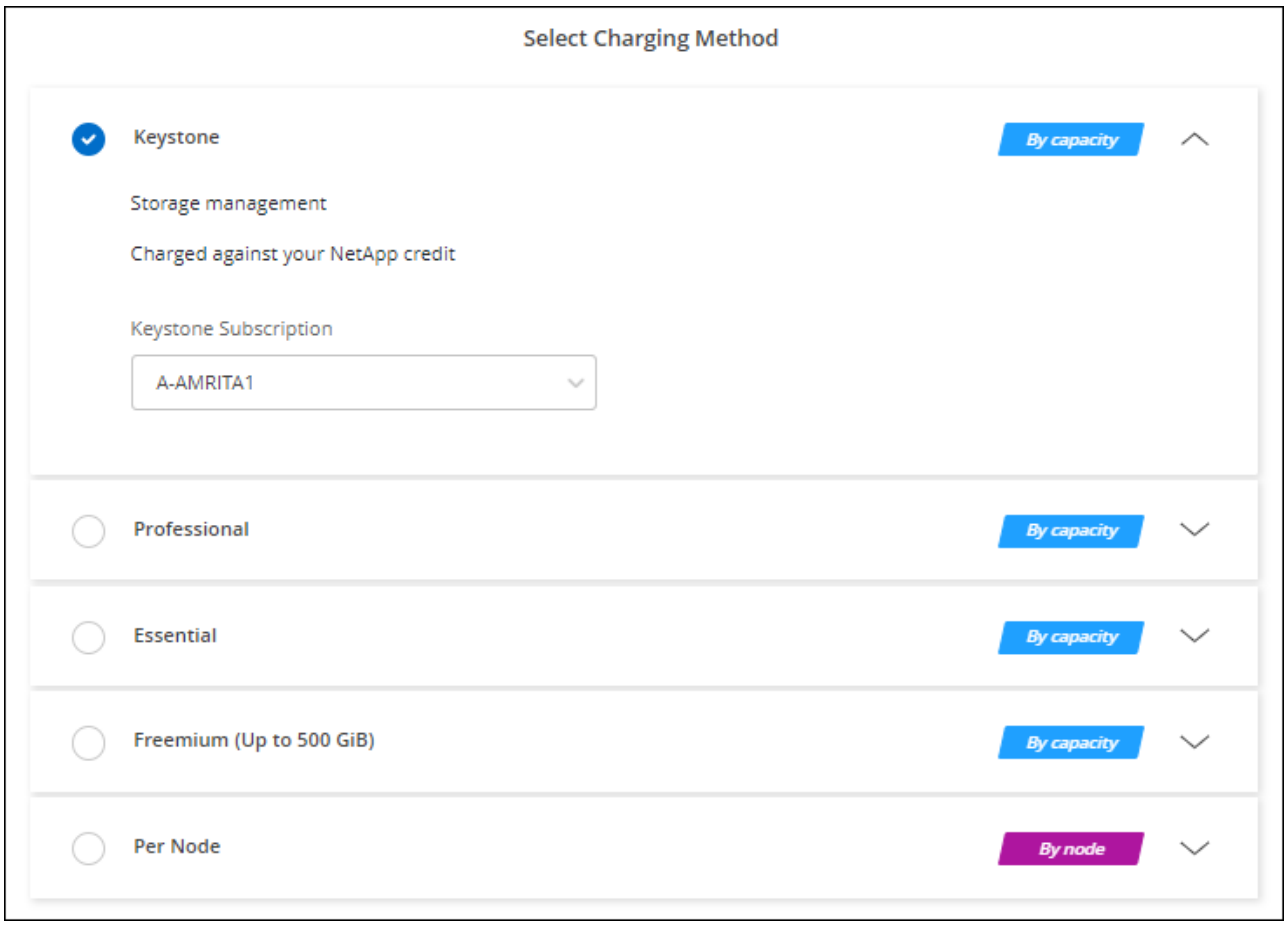
Keystone 구독

Keystone 가입은 종량제 구독 기반 서비스입니다. "NetApp Keystone 구독에 대해 자세히 알아보십시오".

