시작하십시오
Cloud Volumes ONTAP

NetApp
June 27, 2024

목차

시작하십시오

Cloud Volumes ONTAP에 대해 자세히 알아보십시오

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

Cloud Volumes ONTAP은 클라우드에서 ONTAP 데이터 관리 소프트웨어를 실행하는 소프트웨어 전용 스토리지 어플라이언스입니다. 엔터프라이즈급 스토리지에 다음 주요 기능을 제공하며 다음 테스트 시 다음과 같습니다.

- 스토리지 효율성

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

- 고가용성

  클라우드 환경에서 장애가 발생할 경우 엔터프라이즈급 안정성과 지속적인 운영을 보장합니다.

- 데이터 보호

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

  또한 Cloud Volumes ONTAP는 BlueXP 백업 및 복구 기능과 통합되어 클라우드 데이터의 보호 및 장기 아카이브를 위한 백업 및 복원 기능을 제공합니다.

  "BlueXP 백업 및 복구에 대해 자세히 알아보십시오"

- 데이터 계층화

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

- 애플리케이션 정합성

  NetApp SnapCenter를 사용하여 NetApp Snapshot 복사본의 일관성을 보장합니다.

  "SnapCenter에 대해 자세히 알아보십시오"

- 데이터 보안

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

- 개인 정보 보호 규정 준수 관리

  BlueXP 분류와의 통합으로 데이터 컨텍스트를 이해하고 중요한 데이터를 식별할 수 있습니다.

  "BlueXP 분류에 대해 자세히 알아보십시오"

ONTAP 기능에 대한 라이센스는 Cloud Volumes ONTAP에 포함되어 있습니다.

"지원되는 Cloud Volumes ONTAP 구성을 봅니다"

"Cloud Volumes ONTAP에 대해 자세히 알아보십시오"

새로운 배포에 지원되는 버전입니다

BlueXP를 사용하면 새로운 Cloud Volumes ONTAP 작업 환경을 만들 때 여러 ONTAP 버전 중에서 선택할 수 있습니다.

다른 모든 Cloud Volumes ONTAP 버전은 새 배포에서 지원되지 않습니다.

설치하고

단일 노드

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

HA 쌍

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

Azure를 지원합니다

단일 노드

- 9.13.1 GA
- 9.12.1 GA

- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3입니다
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6
- 9.5 P6

HA 쌍

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3입니다
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6

Google 클라우드

단일 노드

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

HA 쌍

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1

- 9.9.1 P6
- 9.8

Amazon Web Services에서 시작하십시오

AWS에서 Cloud Volumes ONTAP를 빠르게 시작합니다

몇 가지 단계를 통해 AWS에서 Cloud Volumes ONTAP를 시작하십시오.


커넥터를 작성합니다

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

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"


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".


네트워크 설정

1. VPC와 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.
3. VPC 엔드포인트를 S3 서비스로 설정합니다.

   Cloud Volumes ONTAP의 콜드 데이터를 저비용 오브젝트 스토리지로 계층화하려는 경우 VPC 엔드포인트가 필요합니다.

"네트워킹 요구 사항에 대해 자세히 알아보십시오".


AWS KMS를 설정합니다

Cloud Volumes ONTAP에서 아마존 암호화를 사용하려면 활성 CMK(고객 마스터 키)가 있는지 확인해야 합니다. 또한 Connector에 대한 권한을 제공하는 IAM 역할을 _KEY USER_로 추가하여 각 CMK에 대한 키 정책을 수정해야 합니다. "자세한 정보".


BlueXP를 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"
- "AWS Marketplace에서 커넥터 실행"
- "Linux 호스트에 Connector 소프트웨어 설치"
- "BlueXP에서 AWS 권한을 사용하는 경우"

AWS에서 Cloud Volumes ONTAP 구성 계획

AWS에 Cloud Volumes ONTAP를 구축할 때 워크로드 요구사항에 맞게 사전 구성된 시스템을 선택하거나 자체 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 AWS 지역에서 지원됩니다. "지원되는 영역의 전체 목록을 봅니다".

해당 지역에서 리소스를 생성하고 관리하려면 먼저 새로운 AWS 영역을 활성화해야 합니다. "지역 활성화 방법을 알아보십시오".

지원되는 인스턴스를 선택합니다

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

"AWS에서 Cloud Volumes ONTAP가 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.

"AWS의 Cloud Volumes ONTAP에 대한 스토리지 제한"

AWS에서 시스템 크기 조정

Cloud Volumes ONTAP 시스템을 사이징하면 성능 및 용량 요구사항을 충족하는 데 도움이 될 수 있습니다. 인스턴스 유형, 디스크 유형 및 디스크 크기를 선택할 때 몇 가지 주요 사항을 알고 있어야 합니다.

인스턴스 유형

- 각 EC2 인스턴스 유형별 최대 처리량과 IOPS에 맞춰 워크로드 요구사항을 충족합니다.
- 여러 사용자가 동시에 시스템에 쓸 경우 요청을 관리할 CPU가 충분한 인스턴스 유형을 선택합니다.
- 대부분 읽혀지는 응용 프로그램이 있는 경우 충분한 RAM이 있는 시스템을 선택합니다.
  - "AWS 문서: Amazon EC2 인스턴스 유형"
  - "AWS 문서: Amazon EBS – 최적화된 인스턴스"

EBS 디스크 유형입니다

EBS 디스크 유형의 차이점은 다음과 같습니다. EBS 디스크의 사용 사례에 대한 자세한 내용은 을 참조하십시오 "AWS 설명서:EBS 볼륨 유형".

- _GP3(General Purpose SSD)_디스크는 광범위한 워크로드에 대해 비용과 성능의 균형을 유지하는 가장 저렴한 SSD입니다. 성능은 IOPS 및 처리량 측면에서 정의됩니다. GP3 디스크는 Cloud Volumes ONTAP 9.7 이상에서 지원됩니다.

  GP3 디스크를 선택할 때 BlueXP는 기본 IOPS와 처리량 값을 채워 선택한 디스크 크기를 기준으로 GP2 디스크와 동일한 성능을 제공합니다. 더 높은 비용으로 더 나은 성능을 얻기 위해 값을 늘릴 수 있지만 성능이 저하될 수 있으므로 더 낮은 값을 지원하지 않습니다. 즉, 기본값을 그대로 사용하거나 값을 늘립니다. 낮추지 마십시오. "GP3 디스크 및 성능에 대해 자세히 알아보십시오".

  Cloud Volumes ONTAP는 GP3 디스크를 사용하는 Amazon EBS Elastic Volumes 기능을 지원합니다. "Elastic Volumes 지원에 대해 자세히 알아보십시오".

- _GP2(General Purpose SSD)_디스크는 광범위한 워크로드에 대해 비용과 성능의 균형을 맞춥니다. 성능은 IOPS 측면에서 정의됩니다.
- _provisioned IOPS ssd(i1)_disk는 높은 비용으로 최고의 성능을 요구하는 중요한 응용 프로그램을 위한 것입니다.

  Cloud Volumes ONTAP는 iio1 디스크에서 Amazon EBS Elastic Volumes 기능을 지원합니다. "Elastic Volumes 지원에 대해 자세히 알아보십시오".

- _Throughput Optimized HDD(st1)_디스크는 낮은 가격으로 빠르고 일관된 처리량을 필요로 하는 자주 액세스되는 워크로드에 적합합니다.

  ⓘ 처리량 최적화 HDD(st1)를 사용하는 경우에는 데이터를 오브젝트 스토리지에 계층화하지 않는 것이 좋습니다.

EBS 디스크 크기입니다

를 지원하지 않는 구성을 선택하는 경우 "Amazon EBS Elastic Volumes 기능"그런 다음 Cloud Volumes ONTAP 시스템을 시작할 때 초기 디스크 크기를 선택해야 합니다. 그 이후에는 가능합니다 "BlueXP에서 시스템 용량을 관리할 수 있습니다"하지만 원하는 경우 "스스로 애그리게이트를 생성합니다"다음 사항에 유의하십시오.

- Aggregate의 모든 디스크는 동일한 크기여야 합니다.
- EBS 디스크의 성능은 디스크 크기와 관련이 있습니다. 이 크기는 SSD 디스크의 기준 IOPS 및 최대 버스트 지속 시간과 HDD 디스크의 기준 및 버스트 처리량을 결정합니다.
- 궁극적으로 필요한 _ 지속적인 성능 _ 을(를) 제공하는 디스크 크기를 선택해야 합니다.
- 더 큰 디스크(예: 4TiB 디스크 6개)를 선택하더라도 EC2 인스턴스가 대역폭 제한에 도달할 수 있으므로 모든

IOPS를 가져오지 못할 수 있습니다.

EBS 디스크 성능에 대한 자세한 내용은 을 참조하십시오 "AWS 설명서:EBS 볼륨 유형".

위에서 설명한 것처럼, Amazon EBS Elastic Volumes 기능을 지원하는 Cloud Volumes ONTAP 구성에서는 디스크 크기를 선택할 수 없습니다. "Elastic Volumes 지원에 대해 자세히 알아보십시오".

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.

"AWS에서 Cloud Volumes ONTAP 시스템 데이터의 기본 디스크를 봅니다".

커넥터에는 시스템 디스크도 필요합니다. "커넥터의 기본 설정에 대한 세부 정보를 봅니다".

AWS 아웃포스트에 **Cloud Volumes ONTAP** 구축 준비

AWS 아웃포스트가 있는 경우 작업 환경 마법사에서 아웃포스트 VPC를 선택하여 해당 아웃포스트에 Cloud Volumes ONTAP를 구축할 수 있습니다. 이러한 경험은 AWS에 상주하는 다른 VPC와 동일합니다. 먼저 AWS Outpost에 Connector를 구축해야 합니다.

몇 가지 제한 사항이 있습니다.

- 현재 단일 노드 Cloud Volumes ONTAP 시스템만 지원됩니다
- Cloud Volumes ONTAP와 함께 사용할 수 있는 EC2 인스턴스는 Outpost에서 사용할 수 있는 인스턴스로 제한됩니다
- 현재 GP2(범용 SSD)만 지원됩니다

네트워킹 정보를 수집합니다

AWS에서 Cloud Volumes ONTAP를 시작할 때 VPC 네트워크에 대한 세부 정보를 지정해야 합니다. 워크시트를 사용하여 관리자로부터 정보를 수집할 수 있습니다.

단일 노드 또는 **HA 2**노드 **AZ**

확인하십시오	귀사의 가치
지역	
VPC	
서브넷	
보안 그룹(자체 보안 그룹 사용 시)	

여러 대의 **AZs**에서 **HA** 쌍

확인하십시오	귀사의 가치
지역	

확인하십시오	귀사의 가치
VPC	
보안 그룹(자체 보안 그룹 사용 시)	
노드 1 가용성 영역	
노드 1 서브넷	
노드 2 가용성 영역	
노드 2 서브넷	
중재자 가용성 영역	
중재자 서브넷	
중재자를 위한 키 쌍입니다	
클러스터 관리 포트의 부동 IP 주소입니다	
노드 1의 데이터에 대한 유동 IP 주소입니다	
노드 2의 데이터에 대한 부동 IP 주소입니다	
부동 IP 주소에 대한 라우팅 테이블	

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.

네트워크 설정

AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항

BlueXP는 IP 주소, 넷마스크 및 라우트와 같은 Cloud Volumes ONTAP용 네트워킹 구성 요소 설정을 처리합니다. 아웃바운드 인터넷 액세스를 사용할 수 있는지, 충분한 전용 IP 주소를 사용할 수 있는지, 올바른 연결이 있는지 등을 확인해야 합니다.

일반 요구 사항

AWS에서 다음 요구사항을 충족해야 합니다.

Cloud Volumes ONTAP 노드에 대한 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

NAT 인스턴스가 있는 경우 개인 서브넷에서 인터넷으로 HTTPS 트래픽을 허용하는 인바운드 보안 그룹 규칙을 정의해야 합니다.

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".

HA 중재자를 위한 아웃바운드 인터넷 액세스

HA 중재자 인스턴스는 스토리지 페일오버를 지원할 수 있도록 AWS EC2 서비스에 대한 아웃바운드 연결이 있어야 합니다. 연결을 제공하기 위해 공용 IP 주소를 추가하거나 프록시 서버를 지정하거나 수동 옵션을 사용할 수 있습니다.

수동 옵션은 대상 서브넷에서 AWS EC2 서비스로 연결되는 NAT 게이트웨이 또는 인터페이스 VPC 엔드포인트일 수 있습니다. VPC 엔드포인트에 대한 자세한 내용은 을 참조하십시오 "AWS 문서:인터페이스 VPC 엔드포인트(AWS PrivateLink)".

전용 IP 주소

BlueXP는 필요한 수의 전용 IP 주소를 Cloud Volumes ONTAP에 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.

단일 노드 시스템의 **IP** 주소입니다

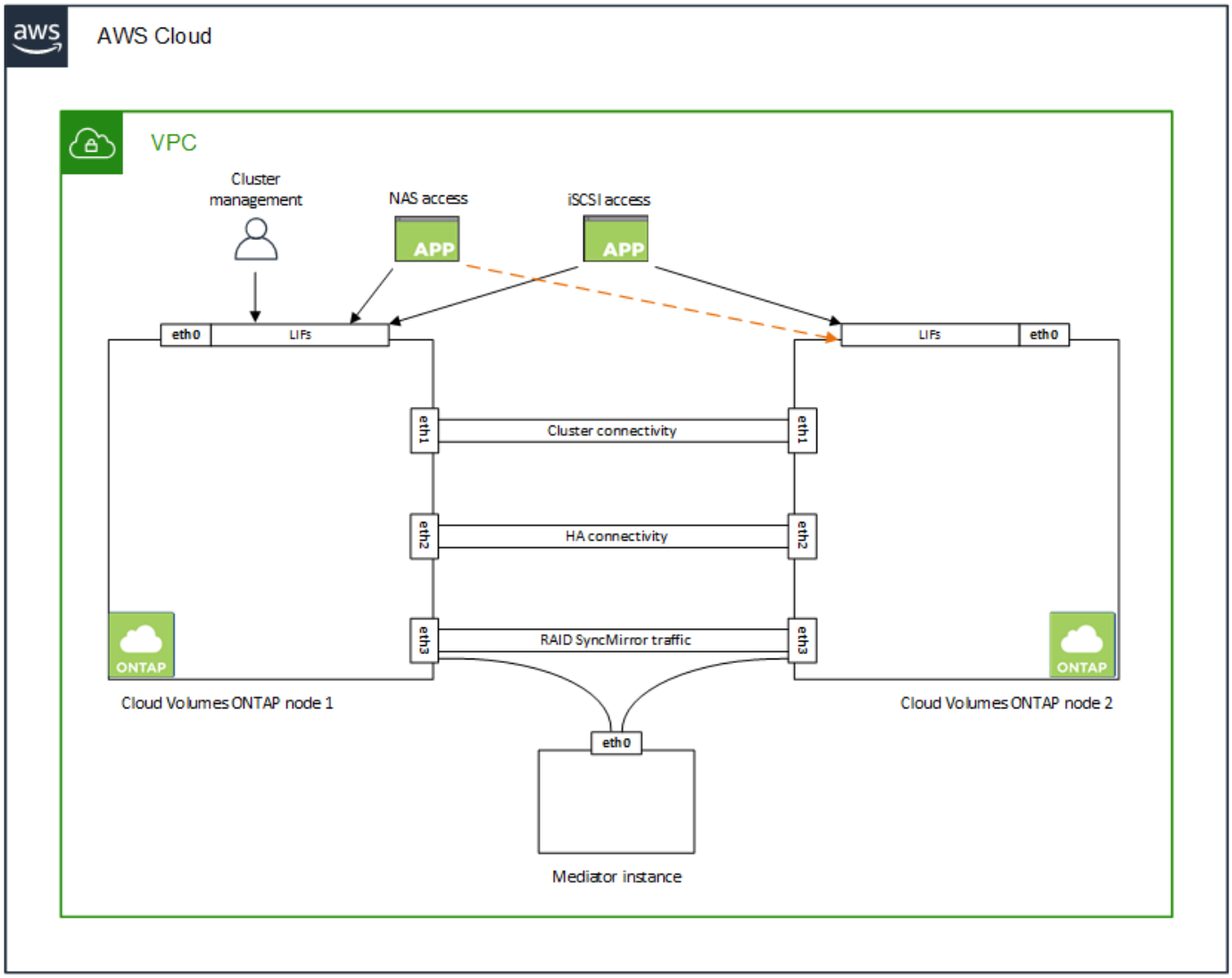
BlueXP는 단일 노드 시스템에 6개의 IP 주소를 할당합니다.

다음 표에는 각 프라이빗 IP 주소와 연결된 LIF에 대한 자세한 정보가 나와 있습니다.

LIF	목적
클러스터 관리	전체 클러스터(HA 쌍)의 관리
노드 관리	노드의 관리.
인터클러스터	클러스터 간 통신, 백업 및 복제
NAS 데이터	NAS 프로토콜을 통한 클라이언트 액세스
iSCSI 데이터	iSCSI 프로토콜을 통한 클라이언트 액세스. 또한 시스템에서 다른 중요한 네트워킹 워크플로우에 사용됩니다. 이 LIF는 필수 항목이므로 삭제할 수 없습니다.
스토리지 VM 관리	스토리지 VM 관리 LIF는 SnapCenter와 같은 관리 툴과 함께 사용됩니다.

HA 쌍의 **IP** 주소

HA Pair의 경우 단일 노드 시스템보다 더 많은 IP 주소가 필요합니다. 이러한 IP 주소는 다음 이미지와 같이 서로 다른 이더넷 인터페이스에 분산됩니다.



HA 쌍에 필요한 사설 IP 주소의 수는 선택한 구축 모델에 따라 다릅니다. AZ(Single_AWS Availability Zone)에 구축된 HA 쌍에는 15개의 프라이빗 IP 주소가 필요하고, _multiple_AZs에 구축된 HA 쌍에는 13개의 프라이빗 IP 주소가 필요합니다.

다음 표에는 각 프라이빗 IP 주소와 연결된 LIF에 대한 자세한 정보가 나와 있습니다.

단일 **AZ**에서 **HA** 쌍을 지원하는 **LIF**

LIF	인터페이스	노드	목적
클러스터 관리	eth0	노드 1	전체 클러스터(HA 쌍)의 관리
노드 관리	eth0	노드 1 및 노드 2	노드의 관리.
인터클러스터	eth0	노드 1 및 노드 2	클러스터 간 통신, 백업 및 복제
NAS 데이터	eth0	노드 1	NAS 프로토콜을 통한 클라이언트 액세스
iSCSI 데이터	eth0	노드 1 및 노드 2	iSCSI 프로토콜을 통한 클라이언트 액세스. 또한 시스템에서 다른 중요한 네트워킹 워크플로우에 사용됩니다. 이러한 LIF는 필수 항목이므로 삭제할 수 없습니다.

LIF	인터페이스	노드	목적
클러스터 연결	eth1	노드 1 및 노드 2	노드가 서로 통신하고 클러스터 내에서 데이터를 이동할 수 있도록 지원합니다.
HA 연결	윤리2	노드 1 및 노드 2	페일오버 시 두 노드 간의 통신.
RSM iSCSI 트래픽입니다	eth3	노드 1 및 노드 2	RAID SyncMirror iSCSI 트래픽과 두 Cloud Volumes ONTAP 노드 및 중재자 간의 통신
중재자	eth0	중재자	스토리지 테이크오버 및 반환 프로세스를 지원하는 노드와 중재자 간의 통신 채널

여러 **AZs**의 **HA** 쌍에 대한 **LIF**

LIF	인터페이스	노드	목적
노드 관리	eth0	노드 1 및 노드 2	노드의 관리.
인터클러스터	eth0	노드 1 및 노드 2	클러스터 간 통신, 백업 및 복제
iSCSI 데이터	eth0	노드 1 및 노드 2	iSCSI 프로토콜을 통한 클라이언트 액세스. 이러한 LIF는 노드 간 부동 IP 주소의 마이그레이션도 관리합니다. 이러한 LIF는 필수 항목이므로 삭제할 수 없습니다.
클러스터 연결	eth1	노드 1 및 노드 2	노드가 서로 통신하고 클러스터 내에서 데이터를 이동할 수 있도록 지원합니다.
HA 연결	윤리2	노드 1 및 노드 2	페일오버 시 두 노드 간의 통신.
RSM iSCSI 트래픽입니다	eth3	노드 1 및 노드 2	RAID SyncMirror iSCSI 트래픽과 두 Cloud Volumes ONTAP 노드 및 중재자 간의 통신
중재자	eth0	중재자	스토리지 테이크오버 및 반환 프로세스를 지원하는 노드와 중재자 간의 통신 채널

여러 가용성 영역에 구축된 경우 여러 LIF가 에 연결됩니다 "유동 IP 주소"이는 AWS 프라이빗 IP 제한에 계산되지 않습니다.

보안 그룹

BlueXP에서는 보안 그룹을 만들 필요가 없습니다. 직접 사용해야 하는 경우 을 참조하십시오 "보안 그룹 규칙".

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

데이터 계층화를 위한 연결

EBS를 성능 계층으로 사용하고 AWS S3를 용량 계층으로 사용하려면 Cloud Volumes ONTAP이 S3에 연결되어 있는지 확인해야 합니다. 이 연결을 제공하는 가장 좋은 방법은 S3 서비스에 VPC 엔드포인트를 생성하는 것입니다. 자세한 내용은 을 참조하십시오 "AWS 설명서: 게이트웨이 엔드포인트 생성".

VPC 끝점을 만들 때 Cloud Volumes ONTAP 인스턴스에 해당하는 영역, VPC 및 라우팅 테이블을 선택해야 합니다. 또한 S3 엔드포인트에 대한 트래픽을 활성화하는 아웃바운드 HTTPS 규칙을 추가하려면 보안 그룹을 수정해야 합니다. 그렇지 않으면 Cloud Volumes ONTAP에서 S3 서비스에 연결할 수 없습니다.

문제가 발생하면 을 참조하십시오 "AWS 지원 지식 센터: 게이트웨이 VPC 엔드포인트를 사용하여 S3 버킷에 연결할 수 없는 이유는 무엇입니까?"

ONTAP 시스템에 대한 연결

AWS의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 AWS VPC와 회사 네트워크 같은 다른 네트워크 간에 VPN 연결을 설정해야 합니다. 자세한 내용은 을 참조하십시오 "AWS 설명서: AWS VPN 연결 설정".

CIFS용 **DNS** 및 **Active Directory**

CIFS 스토리지를 프로비저닝하려면 AWS에서 DNS 및 Active Directory를 설정하거나 사내 설정을 AWS로 확장해야 합니다.

DNS 서버는 Active Directory 환경에 대한 이름 확인 서비스를 제공해야 합니다. Active Directory 환경에서 사용되는 DNS 서버가 아니어야 하는 기본 EC2 DNS 서버를 사용하도록 DHCP 옵션 집합을 구성할 수 있습니다.

자세한 지침은 을 참조하십시오 "AWS 설명서: AWS 클라우드의 Active Directory 도메인 서비스: 빠른 시작 참조 배포".

VPC 공유

9.11.1 릴리즈부터 VPC 공유를 지원하는 AWS에서 Cloud Volumes ONTAP HA 쌍이 지원됩니다. VPC 공유를 사용하면 서브넷을 다른 AWS 계정과 공유할 수 있습니다. 이 구성을 사용하려면 AWS 환경을 설정한 다음 API를 사용하여 HA 쌍을 구축해야 합니다.

"공유 서브넷에 HA 쌍을 구축하는 방법을 알아보십시오".

여러 대의 **AZs**에서 **HA** 쌍에 대한 요구 사항

추가 AWS 네트워킹 요구사항은 ZS(Multiple Availability Zones)를 사용하는 Cloud Volumes ONTAP HA 구성에 적용됩니다. 작업 환경을 생성할 때 BlueXP에 네트워킹 세부 정보를 입력해야 하므로 HA 쌍을 실행하기 전에 이러한 요구 사항을 검토해야 합니다.

HA 쌍의 작동 방식을 이해하려면 를 참조하십시오 "고가용성 쌍".

가용성 영역

이 HA 구축 모델은 여러 대의 AZs를 사용하여 데이터의 고가용성을 보장합니다. 각 Cloud Volumes ONTAP 인스턴스와 중재자 인스턴스에 전용 AZ를 사용해야 하며 HA 쌍 간의 통신 채널을 제공합니다.

각 가용성 영역에서 서브넷을 사용할 수 있어야 합니다.

NAS 데이터 및 클러스터**/SVM** 관리를 위한 부동 **IP** 주소

여러 AZs의 HA 구성에서는 장애가 발생할 경우 노드 간에 이동하는 부동 IP 주소를 사용합니다. 고객이 아니라면 VPC 외부에서 기본적으로 액세스할 수 없습니다 "AWS 전송 게이트웨이를 설정합니다".

하나의 부동 IP 주소는 클러스터 관리용, 하나는 노드 1의 NFS/CIFS 데이터용으로, 다른 하나는 노드 2의 NFS/CIFS 데이터용으로 사용됩니다. SVM 관리를 위한 네 번째 유동 IP 주소는 선택 사항입니다.

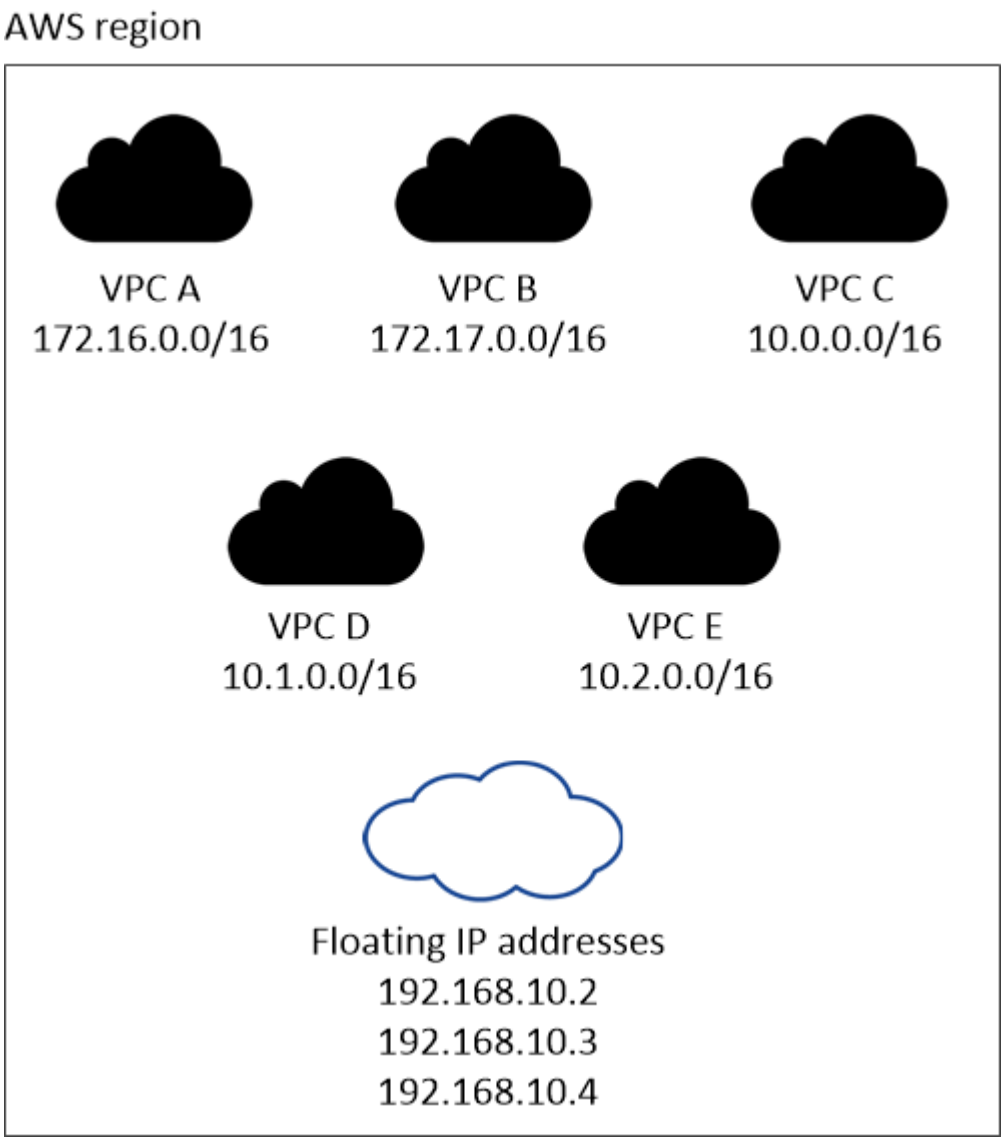
Windows용 SnapDrive 또는 HA 쌍을 지원하는 SnapCenter를 사용하는 경우 SVM 관리 LIF에는 부동 IP 주소가 필요합니다.

Cloud Volumes ONTAP HA 작업 환경을 생성할 때 BlueXP에서 부동 IP 주소를 입력해야 합니다. BlueXP는

시스템을 시작할 때 HA 쌍에 IP 주소를 할당합니다.

부동 IP 주소는 HA 구성을 배포하는 AWS 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 합니다. 유동 IP 주소를 해당 지역의 VPC 외부에 있는 논리적 서브넷으로 생각해 보십시오.

다음 예에서는 AWS 영역에 있는 VPC와 유동 IP 주소 간의 관계를 보여 줍니다. 부동 IP 주소는 모든 VPC에 대한 CIDR 블록 외부에 있지만 라우팅 테이블을 통해 서브넷으로 라우팅할 수 있습니다.



BlueXP는 VPC 외부의 클라이언트에서 iSCSI 액세스 및 NAS 액세스를 위해 정적 IP 주소를 자동으로 생성합니다. 이러한 유형의 IP 주소에 대한 요구 사항을 충족할 필요는 없습니다.

VPC 외부에서 유동 **IP** 액세스를 지원하는 전송 게이트웨이

필요한 경우 "AWS 전송 게이트웨이를 설정합니다" HA 쌍이 상주하는 VPC 외부에서 HA 쌍의 부동 IP 주소에 액세스할 수 있도록 합니다.

배관 테이블

BlueXP에서 부동 IP 주소를 지정한 후 부동 IP 주소에 대한 경로를 포함해야 하는 라우팅 테이블을 선택하라는 메시지가 표시됩니다. 이렇게 하면 클라이언트가 HA 쌍에 액세스할 수 있습니다.

VPC(주 경로 테이블)에 있는 서브넷을 위한 경로 테이블이 하나만 있는 경우 BlueXP는 해당 라우팅 테이블에 부동 IP 주소를 자동으로 추가합니다. 둘 이상의 라우트 테이블이 있는 경우 HA 쌍을 시작할 때 올바른 라우트 테이블을 선택하는 것이 매우 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP에 액세스하지 못할 수 있습니다.

예를 들어, 서로 다른 라우팅 테이블에 연결된 두 개의 서브넷이 있을 수 있습니다. 라우트 테이블 A를 선택했지만 라우트 테이블 B는 선택하지 않은 경우, 라우트 테이블 A와 연결된 서브넷에 있는 클라이언트는 HA 쌍에 액세스할 수 있지만, 라우트 테이블 B와 연결된 서브넷에 있는 클라이언트는 액세스할 수 없습니다.

라우팅 테이블에 대한 자세한 내용은 을 참조하십시오 "AWS 설명서: 경로 테이블".