단계

1. 아직 구독이 없는 경우 "NetApp에 문의하십시오"
2. mailto:ng-keystone-success@netapp.com [NetApp에 문의]하여 하나 이상의 Keystone 구독으로 BlueXP 사용자 계정을 인증하십시오.

3. NetApp이 사용자 계정을 승인한 후 "Cloud Volumes ONTAP에서 사용할 수 있도록 구독을 연결합니다".
4. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 BlueXP의 단계를 따릅니다.
   a. 충전 방법을 선택하라는 메시지가 표시되면 Keystone 가입 충전 방법을 선택합니다.



"Azure에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".

Azure에서 고가용성 모드를 활성화합니다

계획되지 않은 페일오버 시간을 줄이고 Cloud Volumes ONTAP에 대한 NFSv4 지원을 활성화하려면 Microsoft Azure의 고가용성 모드를 활성화해야 합니다.

Cloud Volumes ONTAP 9.10.1 릴리즈부터 Microsoft Azure에서 실행되는 Cloud Volumes ONTAP HA 쌍의 계획되지 않은 페일오버 시간을 줄이고 NFSv4에 대한 지원을 추가했습니다. Cloud Volumes ONTAP에서 이러한 향상된 기능을 사용하려면 Azure 구독에서 고가용성 기능을 활성화해야 합니다.

Azure 구독에서 이 기능을 활성화해야 하는 경우 BlueXP에서 작업 필요 메시지에 이러한 세부 정보를 표시합니다.

다음 사항에 유의하십시오.

- Cloud Volumes ONTAP HA 쌍의 고가용성에는 문제가 없습니다. 이 Azure 기능은 ONTAP와 함께 작동하여 계획되지 않은 페일오버 이벤트로 인해 NFS 프로토콜에 대해 클라이언트에서 관측된 애플리케이션 중단 시간을 줄입니다.

- 이 기능을 사용하도록 설정하는 것은 Cloud Volumes ONTAP HA 쌍의 무중단 기능입니다.
- Azure 구독에서 이 기능을 활성화해도 다른 VM에 문제가 발생하지 않습니다.

"소유자" 권한이 있는 Azure 사용자는 Azure CLI에서 이 기능을 활성화할 수 있습니다.

단계

1. "Azure Portal에서 Azure Cloud Shell에 액세스합니다"
2. 고가용성 모드 기능 등록:

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

3. 필요한 경우 기능이 지금 등록되었는지 확인합니다.

```
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"
}
```

Azure에서 Cloud Volumes ONTAP 실행

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

필요한 것

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".

- Cloud Volumes ONTAP에 대한 라이센스 설정에 필요한 사항을 이해합니다.

  "라이센스 설정 방법에 대해 알아보십시오".

이 작업에 대해

BlueXP는 Azure에서 Cloud Volumes ONTAP 시스템을 생성할 때 리소스 그룹, 네트워크 인터페이스 및 스토리지 계정과 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. BlueXP는 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.

Azure에서 단일 노드 Cloud Volumes ONTAP 시스템 시작

Azure에서 단일 노드 Cloud Volumes ONTAP 시스템을 실행하려면 BlueXP에서 단일 노드 작업 환경을 만들어야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 * Storage > Canvas * 를 선택합니다.
2. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 화면의 지시를 따릅니다.
3. * 위치 선택 *: * Microsoft Azure * 및 * Cloud Volumes ONTAP 단일 노드 * 를 선택합니다.
4. 메시지가 표시되면 "커넥터를 작성합니다".
5. * 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	BlueXP는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Azure 가상 시스템 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.

필드에 입력합니다	설명
리소스 그룹 태그	태그는 Azure 리소스에 대한 메타데이터입니다. 이 필드에 태그를 입력하면 BlueXP가 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 System Manager 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다. default_admin_user 이름을 유지하거나 사용자 지정 사용자 이름으로 변경합니다.
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/test//media/video_subscribing_azure.mp4 *(video)*

6. * 서비스 *: Cloud Volumes ONTAP에서 사용하지 않을 개별 서비스를 활성화 또는 비활성화합니다.
   - "BlueXP 분류에 대해 자세히 알아보십시오"
   - "BlueXP 백업 및 복구에 대해 자세히 알아보십시오"

   WORM 및 데이터 계층화를 사용하려면 BlueXP 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 작업 환경을 구축해야 합니다.

7. * Location *: 지역, 가용성 영역, VNET 및 서브넷을 선택한 다음 확인란을 선택하여 Connector와 대상 위치 간의 네트워크 연결을 확인합니다.

   단일 노드 시스템의 경우 Cloud Volumes ONTAP를 구축할 가용성 영역을 선택할 수 있습니다. AZ를 선택하지 않으면 BlueXP가 사용자를 위해 하나를 선택합니다.

8. * 연결 *: 새 리소스 그룹 또는 기존 리소스 그룹을 선택한 다음 미리 정의된 보안 그룹을 사용할지 아니면 직접 사용할 것인지 선택합니다.

   다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
리소스 그룹	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. 사용 중인 Azure 계정에 가 있는 경우 "필수 권한", BlueXP는 배포 실패 또는 삭제 시 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거합니다.
보안 그룹을 생성했습니다	BlueXP에서 보안 그룹을 생성하도록 하면 트래픽을 허용하는 방법을 선택해야 합니다. • 선택한 VNET만 * 을 선택한 경우 인바운드 트래픽의 소스는 선택한 VNET의 서브넷 범위와 커넥터가 상주하는 VNET의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다. • All VNets * 를 선택한 경우 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
기존 항목 사용	기존 보안 그룹을 선택하는 경우 Cloud Volumes ONTAP 요구 사항을 충족해야 합니다. "기본 보안 그룹을 봅니다".

9. * 충전 방법 및 NSS 계정 *: 이 시스템에서 사용할 충전 옵션을 지정한 다음 NetApp Support 사이트 계정을 지정합니다.
   - "Cloud Volumes ONTAP의 라이센스 옵션에 대해 자세히 알아보십시오".
   - "라이센스 설정 방법에 대해 알아보십시오".
10. * 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.
11. * 라이선스 *: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 가상 머신 유형을 선택합니다.

    선택한 버전에 대해 최신 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우 BlueXP는 작업 환경을 만들 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.10.1 및 9.10.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리즈에서 다른 릴리즈로 발생하지 않습니다(예: 9.6에서 9.7로).
12. * Azure Marketplace * 구독: BlueXP가 Cloud Volumes ONTAP의 프로그래밍 방식 배포를 활성화할 수 없는 경우 다음 단계를 따르십시오.
13. * 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 간단한 프로비저닝 옵션을 사용할 때 BlueXP가 생성하는

추가 애그리게이트에서 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".

14. * 쓰기 속도 및 WORM *:

    a. 필요한 경우 * Normal * (정상 *) 또는 * High * (높음 *) 쓰기 속도를 선택합니다.

    "쓰기 속도에 대해 자세히 알아보십시오".

    b. 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

    이 옵션은 특정 VM 유형에만 사용할 수 있습니다. 지원되는 VM 유형에 대한 자세한 내용은 을 참조하십시오 "HA Pair에 대한 라이센스에서 지원되는 구성".

    Cloud Volumes ONTAP 9.7 이하 버전에서 데이터 계층화가 활성화된 경우 WORM을 사용할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로의 되돌리기 또는 다운그레이드가 차단됩니다.

    "WORM 스토리지에 대해 자세히 알아보십시오".

    a. WORM 스토리지를 활성화한 경우 보존 기간을 선택합니다.