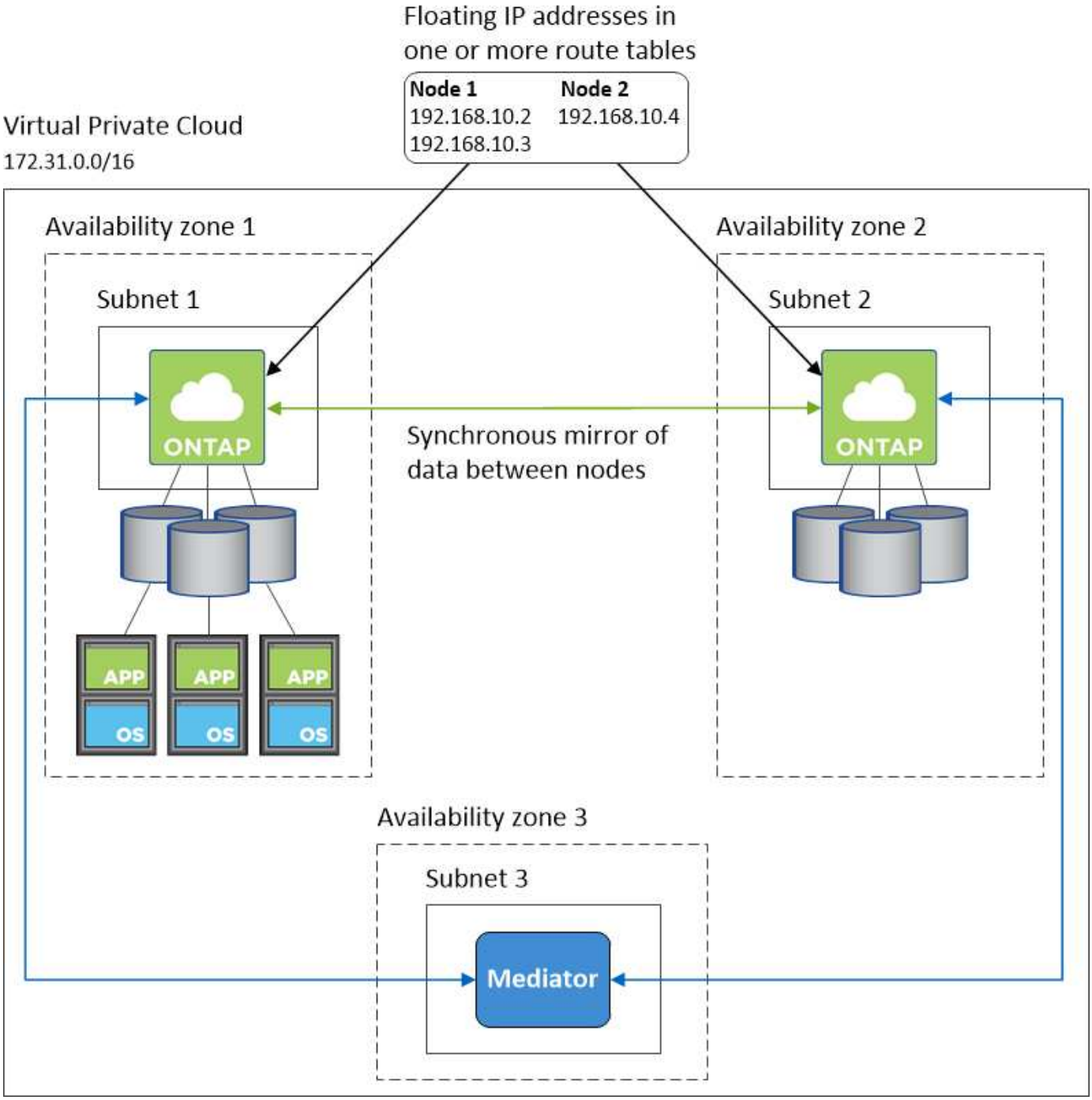
NetApp 관리 툴에 연결

여러 AZs에 있는 HA 구성에서 NetApp 관리 툴을 사용하려면 다음 두 가지 연결 옵션을 사용할 수 있습니다.

1. NetApp 관리 툴을 다른 VPC 및 에 구축할 수 있습니다 "AWS 전송 게이트웨이를 설정합니다". 게이트웨이를 사용하면 VPC 외부에서 클러스터 관리 인터페이스의 부동 IP 주소에 액세스할 수 있습니다.
2. NAS 클라이언트와 비슷한 라우팅 구성을 사용하여 동일한 VPC에 NetApp 관리 툴을 구축합니다.

HA 구성의 예

다음 그림에서는 여러 AZs의 HA 쌍, 즉 가용성 영역 3개, 서브넷 3개, 부동 IP 주소 및 라우팅 테이블과 같은 네트워크 구성 요소를 보여 줍니다.



커넥터 요구 사항

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

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

여러 **AZs**에서 **HA** 쌍에 대한 **AWS** 전송 게이트웨이 설정

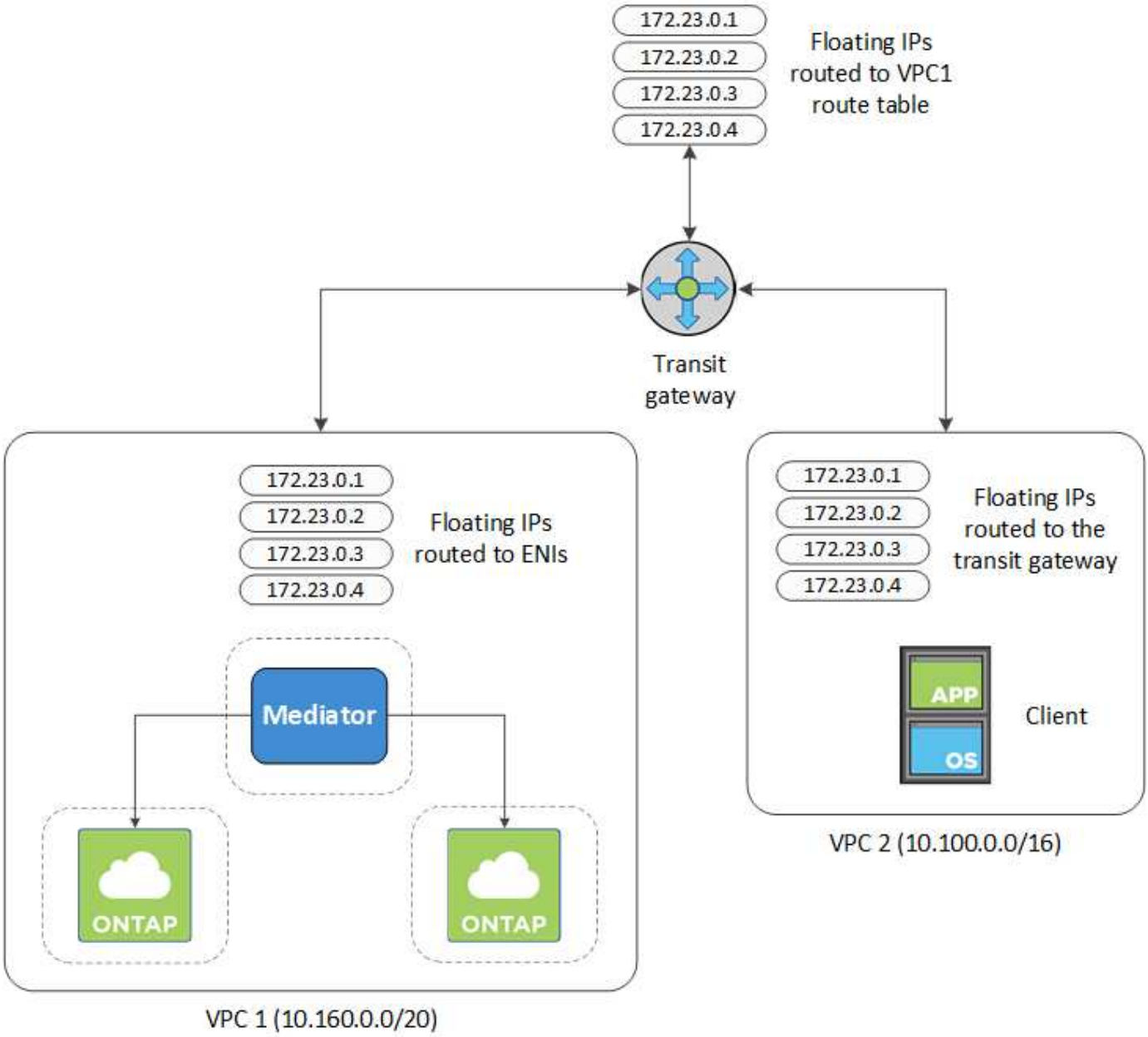
HA 쌍에 대한 액세스를 지원하는 AWS 전송 게이트웨이를 설정합니다 "유동 IP 주소" HA 쌍이 상주하는 VPC 외부에서

Cloud Volumes ONTAP HA 구성이 여러 AWS 가용성 영역에 분산되면 VPC 내에서 NAS 데이터 액세스에 유동 IP 주소가 필요합니다. 이러한 부동 IP 주소는 장애가 발생할 때 노드 간에 마이그레이션할 수 있지만 VPC 외부에서 기본적으로 액세스할 수 없습니다. 별도의 프라이빗 IP 주소를 통해 VPC 외부에서 데이터에 액세스할 수 있지만 자동 페일오버를 제공하지 않습니다.

클러스터 관리 인터페이스와 선택적 SVM 관리 LIF에도 부동 IP 주소가 필요합니다.

AWS 전송 게이트웨이를 설정한 경우 HA 쌍이 상주하는 VPC 외부의 유동 IP 주소에 액세스할 수 있습니다. 즉, VPC 외부에 있는 NAS 클라이언트와 NetApp 관리 툴이 유동 IP에 액세스할 수 있습니다.

다음은 전송 게이트웨이에 의해 연결된 두 대의 VPC를 보여 주는 예입니다. HA 시스템은 VPC 하나에 상주하고 클라이언트는 다른 VPC에 상주합니다. 그런 다음 부동 IP 주소를 사용하여 클라이언트에 NAS 볼륨을 마운트할 수 있습니다.

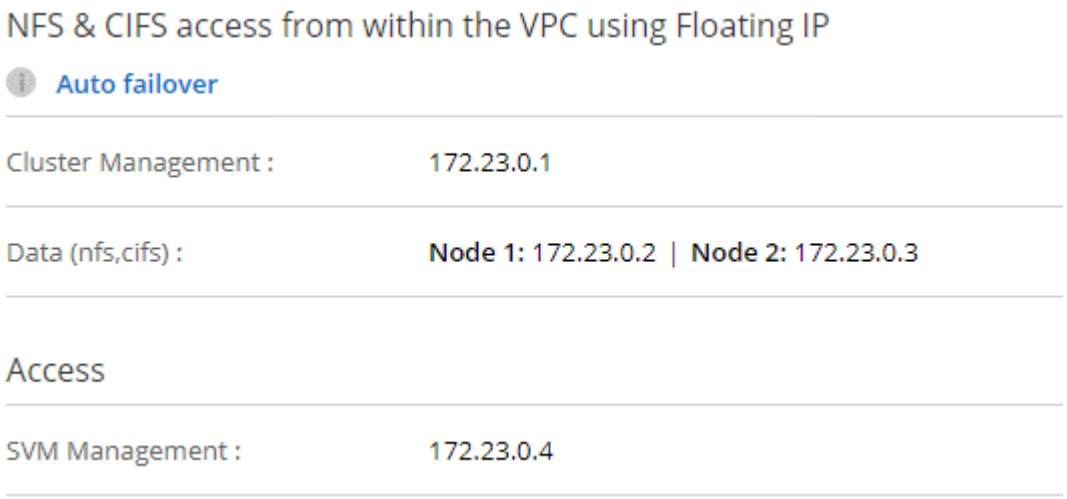


다음 단계에서는 유사한 구성을 설정하는 방법을 보여 줍니다.

단계

1. "전송 게이트웨이를 만들고 VPC를 게이트웨이에 연결합니다".
2. VPC를 전송 게이트웨이 경로 테이블에 연결합니다.
   a. VPC * 서비스에서 * Transit Gateway Route Tables * 를 클릭합니다.
   b. 라우팅 테이블을 선택합니다.
   c. 연결 * 을 클릭한 다음 * 연결 생성 * 을 선택합니다.
   d. 연결할 첨부 파일(VPC)을 선택한 다음 * 연결 생성 * 을 클릭합니다.
3. HA 쌍의 부동 IP 주소를 지정하여 전송 게이트웨이의 라우팅 테이블에서 경로를 만듭니다.

   BlueXP의 작업 환경 정보 페이지에서 부동 IP 주소를 찾을 수 있습니다. 예를 들면 다음과 같습니다.

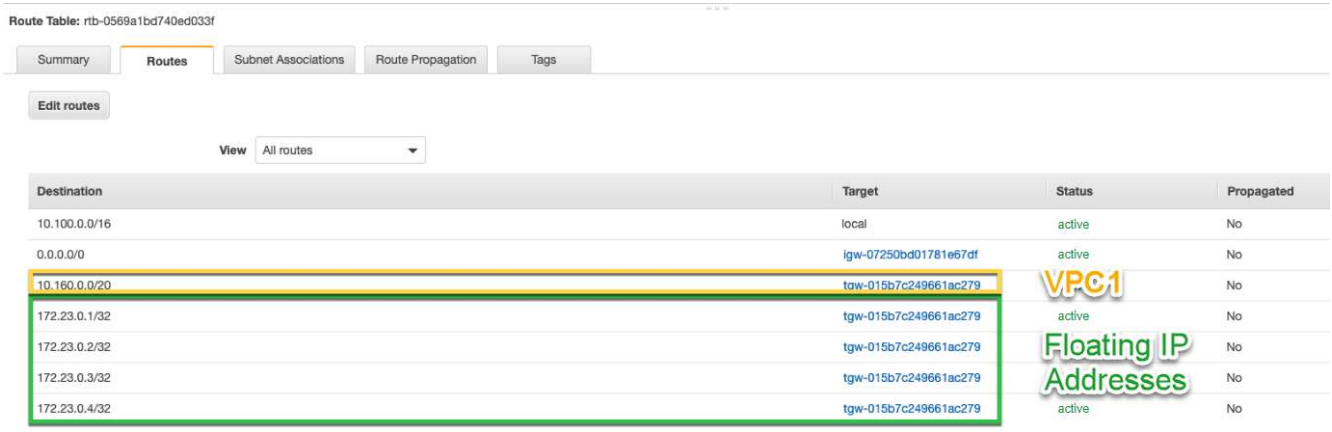


   다음 샘플 이미지는 전송 게이트웨이의 라우트 테이블을 보여 줍니다. 여기에는 2개의 VPC의 CIDR 블록에 대한 경로와 Cloud Volumes ONTAP에서 사용하는 4개의 부동 IP 주소가 포함됩니다.

4. 부동 IP 주소에 액세스해야 하는 VPC의 라우팅 테이블을 수정합니다.
   a. 부동 IP 주소에 라우트 항목을 추가합니다.

b. HA 쌍이 상주하는 VPC의 CIDR 블록에 경로 항목을 추가합니다.

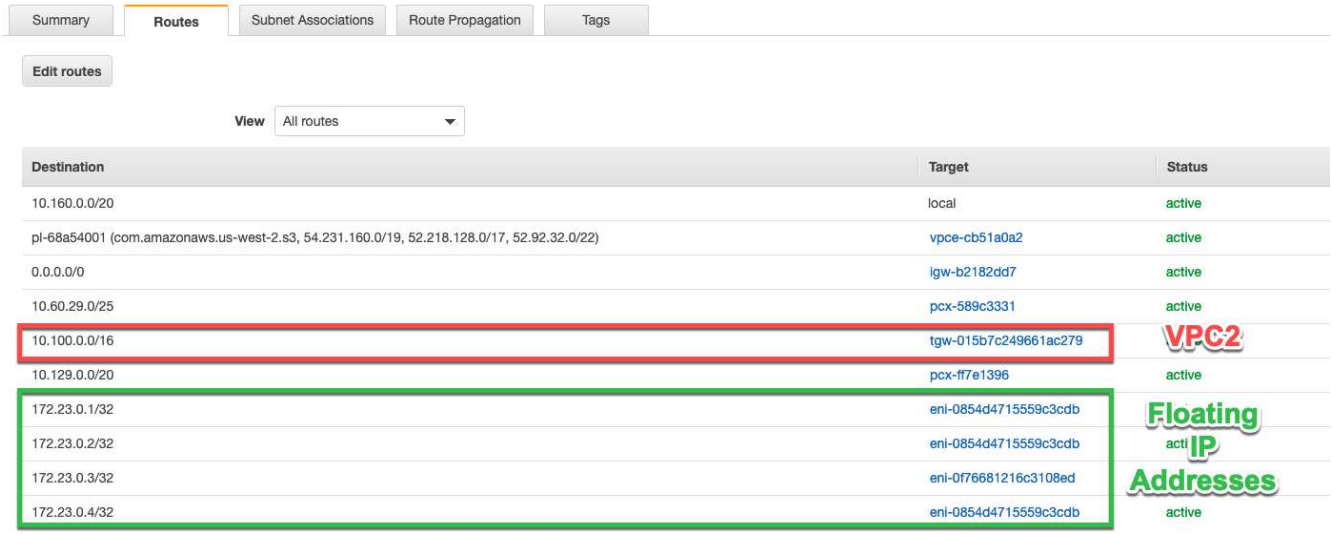
다음 샘플 이미지는 VPC 1에 대한 라우트 및 부동 IP 주소를 포함하는 VPC 2용 라우팅 테이블을 보여 줍니다.



5. 유동 IP 주소에 액세스해야 하는 VPC에 경로를 추가하여 HA 쌍 VPC의 경로 테이블을 수정합니다.

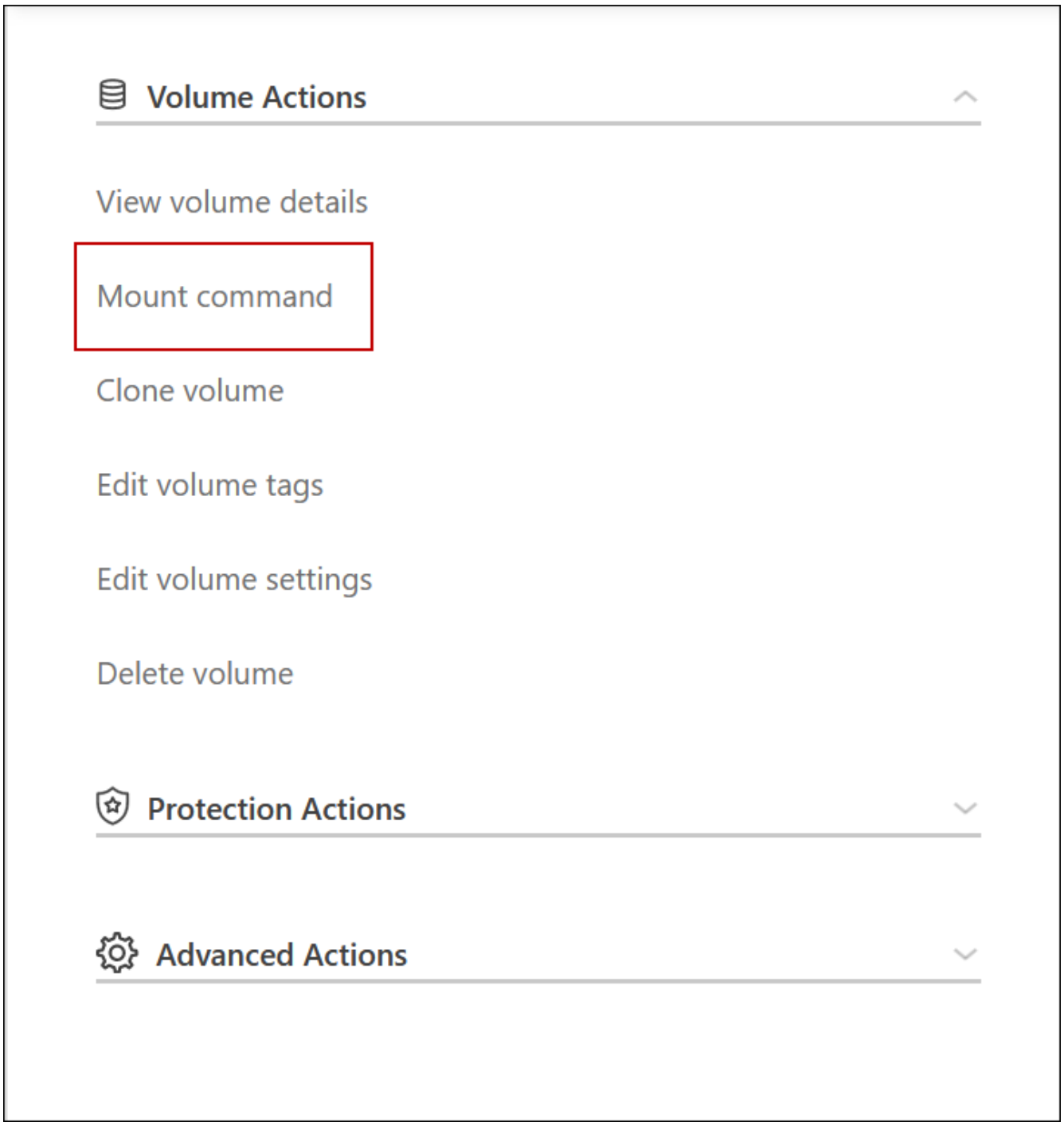
이 단계는 VPC 간 라우팅을 완료하기 때문에 중요합니다.

다음 샘플 이미지는 VPC 1의 라우트 테이블을 보여 줍니다. 여기에는 부동 IP 주소 및 클라이언트가 있는 VPC 2로의 라우트가 포함됩니다. BlueXP는 HA 쌍을 배포할 때 라우팅 테이블에 유동 IP를 자동으로 추가했습니다.



6. 부동 IP 주소를 사용하여 클라이언트에 볼륨을 마운트합니다.

BlueXP의 볼륨 관리 패널의 * 탑재 명령 * 옵션을 통해 BlueXP에서 올바른 IP 주소를 찾을 수 있습니다.



7. NFS 볼륨을 마운트하는 경우 클라이언트 VPC의 서브넷에 일치하도록 엑스포트 정책을 구성합니다.

   "볼륨을 편집하는 방법에 대해 알아봅니다".

   - 관련 링크 *
   - "AWS의 고가용성 쌍"
   - "AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항"

공유 서브넷에 **HA** 쌍 구축

9.11.1 릴리즈부터 VPC 공유를 지원하는 AWS에서 Cloud Volumes ONTAP HA 쌍이

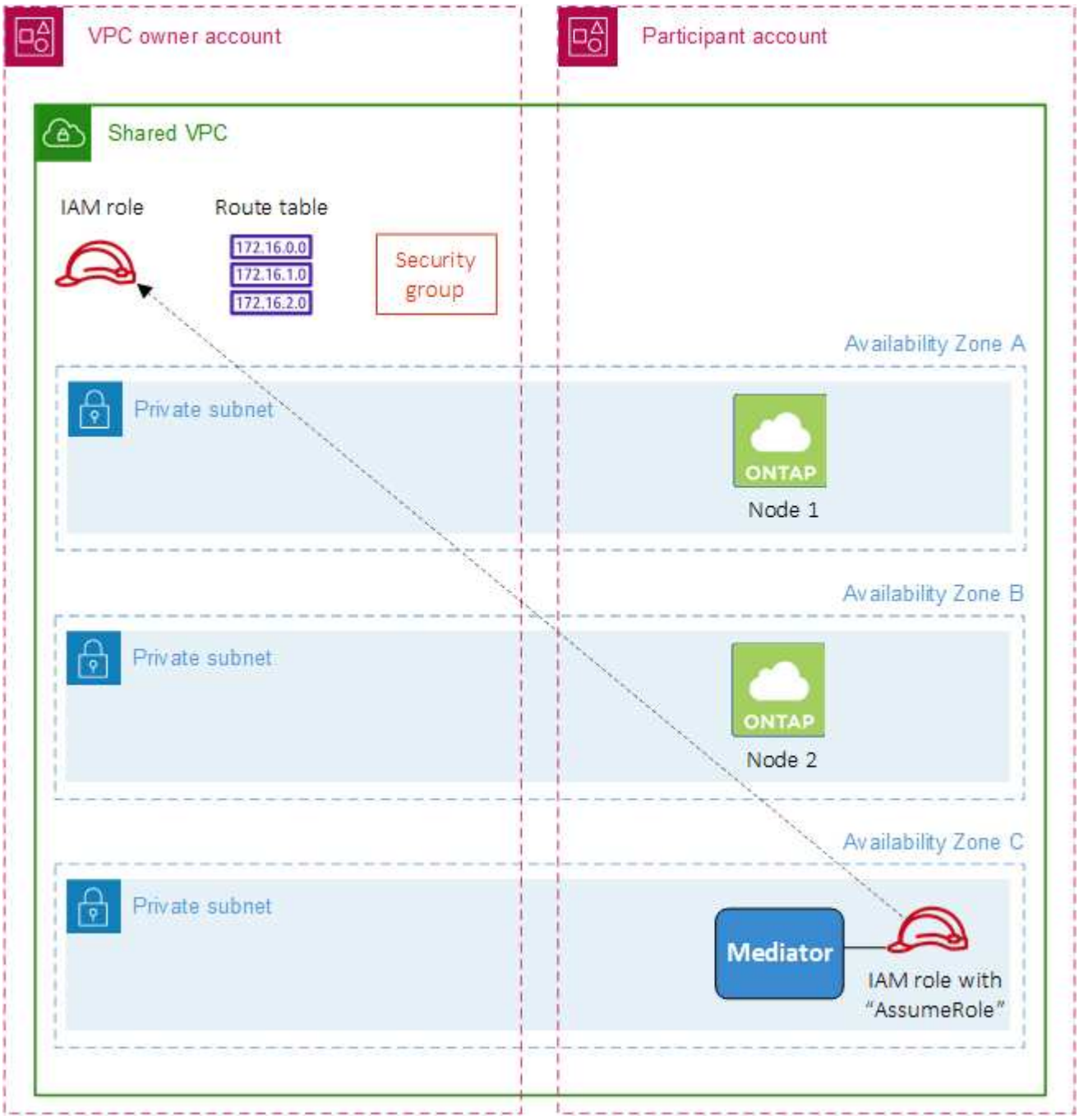
지원됩니다. VPC 공유를 사용하면 서브넷을 다른 AWS 계정과 공유할 수 있습니다. 이 구성을 사용하려면 AWS 환경을 설정한 다음 API를 사용하여 HA 쌍을 구축해야 합니다.

와 함께 "VPC 공유"Cloud Volumes ONTAP HA 구성은 다음 두 계정에 분산됩니다.

- 네트워킹을 소유하는 VPC 소유자 계정(VPC, 서브넷, 라우팅 테이블 및 Cloud Volumes ONTAP 보안 그룹)
- 참가자 계정으로, EC2 인스턴스가 공유 서브넷에 구축됩니다(여기에는 2개의 HA 노드와 중재자가 포함됨).

여러 가용성 영역에 배포된 Cloud Volumes ONTAP HA 구성의 경우 HA 중재자가 VPC 소유자 계정의 라우트 테이블에 쓸 수 있는 특정 권한이 필요합니다. 중재자가 추정할 수 있는 IAM 역할을 설정하여 이러한 권한을 제공해야 합니다.

다음 이미지는 이 구축과 관련된 구성 요소를 보여줍니다.



아래 단계에 설명된 대로 참가자 계정과 서브넷을 공유하고 VPC 소유자 계정에서 IAM 역할 및 보안 그룹을 만들어야 합니다.

Cloud Volumes ONTAP 작업 환경을 만들면 BlueXP는 자동으로 IAM 역할을 생성하여 중재자에 연결합니다. 이 역할은 HA 쌍과 연결된 경로 테이블을 변경하기 위해 VPC 소유자 계정에서 생성한 IAM 역할을 가정합니다.

단계

1. VPC 소유자 계정의 서브넷을 참가자 계정과 공유합니다.

   이 단계는 공유 서브넷에 HA 쌍을 구축하는 데 필요합니다.

   "AWS 설명서: 서브넷을 공유합니다"

2. VPC 소유자 계정에서 Cloud Volumes ONTAP용 보안 그룹을 생성합니다.

   "Cloud Volumes ONTAP의 보안 그룹 규칙을 참조하십시오". HA 중재자를 위한 보안 그룹을 만들 필요는 없습니다. BlueXP가 이러한 작업을 수행합니다.

3. VPC 소유자 계정에서 다음 권한이 포함된 IAM 역할을 생성합니다.

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. BlueXP API를 사용하여 새로운 Cloud Volumes ONTAP 작업 환경을 만듭니다.

   다음 필드를 지정해야 합니다.

   - "보안 그룹 ID"

     "securityGroupId" 필드는 VPC 소유자 계정에서 만든 보안 그룹을 지정해야 합니다(위의 2단계 참조).

   - "haParams" 개체의 "assumeRoleArn

     "assumeRoleArn" 필드에는 VPC 소유자 계정에서 만든 IAM 역할의 ARN이 포함되어야 합니다(위의 3단계 참조).

     예를 들면 다음과 같습니다.

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

+
"Cloud Volumes ONTAP API에 대해 자세히 알아보십시오"

AWS의 보안 그룹 규칙

BlueXP는 Cloud Volumes ONTAP의 성공적인 운영에 필요한 인바운드 및 아웃바운드 규칙을 포함하는 AWS 보안 그룹을 생성합니다. 테스트 목적으로 또는 자체 보안 그룹을 사용하려는 경우 포트를 참조할 수 있습니다.

Cloud Volumes ONTAP 규칙

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

인바운드 규칙

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

- * 선택한 VPC만 해당 *: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템용 VPC의 서브넷 범위와 커넥터가 상주하는 VPC의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다.
- * 모든 VPC *: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.

프로토콜	포트	목적
모든 ICMP	모두	인스턴스에 Ping을 수행 중입니다
HTTP	80	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTP 액세스
HTTPS	443	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 커넥터 및 HTTPS 액세스와의 연결
SSH를 클릭합니다	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다
TCP	111	NFS에 대한 원격 프로시저 호출
TCP	139	CIFS에 대한 NetBIOS 서비스 세션입니다
TCP	161-162	단순한 네트워크 관리 프로토콜
TCP	445	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
TCP	635	NFS 마운트
TCP	749	Kerberos
TCP	2049년	NFS 서버 데몬

프로토콜	포트	목적
TCP	3260입니다	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP	4045로 문의하십시오	NFS 잠금 데몬
TCP	4046으로 문의하십시오	NFS에 대한 네트워크 상태 모니터
TCP	10000	NDMP를 사용한 백업
TCP	11104를 참조하십시오	SnapMirror에 대한 인터클러스터 통신 세션의 관리
TCP	11105를 참조하십시오	인터클러스터 LIF를 사용하여 SnapMirror 데이터 전송
UDP입니다	111	NFS에 대한 원격 프로시저 호출
UDP입니다	161-162	단순한 네트워크 관리 프로토콜
UDP입니다	635	NFS 마운트
UDP입니다	2049년	NFS 서버 데몬
UDP입니다	4045로 문의하십시오	NFS 잠금 데몬
UDP입니다	4046으로 문의하십시오	NFS에 대한 네트워크 상태 모니터
UDP입니다	4049입니다	NFS rquotad 프로토콜

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.

프로토콜	포트	목적
모든 ICMP	모두	모든 아웃바운드 트래픽
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	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	프로토콜	포트	출처	목적지	목적
Active Directory를 클릭합니다	TCP	88을 참조하십시오	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니다	137입니다	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니다	138	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	TCP	139	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP 및 UDP	389	노드 관리 LIF	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	노드 관리 LIF	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	UDP입니다	464	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos 키 관리
	TCP	749	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(RPCSEC_GSS)
	TCP	88을 참조하십시오	데이터 LIF(NFS, CIFS, iSCSI)	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니다	137입니다	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니다	138	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	TCP	139	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP 및 UDP	389	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	UDP입니다	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos 키 관리
	TCP	749	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(RPCSEC_GSS)

서비스	프로토콜	포트	출처	목적지	목적
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
S3로 백업	TCP	5010입니다	인터클러스터 LIF	엔드포인트 백업 또는 복원	S3로 백업 기능의 백업 및 복원 작업
클러스터	모든 교통 정보	모든 교통 정보	모든 LIF가 하나의 노드에 있습니다	다른 노드의 모든 LIF	인터클러스터 통신(Cloud Volumes ONTAP HA에만 해당)
	TCP	3000입니다	노드 관리 LIF	HA 중재자	ZAPI 호출(Cloud Volumes ONTAP HA 전용)
	ICMP	1	노드 관리 LIF	HA 중재자	활성 상태 유지(Cloud Volumes ONTAP HA만 해당)
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	UDP입니다	68	노드 관리 LIF	DHCP를 선택합니다	처음으로 설정하는 DHCP 클라이언트
DHCPS	UDP입니다	67	노드 관리 LIF	DHCP를 선택합니다	DHCP 서버
DNS	UDP입니다	53	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	노드 관리 LIF	대상 서버	NDMP 복제
SMTP	TCP	25	노드 관리 LIF	메일 서버	AutoSupport에 사용할 수 있는 SMTP 경고
SNMP를 선택합니다	TCP	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니다	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	TCP	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니다	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링

서비스	프로토콜	포트	출처	목적지	목적
SnapMirror를 참조하십시오	TCP	11104를 참조하십시오	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror에 대한 인터클러스터 통신 세션의 관리
	TCP	11105를 참조하십시오	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror 데이터 전송
Syslog를 클릭합니다	UDP입니다	514	노드 관리 LIF	Syslog 서버	Syslog 메시지를 전달합니다

외부 보안 그룹의 **HA** 중재자를 위한 규칙

Cloud Volumes ONTAP HA 중재자를 위해 미리 정의된 외부 보안 그룹에는 다음과 같은 인바운드 및 아웃바운드 규칙이 포함됩니다.

인바운드 규칙

HA 중재자를 위해 미리 정의된 보안 그룹에는 다음과 같은 인바운드 규칙이 포함됩니다.

프로토콜	포트	출처	목적
TCP	3000입니다	커넥터의 CIDR	Connector에서 Restful API 액세스

아웃바운드 규칙

HA 중재자를 위한 사전 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

HA 중재자를 위해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

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

고급 아웃바운드 규칙

아웃바운드 트래픽에 대한 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 HA 중재자의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

프로토콜	포트	목적지	목적
HTTP	80	AWS EC2 인스턴스에 있는 Connector의 IP 주소입니다	중재자를 위한 업그레이드 다운로드

프로토콜	포트	목적지	목적
HTTPS	443	ec2.amazonaws.com	스토리지 페일오버 지원
UDP입니다	53	ec2.amazonaws.com	스토리지 페일오버 지원

포트 443과 53을 열지 않고 타겟 서브넷에서 AWS EC2 서비스로 인터페이스 VPC 엔드포인트를 생성할 수 있습니다.

HA 구성 내부 보안 그룹에 대한 규칙입니다

Cloud Volumes ONTAP HA 구성에 대해 미리 정의된 내부 보안 그룹에는 다음 규칙이 포함됩니다. 이 보안 그룹은 HA 노드와 중재자 및 노드 간의 통신을 지원합니다.

BlueXP는 항상 이 보안 그룹을 만듭니다. 자신의 을(를) 사용할 수 있는 옵션이 없습니다.

인바운드 규칙

미리 정의된 보안 그룹에는 다음과 같은 인바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 교통 정보	모두	HA 중재자 및 HA 노드 간 통신

아웃바운드 규칙

미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 교통 정보	모두	HA 중재자 및 HA 노드 간 통신

커넥터 규칙

"Connector에 대한 보안 그룹 규칙을 봅니다"

AWS KMS 설정

Cloud Volumes ONTAP에서 Amazon 암호화를 사용하려면 AWS KMS(키 관리 서비스)를 설정해야 합니다.

단계

1. 활성 CMK(Customer Master Key)가 있는지 확인합니다.

   CMK는 AWS로 관리되는 CMK 또는 고객이 관리하는 CMK가 될 수 있습니다. BlueXP 및 Cloud Volumes ONTAP와 동일한 AWS 계정 또는 다른 AWS 계정에 있을 수 있습니다.

   "AWS 설명서:CMK(Customer Master Key)"

2. BlueXP에 대한 권한을 제공하는 IAM 역할을 _KEY USER_로 추가하여 각 CMK에 대한 키 정책을 수정합니다.

IAM 역할을 주요 사용자로 추가하면 BlueXP에서 Cloud Volumes ONTAP와 함께 CMK를 사용할 수 있는 권한이 부여됩니다.

"AWS 설명서:키 편집"

3. CMK가 다른 AWS 계정에 있는 경우 다음 단계를 수행하십시오.

   a. CMK가 상주하는 계정에서 KMS 콘솔로 이동합니다.

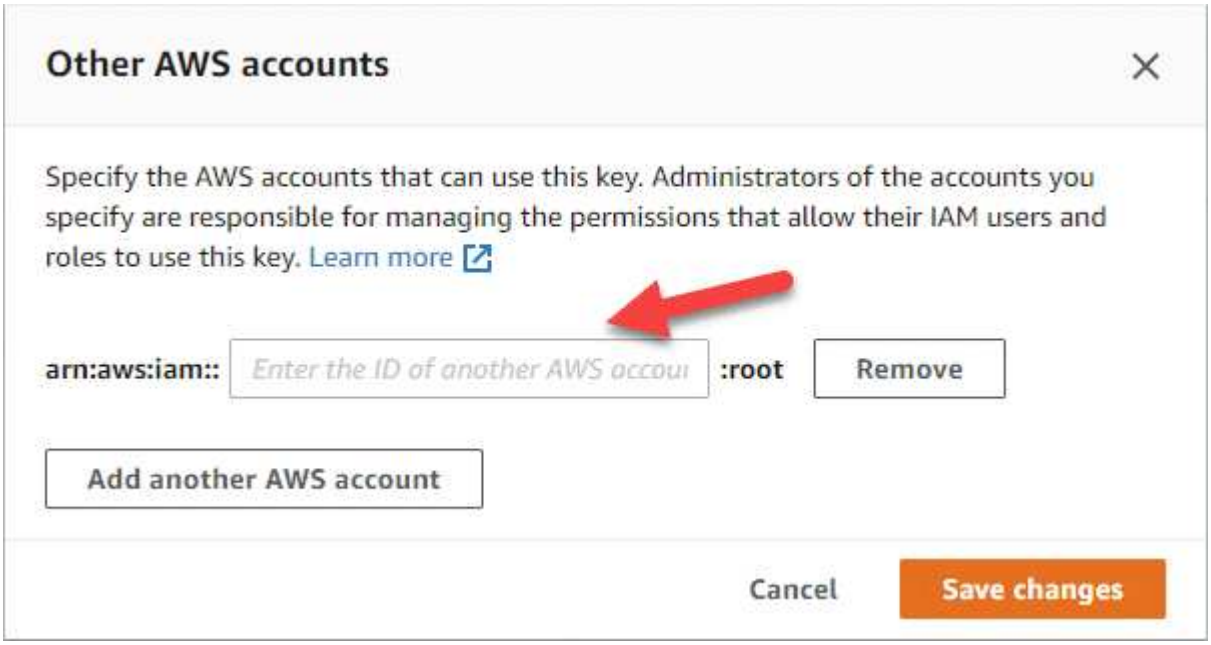
   b. 키를 선택합니다.

   c. General configuration * 창에서 키의 ARN을 복사합니다.

      Cloud Volumes ONTAP 시스템을 생성할 때 ARN을 BlueXP에 제공해야 합니다.

   d. 다른 AWS 계정 * 창에서 BlueXP에 사용 권한을 제공하는 AWS 계정을 추가합니다.

      대부분의 경우 이 계정은 BlueXP가 있는 계정입니다. BlueXP가 AWS에 설치되어 있지 않은 경우 BlueXP에 AWS 액세스 키를 제공한 계정이 됩니다.



   e. 이제 BlueXP에 사용 권한을 제공하고 IAM 콘솔을 여는 AWS 계정으로 전환합니다.

   f. 아래에 나열된 권한을 포함하는 IAM 정책을 생성합니다.

   g. BlueXP에 대한 권한을 제공하는 IAM 역할 또는 IAM 사용자에게 정책을 첨부합니다.

      다음 정책은 BlueXP가 외부 AWS 계정에서 CMK를 사용하는 데 필요한 권한을 제공합니다. "리소스" 섹션에서

지역 및 계정 ID를 수정해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
이 프로세스에 대한 자세한 내용은 을 참조하십시오 "AWS 설명서: 다른 계정의 사용자가 KMS 키를 사용할 수 있도록 허용합니다".

4. 고객이 관리하는 CMK를 사용하는 경우 Cloud Volumes ONTAP IAM 역할을 _KEY USER_로 추가하여 CMK에

대한 주요 정책을 수정합니다.

이 단계는 Cloud Volumes ONTAP에서 데이터 계층화를 활성화한 경우 S3 버킷에 저장된 데이터를 암호화하려는 경우에 필요합니다.

작업 환경을 생성할 때 IAM 역할이 생성되므로 이 단계는 _ After _ Cloud Volumes ONTAP를 구축해야 합니다. (물론 기존 Cloud Volumes ONTAP IAM 역할을 사용할 수 있는 옵션이 있으므로 이 단계를 이전에 수행할 수 있습니다.)

"AWS 설명서:키 편집"

Cloud Volumes ONTAP에 대한 IAM 역할을 설정합니다

필요한 권한이 있는 IAM 역할은 각 Cloud Volumes ONTAP 노드에 연결되어야 합니다. HA 중재자의 경우도 마찬가지입니다. BlueXP에서 IAM 역할을 생성하는 것이 가장 쉽지만 자신의 역할을 사용할 수 있습니다.

이 작업은 선택 사항입니다. Cloud Volumes ONTAP 작업 환경을 생성할 때 기본 옵션은 BlueXP에서 IAM 역할을 생성할 수 있도록 하는 것입니다. 보안 정책에 따라 IAM 역할을 직접 생성해야 하는 경우 다음 단계를 따르십시오.

AWS 상용 클라우드 서비스 환경에서는 IAM의 역할을 직접 제공해야 합니다. "C2S에 Cloud Volumes ONTAP를 배포하는 방법을 알아보십시오".

단계

1. AWS IAM 콘솔로 이동합니다.
2. 다음 권한을 포함하는 IAM 정책을 생성합니다.
    - Cloud Volumes ONTAP 노드에 대한 기본 정책입니다

표준 영역

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud(미국) 지역

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

C2S 환경

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Cloud Volumes ONTAP 노드의 백업 정책

  Cloud Volumes ONTAP 시스템에서 BlueXP 백업 및 복구를 사용하려는 경우 노드에 대한 IAM 역할에 아래에 나와 있는 두 번째 정책이 포함되어야 합니다.

표준 영역

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud(미국) 지역

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

C2S 환경

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- HA 중재자

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
                "sts:AssumeRole"
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. IAM 역할을 생성하고 생성한 정책을 역할에 연결합니다.

결과

이제 새로운 Cloud Volumes ONTAP 작업 환경을 생성할 때 선택할 수 있는 IAM 역할이 있습니다.

추가 정보

- "AWS 설명서: IAM 정책 생성"
- "AWS 설명서: IAM 역할 생성"

AWS에서 Cloud Volumes ONTAP에 대한 라이센스 설정

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".

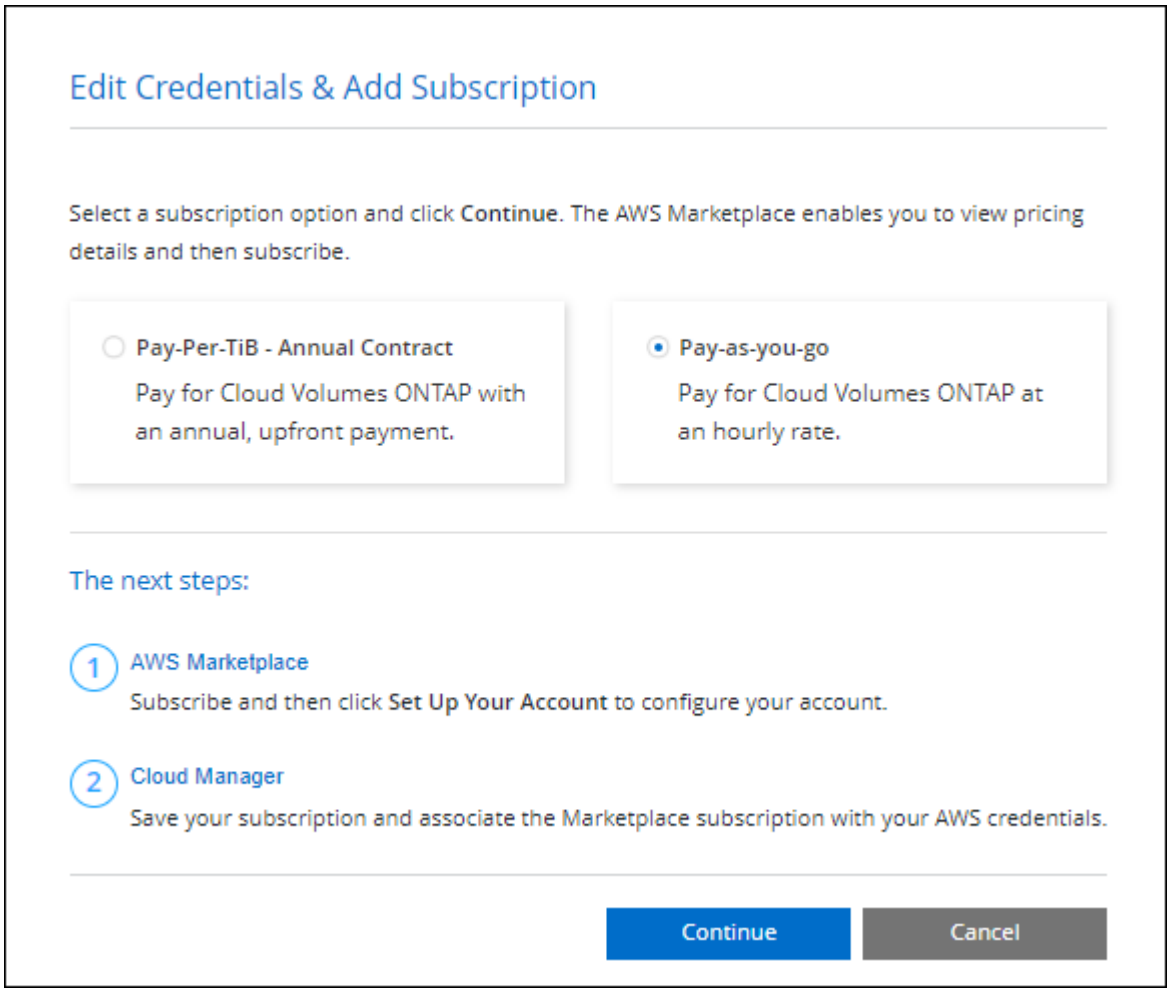
단계

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

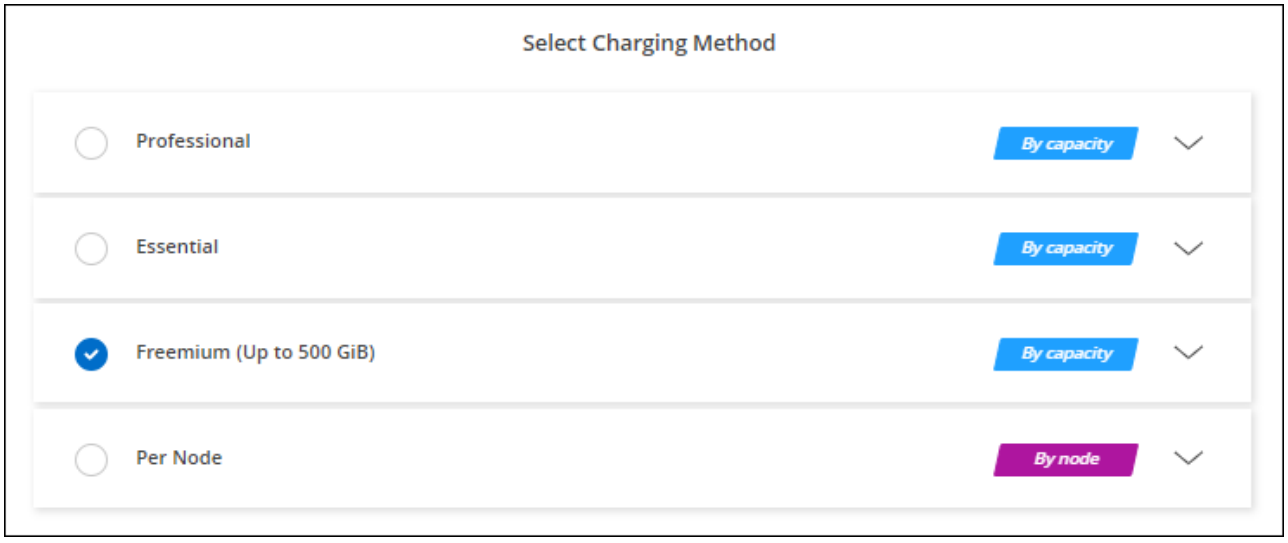
    a. Details and Credentials * 페이지에서 * 자격 증명 편집 > 구독 추가 * 를 클릭한 다음 표시되는 메시지에 따라

AWS Marketplace에서 선불 종량제 오퍼링을 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.



"AWS에서 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
- AWS Marketplace에서 PAYGO(Pay-as-you-go) 방식으로 구독을 지원합니다
- AWS Marketplace에서 연간 계약 체결

"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"

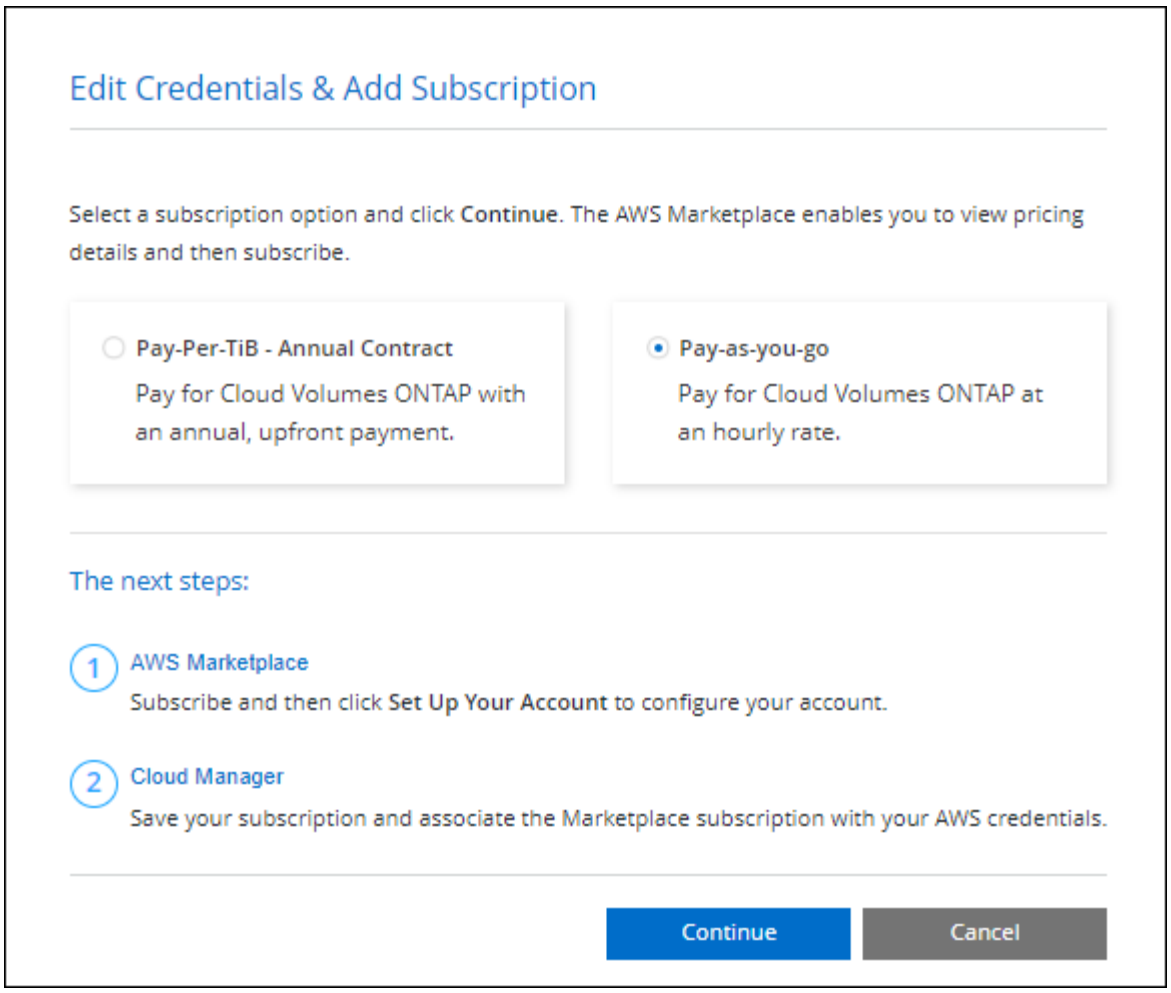
   BlueXP는 NetApp의 라이센스 서비스에 자동으로 쿼리하여 NetApp Support 사이트 계정과 관련된 라이센스에 대한 자세한 정보를 확인합니다. 오류가 없으면 BlueXP는 자동으로 디지털 지갑에 라이센스를 추가합니다.

   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".

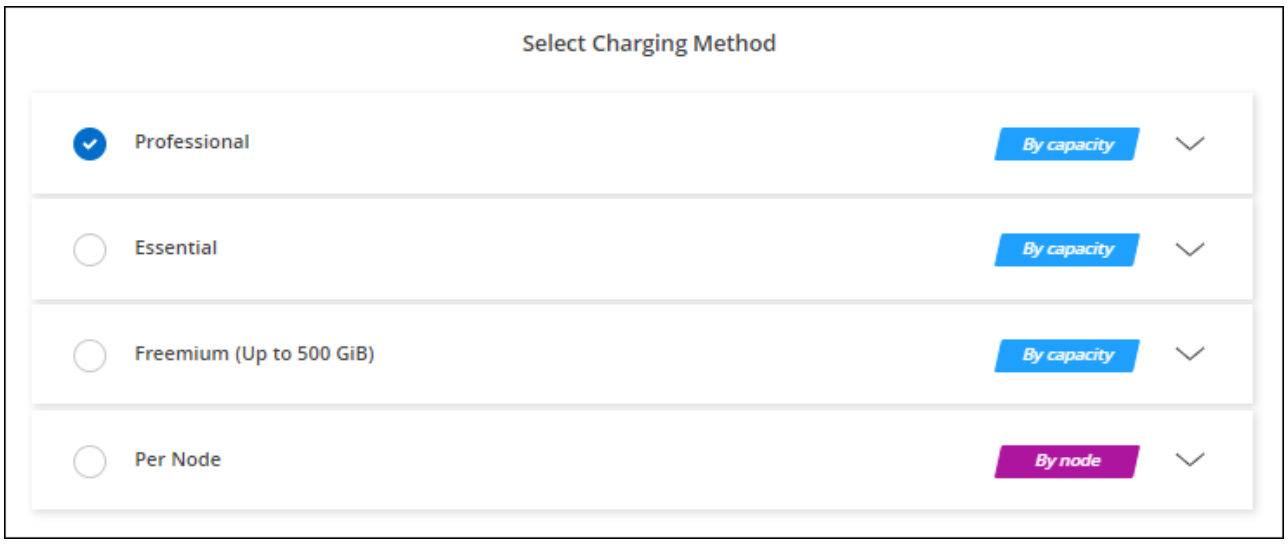
3. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 BlueXP의 단계를 따릅니다.

   a. Details and Credentials * 페이지에서 * 자격 증명 편집 > 구독 추가 * 를 클릭한 다음 표시되는 메시지에 따라 AWS Marketplace에서 선불 종량제 오퍼링을 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.



"AWS에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".

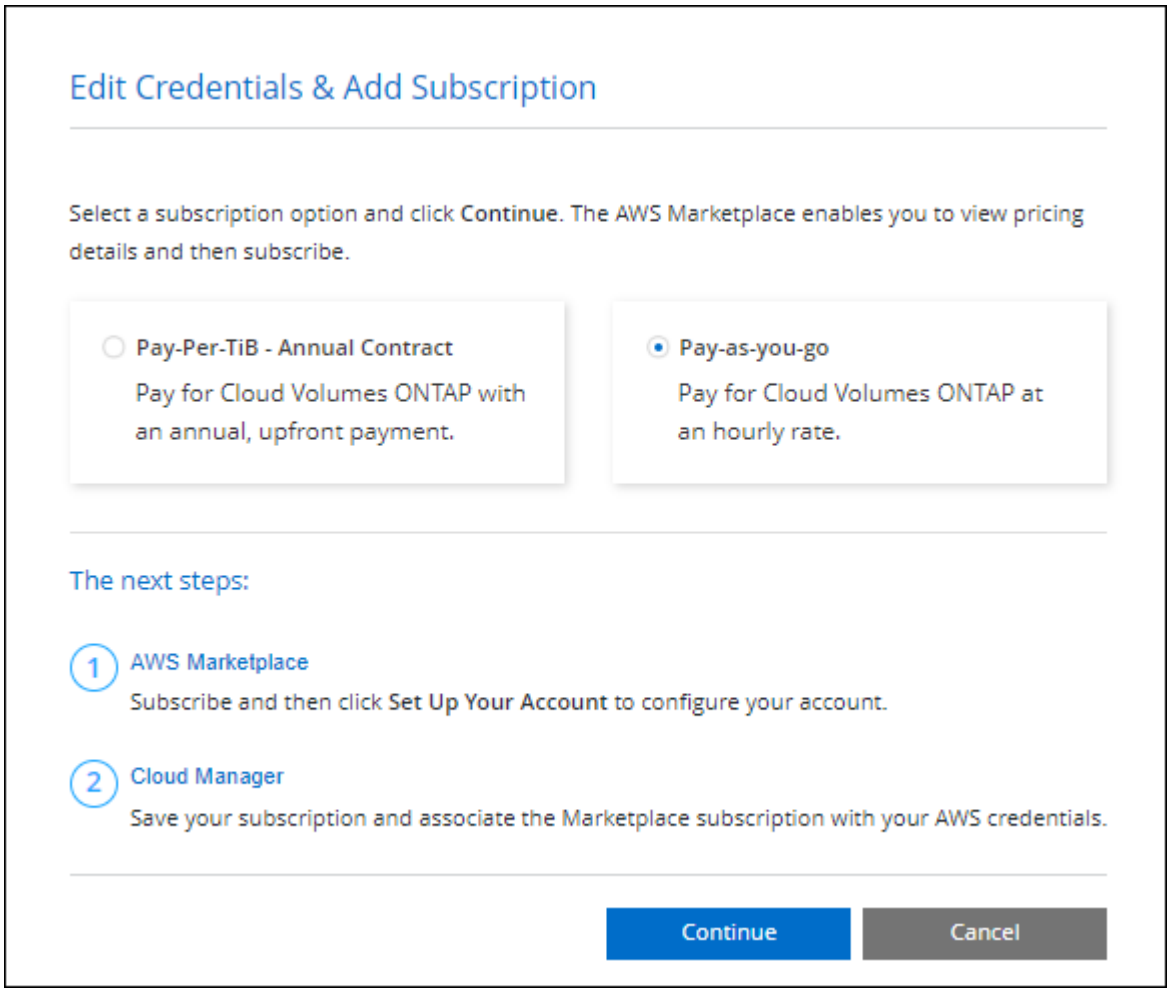
PAYGO 구독

클라우드 공급자 마켓플레이스의 서비스에 가입하여 시간별 비용 지불

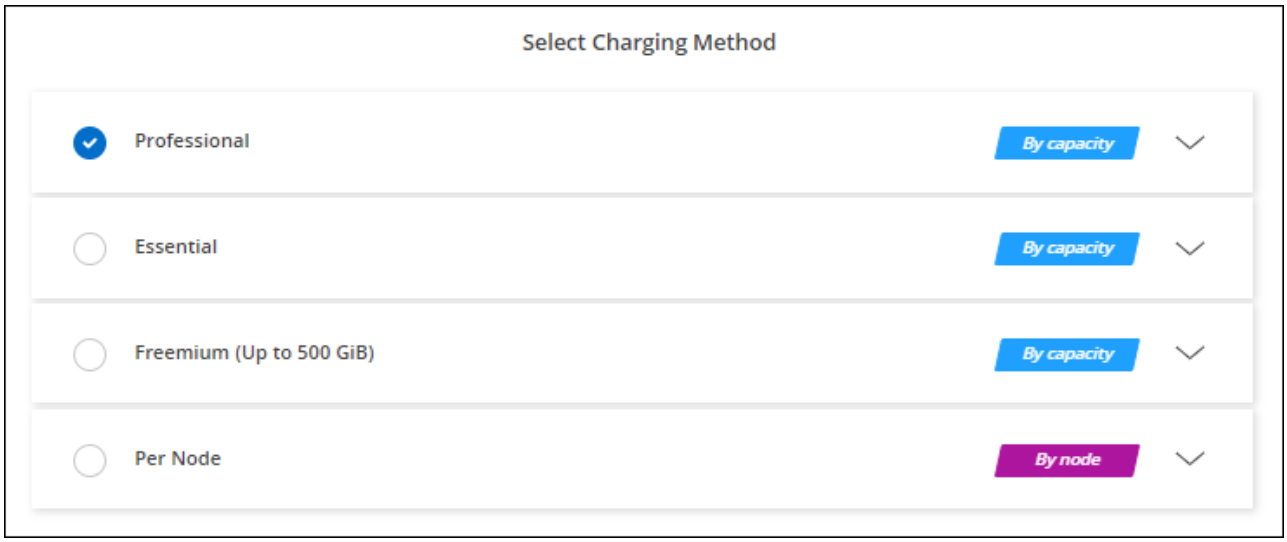
Cloud Volumes ONTAP 작업 환경을 생성할 때 BlueXP는 AWS Marketplace에서 사용 가능한 계약을 구독하라는 메시지를 표시합니다. 그러면 해당 구독이 충전을 위한 작업 환경과 연결됩니다. 추가 작업 환경에 동일한 서브스크립션을 사용할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 * Storage > Canvas * 를 선택합니다.
2. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 BlueXP의 단계를 따릅니다.
   a. Details and Credentials * 페이지에서 * 자격 증명 편집 > 구독 추가 * 를 클릭한 다음 표시되는 메시지에 따라 AWS Marketplace에서 선불 종량제 오퍼링을 구독합니다.



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



"AWS에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".

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

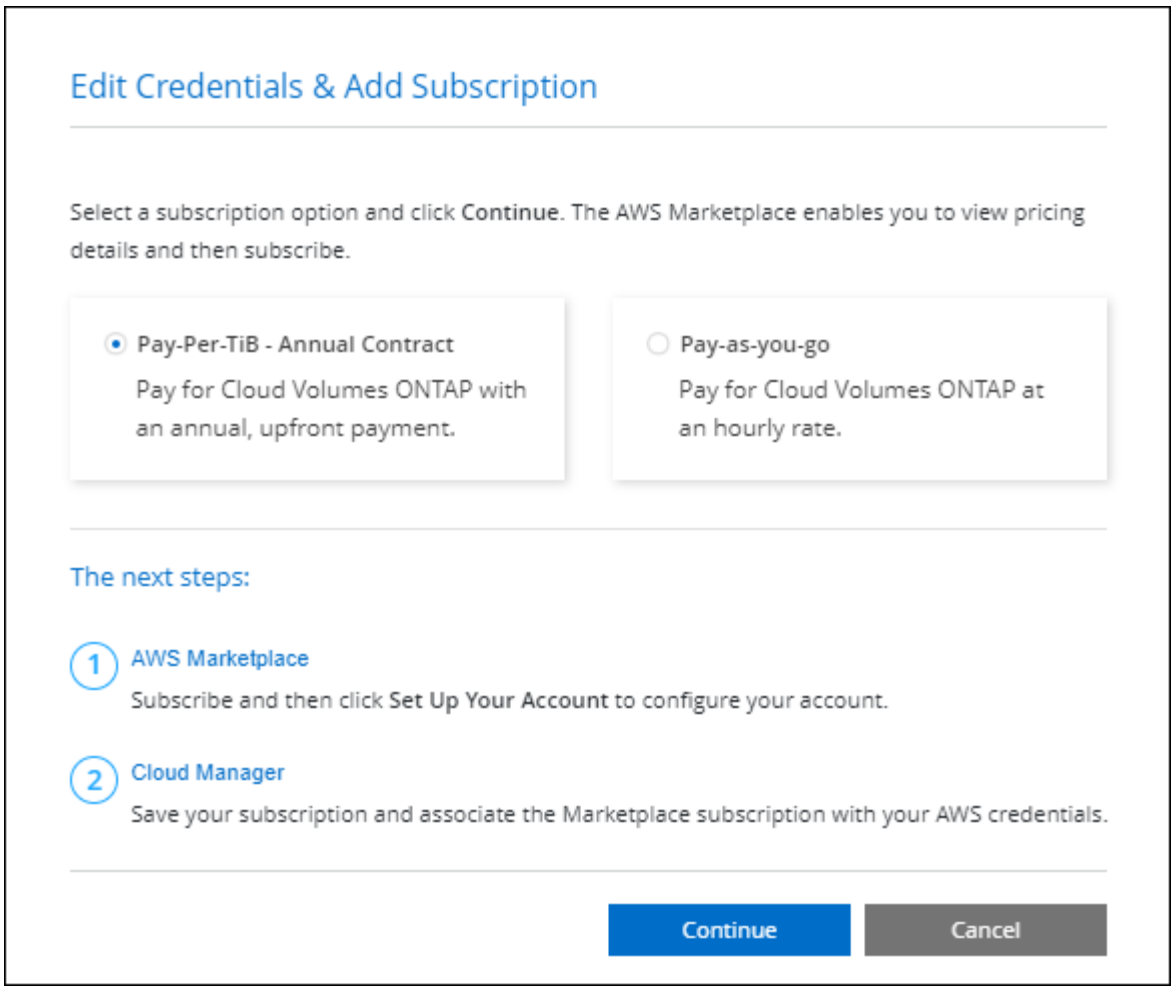
연간 계약

클라우드 공급자 마켓플레이스에서 연간 계약을 구매하여 연간 지불

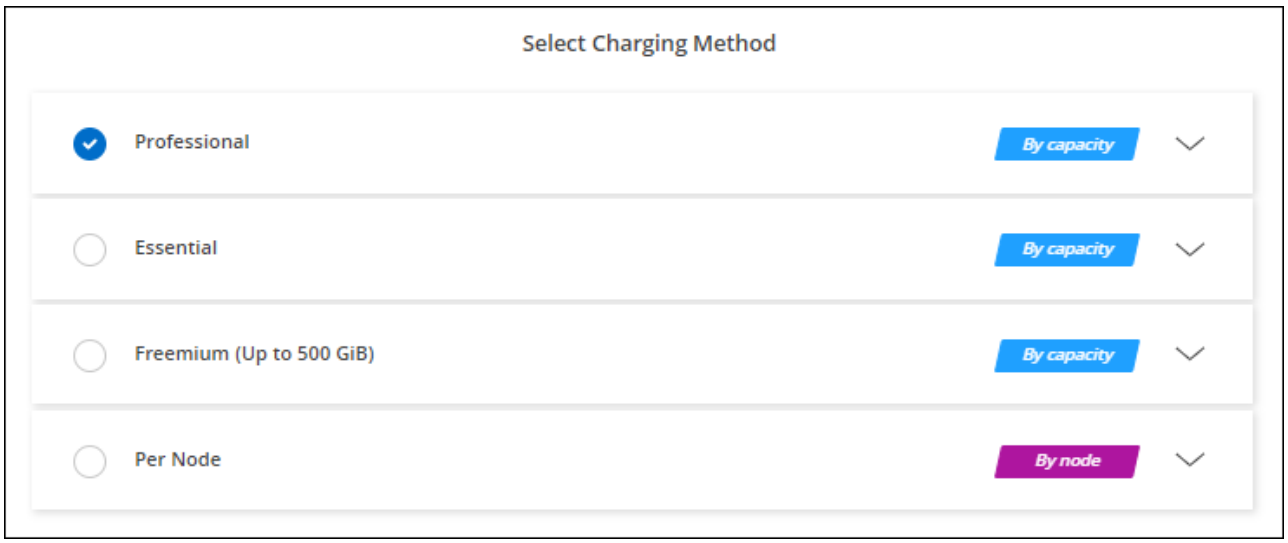
시간별 구독과 마찬가지로, BlueXP는 AWS 마켓플레이스에서 사용 가능한 연간 계약을 구독하라는 메시지를 표시합니다.