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

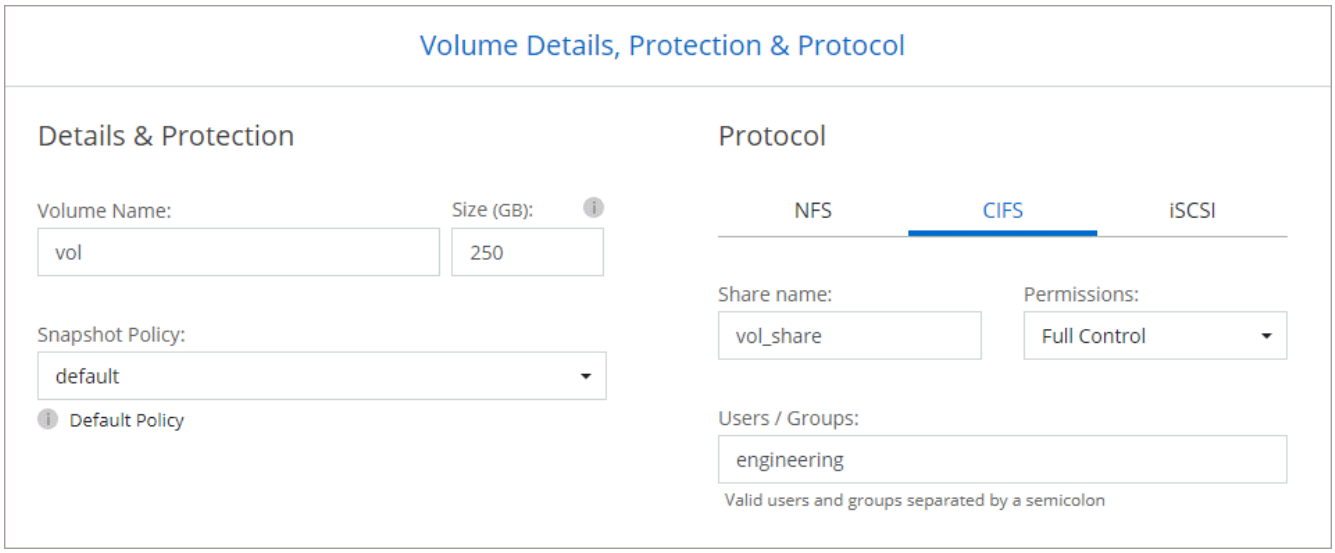
    "지원되는 클라이언트 프로토콜 및 버전에 대해 알아보십시오".

    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 서브넷의 클라이언트를 정의합니다. 기본적으로 BlueXP는 서브넷의 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.

필드에 입력합니다	설명
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 BlueXP에서 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.



16. * 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.

필드에 입력합니다	설명
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. "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 "BlueXP 자동화 문서" 를 참조하십시오. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 생성한 후에는 구성할 수 없습니다.

17. * 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".

18. * 검토 및 승인 *: 선택 사항을 검토 및 확인합니다.
    a. 구성에 대한 세부 정보를 검토합니다.
    b. BlueXP가 구매할 지원 및 Azure 리소스에 대한 세부 정보를 검토하려면 * 추가 정보 * 를 클릭합니다.
    c. 이해함… * 확인란을 선택합니다.
    d. Go * 를 클릭합니다.

결과

BlueXP는 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.

Azure에서 Cloud Volumes ONTAP HA 쌍 시작

Azure에서 Cloud Volumes ONTAP HA 쌍을 실행하려면 BlueXP에서 HA 작업 환경을 만들어야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 * Storage > Canvas * 를 선택합니다.
2. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 화면의 지시를 따릅니다.
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	BlueXP는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Azure 가상 시스템 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 BlueXP가 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 System Manager 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다. default_admin_user 이름을 유지하거나 사용자 지정 사용자 이름으로 변경합니다.
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/test//media/video_subscribing_azure.mp4 *(video)*

5. * 서비스 *: Cloud Volumes ONTAP에서 사용하지 않을 개별 서비스를 활성화 또는 비활성화합니다.
   - "BlueXP 분류에 대해 자세히 알아보십시오"
   - "BlueXP 백업 및 복구에 대해 자세히 알아보십시오"

   WORM 및 데이터 계층화를 사용하려면 BlueXP 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 작업 환경을 구축해야 합니다.

6. * HA 구축 모델 *:
   a. 단일 가용성 영역 * 또는 * 다중 가용성 영역 * 을 선택합니다.
   b. * 위치 및 연결 * (단일 AZ) 및 * 지역 및 연결 * (다중 AZs)

- 단일 AZ의 경우 지역, VNET 및 서브넷을 선택합니다.
- 여러 AZs의 경우 노드 1의 영역, VNET, 서브넷, 영역 및 노드 2의 영역을 선택합니다.

c. 네트워크 연결을 확인했습니다. * 확인란을 선택합니다.

7. * 연결 *: 새 리소스 그룹 또는 기존 리소스 그룹을 선택한 다음 미리 정의된 보안 그룹을 사용할지 아니면 직접 사용할 것인지 선택합니다.

   다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
리소스 그룹	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. 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 배포하려고 하면 BlueXP에서 연결 문제가 발생합니다. 사용 중인 Azure 계정에 가 있는 경우 "필수 권한", BlueXP는 배포 실패 또는 삭제 시 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거합니다.
보안 그룹을 생성했습니다	BlueXP에서 보안 그룹을 생성하도록 하면 트래픽을 허용하는 방법을 선택해야 합니다. • 선택한 VNET만 * 을 선택한 경우 인바운드 트래픽의 소스는 선택한 VNET의 서브넷 범위와 커넥터가 상주하는 VNET의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다. • All VNets * 를 선택한 경우 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
기존 항목 사용	기존 보안 그룹을 선택하는 경우 Cloud Volumes ONTAP 요구 사항을 충족해야 합니다. "기본 보안 그룹을 봅니다".

8. * 충전 방법 및 NSS 계정 *: 이 시스템에서 사용할 충전 옵션을 지정한 다음 NetApp Support 사이트 계정을 지정합니다.
   - "Cloud Volumes ONTAP의 라이센스 옵션에 대해 자세히 알아보십시오".
   - "라이센스 설정 방법에 대해 알아보십시오".
9. 사전 구성된 패키지 *: Cloud Volumes ONTAP 시스템을 신속하게 배포하려면 패키지 중 하나를 선택하거나 * 구성 변경 * 을 클릭합니다.

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

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

선택한 버전에 대해 최신 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우 BlueXP는 작업 환경을 만들 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.10.1 및 9.10.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리즈에서 다른 릴리즈로 발생하지 않습니다(예: 9.6에서 9.7로).

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

    다음 사항에 유의하십시오.

    - 디스크 크기는 초기 애그리게이트의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 BlueXP가 생성하는 추가 애그리게이트에서 사용됩니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.

      디스크 크기 선택에 대한 도움말은 를 참조하십시오 "Azure에서 시스템 크기 조정".

    - 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".

13. * 쓰기 속도 및 WORM *:

    a. 필요한 경우 * Normal * (정상 *) 또는 * High * (높음 *) 쓰기 속도를 선택합니다.

       "쓰기 속도에 대해 자세히 알아보십시오".

    b. 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

       이 옵션은 특정 VM 유형에만 사용할 수 있습니다. 지원되는 VM 유형에 대한 자세한 내용은 을 참조하십시오 "HA Pair에 대한 라이센스에서 지원되는 구성".

       Cloud Volumes ONTAP 9.7 이하 버전에서 데이터 계층화가 활성화된 경우 WORM을 사용할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로의 되돌리기 또는 다운그레이드가 차단됩니다.