단계

1. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 BlueXP의 단계를 따릅니다.
   a. Details and Credentials * 페이지에서 * 자격 증명 편집 > 구독 추가 * 를 클릭한 다음 표시되는 메시지에 따라 AWS Marketplace에서 연간 계약을 구독합니다.



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



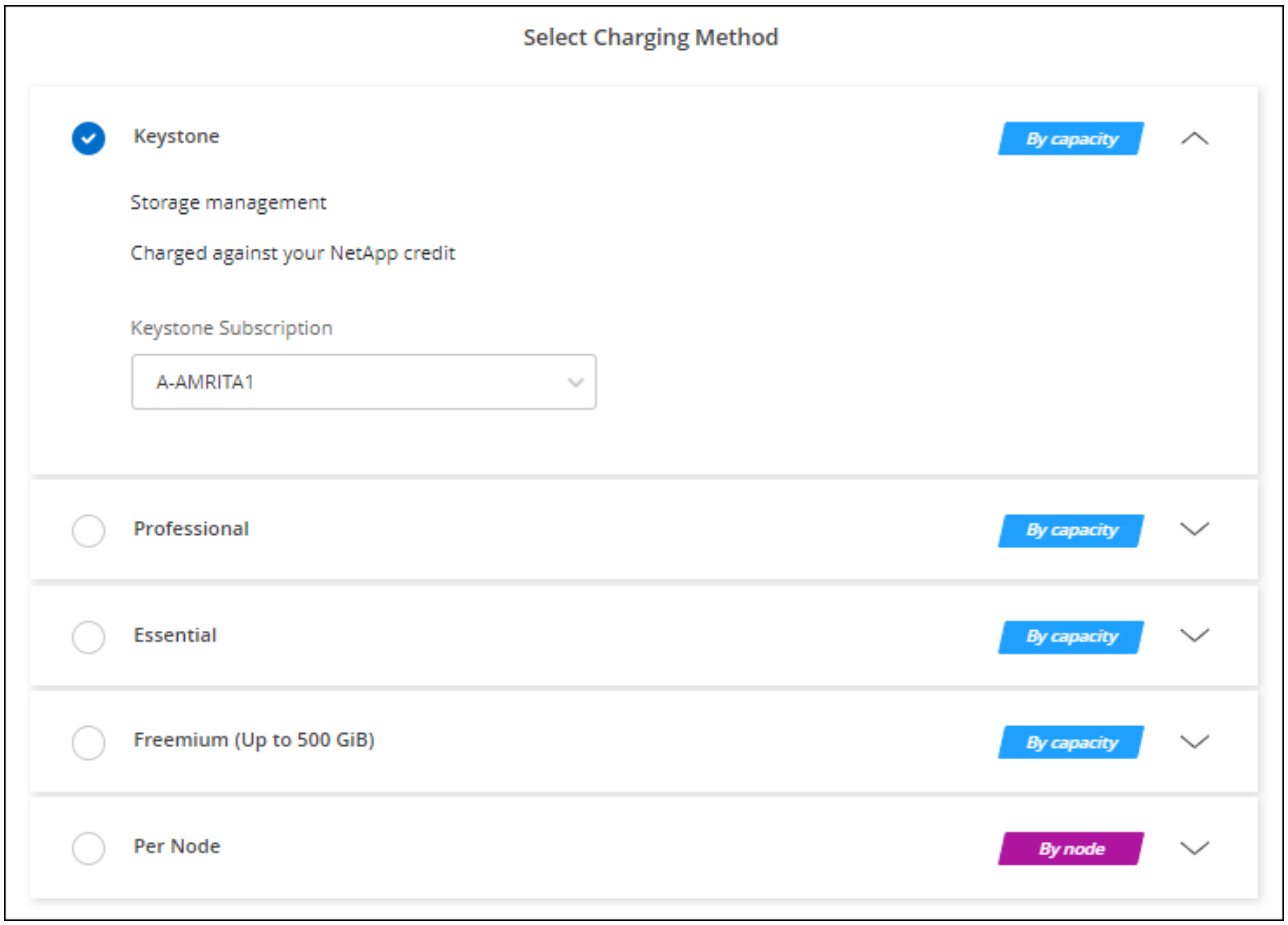
"AWS에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".

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.



"AWS에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".

AWS에서 Cloud Volumes ONTAP 실행

Cloud Volumes ONTAP는 단일 시스템 구성에서 실행하거나 AWS에서 HA 쌍으로 실행할 수 있습니다.

시작하기 전에

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 AWS 네트워킹 정보를 받아 준비해야 합니다. 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP 구성 계획".

- Cloud Volumes ONTAP에 대한 라이센스 설정에 필요한 사항을 이해합니다.

  "라이센스 설정 방법에 대해 알아보십시오".

- CIFS 구성을 위한 DNS 및 Active Directory

  자세한 내용은 을 참조하십시오 "AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항".

AWS에서 단일 노드 **Cloud Volumes ONTAP** 시스템 시작

AWS에서 Cloud Volumes ONTAP를 실행하려면 BlueXP에서 새로운 작업 환경을 만들어야 합니다

이 작업에 대해

작업 환경을 생성한 직후 BlueXP는 지정된 VPC에서 테스트 인스턴스를 시작하여 연결을 확인합니다. 성공하면 즉시 BlueXP가 인스턴스를 종료한 다음 Cloud Volumes ONTAP 시스템 배포를 시작합니다. BlueXP에서 연결을 확인할 수 없는 경우 작업 환경 생성이 실패합니다. 테스트 인스턴스는 T2.nano(기본 VPC 테넌시의 경우) 또는 m3.medium(전용 VPC 테넌시의 경우)입니다.

단계

1. 왼쪽 탐색 메뉴에서 * Storage > Canvas * 를 선택합니다.
2. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 화면의 지시를 따릅니다.
3. * 위치 선택 *: * 아마존 웹 서비스 * 및 * Cloud Volumes ONTAP 단일 노드 * 를 선택합니다.
4. 메시지가 표시되면 "커넥터를 작성합니다".
5. * 세부 정보 및 자격 증명 *: AWS 자격 증명과 구독을 선택적으로 변경하고, 작업 환경 이름을 입력하고, 필요한 경우 태그를 추가한 다음 암호를 입력합니다.

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

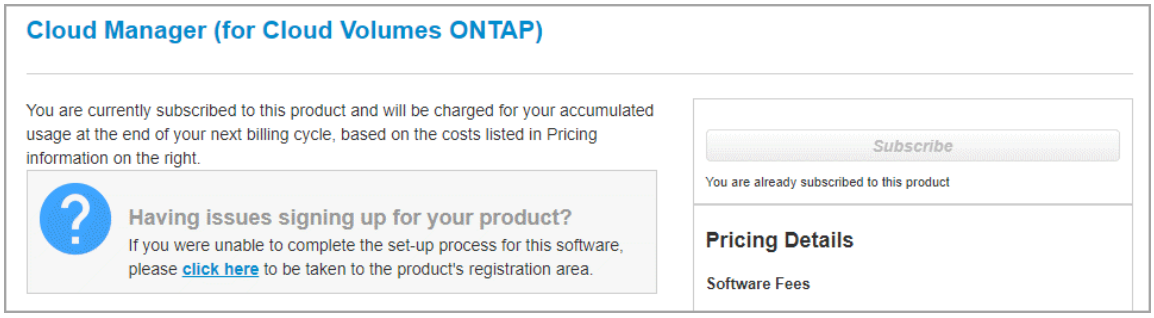
필드에 입력합니다	설명
작업 환경 이름	BlueXP는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Amazon EC2 인스턴스 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
태그 추가	AWS 태그는 AWS 리소스에 대한 메타데이터입니다. BlueXP는 Cloud Volumes ONTAP 인스턴스 및 인스턴스와 연관된 각 AWS 리소스에 태그를 추가합니다. 작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 생성된 후에는 더 많은 태그를 추가할 수 있습니다. API는 작업 환경을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 자세한 내용은 을 참조하십시오 "AWS 문서: Amazon EC2 리소스에 태그 달기".

필드에 입력합니다	설명
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 시스템을 구축할 계정과 연결된 AWS 자격 증명을 선택합니다. AWS Marketplace 구독을 연결하여 이 Cloud Volumes ONTAP 시스템에 사용할 수도 있습니다. 선택한 자격 증명을 새 AWS Marketplace 구독에 연결하려면 * Add Subscription * 을 클릭합니다. 이 구독은 연간 계약을 기준으로 하거나 시간당 요율로 Cloud Volumes ONTAP에 대한 비용을 지불할 수 있습니다. "BlueXP에 AWS 자격 증명을 추가하는 방법에 대해 알아보십시오".

다음 비디오에서는 용량제 마켓플레이스 구독을 AWS 자격 증명에 연결하는 방법을 보여줍니다.

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

여러 IAM 사용자가 동일한 AWS 계정으로 작업하는 경우 각 사용자는 가입해야 합니다. 첫 번째 사용자가 구독한 후 AWS Marketplace는 아래 이미지에 표시된 것처럼 후속 사용자에게 이미 구독했음을 알립니다. AWS_ACCOUNT_에 가입되어 있는 동안 각 IAM 사용자는 자신을 해당 구독과 연결해야 합니다. 아래 메시지가 표시되면 * 여기를 클릭 * 링크를 클릭하여 BlueXP 웹 사이트로 이동하여 프로세스를 완료합니다.



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. * 위치 및 연결 *: 에 기록한 네트워크 정보를 입력합니다 "AWS 워크시트".

   다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
VPC	AWS 아웃포스트가 있는 경우 아웃포스트 VPC를 선택하여 해당 아웃포스트에 단일 노드 Cloud Volumes ONTAP 시스템을 구축할 수 있습니다. 이러한 경험은 AWS에 상주하는 다른 VPC와 동일합니다.

필드에 입력합니다	설명
보안 그룹을 생성했습니다	BlueXP에서 보안 그룹을 생성하도록 하면 트래픽을 허용하는 방법을 선택해야 합니다. • 선택한 VPC 전용 * 을 선택한 경우 인바운드 트래픽의 소스는 선택한 VPC의 서브넷 범위와 커넥터가 상주하는 VPC의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다. • 모든 VPC * 를 선택한 경우 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
기존 보안 그룹을 사용합니다	기존 방화벽 정책을 사용하는 경우 필수 규칙이 포함되어 있는지 확인합니다. "Cloud Volumes ONTAP의 방화벽 규칙에 대해 알아보십시오".

8. * 데이터 암호화 *: 데이터 암호화 또는 AWS로 관리되는 암호화를 선택하지 않습니다.

   AWS로 관리되는 암호화의 경우 사용자 계정 또는 다른 AWS 계정에서 다른 CMK(Customer Master Key)를 선택할 수 있습니다.

   Cloud Volumes ONTAP 시스템을 생성한 후에는 AWS 데이터 암호화 방법을 변경할 수 없습니다.

   "Cloud Volumes ONTAP용 AWS KMS를 설정하는 방법에 대해 알아보십시오".

   "지원되는 암호화 기술에 대해 자세히 알아보십시오".

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. * Cloud Volumes ONTAP 구성 * (연간 AWS 마켓플레이스 계약만 해당): 기본 구성을 검토하고 * 계속 * 을 클릭하거나 * 구성 변경 * 을 클릭하여 원하는 구성을 선택합니다.

    기본 구성을 유지하는 경우 볼륨을 지정한 다음 구성을 검토 및 승인하기만 하면 됩니다.

11. * 사전 구성된 패키지 *: 패키지 중 하나를 선택하여 Cloud Volumes ONTAP를 빠르게 시작하거나 * 구성 변경 * 을 클릭하여 원하는 구성을 선택합니다.

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

12. * IAM Role *: BlueXP가 역할을 생성할 수 있도록 기본 옵션을 유지하는 것이 가장 좋습니다.

    자체 정책을 사용하려면 이 정책이 충족해야 합니다 "Cloud Volumes ONTAP 노드의 정책 요구사항".

13. * 라이선스 *: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 인스턴스 유형 및 인스턴스 테넌시를 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).

14. * 기본 스토리지 리소스 *: 디스크 유형을 선택하고 기본 스토리지를 구성한 다음 데이터 계층화를 사용할 것인지 선택합니다.

    다음 사항에 유의하십시오.

    - 디스크 유형은 초기 볼륨(및 애그리게이트)에 사용됩니다. 이후 볼륨 및 애그리게이트에 대해 다른 디스크 유형을 선택할 수 있습니다.
    - GP3 또는 io1 디스크를 선택하는 경우 BlueXP는 AWS의 Elastic Volumes 기능을 사용하여 기본 스토리지 디스크 용량을 필요에 따라 자동으로 늘립니다. 스토리지 요구사항에 따라 초기 용량을 선택하고 Cloud Volumes ONTAP를 구축한 후 수정할 수 있습니다. "AWS의 Elastic Volumes 지원에 대해 자세히 알아보십시오".
    - GP2 또는 st1 디스크를 선택하는 경우 초기 애그리게이트의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 BlueXP가 생성하는 추가 애그리게이트에서 디스크 크기를 선택할 수 있습니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.
    - 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 계층화의 작동 방식에 대해 알아보십시오".

15. * 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.

       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.

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

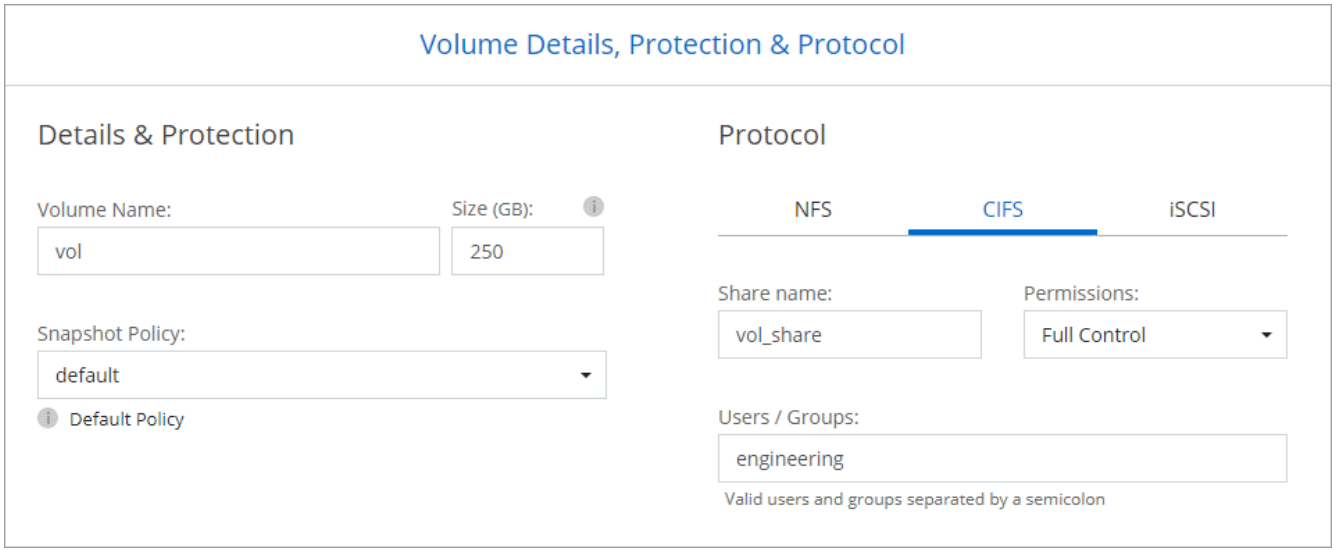
    "지원되는 클라이언트 프로토콜 및 버전에 대해 알아보십시오".

    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.

필드에 입력합니다	설명
권한 및 사용자/그룹(CIFS 전용)	이러한 필드를 사용하면 사용자 및 그룹의 공유에 대한 액세스 수준(액세스 제어 목록 또는 ACL라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자 또는 그룹, UNIX 사용자 또는 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자의 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사본 정책은 자동으로 생성되는 NetApp 스냅샷 복사본의 수와 빈도를 지정합니다. NetApp 스냅샷 복사본은 성능 영향이 없고 최소한의 스토리지가 필요한 시점 파일 시스템 이미지입니다. 기본 정책을 선택하거나 선택하지 않을 수 있습니다. Microsoft SQL Server의 tempdb와 같이 임시 데이터에 대해 없음을 선택할 수 있습니다.
고급 옵션(NFS에만 해당)	볼륨의 NFS 버전 선택: NFSv3 또는 NFSv4
이니시에이터 그룹 및 IQN(iSCSI 전용)	iSCSI 스토리지 타겟을 LUN(논리 유닛)이라고 하며 호스트에 표준 블록 디바이스로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름의 테이블이며 어떤 이니시에이터가 어떤 LUN을 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 통합 네트워크 어댑터(CNA) 또는 전용 호스트 파스트 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 공인 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성할 때 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.



17. * 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. AWS 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하는 경우 이 필드에 * OU=Computers, OU=Corp * 를 입력해야 합니다.
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.

18. * Usage Profile, Disk Type 및 Tiering Policy *: 스토리지 효율성 기능을 사용하도록 설정하고 필요한 경우 볼륨 계층화 정책을 편집할지 여부를 선택합니다.

    자세한 내용은 을 참조하십시오 "볼륨 사용 프로필 이해" 및 "데이터 계층화 개요".

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

결과

BlueXP에서 Cloud Volumes ONTAP 인스턴스를 시작합니다. 타임라인에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 인스턴스를 시작하는 데 문제가 있는 경우 실패 메시지를 검토합니다. 작업 환경을 선택하고 환경 다시 생성 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.

AWS에서 Cloud Volumes ONTAP HA 쌍 시작

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

제한

현재 HA 쌍은 AWS 아웃포스트에서 지원되지 않습니다.

이 작업에 대해

작업 환경을 생성한 직후 BlueXP는 지정된 VPC에서 테스트 인스턴스를 시작하여 연결을 확인합니다. 성공하면 즉시 BlueXP가 인스턴스를 종료한 다음 Cloud Volumes ONTAP 시스템 배포를 시작합니다. BlueXP에서 연결을 확인할 수 없는 경우 작업 환경 생성이 실패합니다. 테스트 인스턴스는 T2.nano(기본 VPC 테넌시의 경우) 또는 m3.medium(전용 VPC 테넌시의 경우)입니다.

단계

1. 왼쪽 탐색 메뉴에서 * Storage > Canvas * 를 선택합니다.
2. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 화면의 지시를 따릅니다.
3. * 위치 선택 *: * 아마존 웹 서비스 * 및 * Cloud Volumes ONTAP HA * 를 선택합니다.
4. * 세부 정보 및 자격 증명 *: AWS 자격 증명과 구독을 선택적으로 변경하고, 작업 환경 이름을 입력하고, 필요한 경우 태그를 추가한 다음 암호를 입력합니다.

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

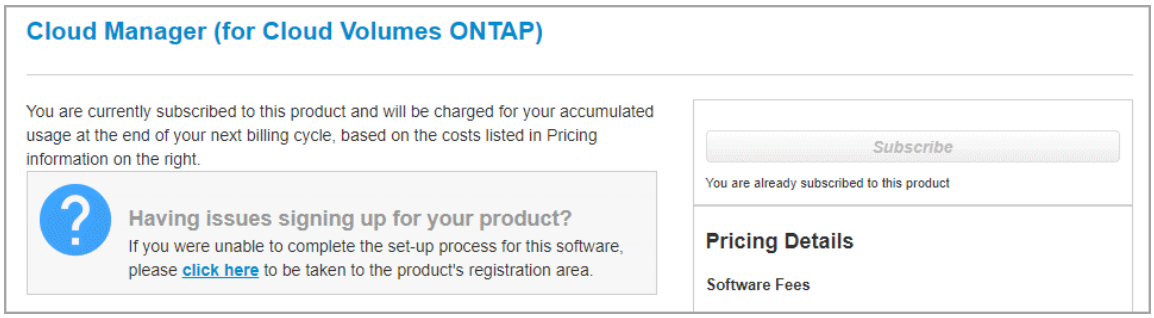
필드에 입력합니다	설명
작업 환경 이름	BlueXP는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Amazon EC2 인스턴스 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
태그 추가	AWS 태그는 AWS 리소스에 대한 메타데이터입니다. BlueXP는 Cloud Volumes ONTAP 인스턴스 및 인스턴스와 연관된 각 AWS 리소스에 태그를 추가합니다. 작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 생성된 후에는 더 많은 태그를 추가할 수 있습니다. API는 작업 환경을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 자세한 내용은 을 참조하십시오 "AWS 문서: Amazon EC2 리소스에 태그 달기".
사용자 이름 및 암호	Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하여 System Manager 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다. default_admin_user 이름을 유지하거나 사용자 지정 사용자 이름으로 변경합니다.

필드에 입력합니다	설명
자격 증명 편집	이 Cloud Volumes ONTAP 시스템에서 사용할 AWS 자격 증명과 마켓플레이스 구독을 선택하십시오. 선택한 자격 증명을 새 AWS Marketplace 구독에 연결하려면 * Add Subscription * 을 클릭합니다. 이 구독은 연간 계약을 기준으로 하거나 시간당 요율로 Cloud Volumes ONTAP에 대한 비용을 지불할 수 있습니다. NetApp(BYOL)에서 직접 라이센스를 구입한 경우에는 AWS 가입이 필요하지 않습니다. "BlueXP에 AWS 자격 증명을 추가하는 방법에 대해 알아보십시오".

다음 비디오에서는 용량제 마켓플레이스 구독을 AWS 자격 증명에 연결하는 방법을 보여줍니다.

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

여러 IAM 사용자가 동일한 AWS 계정으로 작업하는 경우 각 사용자는 가입해야 합니다. 첫 번째 사용자가 구독한 후 AWS Marketplace는 아래 이미지에 표시된 것처럼 후속 사용자에게 이미 구독했음을 알립니다. AWS_ACCOUNT_에 가입되어 있는 동안 각 IAM 사용자는 자신을 해당 구독과 연결해야 합니다. 아래 메시지가 표시되면 * 여기를 클릭 * 링크를 클릭하여 BlueXP 웹 사이트로 이동하여 프로세스를 완료합니다.



5. * 서비스 *: 이 Cloud Volumes ONTAP 시스템에서 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 배포 모델 *: HA 구성을 선택합니다.

   배포 모델에 대한 개요는 을 참조하십시오 "AWS용 Cloud Volumes ONTAP HA".

7. * 위치 및 연결 * (단일 AZ) 또는 * 지역 및 VPC * (다중 AZs): AWS 워크시트에 기록한 네트워크 정보를 입력합니다.

   다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
보안 그룹을 생성했습니다	BlueXP에서 보안 그룹을 생성하도록 하면 트래픽을 허용하는 방법을 선택해야 합니다. • 선택한 VPC 전용 * 을 선택한 경우 인바운드 트래픽의 소스는 선택한 VPC의 서브넷 범위와 커넥터가 상주하는 VPC의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다. • 모든 VPC * 를 선택한 경우 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
기존 보안 그룹을 사용합니다	기존 방화벽 정책을 사용하는 경우 필수 규칙이 포함되어 있는지 확인합니다. "Cloud Volumes ONTAP의 방화벽 규칙에 대해 알아보십시오".

8. * 연결 및 SSH 인증 *: HA 쌍선 및 중재자의 연결 방법을 선택합니다.
9. * 부동 IP *: 여러 AZs를 선택한 경우 부동 IP 주소를 지정합니다.

   IP 주소는 해당 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 합니다. 자세한 내용은 을 참조하십시오 "여러 AZs에서 Cloud Volumes ONTAP HA를 위한 AWS 네트워킹 요구사항".

10. * 루트 테이블 *: 여러 AZs를 선택한 경우 부동 IP 주소에 대한 라우트를 포함해야 하는 라우팅 테이블을 선택합니다.

    둘 이상의 라우팅 테이블이 있는 경우 올바른 라우팅 테이블을 선택하는 것이 매우 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP HA 쌍에 액세스하지 못할 수 있습니다. 라우팅 테이블에 대한 자세한 내용은 을 참조하십시오 "AWS 설명서: 경로 테이블".

11. * 데이터 암호화 *: 데이터 암호화 또는 AWS로 관리되는 암호화를 선택하지 않습니다.

    AWS로 관리되는 암호화의 경우 사용자 계정 또는 다른 AWS 계정에서 다른 CMK(Customer Master Key)를 선택할 수 있습니다.

    Cloud Volumes ONTAP 시스템을 생성한 후에는 AWS 데이터 암호화 방법을 변경할 수 없습니다.

    "Cloud Volumes ONTAP용 AWS KMS를 설정하는 방법에 대해 알아보십시오".

    "지원되는 암호화 기술에 대해 자세히 알아보십시오".

12. * 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".
13. * Cloud Volumes ONTAP 구성 * (연간 AWS 마켓플레이스 계약만 해당): 기본 구성을 검토하고 * 계속 * 을 클릭하거나 * 구성 변경 * 을 클릭하여 원하는 구성을 선택합니다.

    기본 구성을 유지하는 경우 볼륨을 지정한 다음 구성을 검토 및 승인하기만 하면 됩니다.

14. * 사전 구성된 패키지 * (시간별 또는 BYOL 전용): Cloud Volumes ONTAP를 빠르게 시작하려면 패키지 중 하나를 선택하고, 원하는 구성을 선택하려면 * 구성 변경 * 을 클릭합니다.

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

15. * IAM Role *: BlueXP가 역할을 생성할 수 있도록 기본 옵션을 유지하는 것이 가장 좋습니다.

    자체 정책을 사용하려면 이 정책이 충족해야 합니다 "Cloud Volumes ONTAP 노드 및 HA 중재자의 정책 요구사항".

16. * 라이선스 *: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 인스턴스 유형 및 인스턴스 테넌시를 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).

17. * 기본 스토리지 리소스 *: 디스크 유형을 선택하고 기본 스토리지를 구성한 다음 데이터 계층화를 사용할 것인지 선택합니다.

    다음 사항에 유의하십시오.

    - 디스크 유형은 초기 볼륨(및 애그리게이트)에 사용됩니다. 이후 볼륨 및 애그리게이트에 대해 다른 디스크 유형을 선택할 수 있습니다.
    - GP3 또는 io1 디스크를 선택하는 경우 BlueXP는 AWS의 Elastic Volumes 기능을 사용하여 기본 스토리지 디스크 용량을 필요에 따라 자동으로 늘립니다. 스토리지 요구사항에 따라 초기 용량을 선택하고 Cloud Volumes ONTAP를 구축한 후 수정할 수 있습니다. "AWS의 Elastic Volumes 지원에 대해 자세히 알아보십시오".
    - GP2 또는 st1 디스크를 선택하는 경우 초기 애그리게이트의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 BlueXP가 생성하는 추가 애그리게이트에서 디스크 크기를 선택할 수 있습니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.
    - 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 계층화의 작동 방식에 대해 알아보십시오".

18. * 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.

       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.

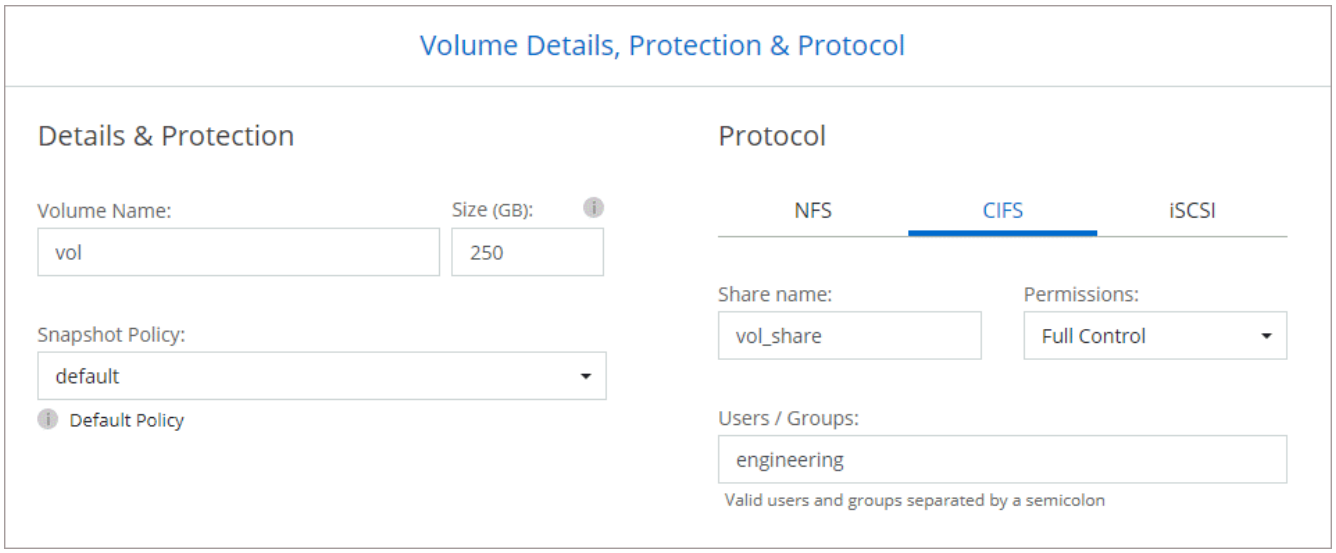
19. * 볼륨 생성 *: 새 볼륨에 대한 세부 정보를 입력하거나 * 건너뛰기 * 를 클릭합니다.

"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.



20. * 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. AWS 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하는 경우 이 필드에 * OU=Computers, OU=Corp * 를 입력해야 합니다.
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.

21. * Usage Profile, Disk Type 및 Tiering Policy *: 스토리지 효율성 기능을 사용하도록 설정하고 필요한 경우 볼륨 계층화 정책을 편집할지 여부를 선택합니다.

    자세한 내용은 을 참조하십시오 "볼륨 사용 프로필을 선택합니다" 및 "데이터 계층화 개요".

22. * 검토 및 승인 *: 선택 사항을 검토 및 확인합니다.

a. 구성에 대한 세부 정보를 검토합니다.

b. BlueXP가 구매할 지원 및 AWS 리소스에 대한 세부 정보를 검토하려면 * 추가 정보 * 를 클릭합니다.

c. 이해함… * 확인란을 선택합니다.

d. Go * 를 클릭합니다.

결과

BlueXP에서 Cloud Volumes ONTAP HA 쌍을 시작합니다. 타임라인에서 진행 상황을 추적할 수 있습니다.

HA 쌍 실행에 문제가 있는 경우 장애 메시지를 검토하십시오. 작업 환경을 선택하고 환경 다시 생성 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.

AWS C2S 환경에서 Cloud Volumes ONTAP를 시작하십시오

표준 AWS 지역과 마찬가지로, 에서 Cloud Manager를 사용할 수 있습니다 "AWS C2S(Commercial Cloud Services)" 구축할 환경: 클라우드 스토리지에 엔터프라이즈급 기능을 제공하는 Cloud Volumes ONTAP AWS C2S는 미국 고유의 폐쇄된 지역입니다 Intelligence Community - 이 페이지의 지침은 AWS C2S 지역 사용자에게만 적용됩니다.

C2S에서 지원되는 버전입니다

- Cloud Volumes ONTAP 9.8이 지원됩니다
- 커넥터 버전 3.9.4가 지원됩니다

  Connector는 AWS에서 Cloud Volumes ONTAP를 구축하고 관리하는 데 필요한 소프트웨어입니다. Connector 인스턴스에 설치되는 소프트웨어에서 Cloud Manager에 로그인합니다. Cloud Manager용 SaaS 웹 사이트는 C2S 환경에서 지원되지 않습니다.

> Cloud Manager는 최근 BlueXP로 이름이 바뀌었지만 Connector 버전 3.9.4 에 포함된 사용자 인터페이스가 Cloud Manager라고 불리기 때문에 C2S에서 Cloud Manager로 계속 언급하고 있습니다.

C2S에서 지원되는 기능

C2S 환경의 Cloud Manager에서 사용할 수 있는 기능은 다음과 같습니다.

- Cloud Volumes ONTAP
- 데이터 복제

- 감사 시간 표시 막대입니다

Cloud Volumes ONTAP의 경우 단일 노드 시스템 또는 HA 쌍을 생성할 수 있습니다. 두 가지 라이센스 옵션 모두 사용 가능: 용량제 및 BYOL(Bring Your Own License)

C2S의 Cloud Volumes ONTAP에서는 S3에 대한 데이터 계층화도 지원됩니다.

제한 사항

- Cloud Manager에서 제공되는 NetApp 클라우드 서비스가 없습니다.
- C2S 환경에는 인터넷 액세스가 없으므로 다음 기능을 사용할 수 없습니다.
  - Cloud Manager에서 소프트웨어 업그레이드 자동화
  - NetApp AutoSupport를 참조하십시오
  - Cloud Volumes ONTAP 리소스에 대한 AWS 비용 정보입니다
- C2S 환경에서는 Freemium 라이센스가 지원되지 않습니다.

구축 개요

C2S에서 Cloud Volumes ONTAP 시작하기 에는 몇 가지 단계가 포함되어 있습니다.

1. AWS 환경 준비

   여기에는 네트워킹 설정, Cloud Volumes ONTAP 가입, 권한 설정 및 AWS KMS 설정 옵션이 포함됩니다.

2. Connector 설치 및 Cloud Manager 설정

   Cloud Manager를 사용하여 Cloud Volumes ONTAP를 구축하기 전에 _Connector_를 작성해야 합니다. Connector를 사용하면 Cloud Manager에서 퍼블릭 클라우드 환경(Cloud Volumes ONTAP 포함)의 리소스와 프로세스를 관리할 수 있습니다.

   Connector 인스턴스에 설치되는 소프트웨어에서 Cloud Manager에 로그인합니다.

3. Cloud Manager에서 Cloud Volumes ONTAP 실행

이러한 각 단계는 아래에 설명되어 있습니다.

AWS 환경 준비

AWS 환경은 몇 가지 요구사항을 충족해야 합니다.

네트워크 설정

Cloud Volumes ONTAP가 제대로 작동할 수 있도록 AWS 네트워킹을 설정합니다.

단계

1. 커넥터 인스턴스 및 Cloud Volumes ONTAP 인스턴스를 시작할 VPC 및 서브넷을 선택합니다.
2. VPC와 서브넷이 커넥터와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인합니다.
3. VPC 엔드포인트를 S3 서비스로 설정합니다.

Cloud Volumes ONTAP의 콜드 데이터를 저비용 오브젝트 스토리지로 계층화하려는 경우 VPC 엔드포인트가 필요합니다.

Cloud Volumes ONTAP에 가입하십시오

Cloud Manager에서 Cloud Volumes ONTAP를 구축하려면 Marketplace에 가입해야 합니다.

단계

1. AWS 인텔리전스 커뮤니티 마켓플레이스로 이동하여 Cloud Volumes ONTAP를 검색합니다.
2. 구축할 오퍼링을 선택합니다.
3. 약관을 검토하고 * Accept * (수락 *)를 클릭합니다.
4. 다른 서비스를 배포하려는 경우 해당 서비스에 대해 이 단계를 반복합니다.

   Cloud Volumes ONTAP 인스턴스를 시작하려면 Cloud Manager를 사용해야 합니다. EC2 콘솔에서 Cloud Volumes ONTAP 인스턴스를 시작하면 안 됩니다.

권한 설정

Connector 및 Cloud Volumes ONTAP에 AWS 상용 클라우드 서비스 환경에서 작업을 수행하는 데 필요한 권한을 제공하는 IAM 정책 및 역할을 설정합니다.

다음 각 항목에 대해 IAM 정책 및 IAM 역할이 필요합니다.

- 커넥터 인스턴스
- Cloud Volumes ONTAP 인스턴스
- Cloud Volumes ONTAP HA 중재자 인스턴스(HA 쌍을 구축하려는 경우)

단계

1. AWS IAM 콘솔로 이동하여 * Policies * 를 클릭합니다.
2. Connector 인스턴스에 대한 정책을 만듭니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
```

```
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
```

```
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
```

```
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

3. Cloud Volumes ONTAP에 대한 정책을 생성합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

4. Cloud Volumes ONTAP HA 쌍을 구축하려는 경우 HA 중재자를 위한 정책을 생성합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Amazon EC2 역할 유형으로 IAM 역할을 생성하고 이전 단계에서 생성한 정책을 첨부합니다.

   정책과 마찬가지로, Connector에 IAM 역할 1개, Cloud Volumes ONTAP 노드에 대해 1개, HA 중재자를 위한 IAM 역할 1개가 있어야 합니다(HA 쌍을 구축하려는 경우).

   Connector 인스턴스를 실행할 때 Connector IAM 역할을 선택해야 합니다.

   Cloud Manager에서 Cloud Volumes ONTAP 작업 환경을 생성할 때 Cloud Volumes ONTAP의 IAM 역할과 HA 중재자를 선택할 수 있습니다.

AWS KMS를 설정합니다

Cloud Volumes ONTAP에서 Amazon 암호화를 사용하려면 AWS 키 관리 서비스에 대한 요구 사항이 충족되는지 확인합니다.

단계

1. 사용자 계정 또는 다른 AWS 계정에 활성 CMK(Customer Master Key)가 있는지 확인합니다.

   CMK는 AWS로 관리되는 CMK 또는 고객이 관리하는 CMK가 될 수 있습니다.

2. CMK가 Cloud Volumes ONTAP를 배포할 계정과 별도로 AWS 계정에 있는 경우 해당 키의 ARN을 얻어야 합니다.

   Cloud Volumes ONTAP 시스템을 생성할 때 클라우드 관리자에게 ARN을 제공해야 합니다.

3. Connector 인스턴스의 IAM 역할을 CMK의 주요 사용자 목록에 추가합니다.

   이렇게 하면 Cloud Volumes ONTAP에서 CMK를 사용할 수 있는 클라우드 관리자 권한이 부여됩니다.

Connector 설치 및 Cloud Manager 설정

AWS에서 Cloud Volumes ONTAP 시스템을 시작하려면 먼저 AWS Marketplace에서 Connector 인스턴스를 시작한 다음 로그인하고 Cloud Manager를 설정해야 합니다.

단계

1. PEM(Privacy Enhanced Mail) Base-64로 인코딩된 X.509 형식으로 CA(인증 기관)에서 서명한 루트 인증서를 받습니다. 인증서를 얻으려면 조직의 정책 및 절차를 참조하십시오.

   설치 프로세스 중에 인증서를 업로드해야 합니다. Cloud Manager는 HTTPS를 통해 AWS로 요청을 보낼 때 신뢰할 수 있는 인증서를 사용합니다.

2. 커넥터 인스턴스를 시작합니다.
   a. Cloud Manager의 AWS Intelligence Community Marketplace 페이지로 이동합니다.
   b. Custom Launch 탭에서 EC2 콘솔에서 인스턴스를 시작하는 옵션을 선택합니다.
   c. 프롬프트에 따라 인스턴스를 구성합니다.

      인스턴스를 구성할 때 다음 사항에 유의하십시오.

      - T3.xLarge를 권장합니다.
      - AWS 환경을 준비할 때 생성한 IAM 역할을 선택해야 합니다.
      - 기본 스토리지 옵션을 유지해야 합니다.
      - Connector에 필요한 연결 방법은 SSH, HTTP, HTTPS입니다.
3. Connector 인스턴스에 연결된 호스트에서 Cloud Manager를 설정합니다.
   a. 웹 브라우저를 열고 를 입력합니다 https://ipaddress 여기서 _ipaddress_는 Connector를 설치한 Linux 호스트의 IP 주소입니다.
   b. AWS 서비스 연결을 위한 프록시 서버를 지정합니다.
   c. 1단계에서 얻은 인증서를 업로드합니다.
   d. 설정 마법사의 단계를 완료하여 Cloud Manager를 설정합니다.
      - * 시스템 세부 정보 *: 이 Cloud Manager 인스턴스의 이름을 입력하고 회사 이름을 입력합니다.
      - * 사용자 생성 *: Cloud Manager 관리에 사용할 관리자 사용자를 생성합니다.
      - * 검토 *: 세부 정보를 검토하고 최종 사용자 사용권 계약을 승인합니다.
   e. CA 서명 인증서의 설치를 완료하려면 EC2 콘솔에서 Connector 인스턴스를 다시 시작합니다.
4. Connector가 다시 시작된 후 설치 마법사에서 만든 관리자 사용자 계정을 사용하여 로그인합니다.

Cloud Manager에서 Cloud Volumes ONTAP 실행

Cloud Manager에서 새로운 작업 환경을 생성하여 AWS 상용 클라우드 서비스 환경에서 Cloud Volumes ONTAP 인스턴스를 시작할 수 있습니다.

필요한 것

- 라이센스를 구입한 경우 NetApp에서 받은 라이센스 파일이 있어야 합니다. 라이센스 파일은 JSON 형식의 .NLF 파일입니다.

- HA 중재자가 키 기반 SSH 인증을 사용할 수 있도록 키 쌍이 필요합니다.

단계

1. 작업 환경 페이지에서 * 작업 환경 추가 * 를 클릭합니다.
2. 생성 아래에서 Cloud Volumes ONTAP 또는 Cloud Volumes ONTAP HA를 선택합니다.
3. 마법사의 단계를 완료하여 Cloud Volumes ONTAP 시스템을 시작합니다.

   마법사를 완료하면 다음 사항에 유의하십시오.

   - 여러 가용성 영역에 Cloud Volumes ONTAP HA를 배포하려는 경우 게시 시점에 AWS 상용 클라우드 서비스 환경에서 AZs를 두 개만 사용할 수 있으므로 다음과 같이 구성을 구축합니다.
     - 노드 1: 가용성 영역 A
     - 노드 2: 가용성 영역 B
     - 중재자: 가용성 영역 A 또는 B
   - 생성된 보안 그룹을 사용하려면 기본 옵션을 그대로 두어야 합니다.

     미리 정의된 보안 그룹에는 Cloud Volumes ONTAP가 제대로 작동하는 데 필요한 규칙이 포함됩니다. 사용자 고유의 사용이 필요한 경우 아래의 보안 그룹 섹션을 참조할 수 있습니다.
   - AWS 환경을 준비할 때 생성한 IAM 역할을 선택해야 합니다.
   - 기본 AWS 디스크 유형은 초기 Cloud Volumes ONTAP 볼륨에 사용됩니다.

     이후 볼륨에 대해 다른 디스크 유형을 선택할 수 있습니다.
   - AWS 디스크의 성능은 디스크 크기와 연관되어 있습니다.

     필요한 일관된 성능을 제공하는 디스크 크기를 선택해야 합니다. EBS 성능에 대한 자세한 내용은 AWS 설명서를 참조하십시오.
   - 디스크 크기는 시스템의 모든 디스크에 대한 기본 크기입니다.

     나중에 다른 크기가 필요한 경우 고급 할당 옵션을 사용하여 특정 크기의 디스크를 사용하는 Aggregate를 생성할 수 있습니다.
   - 스토리지 효율성 기능을 사용하면 스토리지 활용률을 개선하고 필요한 총 스토리지 양을 줄일 수 있습니다.

결과

Cloud Manager가 Cloud Volumes ONTAP 인스턴스를 시작합니다. 타임라인에서 진행 상황을 추적할 수 있습니다.

보안 그룹 규칙

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

커넥터의 보안 그룹

Connector의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

인바운드 규칙

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

아웃바운드 규칙

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

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

Cloud Volumes ONTAP의 보안 그룹입니다

Cloud Volumes ONTAP 노드의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

인바운드 규칙

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

- * 선택한 VPC만 해당 *: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템용 VPC의 서브넷 범위와 커넥터가 상주하는 VPC의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다.
- * 모든 VPC *: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.

프로토콜	포트	목적
모든 ICMP	모두	인스턴스에 Ping을 수행 중입니다
HTTP	80	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTP 액세스
HTTPS	443	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTPS 액세스
SSH를 클릭합니다	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다
TCP	111	NFS에 대한 원격 프로시저 호출
TCP	139	CIFS에 대한 NetBIOS 서비스 세션입니다
TCP	161-162	단순한 네트워크 관리 프로토콜

프로토콜	포트	목적
TCP	445	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
TCP	635	NFS 마운트
TCP	749	Kerberos
TCP	2049년	NFS 서버 데몬
TCP	3260입니다	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP	4045로 문의하십시오	NFS 잠금 데몬
TCP	4046으로 문의하십시오	NFS에 대한 네트워크 상태 모니터
TCP	10000	NDMP를 사용한 백업
TCP	11104를 참조하십시오	SnapMirror에 대한 인터클러스터 통신 세션의 관리
TCP	11105를 참조하십시오	인터클러스터 LIF를 사용하여 SnapMirror 데이터 전송
UDP입니다	111	NFS에 대한 원격 프로시저 호출
UDP입니다	161-162	단순한 네트워크 관리 프로토콜
UDP입니다	635	NFS 마운트
UDP입니다	2049년	NFS 서버 데몬
UDP입니다	4045로 문의하십시오	NFS 잠금 데몬
UDP입니다	4046으로 문의하십시오	NFS에 대한 네트워크 상태 모니터
UDP입니다	4049입니다	NFS rquotad 프로토콜

아웃바운드 규칙

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

프로토콜	포트	목적
모든 ICMP	모두	모든 아웃바운드 트래픽
모든 TCP	모두	모든 아웃바운드 트래픽

프로토콜	포트	목적
모든 UDP	모두	모든 아웃바운드 트래픽

HA 중재자를 위한 외부 보안 그룹

Cloud Volumes ONTAP HA 중재자를 위해 미리 정의된 외부 보안 그룹에는 다음과 같은 인바운드 및 아웃바운드 규칙이 포함됩니다.

인바운드 규칙

인바운드 규칙의 소스는 Connector가 상주하는 VPC의 트래픽입니다.

프로토콜	포트	목적
SSH를 클릭합니다	22	HA 중재자로 SSH 연결
TCP	3000입니다	Connector에서 Restful API 액세스

아웃바운드 규칙

HA 중재자를 위해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

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

HA 중재자를 위한 내부 보안 그룹

Cloud Volumes ONTAP HA 중재자를 위해 미리 정의된 내부 보안 그룹에는 다음 규칙이 포함됩니다. Cloud Manager는 항상 이 보안 그룹을 생성합니다. 자체 옵션을 사용할 수 없습니다.

인바운드 규칙

미리 정의된 보안 그룹에는 다음과 같은 인바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 교통 정보	모두	HA 중재자 및 HA 노드 간 통신

아웃바운드 규칙

미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 교통 정보	모두	HA 중재자 및 HA 노드 간 통신

Microsoft Azure에서 시작하십시오

Azure에서 Cloud Volumes ONTAP를 빠르게 시작합니다

몇 가지 단계를 통해 Azure용 Cloud Volumes ONTAP를 시작하십시오.


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"


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".


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".


BlueXP를 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)	
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
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

우선 순위 및 이름	포트 및 프로토콜	소스 및 대상	설명
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
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

우선 순위 및 이름	포트 및 프로토콜	소스 및 대상	설명
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
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	포트	프로토콜	출처	목적
	464	TCP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	464	UDP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos 키 관리
	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	UDP입니다	노드 관리 LIF	DHCP를 선택합니다	처음으로 설정하는 DHCP 클라이언트
DHCPS	67	UDP입니다	노드 관리 LIF	DHCP를 선택합니다	DHCP 서버
DNS	53	UDP입니다	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	UDP입니다	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	162	TCP	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	162	UDP입니다	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	UDP입니다	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 **ID**를 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.

프리모듐

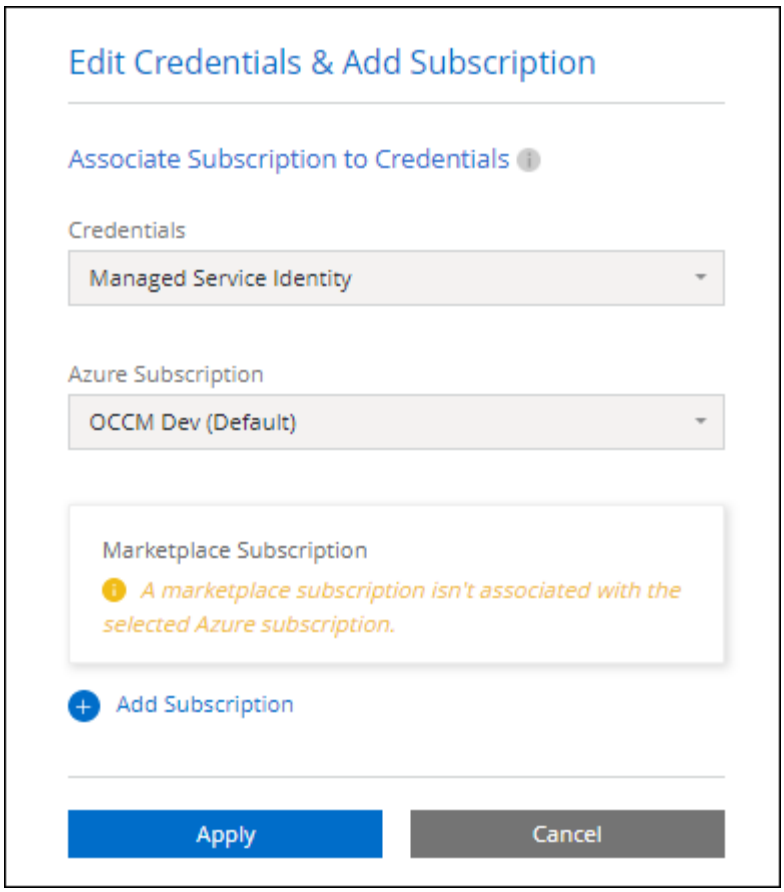
최대 500GiB의 용량을 제공하는 Cloud Volumes ONTAP를 무료로 사용할 수 있는 Freemium 오퍼링을 선택하십시오. "Freemium 제품에 대해 자세히 알아보십시오".

단계

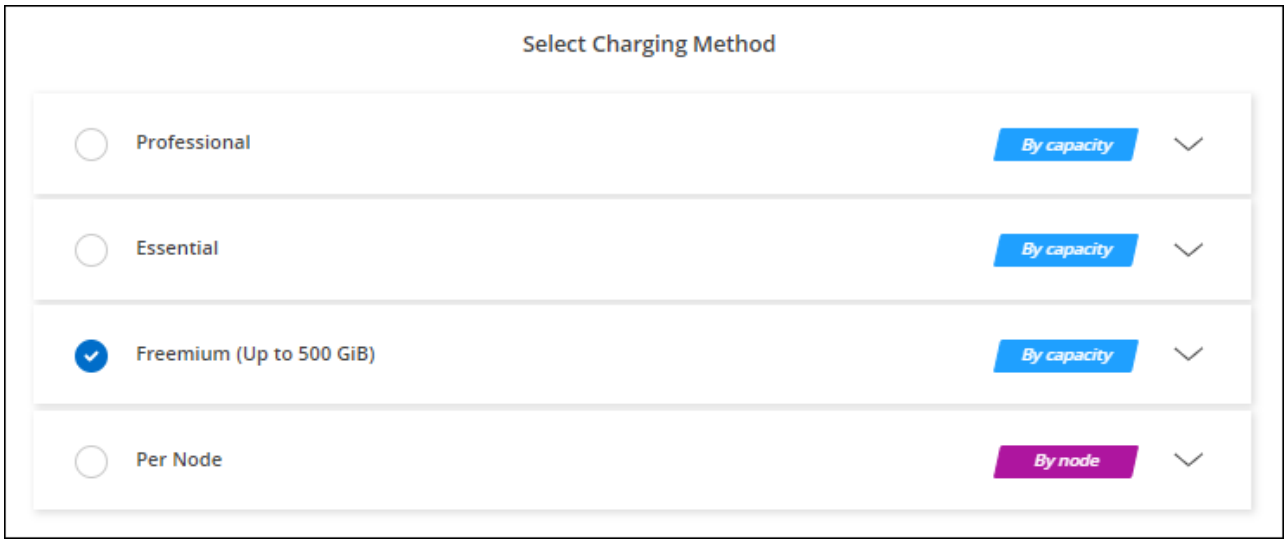
1. 왼쪽 탐색 메뉴에서 * Storage > Canvas * 를 선택합니다.
2. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 BlueXP의 단계를 따릅니다.

    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"

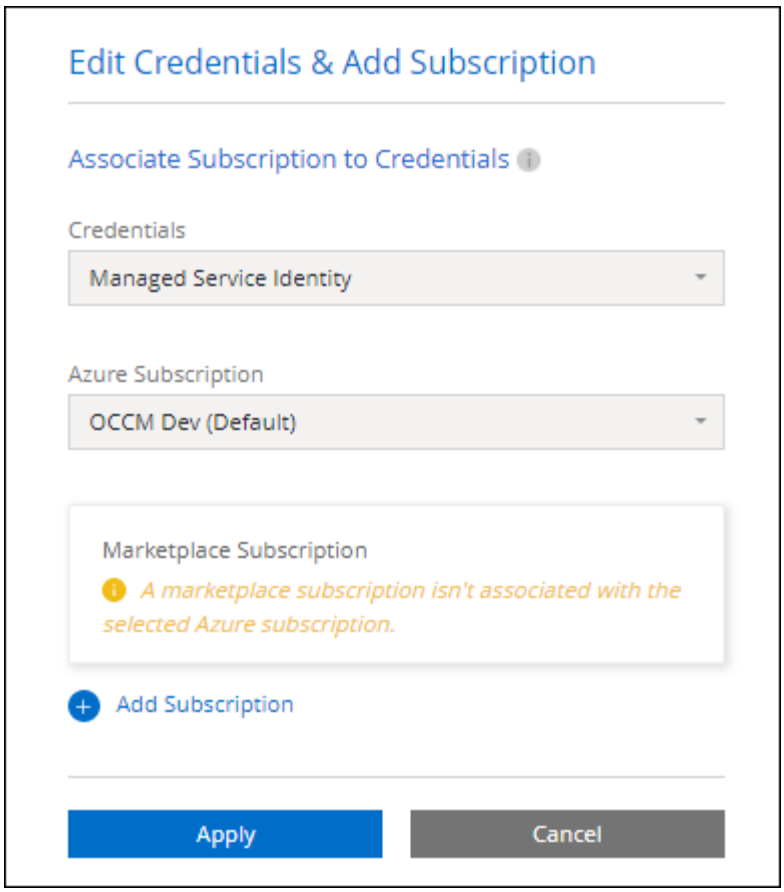
   BlueXP는 NetApp의 라이센스 서비스에 자동으로 쿼리하여 NetApp Support 사이트 계정과 관련된 라이센스에 대한 자세한 정보를 확인합니다. 오류가 없으면 BlueXP는 자동으로 디지털 지갑에 라이센스를 추가합니다.

   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".

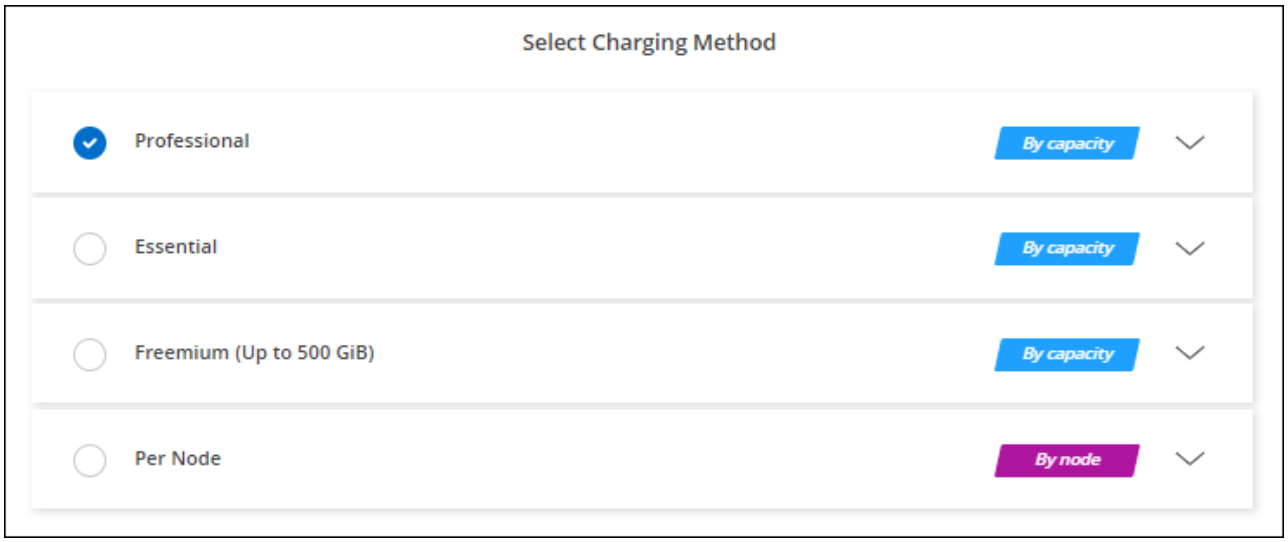
3. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 BlueXP의 단계를 따릅니다.

   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

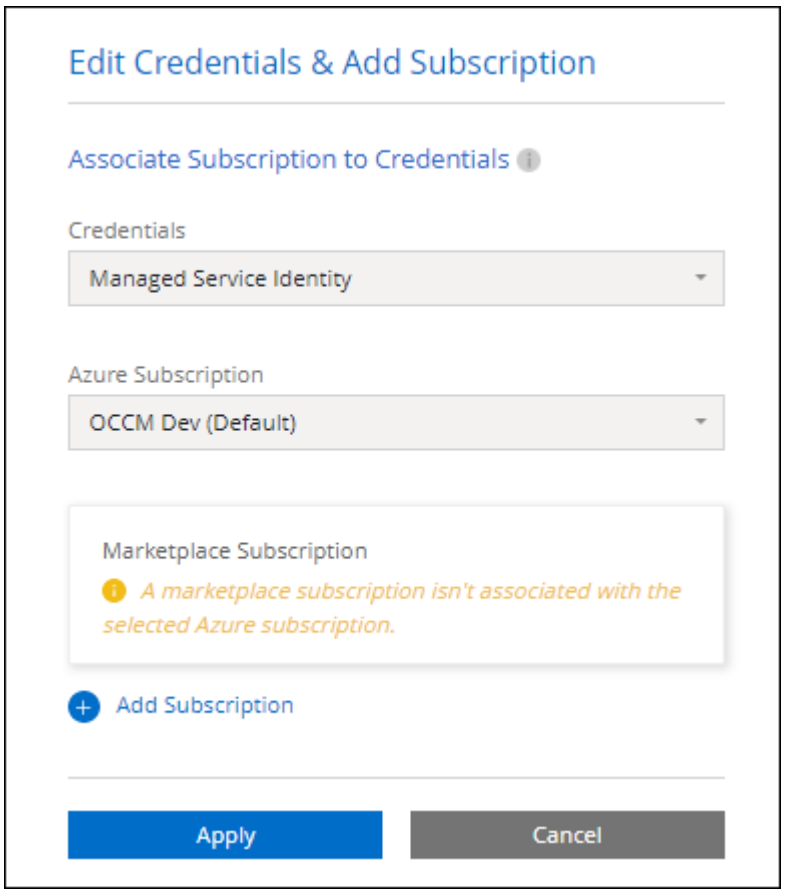
클라우드 공급자 마켓플레이스의 서비스에 가입하여 시간별 비용 지불

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

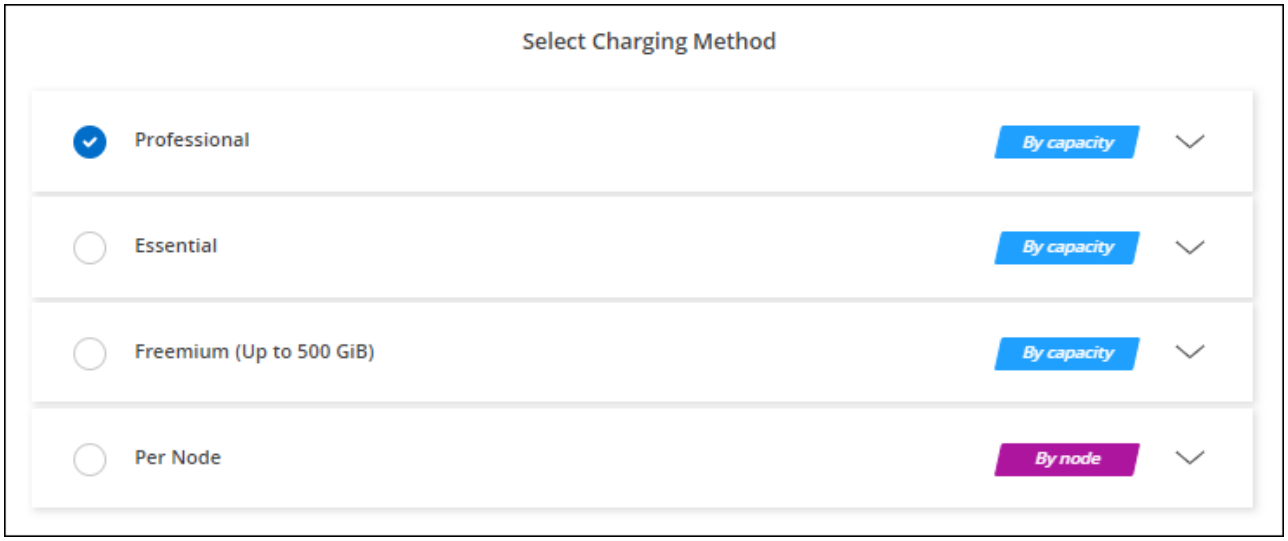
서브스크립션을 사용할 수 있습니다.

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.

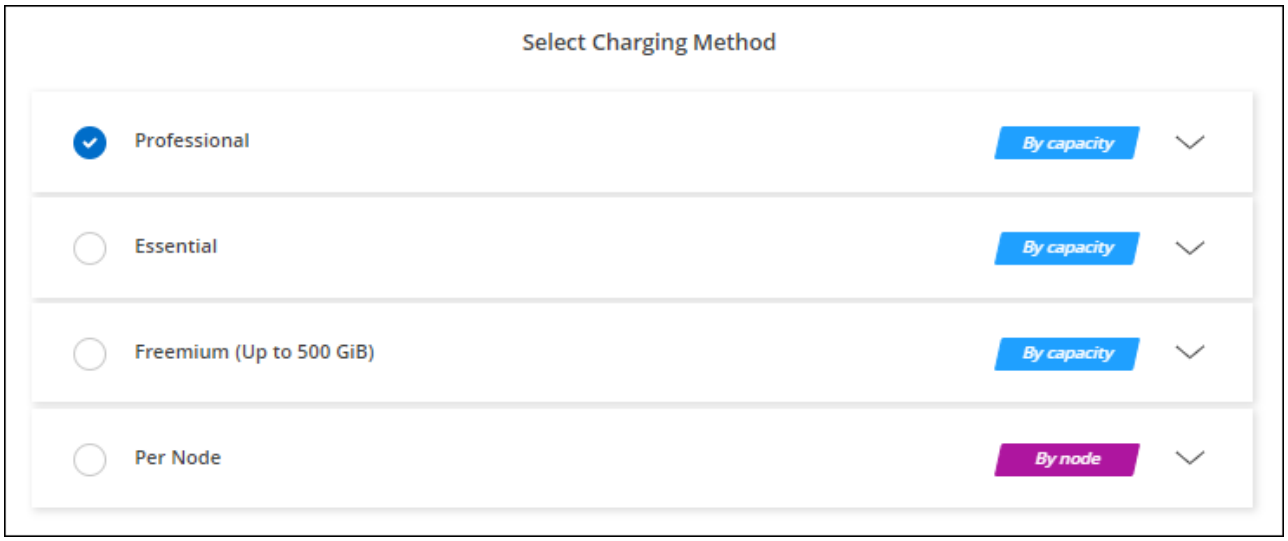
단계

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".