    "WORM 스토리지에 대해 자세히 알아보십시오".

    a. WORM 스토리지를 활성화한 경우 보존 기간을 선택합니다.

14. * 스토리지와 WORM * 에 대한 보안 통신: Azure 스토리지 계정에 대한 HTTPS 연결을 사용하도록 설정하고 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화할지 여부를 선택합니다.

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

    "WORM 스토리지에 대해 자세히 알아보십시오".

    데이터 계층화가 설정된 경우 WORM을 설정할 수 없습니다.

"WORM 스토리지에 대해 자세히 알아보십시오".

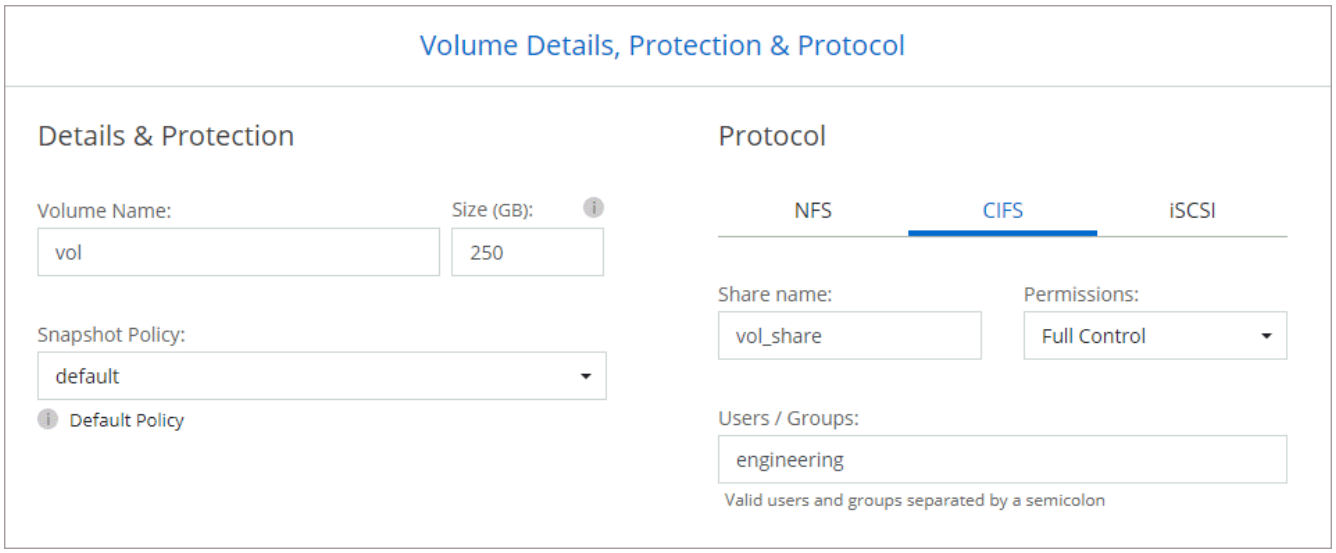
15. * 볼륨 생성 *: 새 볼륨에 대한 세부 정보를 입력하거나 * 건너뛰기 * 를 클릭합니다.

    "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 서브넷의 클라이언트를 정의합니다. 기본적으로 BlueXP는 서브넷의 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 BlueXP에서 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.



16. * 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. "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 "BlueXP 자동화 문서" 를 참조하십시오. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 생성한 후에는 구성할 수 없습니다.

17. * 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 프로필을 선택합니다" 및 "데이터 계층화 개요".

18. * 검토 및 승인 *: 선택 사항을 검토 및 확인합니다.
    a. 구성에 대한 세부 정보를 검토합니다.
    b. BlueXP가 구매할 지원 및 Azure 리소스에 대한 세부 정보를 검토하려면 * 추가 정보 * 를 클릭합니다.
    c. 이해함… * 확인란을 선택합니다.
    d. Go * 를 클릭합니다.

결과

BlueXP는 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 인쇄됨 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.