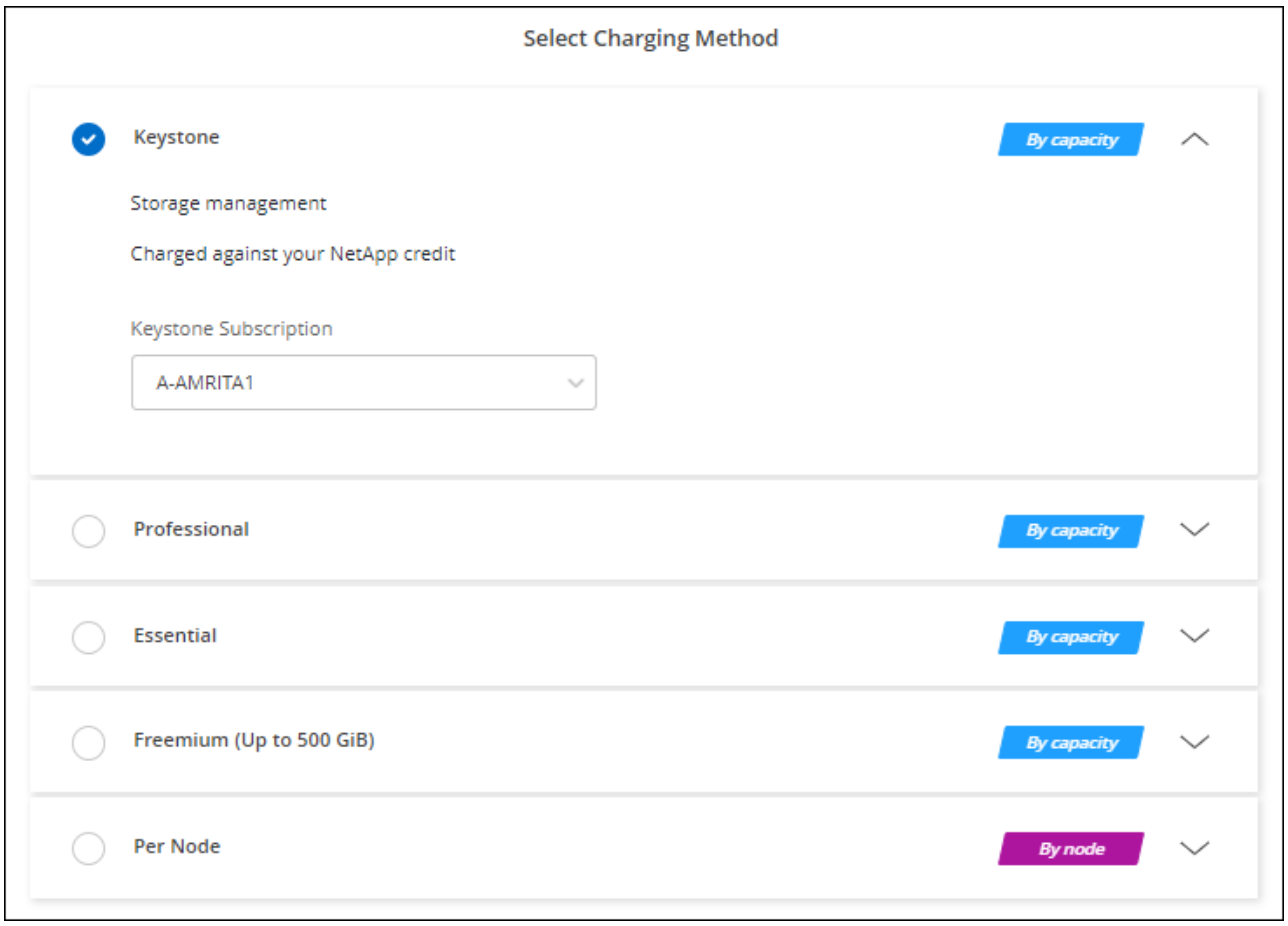
Keystone 구독

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.

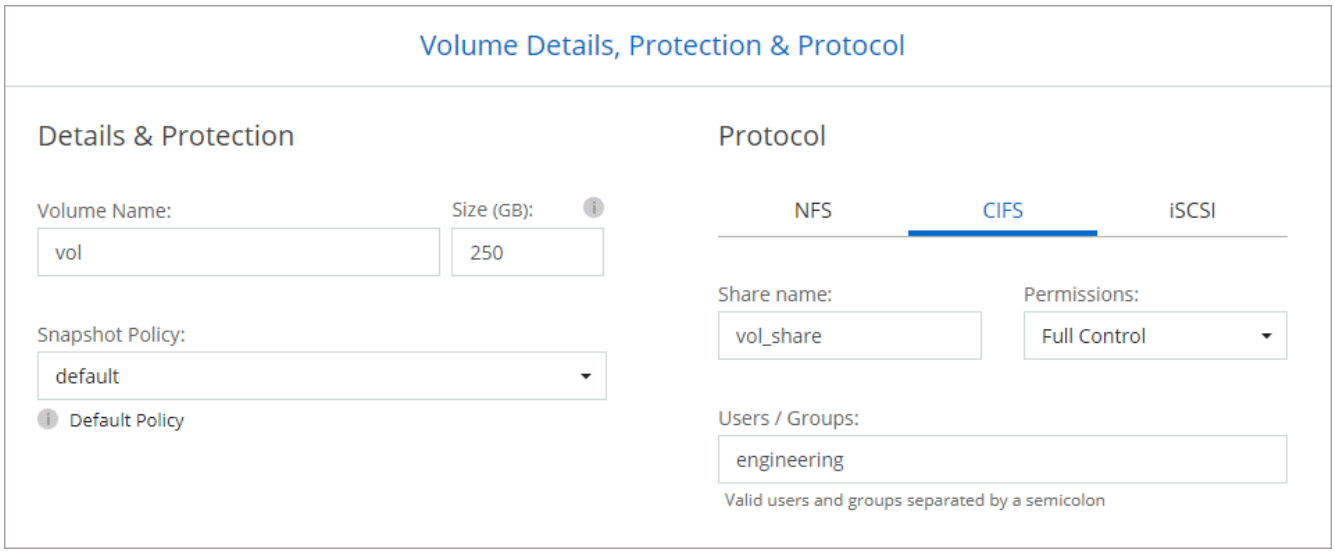
    "지원되는 클라이언트 프로토콜 및 버전에 대해 알아보십시오".

    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".

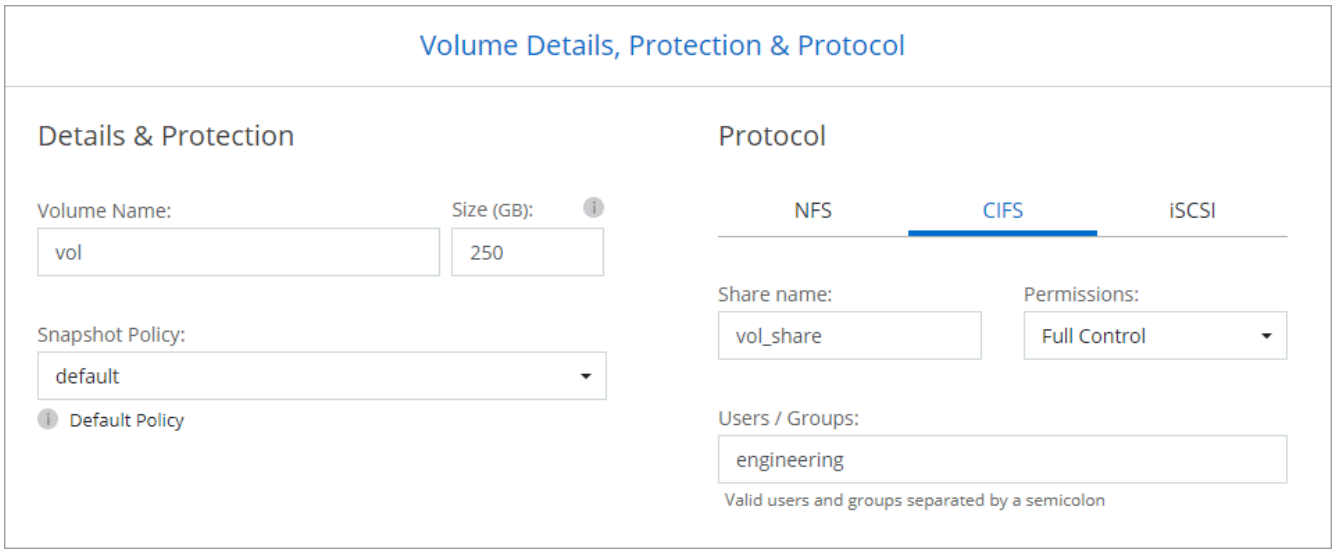
15. * 볼륨 생성 *: 새 볼륨에 대한 세부 정보를 입력하거나 * 건너뛰기 * 를 클릭합니다.

    "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.

Google Cloud에서 시작하십시오

Google Cloud에서 Cloud Volumes ONTAP를 빠르게 시작합니다

몇 가지 단계로 Cloud Volumes ONTAP for Google Cloud를 시작하십시오.


커넥터를 작성합니다

가 없는 경우 "커넥터" 그러나 계정 관리자는 계정을 만들어야 합니다. "Google Cloud에서 Connector를 만드는 방법을 알아보십시오"

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"


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.

"구성 계획에 대해 자세히 알아보십시오".


네트워크 설정

1. VPC와 서브넷이 커넥터와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인합니다.
2. 데이터 계층화를 사용할 계획이라면 "개인 Google 액세스를 위한 Cloud Volumes ONTAP 서브넷을 구성합니다".
3. HA 쌍을 구축하는 경우 각각 고유한 서브넷이 있는 4개의 VPC가 있는지 확인합니다.
4. 공유 VPC를 사용하는 경우 Connector 서비스 계정에 _Compute Network User_역할을 제공합니다.
5. 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".

서비스 계정을 설정합니다

Cloud Volumes ONTAP를 사용하려면 Google Cloud 서비스 계정이 두 가지 용도로 필요합니다. 첫 번째는 를 활성화하는 것입니다 "데이터 계층화" Google Cloud에서 콜드 데이터를 저비용 오브젝트 스토리지로 계층화합니다. 두 번째는 를 활성화하는 것입니다 "BlueXP 백업 및 복구" 볼륨을 저렴한 오브젝트 스토리지에 백업

하나의 서비스 계정을 설정하고 두 가지 용도로 사용할 수 있습니다. 서비스 계정에는 * 스토리지 관리자 * 역할이 있어야 합니다.

"단계별 지침을 읽습니다".

Google Cloud API를 활성화합니다

"프로젝트에서 다음 Google Cloud API를 활성화합니다". 이러한 API는 Connector 및 Cloud Volumes ONTAP를 구축하는 데 필요합니다.

- Cloud Deployment Manager V2 API
- 클라우드 로깅 API
- Cloud Resource Manager API를 참조하십시오
- 컴퓨팅 엔진 API
- IAM(Identity and Access Management) API

BlueXP를 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"
- "Linux 호스트에 Connector 소프트웨어 설치"
- "BlueXP가 Google Cloud 사용 권한으로 수행하는 기능"

Google Cloud에서 Cloud Volumes ONTAP 구성을 계획하십시오

Google Cloud에 Cloud Volumes ONTAP를 배포할 때 워크로드 요구 사항에 맞는 사전 구성된 시스템을 선택하거나 자신만의 구성을 만들 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 Google 클라우드 지역에서 지원됩니다. "지원되는 영역의 전체 목록을 봅니다".

지원되는 시스템 유형을 선택합니다

Cloud Volumes ONTAP는 선택한 라이센스 유형에 따라 여러 가지 시스템 유형을 지원합니다.

"GCP에서 Cloud Volumes ONTAP에 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.

"GCP의 Cloud Volumes ONTAP에 대한 스토리지 제한입니다"

GCP에서 시스템 크기를 조정합니다

Cloud Volumes ONTAP 시스템을 사이징하면 성능 및 용량 요구사항을 충족하는 데 도움이 될 수 있습니다. 시스템 유형, 디스크 유형 및 디스크 크기를 선택할 때 몇 가지 주요 사항을 알고 있어야 합니다.

기계 유형

에서 지원되는 기계 유형을 확인합니다 "Cloud Volumes ONTAP 릴리즈 노트" 지원되는 각 시스템 유형에 대한 자세한 내용은 Google에서 확인하십시오. 워크로드 요구 사항을 시스템 유형에 대한 vCPU 및 메모리 수와 일치시킵니다. 각 CPU 코어는 네트워킹 성능을 향상시킵니다.

자세한 내용은 다음을 참조하십시오.

- "Google Cloud 설명서: N1 표준 컴퓨터 유형"
- "Google Cloud 설명서: 성능"

GCP 디스크 유형입니다

Cloud Volumes ONTAP용 볼륨을 생성할 때 Cloud Volumes ONTAP이 디스크에 사용하는 기본 클라우드 스토리지를 선택해야 합니다. 디스크 유형은 다음 중 하나일 수 있습니다.

- *Zonal SSD* 영구 디스크: SSD 영구 디스크는 높은 속도의 랜덤 IOPS가 필요한 워크로드에 가장 적합합니다.
- _Zonal Balanced 영구 디스크 _: 이 SSD는 GB당 더 낮은 IOPS를 제공하여 성능과 비용을 균형 있게 조정합니다.
- *Zonal Standard* 영구 디스크: 표준 영구 디스크는 경제적이며 순차적 읽기/쓰기 작업을 처리할 수 있습니다.

  자세한 내용은 을 참조하십시오 "Google Cloud 설명서: Zonal Persistent 디스크(Standard 및 SSD)".

GCP 디스크 크기입니다

Cloud Volumes ONTAP 시스템을 배포할 때 초기 디스크 크기를 선택해야 합니다. 그런 다음 BlueXP에서 시스템 용량을 관리할 수 있지만 자체적으로 집계를 구축하려는 경우 다음 사항에 유의하십시오.

- Aggregate의 모든 디스크는 동일한 크기여야 합니다.
- 성능을 고려하면서 필요한 공간을 결정합니다.
- 영구 디스크의 성능은 디스크 크기와 시스템에서 사용할 수 있는 vCPU 수에 따라 자동으로 확장됩니다.

  자세한 내용은 다음을 참조하십시오.

  - "Google Cloud 설명서: Zonal Persistent 디스크(Standard 및 SSD)"
  - "Google Cloud 설명서: 영구 디스크 및 로컬 SSD 성능 최적화"

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.

- "Google Cloud에서 Cloud Volumes ONTAP 시스템 데이터에 대한 기본 디스크를 봅니다".
- "Google Cloud 문서: 리소스 할당량"

  Google Cloud Compute Engine은 리소스 사용량에 대해 할당량을 적용하므로 Cloud Volumes ONTAP를 배포하기 전에 한계에 도달하지 않았는지 확인해야 합니다.

커넥터에는 시스템 디스크도 필요합니다. "커넥터의 기본 설정에 대한 세부 정보를 봅니다".

네트워킹 정보를 수집합니다

GCP에서 Cloud Volumes ONTAP를 배포할 때 가상 네트워크에 대한 세부 정보를 지정해야 합니다. 워크시트를 사용하여 관리자로부터 정보를 수집할 수 있습니다.

- 단일 노드 시스템에 대한 네트워크 정보 *

GCP 정보	귀사의 가치
지역	
Zone(영역)	
VPC 네트워크	

GCP 정보	귀사의 가치
서브넷	
방화벽 정책(자체 사용 시)	

- 여러 존의 HA 쌍에 대한 네트워크 정보 *

GCP 정보	귀사의 가치
지역	
노드 1의 영역	
노드 2의 영역입니다	
중재자를 위한 구역	
VPC-0 및 서브넷	
VPC-1 및 서브넷	
VPC-2 및 서브넷	
VPC-3 및 서브넷	
방화벽 정책(자체 사용 시)	

- 단일 영역의 HA 쌍에 대한 네트워크 정보 *

GCP 정보	귀사의 가치
지역	
Zone(영역)	
VPC-0 및 서브넷	
VPC-1 및 서브넷	
VPC-2 및 서브넷	
VPC-3 및 서브넷	
방화벽 정책(자체 사용 시)	

쓰기 속도를 선택합니다

BlueXP에서는 Google Cloud의 고가용성(HA) 쌍을 제외하고 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.

Google Cloud의 Cloud Volumes ONTAP에 대한 네트워킹 요구 사항

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

HA 쌍을 구축하려는 경우 "HA 쌍이 Google Cloud에서 어떻게 작동하는지를 알아보십시오".

Cloud Volumes ONTAP에 대한 요구사항

Google Cloud에서 다음 요구사항을 충족해야 합니다.

요구사항을 충족해야 합니다

단일 노드 시스템을 배포하려는 경우 네트워킹이 다음 요구 사항을 충족하는지 확인합니다.

VPC 1개

단일 노드 시스템을 위해 VPC(가상 프라이빗 클라우드) 1개가 필요합니다.

전용 **IP** 주소

BlueXP는 Google Cloud의 단일 노드 시스템에 3개 또는 4개의 사설 IP 주소를 할당합니다.

API를 사용하여 Cloud Volumes ONTAP를 구축하고 다음 플래그를 지정한 경우 SVM(스토리지 VM) 관리 LIF의 생성을 건너뛸 수 있습니다.

```
skipSvmManagementLif: true
```

LIF는 물리적 포트와 연결된 IP 주소입니다. SnapCenter와 같은 관리 툴을 사용하려면 스토리지 VM(SVM) 관리 LIF가 필요합니다.

HA 쌍 관련 요구사항

HA 쌍을 구축하려는 경우 네트워킹이 다음 요구사항을 충족하는지 확인합니다.

하나 또는 여러 개의 영역

여러 영역 또는 단일 영역에 HA 구성을 배포하여 데이터의 고가용성을 보장할 수 있습니다. HA 쌍을 생성할 때

BlueXP에서 여러 존 또는 단일 존을 선택하라는 메시지가 표시됩니다.

- 다중 영역(권장)

  3개 존에 HA 구성을 구축하면 존 내에서 장애가 발생하더라도 지속적인 데이터 가용성을 보장할 수 있습니다. 쓰기 성능은 단일 존을 사용할 때보다 약간 낮지만, 이는 최소화됩니다.

- 단일 영역

  단일 영역에 배포되면 Cloud Volumes ONTAP HA 구성에서 분산 배치 정책을 사용합니다. 이 정책은 별도의 존을 사용하여 장애를 격리하지 않고도 존 내의 단일 장애 지점으로부터 HA 구성을 보호합니다.

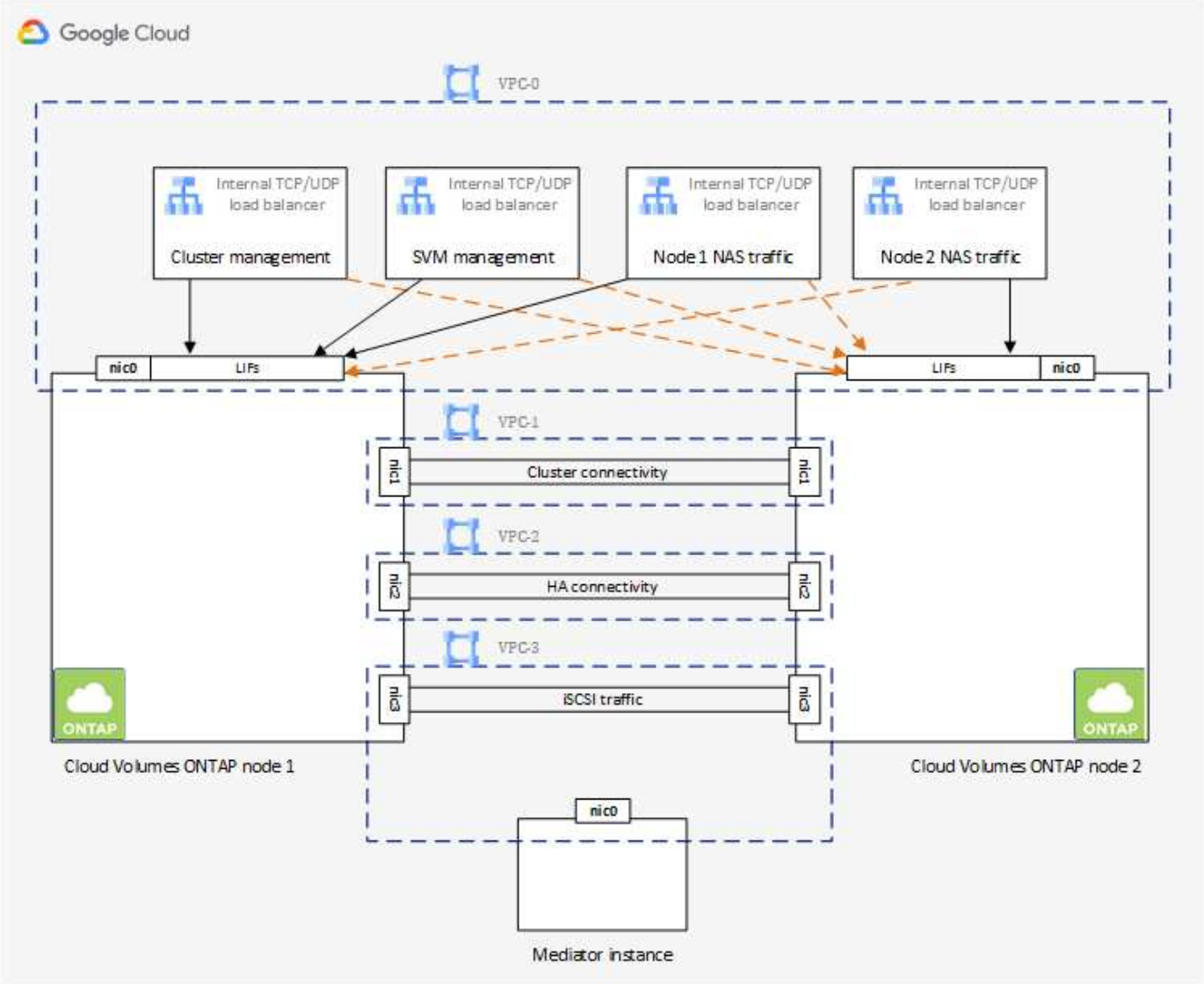
  이 구축 모델은 구역 간 데이터 유출 비용이 없으므로 비용이 절감됩니다.

4개의 가상 프라이빗 클라우드

HA 구성을 위해서는 4개의 가상 프라이빗 클라우드(VPC)가 필요합니다. Google Cloud에서는 각 네트워크 인터페이스가 별도의 VPC 네트워크에 상주해야 하므로 4대의 VPC가 필요합니다.

HA 쌍을 생성할 때 BlueXP에서 네 개의 VPC를 선택하라는 메시지가 표시됩니다.

- 데이터 및 노드에 대한 인바운드 연결을 위한 VPC-0
- 노드와 HA 중재자 간의 내부 통신을 위한 VPC-1, VPC-2 및 VPC-3



서브넷

각 VPC에 전용 서브넷이 필요합니다.

Connector를 VPC-0에 배치한 경우 서브넷에서 Private Google Access를 활성화하여 API에 액세스하고 데이터 계층화를 활성화해야 합니다.

이러한 VPC에 있는 서브넷에는 고유한 CIDR 범위가 있어야 합니다. CIDR 범위가 중복될 수 없습니다.

전용 **IP** 주소

BlueXP는 필요한 수의 사설 IP 주소를 Google Cloud의 Cloud Volumes ONTAP에 자동으로 할당합니다. 네트워킹에 사용 가능한 개인 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.

- * 단일 노드 *
  BlueXP는 단일 노드 시스템에 4개의 IP 주소를 할당합니다.

- 노드 관리 LIF
- 클러스터 관리 LIF
- iSCSI 데이터 LIF

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

- NAS LIF

  API를 사용하여 Cloud Volumes ONTAP를 구축하고 다음 플래그를 지정한 경우 SVM(스토리지 VM) 관리 LIF의 생성을 건너뛸 수 있습니다.

```
skipSvmManagementLif: true
```

- * HA 쌍 *
  BlueXP는 HA 쌍에 12~13개의 IP 주소를 할당:
  - 노드 관리 LIF 2개(e0a)
  - 클러스터 관리 LIF 1개(e0a)
  - iSCSI LIF 2개(e0a)

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

  - 1~2개의 NAS LIF(e0a)
  - 클러스터 LIF 2개(e0b)
  - HA 인터커넥트 IP 주소 2개(e0c)
  - RSM iSCSI IP 주소(e0d) 2개

    API를 사용하여 Cloud Volumes ONTAP를 구축하고 다음 플래그를 지정한 경우 SVM(스토리지 VM) 관리 LIF의 생성을 건너뛸 수 있습니다.

```
skipSvmManagementLif: true
```

내부 로드 밸런서

BlueXP는 들어오는 트래픽을 Cloud Volumes ONTAP HA 쌍으로 관리하는 4개의 Google 클라우드 내부 로드 밸런서(TCP/UDP)를 자동으로 생성합니다. 설정을 마칠 필요가 없습니다 이를 단순히 네트워크 트래픽을 알리고 보안 문제를 완화하기 위한 요구 사항으로 나열했습니다.

로드 밸런싱 장치 하나는 클러스터 관리이고, 하나는 SVM(스토리지 VM) 관리이고, 하나는 노드 1에 대한 NAS 트래픽이고, 나머지 하나는 노드 2에 대한 NAS 트래픽입니다.

각 부하 분산 장치에 대한 설정은 다음과 같습니다.

- 공유 개인 IP 주소 1개
- 글로벌 상태 점검 1회

  기본적으로 상태 확인에 사용되는 포트는 63001, 63002 및 63003입니다.

- 지역 TCP 백엔드 서비스 1개
- 하나의 지역 UDP 백엔드 서비스입니다
- 하나의 TCP 전달 규칙
- UDP 포워딩 규칙 1개
- 전역 액세스가 비활성화되었습니다

  전역 액세스는 기본적으로 해제되어 있지만 사후 배포를 사용하도록 설정하는 것이 지원됩니다. 지역 간 트래픽의 지연 시간이 훨씬 더 길기 때문에 이 기능을 비활성화했습니다. 우발적인 교차 부위 장착으로 인해 부정적인 경험을 하지 않으려 했습니다. 이 옵션의 활성화는 비즈니스 요구 사항에 따라 다릅니다.

공유 **VPC**

Cloud Volumes ONTAP 및 Connector는 Google Cloud 공유 VPC 및 독립 실행형 VPC에서도 지원됩니다.

단일 노드 시스템의 경우 VPC는 공유 VPC 또는 독립형 VPC가 될 수 있습니다.

HA 쌍의 경우 4개의 VPC가 필요합니다. 각 VPC는 공유 또는 독립 실행형으로 사용할 수 있습니다. 예를 들어 VPC-0은 공유 VPC가 될 수 있고 VPC-1, VPC-2 및 VPC-3은 독립 실행형 VPC가 될 수 있습니다.

공유 VPC를 사용하면 여러 프로젝트에서 가상 네트워크를 구성하고 중앙에서 관리할 수 있습니다. _host project_에서 공유 VPC 네트워크를 설정하고 _service project_에서 Connector 및 Cloud Volumes ONTAP 가상 머신 인스턴스를 배포할 수 있습니다. "Google Cloud 설명서: 공유 VPC 개요".

"Connector 구축에서 적용되는 필수 공유 VPC 사용 권한을 검토합니다"

VPC의 패킷 미러링

"패킷 미러링" Cloud Volumes ONTAP를 구축하는 Google Cloud VPC에서 비활성화되어야 합니다. 패킷 미러링이 활성화된 경우 Cloud Volumes ONTAP가 제대로 작동하지 않습니다.

아웃바운드 인터넷 액세스

Cloud Volumes ONTAP를 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 방화벽이 포트 3128을 통한 _INbound_connection을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

Cloud Volumes ONTAP에 대해 엄격한 아웃바운드 규칙을 정의한 경우 Cloud Volumes ONTAP 방화벽에서 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".

HA 쌍을 사용하는 경우 HA 중재자가 아웃바운드 인터넷 액세스를 요구하지 않습니다.

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

방화벽 규칙

BlueXP는 방화벽 규칙을 만들 필요가 없습니다. 직접 사용해야 하는 경우 아래 나열된 방화벽 규칙을 참조하십시오.

HA 구성에는 두 가지 방화벽 규칙 세트가 필요합니다.

- VPC-0의 HA 구성 요소에 대한 하나의 규칙 세트 이러한 규칙을 통해 Cloud Volumes ONTAP에 대한 데이터 액세스가 가능합니다. 자세한 정보.
- VPC-1, VPC-2 및 VPC-3의 HA 구성 요소에 대한 또 다른 규칙 세트 이러한 규칙은 HA 구성 요소 간의 인바운드 및 아웃바운드 통신에 대해 개방됩니다. 자세한 정보.

콜드 데이터를 Google 클라우드 스토리지 버킷에 계층화하려면 Cloud Volumes ONTAP가 상주하는 서브넷이 프라이빗 Google 액세스용으로 구성되어야 합니다(HA 쌍을 사용하는 경우 VPC-0의 서브넷임). 자세한 지침은 을 참조하십시오 "Google Cloud 설명서: 개인 Google Access 구성".

BlueXP에서 데이터 계층화를 설정하는 데 필요한 추가 단계는 을 참조하십시오 "콜드 데이터를 저비용 오브젝트 스토리지로 계층화".

다른 네트워크의 **ONTAP** 시스템에 대한 연결

Google Cloud의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 VPC와 기업 네트워크 같은 다른 네트워크 간에 VPN 연결이 있어야 합니다.

자세한 지침은 을 참조하십시오 "Google Cloud 설명서: Cloud VPN 개요".

방화벽 규칙

BlueXP는 Cloud Volumes ONTAP가 성공적으로 운영하는 데 필요한 인바운드 및 아웃바운드 규칙을 포함하는 Google Cloud 방화벽 규칙을 생성합니다. 테스트 목적으로 또는 자체 방화벽 규칙을 사용하려는 경우 포트를 참조할 수 있습니다.

Cloud Volumes ONTAP의 방화벽 규칙에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다. HA 구성을 구축할 경우 VPC-0의 Cloud Volumes ONTAP에 대한 방화벽 규칙입니다.

HA 구성에는 두 가지 방화벽 규칙 세트가 필요합니다.

- VPC-0의 HA 구성 요소에 대한 하나의 규칙 세트 이러한 규칙을 통해 Cloud Volumes ONTAP에 대한 데이터 액세스가 가능합니다.
- VPC-1, VPC-2 및 VPC-3의 HA 구성 요소에 대한 또 다른 규칙 세트 이러한 규칙은 HA 구성 요소 간의 인바운드 및 아웃바운드 통신에 대해 개방됩니다. 자세한 정보.

커넥터에 대한 정보를 찾고 계십니까? "Connector의 방화벽 규칙을 봅니다"

인바운드 규칙

작업 환경을 만들 때 배포 중에 미리 정의된 방화벽 정책에 대한 소스 필터를 선택할 수 있습니다.

- * 선택한 VPC만 해당 *: 인바운드 트래픽의 소스 필터는 Cloud Volumes ONTAP 시스템용 VPC의 서브넷 범위와 커넥터가 상주하는 VPC의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다.
- * 모든 VPC *: 인바운드 트래픽의 소스 필터는 0.0.0.0/0 IP 범위입니다.

자체 방화벽 정책을 사용하는 경우 Cloud Volumes ONTAP와 통신해야 하는 모든 네트워크를 추가해야 하지만 내부 Google 로드 밸런서가 올바르게 작동할 수 있도록 두 주소 범위를 모두 추가해야 합니다. 이러한 주소는 130.211.0.0/22 및 35.191.0.0/16입니다. 자세한 내용은 을 참조하십시오 "Google Cloud 설명서: 부하 분산 방화벽 규칙".

프로토콜	포트	목적
모든 ICMP	모두	인스턴스에 Ping을 수행 중입니다
HTTP	80	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTP 액세스
HTTPS	443	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 커넥터 및 HTTPS 액세스와의 연결
SSH를 클릭합니다	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다
TCP	111	NFS에 대한 원격 프로시저 호출
TCP	139	CIFS에 대한 NetBIOS 서비스 세션입니다
TCP	161-162	단순한 네트워크 관리 프로토콜
TCP	445	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
TCP	635	NFS 마운트
TCP	749	Kerberos
TCP	2049년	NFS 서버 데몬
TCP	3260입니다	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP	4045로 문의하십시오	NFS 잠금 데몬
TCP	4046으로 문의하십시오	NFS에 대한 네트워크 상태 모니터
TCP	10000	NDMP를 사용한 백업
TCP	11104를 참조하십시오	SnapMirror에 대한 인터클러스터 통신 세션의 관리

프로토콜	포트	목적
TCP	11105를 참조하십시오	인터클러스터 LIF를 사용하여 SnapMirror 데이터 전송
TCP	63001-63050	로드 밸런싱 프로브 포트를 통해 어떤 노드가 정상 상태인지 확인(HA 쌍에만 필요)
UDP입니다	111	NFS에 대한 원격 프로시저 호출
UDP입니다	161-162	단순한 네트워크 관리 프로토콜
UDP입니다	635	NFS 마운트
UDP입니다	2049년	NFS 서버 데몬
UDP입니다	4045로 문의하십시오	NFS 잠금 데몬
UDP입니다	4046으로 문의하십시오	NFS에 대한 네트워크 상태 모니터
UDP입니다	4049입니다	NFS rquotad 프로토콜

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.

프로토콜	포트	목적
모든 ICMP	모두	모든 아웃바운드 트래픽
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	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	프로토콜	포트	출처	목적지	목적
Active Directory를 클릭합니다	TCP	88을 참조하십시오	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니다	137입니다	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니다	138	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	TCP	139	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP 및 UDP	389	노드 관리 LIF	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	노드 관리 LIF	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	UDP입니다	464	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos 키 관리
	TCP	749	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(RPCSEC_GSS)
	TCP	88을 참조하십시오	데이터 LIF(NFS, CIFS, iSCSI)	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니다	137입니다	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니다	138	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	TCP	139	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP 및 UDP	389	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	UDP입니다	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos 키 관리
	TCP	749	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(RPCSEC_GSS)

서비스	프로토콜	포트	출처	목적지	목적
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
클러스터	모든 교통 정보	모든 교통 정보	모든 LIF가 하나의 노드에 있습니다	다른 노드의 모든 LIF	인터클러스터 통신(Cloud Volumes ONTAP HA에만 해당)
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	UDP입니다	68	노드 관리 LIF	DHCP를 선택합니다	처음으로 설정하는 DHCP 클라이언트
DHCPS	UDP입니다	67	노드 관리 LIF	DHCP를 선택합니다	DHCP 서버
DNS	UDP입니다	53	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	노드 관리 LIF	대상 서버	NDMP 복제
SMTP	TCP	25	노드 관리 LIF	메일 서버	AutoSupport에 사용할 수 있는 SMTP 경고
SNMP를 선택합니다	TCP	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니다	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	TCP	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니다	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
SnapMirror를 참조하십시오	TCP	11104를 참조하십시오	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror에 대한 인터클러스터 통신 세션의 관리
	TCP	11105를 참조하십시오	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror 데이터 전송
Syslog를 클릭합니다	UDP입니다	514	노드 관리 LIF	Syslog 서버	Syslog 메시지를 전달합니다

VPC-1, VPC-2 및 VPC-3에 대한 규칙

Google Cloud에서는 4개의 VPC에 HA 구성이 배포됩니다. VPC-0의 HA 구성에 필요한 방화벽 규칙은 입니다 Cloud Volumes ONTAP에 대해 위에 나열되어 있습니다.

한편, BlueXP가 VPC-1, VPC-2 및 VPC-3의 인스턴스에 대해 생성하는 사전 정의된 방화벽 규칙은 _ALL_PROTOCOLS 및 포트를 통한 수신 통신을 가능하게 합니다. 이 규칙은 HA 노드 간 통신을 지원합니다.

HA 노드와 HA 중재자의 통신은 포트 3260(iSCSI)을 통해 이루어집니다.

> 새로운 Google Cloud HA 쌍 구축에 빠른 쓰기 속도를 사용하려면 VPC-1, VPC-2 및 VPC-3에 최소 8,896바이트의 최대 전송 단위(MTU)가 필요합니다. 기존 VPC-1, VPC-2 및 VPC-3을 MTU가 8,896바이트인 경우 구성 프로세스 중에 이러한 VPC를 사용하여 모든 기존 HA 시스템을 종료해야 합니다.

커넥터 요구 사항

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

- "커넥터에 대한 네트워킹 요구 사항을 봅니다"
- "Google Cloud의 방화벽 규칙"

GCP에서 VPC 서비스 제어 계획

VPC 서비스 제어를 통해 Google 클라우드 환경을 잠그도록 선택할 때는 BlueXP 및 Cloud Volumes ONTAP이 Google 클라우드 API와 상호 작용하는 방식과 BlueXP 및 Cloud Volumes ONTAP를 배포하기 위해 서비스 경계를 구성하는 방법을 이해해야 합니다.

VPC 서비스 제어를 사용하면 신뢰할 수 있는 경계 외부의 Google 관리 서비스에 대한 액세스를 제어하고, 신뢰할 수 없는 위치에서 데이터 액세스를 차단하고, 무단 데이터 전송 위험을 완화할 수 있습니다. "Google Cloud VPC 서비스 컨트롤에 대해 자세히 알아보십시오".

NetApp 서비스가 VPC 서비스 제어와 통신하는 방법

BlueXP는 Google Cloud API와 직접 통신합니다. 이 문제는 Google Cloud 외부의 외부 IP 주소(예: api.services.cloud.netapp.com) 또는 BlueXP Connector에 할당된 내부 주소에서 Google Cloud 내부에서 발생합니다.

Connector의 배포 스타일에 따라 서비스 경계에 대해 특정 예외가 발생할 수 있습니다.

이미지

Cloud Volumes ONTAP와 BlueXP는 모두 NetApp에서 관리하는 GCP 내 프로젝트의 이미지를 사용합니다. 조직 내에서 호스팅되지 않은 이미지의 사용을 차단하는 정책이 조직에 있는 경우 BlueXP Connector 및 Cloud Volumes ONTAP의 배포에 영향을 줄 수 있습니다.

수동 설치 방법을 사용하여 커넥터를 수동으로 배포할 수도 있지만 Cloud Volumes ONTAP는 NetApp 프로젝트에서도 이미지를 가져와야 합니다. 커넥터 및 Cloud Volumes ONTAP를 배포하려면 허용 목록을 제공해야 합니다.

Connector를 배포하는 사용자는 ProjectID_NetApp-cloudmanager_에서 호스팅되는 이미지와 프로젝트 번호_14190056516_를 참조할 수 있어야 합니다.

Cloud Volumes ONTAP 배포

- BlueXP 서비스 계정은 서비스 프로젝트에서 ProjectID_NetApp-cloudmanager_에 호스팅된 이미지와 프로젝트 번호_14190056516_에 호스팅된 이미지를 참조해야 합니다.
- 기본 Google API 서비스 에이전트의 서비스 계정은 ProjectID_NetApp-cloudmanager_에서 호스팅되는 이미지와 서비스 프로젝트의 _14190056516_프로젝트 번호를 참조해야 합니다.

VPC 서비스 제어를 사용하여 이러한 이미지를 가져오는 데 필요한 규칙의 예는 아래에 정의되어 있습니다.

VPC 서비스는 경계 정책을 제어합니다

정책은 VPC 서비스 제어 규칙 집합에 대한 예외를 허용합니다. 정책에 대한 자세한 내용은 를 참조하십시오 "GCP VPC 서비스 제어 정책 문서".

BlueXP에 필요한 정책을 설정하려면 조직 내의 VPC 서비스 제어 경계 로 이동하여 다음 정책을 추가합니다. 이 필드는 VPC 서비스 제어 정책 페이지에 제공된 옵션과 일치해야 합니다. 또한 * 모든 * 규칙이 필요하며 * 또는 * 매개 변수를 규칙 집합에 사용해야 합니다.

수신 규칙

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

또는

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

또는

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

송신 규칙

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

위에 요약된 프로젝트 번호는 Cloud Volumes ONTAP용 커넥터 및 이미지를 저장하는 데 사용되는 PROJECT_NetApp-cloudmanager_입니다.

데이터 계층화 및 백업을 위한 서비스 계정을 생성합니다

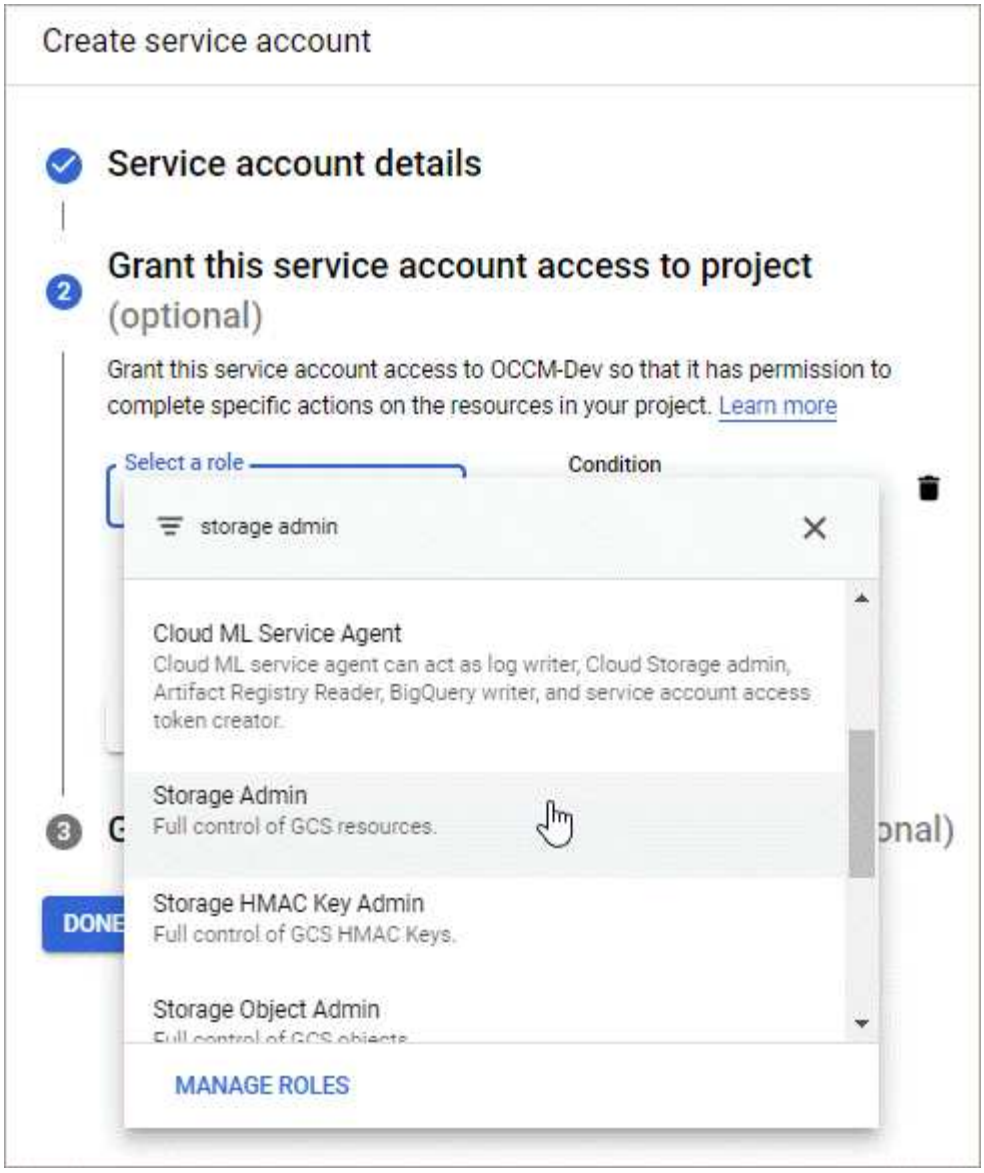
Cloud Volumes ONTAP를 사용하려면 Google Cloud 서비스 계정이 두 가지 용도로 필요합니다. 첫 번째는 를 활성화하는 것입니다 "데이터 계층화" Google Cloud에서 콜드 데이터를 저비용 오브젝트 스토리지로 계층화합니다. 두 번째는 를 활성화하는 것입니다 "BlueXP 백업 및 복구" 볼륨을 저렴한 오브젝트 스토리지에 백업

Cloud Volumes ONTAP는 서비스 계정을 사용하여 계층화된 데이터에 대한 하나의 버킷과 백업을 위한 다른 버킷에 액세스하고 관리합니다.

하나의 서비스 계정을 설정하고 두 가지 용도로 사용할 수 있습니다. 서비스 계정에는 * 스토리지 관리자 * 역할이 있어야 합니다.

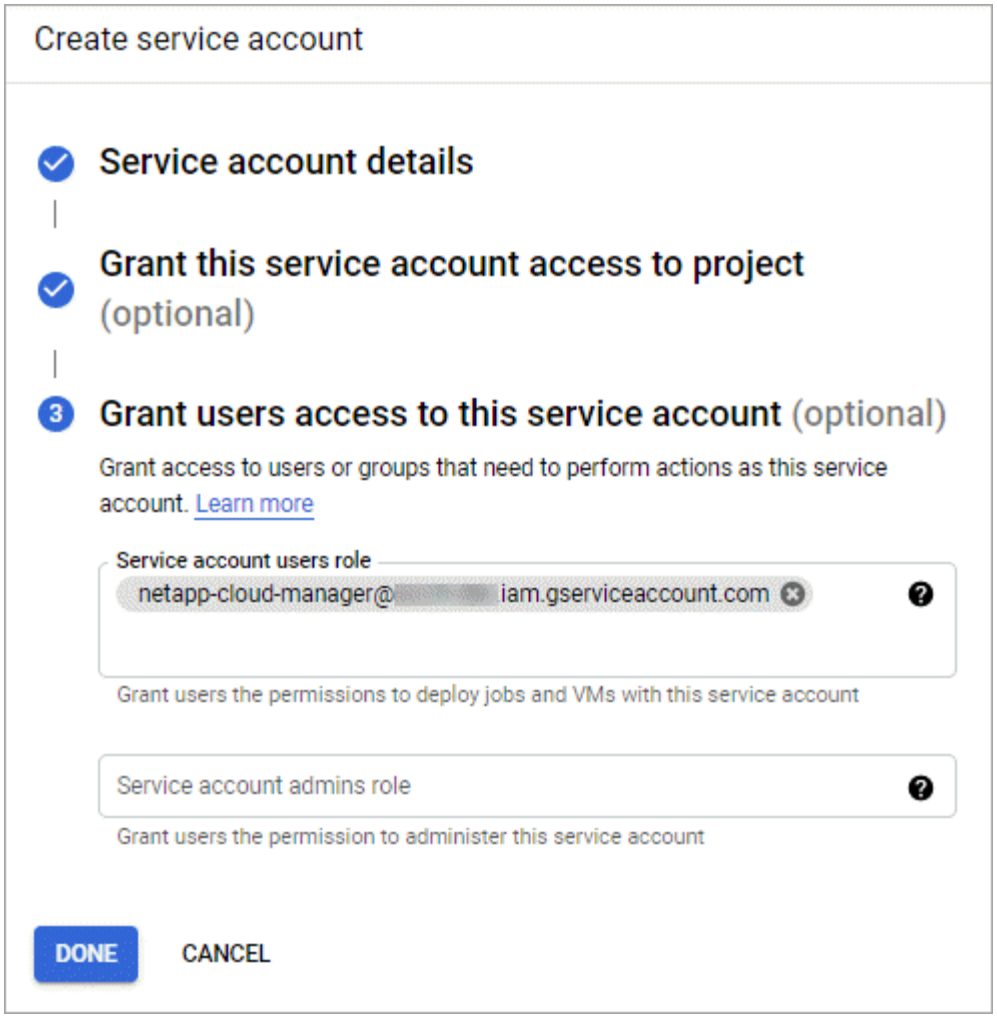
단계

1. Google Cloud 콘솔에서 "서비스 계정 페이지로 이동합니다".
2. 프로젝트를 선택합니다.
3. 서비스 계정 생성 * 을 클릭하고 필요한 정보를 입력합니다.
    a. * 서비스 계정 세부 정보 *: 이름과 설명을 입력합니다.
    b. * 프로젝트에 대한 이 서비스 계정 액세스 권한 부여 *: * 스토리지 관리자 * 역할을 선택합니다.



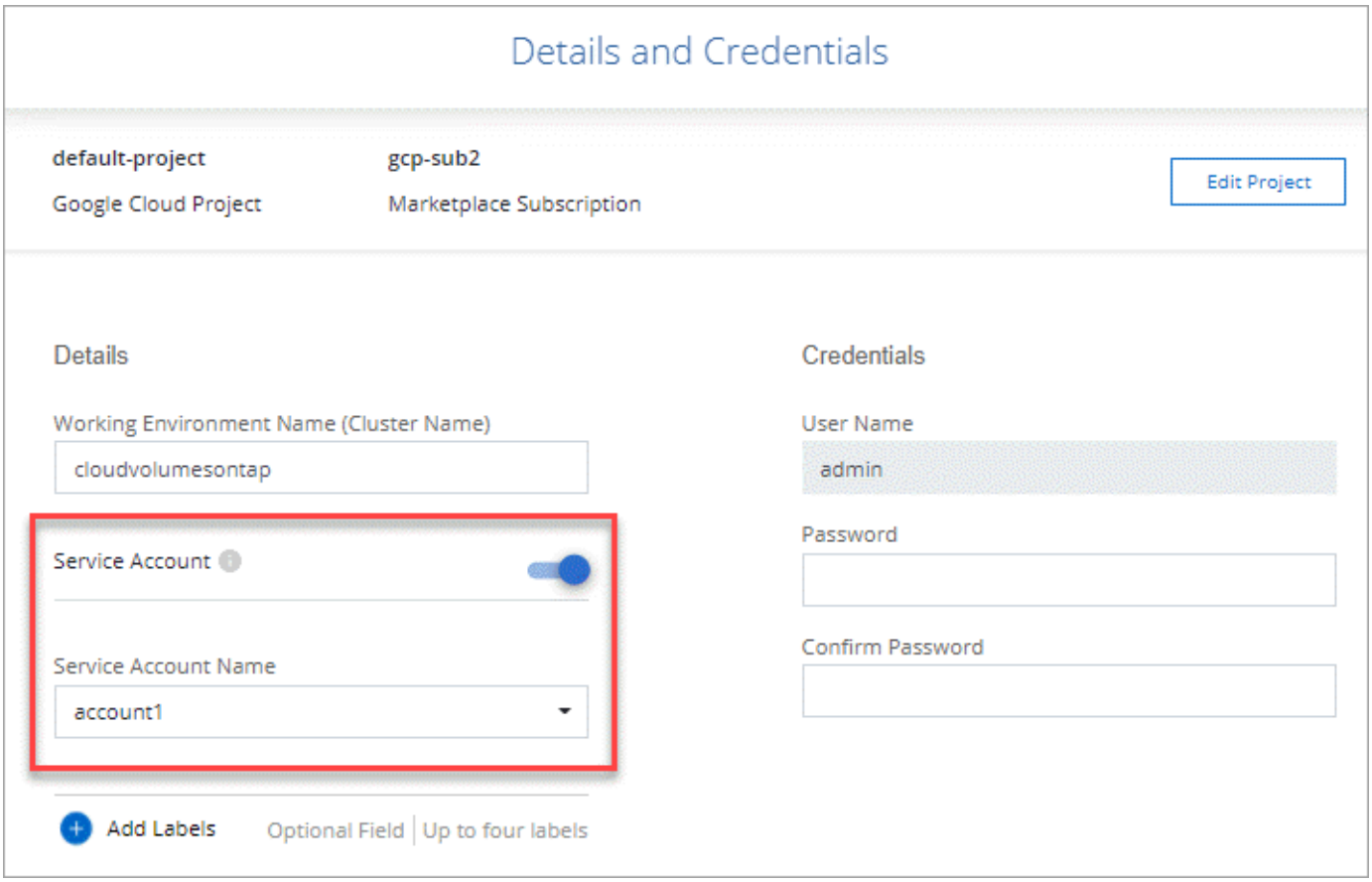
c. 이 서비스 계정에 대한 사용자 액세스 허용 *: Connector 서비스 계정을 이 새 서비스 계정에 _ 서비스 계정 사용자로 추가 _.

이 단계는 데이터 계층화에만 필요합니다. BlueXP 백업 및 복구에는 필요하지 않습니다.



다음 단계

Cloud Volumes ONTAP 작업 환경을 생성할 때 나중에 서비스 계정을 선택해야 합니다.



Cloud Volumes ONTAP에서 고객이 관리하는 암호화 키 사용

Google 클라우드 스토리지는 디스크에 데이터를 쓰기 전에 항상 데이터를 암호화하지만 BlueXP API를 사용하여 고객이 관리하는 암호화 키 를 사용하는 Cloud Volumes ONTAP 시스템을 만들 수 있습니다. 클라우드 키 관리 서비스를 사용하여 GCP에서 생성하고 관리하는 키입니다.

단계

1. BlueXP Connector 서비스 계정의 프로젝트 수준에서 키가 저장된 프로젝트에 대한 올바른 권한이 있는지 확인합니다.

   사용 권한은 에 제공됩니다 "기본적으로 커넥터 서비스 계정 권한이 있습니다", 그러나 클라우드 키 관리 서비스에 대체 프로젝트를 사용하는 경우에는 적용되지 않을 수 있습니다.

   사용 권한은 다음과 같습니다.

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. 에 대한 서비스 계정이 있는지 확인합니다 "Google Compute Engine 서비스 에이전트입니다" Cloud KMS Encrypter/Decrypter 권한이 키에 있습니다.

서비스 계정 이름은 "service-[service_project_number]@compute-system.iam.gserviceaccount.com" 형식을 사용합니다.

"Google Cloud 설명서: IAM을 Cloud KMS-Granting 역할과 함께 리소스에 사용"

3. 에 대한 get 명령을 호출하여 키의 "id"를 가져옵니다 `/gcp/vsa/metadata/gcp-encryption-keys` API를 호출하거나 GCP 콘솔의 키에서 "Copy Resource Name"을 선택합니다.
4. 고객이 관리하는 암호화 키를 사용하고 데이터를 오브젝트 스토리지에 계층화하는 경우 BlueXP는 영구 디스크를 암호화하는 데 사용되는 동일한 키를 사용하려고 합니다. 하지만 먼저 Google Cloud Storage 버킷을 활성화하여 키를 사용해야 합니다.

   a. 에 따라 Google Cloud Storage 서비스 에이전트를 찾습니다 "Google Cloud 설명서: 클라우드 스토리지 서비스 에이전트 얻기".

   b. 암호화 키로 이동하여 Cloud KMS Encrypter/Decrypter 권한이 있는 Google Cloud Storage 서비스 에이전트를 할당합니다.

   자세한 내용은 을 참조하십시오 "Google Cloud 설명서: 고객이 관리하는 암호화 키 사용"

5. 작업 환경을 만들 때 API 요청과 함께 "GcpEncryption" 매개 변수를 사용합니다.

   ◦ 예 *

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-
1/cryptoKeys/generatedkey1"
  }
```

을 참조하십시오 "BlueXP 자동화 문서" "GcpEncryption" 매개 변수 사용에 대한 자세한 내용은 를 참조하십시오.

Google Cloud에서 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".

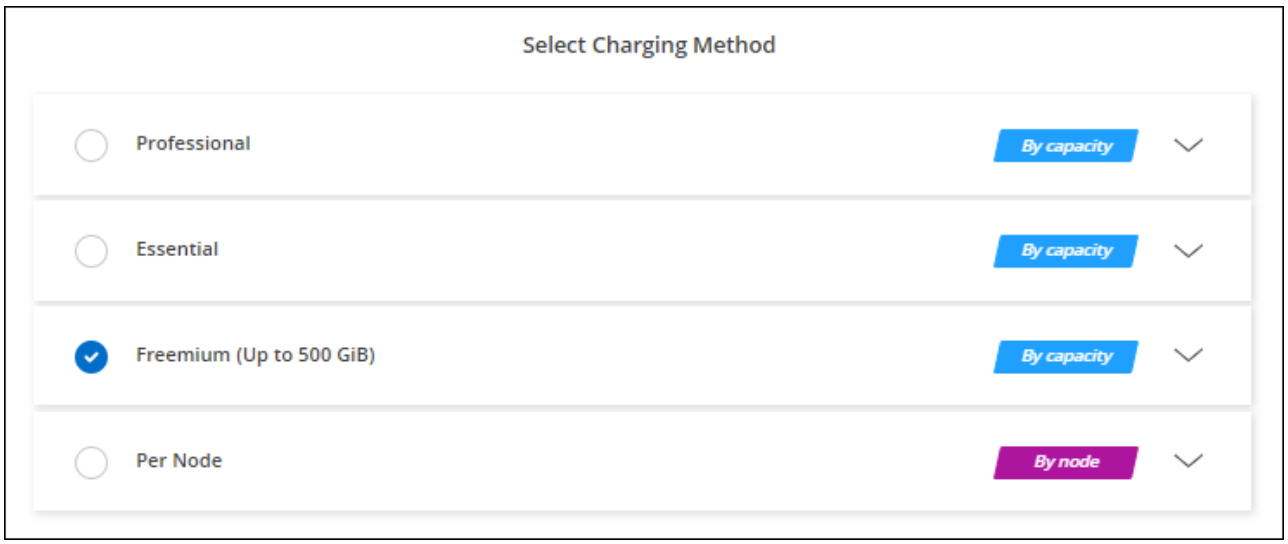
단계

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

   a. 상세 정보 및 자격 증명 * 페이지에서 * 자격 증명 편집 > 구독 추가 * 를 클릭한 다음 화면의 지시에 따라 Google Cloud 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".

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



"Google Cloud에서 Cloud Volumes ONTAP를 실행하기 위한 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
- Google Cloud Marketplace에서 PAYGO(pay-as-you-go) 방식으로 구독을 지원합니다
- 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.

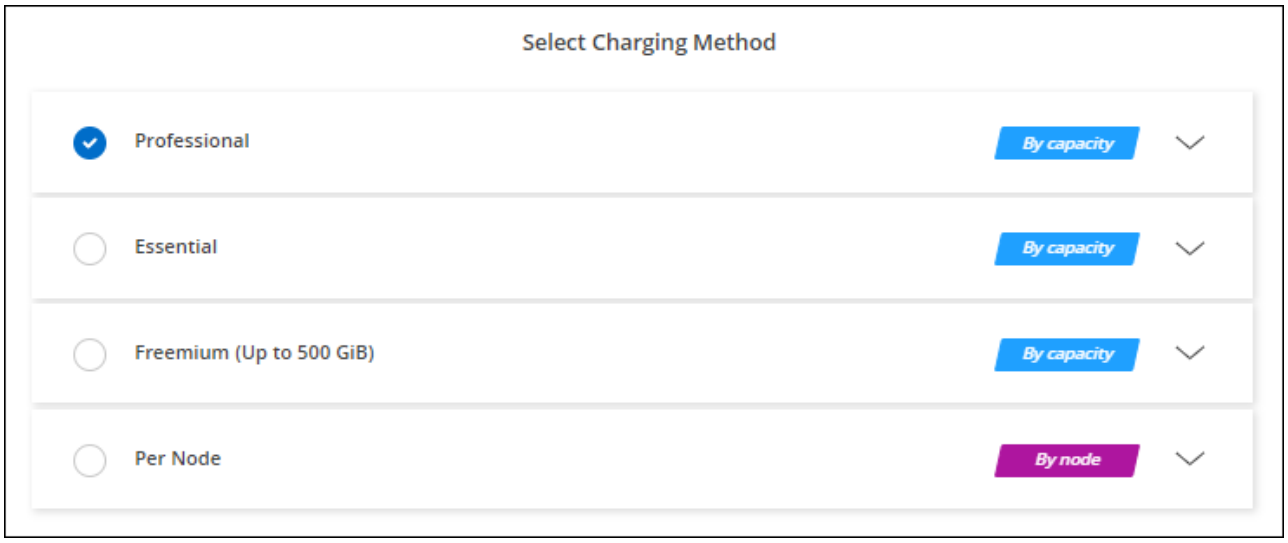
   Cloud Volumes ONTAP와 함께 사용하기 전에 BlueXP 디지털 지갑에서 라이센스를 사용할 수 있어야 합니다. 필요한 경우, 할 수 있습니다 "BlueXP 디지털 지갑에 라이센스를 수동으로 추가합니다".

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

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

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

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



"Google Cloud에서 Cloud Volumes ONTAP를 실행하기 위한 단계별 지침을 확인하십시오".

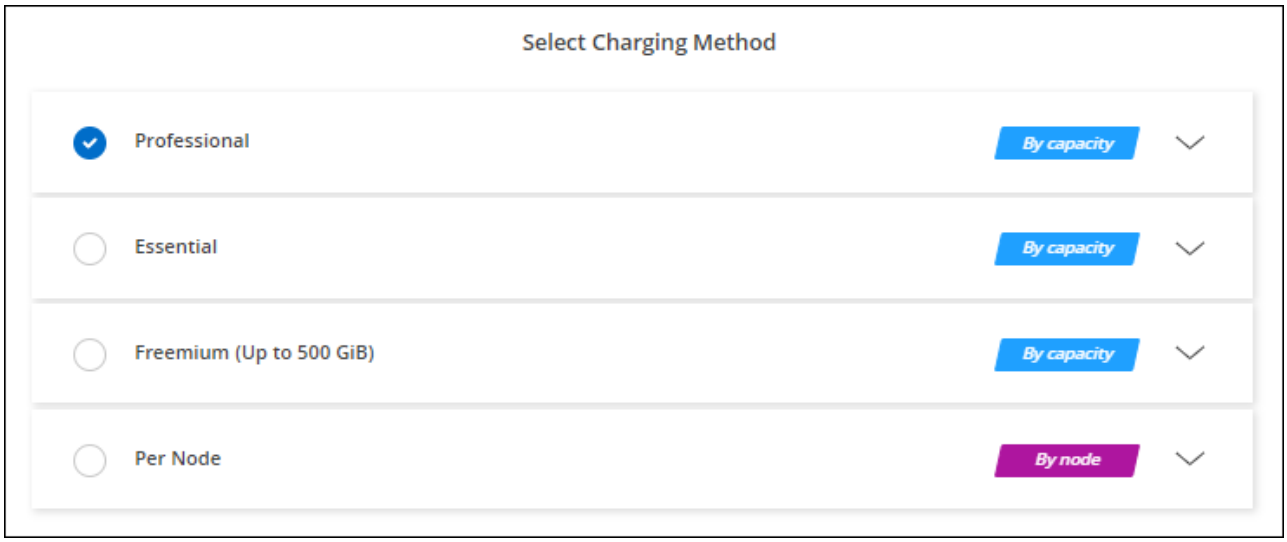
PAYGO 구독

클라우드 공급자 마켓플레이스의 서비스에 가입하여 시간별 비용 지불

Cloud Volumes ONTAP 작업 환경을 만들 때 BlueXP는 Google Cloud Marketplace에서 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. 상세 정보 및 자격 증명 * 페이지에서 * 자격 증명 편집 > 구독 추가 * 를 클릭한 다음 화면의 지시에 따라 Google Cloud Marketplace에서 선불 종량제 서비스를 구독합니다.
   b. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 용량 기반 패키지를 선택합니다.



"Google Cloud에서 Cloud Volumes ONTAP를 실행하기 위한 단계별 지침을 확인하십시오".

설정 > 자격 증명 페이지에서 계정과 연결된 Google Cloud Marketplace 구독을 관리할 수 있습니다. "Google Cloud 자격 증명 및 구독을 관리하는 방법을 알아보십시오"

연간 계약

연간 계약을 구매하여 매년 Cloud Volumes ONTAP에 대한 비용을 지불합니다.

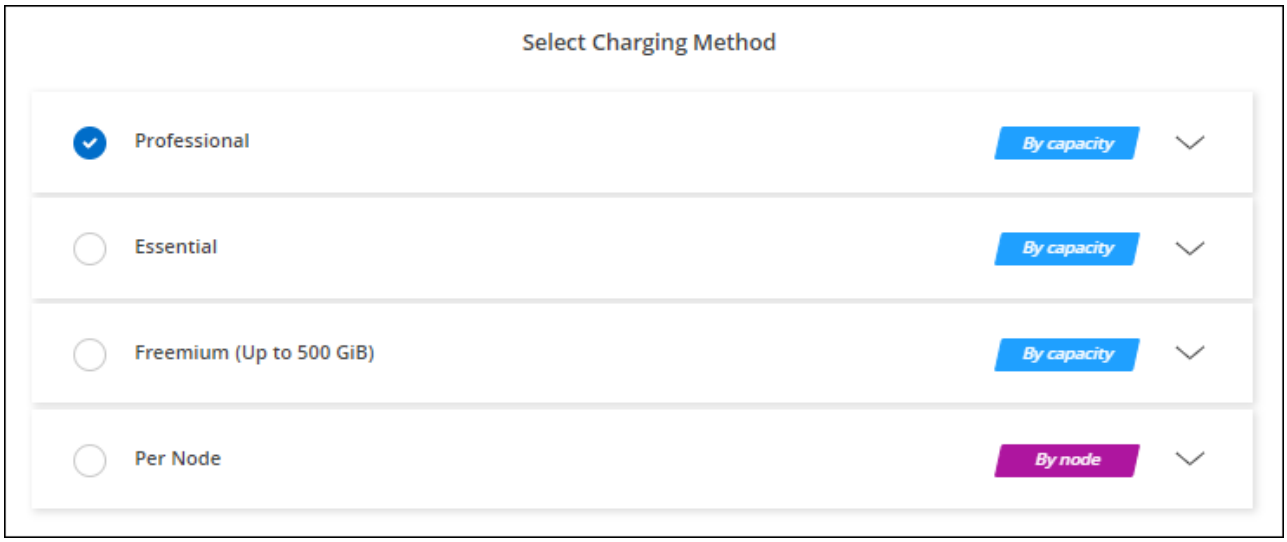
단계

1. 연간 계약을 구입하려면 NetApp 세일즈 담당자에게 문의하십시오.

   이 계약은 Google Cloud Marketplace에서 _private_Offer로 제공됩니다.

   NetApp이 프라이빗 오퍼를 공유하면 근무 환경을 생성하는 동안 Google Cloud Marketplace에서 가입할 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 * 를 클릭한 다음 표시되는 메시지에 따라 Google Cloud Marketplace에서 연간 계획을 구독합니다.
   b. Google Cloud에서 계정과 공유된 연간 계획을 선택한 다음 * 구독 * 을 클릭합니다.
   c. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 용량 기반 패키지를 선택합니다.



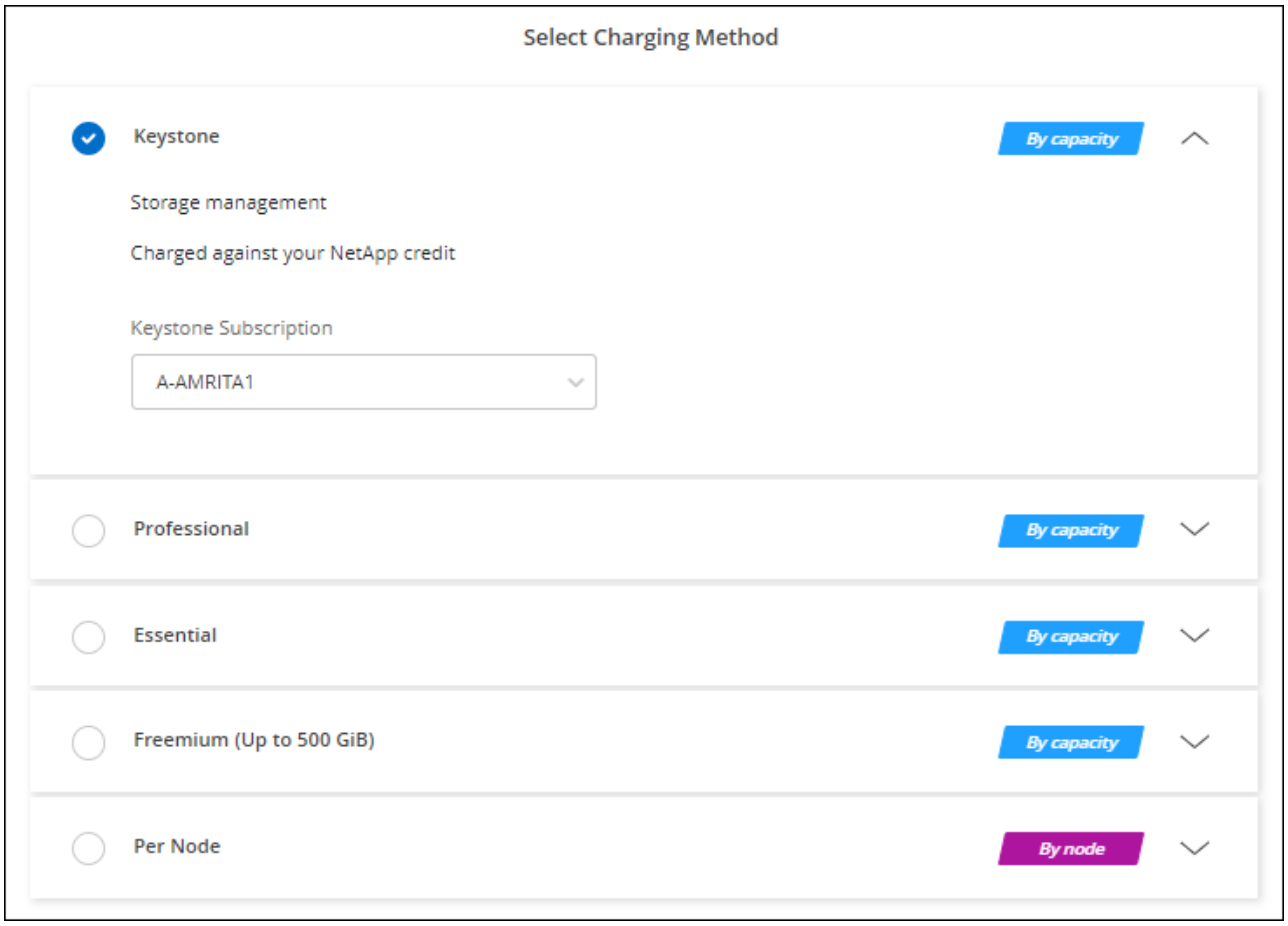
"Google Cloud에서 Cloud Volumes ONTAP를 실행하기 위한 단계별 지침을 확인하십시오".

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.



"Google Cloud에서 Cloud Volumes ONTAP를 실행하기 위한 단계별 지침을 확인하십시오".

Google Cloud에서 Cloud Volumes ONTAP 실행

단일 노드 구성에서 Cloud Volumes ONTAP를 실행하거나 Google Cloud에서 HA 쌍으로 실행할 수 있습니다.

시작하기 전에

작업 환경을 만들려면 다음이 필요합니다.

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

  구성을 선택하고 관리자로부터 Google Cloud 네트워킹 정보를 받아 준비해야 합니다. 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP 구성 계획".

- Cloud Volumes ONTAP에 대한 라이센스 설정에 필요한 사항을 이해합니다.

"라이센스 설정 방법에 대해 알아보십시오".

- Google Cloud API는 입니다 "프로젝트에서 활성화됩니다":
  - Cloud Deployment Manager V2 API
  - 클라우드 로깅 API
  - Cloud Resource Manager API를 참조하십시오
  - 컴퓨팅 엔진 API
  - IAM(Identity and Access Management) API

Google Cloud에서 단일 노드 시스템 실행

BlueXP에서 작업 환경을 만들어 Google Cloud에서 Cloud Volumes ONTAP를 실행합니다.

단계

1. 왼쪽 탐색 메뉴에서 * Storage > Canvas * 를 선택합니다.
2. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 화면의 지시를 따릅니다.
3. * 위치 선택 *: * Google Cloud * 및 * Cloud Volumes ONTAP * 를 선택합니다.
4. 메시지가 표시되면 "커넥터를 작성합니다".
5. * 세부 정보 및 자격 증명 *: 프로젝트를 선택하고 클러스터 이름을 지정한 다음 서비스 계정을 선택하고 선택적으로 레이블을 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 Google Cloud VM 인스턴스 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
서비스 계정 이름입니다	를 사용할 계획인 경우 "데이터 계층화" 또는 "BlueXP 백업 및 복구" Cloud Volumes ONTAP를 사용하는 경우 * 서비스 계정 * 을 활성화하고 사전 정의된 스토리지 관리 역할이 있는 서비스 계정을 선택해야 합니다. "서비스 계정을 만드는 방법에 대해 알아봅니다".
레이블 추가	레이블은 Google Cloud 리소스의 메타데이터입니다. BlueXP는 시스템에 연결된 Cloud Volumes ONTAP 시스템 및 Google Cloud 리소스에 레이블을 추가합니다. 작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 레이블을 추가할 수 있으며, 그런 다음 만든 후에 레이블을 더 추가할 수 있습니다. API는 작업 환경을 만들 때 레이블을 네 개로 제한하지 않습니다. 레이블에 대한 자세한 내용은 을 참조하십시오 "Google Cloud 설명서: 라벨 리소스".
사용자 이름 및 암호	Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하여 System Manager 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다. default_admin_user 이름을 유지하거나 사용자 지정 사용자 이름으로 변경합니다.

필드에 입력합니다	설명
프로젝트 편집	Cloud Volumes ONTAP가 상주할 프로젝트를 선택합니다. 기본 프로젝트는 BlueXP가 있는 프로젝트입니다. 드롭다운 목록에 추가 프로젝트가 표시되지 않으면 BlueXP 서비스 계정을 다른 프로젝트와 연결하지 않은 것입니다. Google Cloud 콘솔로 이동하여 IAM 서비스를 열고 프로젝트를 선택합니다. BlueXP 역할이 있는 서비스 계정을 해당 프로젝트에 추가합니다. 각 프로젝트에 대해 이 단계를 반복해야 합니다. BlueXP에 대해 설정한 서비스 계정입니다. "이 페이지에 설명되어 있습니다". 선택한 자격 증명을 구독과 연결하려면 * 구독 추가 * 를 클릭합니다. 선불 종량제 Cloud Volumes ONTAP 시스템을 생성하려면 Google 클라우드 마켓플레이스에서 Cloud Volumes ONTAP 구독과 연결된 Google Cloud 프로젝트를 선택해야 합니다.

다음 비디오에서는 선불 종량제 마켓플레이스 구독을 Google Cloud 프로젝트에 연결하는 방법을 보여 줍니다. 또는 에 있는 구독 단계를 따릅니다 "Google Cloud 자격 증명과 마켓플레이스 가입 연결" 섹션을 참조하십시오.

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

6. * 서비스 *: 이 시스템에서 사용할 서비스를 선택합니다. BlueXP 백업 및 복구를 선택하거나 BlueXP 계층화를 사용하려면 3단계에서 서비스 계정을 지정해야 합니다.

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

7. * 위치 및 연결 *: 위치를 선택하고 방화벽 정책을 선택한 다음 데이터 계층화를 위해 Google Cloud 스토리지에 대한 네트워크 연결을 확인합니다.

   다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
연결 검증	콜드 데이터를 Google 클라우드 스토리지 버킷에 계층화하려면 Cloud Volumes ONTAP가 상주하는 서브넷을 프라이빗 Google 액세스용으로 구성해야 합니다. 자세한 지침은 을 참조하십시오 "Google Cloud 설명서: 개인 Google Access 구성".
방화벽 정책을 생성했습니다	BlueXP에서 방화벽 정책을 생성하도록 허용할 경우 트래픽을 허용하는 방법을 선택해야 합니다. • 선택한 VPC 전용 * 을 선택한 경우 인바운드 트래픽에 대한 소스 필터는 선택한 VPC의 서브넷 범위와 커넥터가 있는 VPC의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다. • 모든 VPC * 를 선택한 경우 인바운드 트래픽의 소스 필터는 0.0.0.0/0 IP 범위입니다.

필드에 입력합니다	설명
기존 방화벽 정책을 사용합니다	기존 방화벽 정책을 사용하는 경우 필수 규칙이 포함되어 있는지 확인합니다. 링크: Learn Cloud Volumes ONTAP의 방화벽 규칙 정보.

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 *: 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.
10. * 라이선스 *: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 시스템 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. * 기본 스토리지 리소스 *: 초기 집계에 대한 설정(디스크 유형 및 각 디스크의 크기)을 선택합니다.

    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 "Google Cloud에서 시스템 크기를 조정합니다".
12. * Flash Cache, 쓰기 속도 및 WORM *:
    a. 필요한 경우 * Flash Cache * 를 활성화합니다.

       Cloud Volumes ONTAP 9.13.1 부터, _Flash Cache_는 n2-standard-16, n2-standard-32, n2-standard-48, n2-standard-64 인스턴스 유형에서 지원됩니다. 구축 후에는 Flash Cache를 사용하지 않도록 설정할 수 없습니다.

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

       "쓰기 속도에 대해 자세히 알아보십시오".

       고속 * 쓰기 속도 옵션을 통해 896바이트의 고속 쓰기 속도와 높은 최대 전송 단위(MTU)를 사용할 수 있습니다. 또한, 8,896의 MTU가 높을수록 구축을 위해 VPC-1, VPC-2 및 VPC-3을 선택해야 합니다. VPC-1, VPC-2 및 VPC-3에 대한 자세한 내용은 을 참조하십시오 "VPC-1, VPC-2 및 VPC-3에 대한 규칙".

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

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.

13. * Google Cloud Platform의 데이터 계층화 *: 초기 애그리게이트에서 데이터 계층화를 사용할지 여부를 선택하고, 계층형 데이터에 대한 스토리지 클래스를 선택한 다음 사전 정의된 스토리지 관리 역할이 있는 서비스 계정을 선택합니다(Cloud Volumes ONTAP 9.7 이상에 필요). 또는 Google 클라우드 계정을 선택합니다(Cloud Volumes ONTAP 9.6의 경우 필수).

    다음 사항에 유의하십시오.

    - BlueXP는 Cloud Volumes ONTAP 인스턴스에 서비스 계정을 설정합니다. 이 서비스 계정은 Google Cloud Storage 버킷에 대한 데이터 계층화 권한을 제공합니다. Connector 서비스 계정을 계층화 서비스 계정의 사용자로 추가해야 합니다. 그렇지 않으면 BlueXP에서 선택할 수 없습니다
    - Google Cloud 계정 추가에 대한 도움말은 을 참조하십시오 "9.6의 데이터 계층화를 위한 Google Cloud 계정 설정 및 추가".
    - 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
    - 데이터 계층화를 사용하지 않는 경우, 후속 애그리게이트에서 사용하도록 설정할 수 있지만 시스템을 끄고 Google Cloud 콘솔에서 서비스 계정을 추가해야 합니다.

      "데이터 계층화에 대해 자세히 알아보십시오".

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

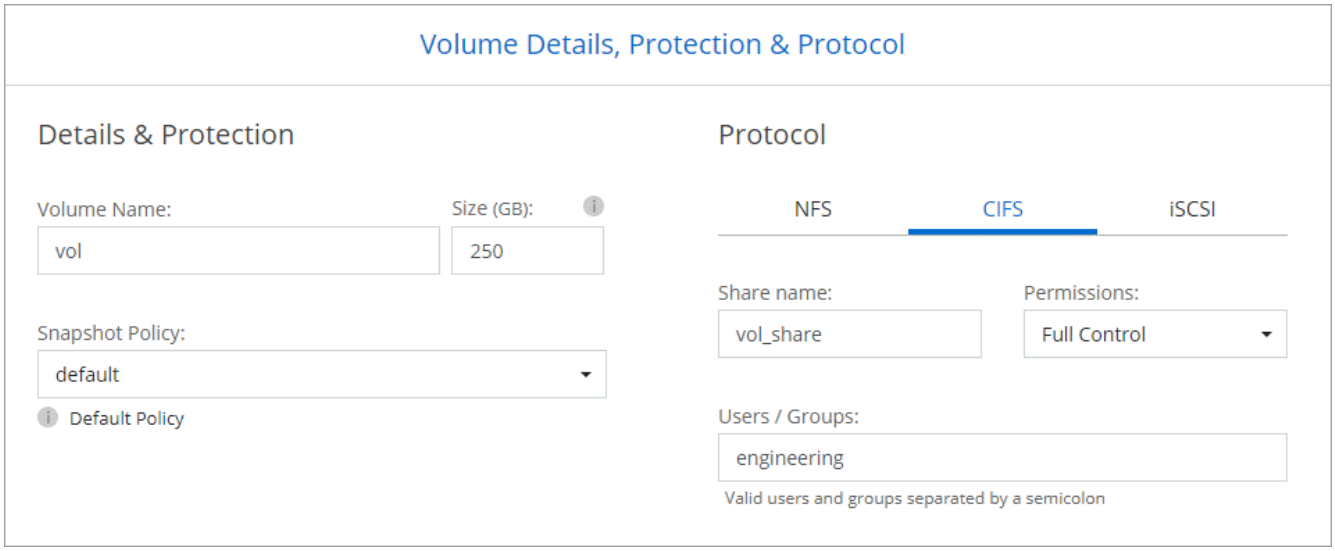
    "지원되는 클라이언트 프로토콜 및 버전에 대해 알아보십시오".

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

필드에 입력합니다	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝의 사용 여부에 따라 크게 달라집니다. 이를 통해 현재 사용 가능한 물리적 스토리지보다 더 큰 볼륨을 생성할 수 있습니다.
액세스 제어(NFS에만 해당)	엑스포트 정책은 볼륨에 액세스할 수 있는 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

필드에 입력합니다	설명
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.



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

필드에 입력합니다	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다. Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다.
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. Google 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 * OU=Computers, OU=Cloud * 를 입력합니다. "Google 클라우드 문서: Google Managed Microsoft AD의 조직 단위"
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.

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

    자세한 내용은 을 참조하십시오 "볼륨 사용 프로필을 선택합니다" 및 "데이터 계층화 개요".

17. * 검토 및 승인 *: 선택 사항을 검토 및 확인합니다.
    a. 구성에 대한 세부 정보를 검토합니다.
    b. BlueXP가 구매할 지원 및 Google Cloud 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.

Google Cloud에서 **HA** 쌍 시작

BlueXP에서 작업 환경을 만들어 Google Cloud에서 Cloud Volumes ONTAP를 실행합니다.

단계

1. 왼쪽 탐색 메뉴에서 * Storage > Canvas * 를 선택합니다.
2. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 화면의 지시를 따릅니다.
3. * 위치 선택 *: * Google Cloud * 및 * Cloud Volumes ONTAP HA * 를 선택합니다.
4. * 세부 정보 및 자격 증명 *: 프로젝트를 선택하고 클러스터 이름을 지정한 다음 서비스 계정을 선택하고 선택적으로 레이블을 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 Google Cloud VM 인스턴스 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
서비스 계정 이름입니다	를 사용할 계획인 경우 "BlueXP 계층화" 또는 "BlueXP 백업 및 복구" 서비스를 사용하려면 * 서비스 계정 * 스위치를 활성화한 다음 미리 정의된 스토리지 관리자 역할이 있는 서비스 계정을 선택해야 합니다.
레이블 추가	레이블은 Google Cloud 리소스의 메타데이터입니다. BlueXP는 시스템에 연결된 Cloud Volumes ONTAP 시스템 및 Google Cloud 리소스에 레이블을 추가합니다. 작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 레이블을 추가할 수 있으며, 그런 다음 만든 후에 레이블을 더 추가할 수 있습니다. API는 작업 환경을 만들 때 레이블을 네 개로 제한하지 않습니다. 레이블에 대한 자세한 내용은 을 참조하십시오 "Google Cloud 설명서: 라벨 리소스".
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.
프로젝트 편집	Cloud Volumes ONTAP가 상주할 프로젝트를 선택합니다. 기본 프로젝트는 BlueXP가 있는 프로젝트입니다. 드롭다운 목록에 추가 프로젝트가 표시되지 않으면 BlueXP 서비스 계정을 다른 프로젝트와 연결하지 않은 것입니다. Google Cloud 콘솔로 이동하여 IAM 서비스를 열고 프로젝트를 선택합니다. BlueXP 역할이 있는 서비스 계정을 해당 프로젝트에 추가합니다. 각 프로젝트에 대해 이 단계를 반복해야 합니다. BlueXP에 대해 설정한 서비스 계정입니다. "이 페이지에 설명되어 있습니다". 선택한 자격 증명을 구독과 연결하려면 * 구독 추가 * 를 클릭합니다. 선불 종량제 Cloud Volumes ONTAP 시스템을 생성하려면 Google 클라우드 마켓플레이스에서 Cloud Volumes ONTAP 구독과 연결된 Google Cloud 프로젝트를 선택해야 합니다.

다음 비디오에서는 선불 종량제 마켓플레이스 구독을 Google Cloud 프로젝트에 연결하는 방법을 보여 줍니다. 또는 에 있는 구독 단계를 따릅니다 "Google Cloud 자격 증명과 마켓플레이스 가입 연결" 섹션을 참조하십시오.

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

5. * 서비스 *: 이 시스템에서 사용할 서비스를 선택합니다. BlueXP 백업 및 복구를 선택하거나 BlueXP 계층화를 사용하려면 3단계에서 서비스 계정을 지정해야 합니다.

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

6. * HA 배포 모델 *: HA 구성에 대해 여러 영역(권장) 또는 단일 영역을 선택합니다. 그런 다음 지역 및 구역을 선택합니다.

   "HA 구축 모델 에 대해 자세히 알아보십시오".

7. * 연결 *: HA 구성을 위한 4개의 서로 다른 VPC, 각 VPC의 서브넷을 선택한 다음 방화벽 정책을 선택합니다.

   "네트워킹 요구 사항에 대해 자세히 알아보십시오".

   다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
생성된 정책	BlueXP에서 방화벽 정책을 생성하도록 허용할 경우 트래픽을 허용하는 방법을 선택해야 합니다. • 선택한 VPC 전용 * 을 선택한 경우 인바운드 트래픽에 대한 소스 필터는 선택한 VPC의 서브넷 범위와 커넥터가 있는 VPC의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다. • 모든 VPC * 를 선택한 경우 인바운드 트래픽의 소스 필터는 0.0.0.0/0 IP 범위입니다.
기존 항목 사용	기존 방화벽 정책을 사용하는 경우 필수 규칙이 포함되어 있는지 확인합니다. "Cloud Volumes ONTAP의 방화벽 규칙에 대해 알아보십시오".

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 *: 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.

10. * 라이선스 *: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 시스템 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. * 기본 스토리지 리소스 *: 초기 집계에 대한 설정(디스크 유형 및 각 디스크의 크기)을 선택합니다.

    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 "Google Cloud에서 시스템 크기를 조정합니다".

12. * Flash Cache, 쓰기 속도 및 WORM *:

    a. 필요한 경우 * Flash Cache * 를 활성화합니다.

    > Cloud Volumes ONTAP 9.13.1 부터, _Flash Cache_는 n2-standard-16, n2-standard-32, n2-standard-48, n2-standard-64 인스턴스 유형에서 지원됩니다. 구축 후에는 Flash Cache를 사용하지 않도록 설정할 수 없습니다.

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

    "쓰기 속도에 대해 자세히 알아보십시오".

    > 고속 쓰기 속도와 896바이트의 최대 전송 단위(MTU)는 n2-standard-16, n2-standard-32, n2-standard-48 및 n2-standard-64 인스턴스 유형의 * 고속 * 쓰기 속도 옵션을 통해 사용할 수 있습니다. 또한, 8,896의 MTU가 높을수록 구축을 위해 VPC-1, VPC-2 및 VPC-3을 선택해야 합니다. 높은 쓰기 속도 및 8,896의 MTU는 기능에 따라 다르며 구성된 인스턴스 내에서 개별적으로 비활성화할 수 없습니다. VPC-1, VPC-2 및 VPC-3에 대한 자세한 내용은 을 참조하십시오 "VPC-1, VPC-2 및 VPC-3에 대한 규칙".

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

    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.

13. * Google Cloud의 데이터 계층화 *: 초기 애그리게이트에서 데이터 계층화를 사용할지 여부를 선택하고, 계층형 데이터에 대한 스토리지 클래스를 선택한 다음 사전 정의된 스토리지 관리 역할이 있는 서비스 계정을 선택합니다.

    다음 사항에 유의하십시오.

    - BlueXP는 Cloud Volumes ONTAP 인스턴스에 서비스 계정을 설정합니다. 이 서비스 계정은 Google Cloud Storage 버킷에 대한 데이터 계층화 권한을 제공합니다. Connector 서비스 계정을 계층화 서비스 계정의 사용자로 추가해야 합니다. 그렇지 않으면 BlueXP에서 선택할 수 없습니다.
    - 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
    - 데이터 계층화를 사용하지 않는 경우, 후속 애그리게이트에서 사용하도록 설정할 수 있지만 시스템을 끄고 Google Cloud 콘솔에서 서비스 계정을 추가해야 합니다.

"데이터 계층화에 대해 자세히 알아보십시오".

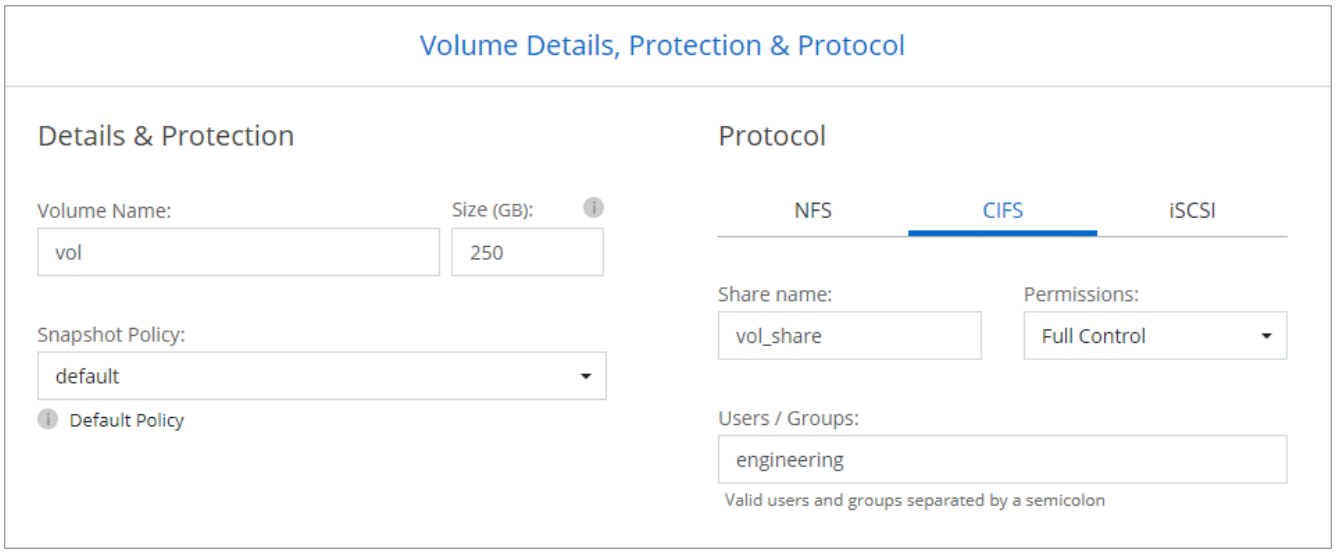
14. * 볼륨 생성 *: 새 볼륨에 대한 세부 정보를 입력하거나 * 건너뛰기 * 를 클릭합니다.

"지원되는 클라이언트 프로토콜 및 버전에 대해 알아보십시오".

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

필드에 입력합니다	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝의 사용 여부에 따라 크게 달라집니다. 이를 통해 현재 사용 가능한 물리적 스토리지보다 더 큰 볼륨을 생성할 수 있습니다.
액세스 제어(NFS에만 해당)	엑스포트 정책은 볼륨에 액세스할 수 있는 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.



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

필드에 입력합니다	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다. Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다.
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. Google 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 * OU=Computers, OU=Cloud * 를 입력합니다. "Google 클라우드 문서: Google Managed Microsoft AD의 조직 단위"
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.

16. * Usage Profile, Disk Type, Tiering Policy *: 스토리지 효율성 기능을 사용하도록 설정하고 필요한 경우 볼륨

계층화 정책을 변경할 것인지 선택합니다.

자세한 내용은 을 참조하십시오 "볼륨 사용 프로필을 선택합니다" 및 "데이터 계층화 개요".

17. * 검토 및 승인 *: 선택 사항을 검토 및 확인합니다.
    a. 구성에 대한 세부 정보를 검토합니다.
    b. BlueXP가 구매할 지원 및 Google Cloud 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.

Google Cloud Platform 이미지 검증

Google Cloud 이미지 검증 개요

Google Cloud 이미지 검증은 향상된 NetApp 보안 요구사항을 준수합니다. 이 작업을 위해 특별히 생성된 개인 키를 사용하여 이미지를 생성하는 스크립트가 변경되었습니다. 를 통해 다운로드할 수 있는 Google Cloud용 서명된 다이제스트 및 공용 인증서를 사용하여 GCP 이미지의 무결성을 확인할 수 있습니다 "NSS" 특정 릴리스에 대해.

Google 클라우드 이미지 확인은 Cloud Volumes ONTAP 소프트웨어 버전 9.13.0 이상에서 지원됩니다.

Google Cloud에서 이미지를 RAW 형식으로 변환합니다

새 인스턴스 배포, 업그레이드 또는 기존 이미지에 사용 중인 이미지는 를 통해 클라이언트와 공유됩니다 "NetApp Support 사이트(NSS)". 서명된 다이제스트 및 인증서는 NSS 포털을 통해 다운로드할 수 있습니다. NetApp Support에서 공유하는 이미지에 해당하는 오른쪽 릴리즈에 대한 다이제스트 및 인증서를 다운로드했는지 확인합니다. 예를 들어 9.13.0 이미지는 9.13.0 서명된 다이제스트와 NSS에서 사용할 수 있는 인증서를 갖습니다.

이 단계가 필요한 이유는 무엇입니까**?**

Google Cloud의 이미지는 직접 다운로드할 수 없습니다. 서명된 다이제스트 및 인증서와 이미지를 비교하려면 두 파일을 비교하여 이미지를 다운로드하는 메커니즘이 있어야 합니다. 이렇게 하려면 이미지를 disk.raw 형식으로 내보내기/변환하고 결과를 Google Cloud의 저장 버킷에 저장해야 합니다. disk.raw 파일이 tarred로 압축되어 있습니다.

사용자/서비스 계정에는 다음 작업을 수행할 수 있는 권한이 필요합니다.

- Google 스토리지 버킷에 액세스
- Google Storage 버킷에 쓰십시오
- 클라우드 구축 작업 생성(내보내기 프로세스 중 사용)
- 원하는 이미지에 액세스합니다
- 이미지 내보내기 작업을 만듭니다

이미지를 확인하려면 disk.raw 형식으로 변환한 다음 다운로드해야 합니다.

Google Cloud 명령줄을 사용하여 **Google Cloud** 이미지를 내보냅니다

이미지를 클라우드 스토리지로 내보내는 기본 방법은 을 사용하는 것입니다 "gcloud 계산 이미지 내보내기 명령". 이 명령은 제공된 이미지를 가져와 tarred와 gzip이 되는 disk.raw 파일로 변환합니다. 생성된 파일은 대상 URL에 저장되며 확인을 위해 다운로드할 수 있습니다.

이 작업을 실행하려면 사용자/계정에 원하는 버킷에 액세스하고 쓰거나 이미지를 내보내고 Google에서 이미지를 내보낼 때 사용하는 클라우드 빌드에 액세스할 수 있는 권한이 있어야 합니다.

- gcloud * 를 사용하여 Google Cloud 이미지를 내보냅니다

스크립트를 표시하려면 클릭합니다

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

압축 파일 압축 풀기 *

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

을 참조하십시오 "이미지 내보내기에 대한 Google Cloud 문서" Google Cloud를 통해 이미지를 내보내는 방법에 대한 자세한 내용은

이미지 서명 확인

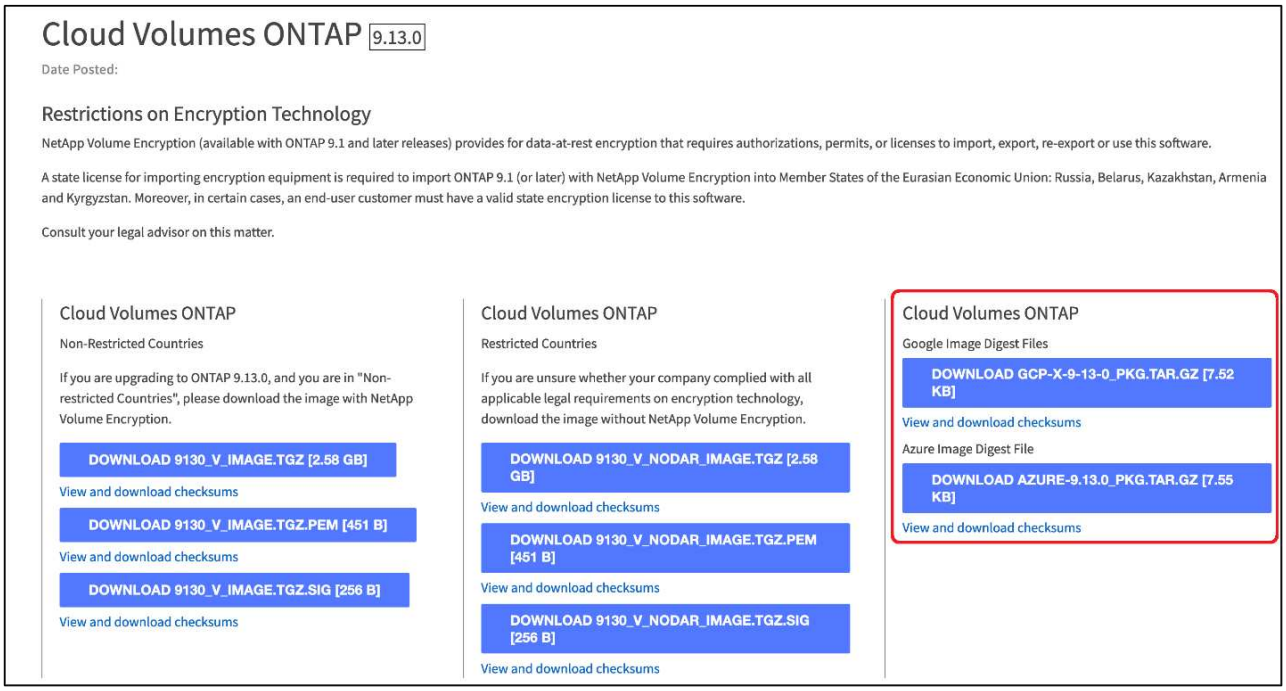
Google Cloud 서명 이미지를 확인합니다

내보낸 Google Cloud 서명 이미지를 확인하려면 NSS에서 이미지 다이제스트 파일을 다운로드하여 disk.raw 파일의 유효성을 검사하고 파일 내용을 다이제해야 합니다.

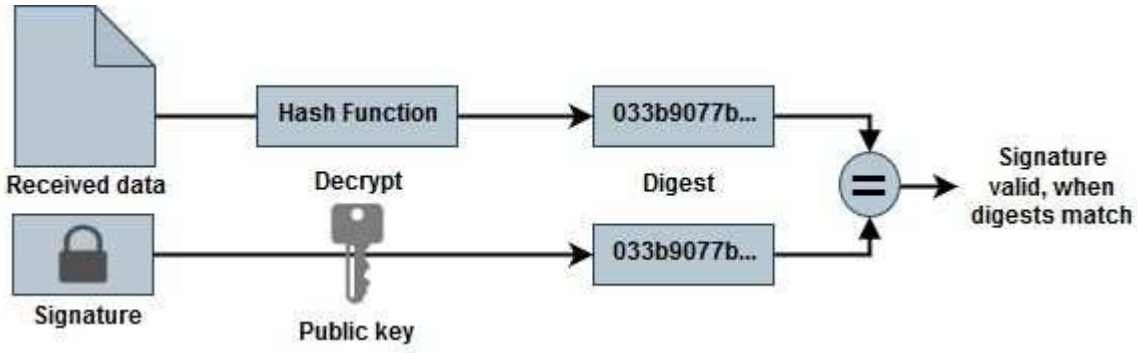
서명된 이미지 검증 워크플로 요약

다음은 Google Cloud 서명 이미지 검증 워크플로 프로세스에 대한 개요입니다.

- 에서 "NSS"에서 다음 파일이 포함된 Google Cloud 아카이브를 다운로드합니다.
  - 서명된 다이제스트(.SIG)
  - 공개 키(.pem)가 포함된 인증서
  - 인증서 체인(.pem)



- 변환된 disk.raw 파일을 다운로드합니다
- 인증서 체인을 사용하여 인증서의 유효성을 검사합니다
- 인증서에 공개 키가 포함되어 있는 서명된 다이제스트를 확인합니다
  - 공개 키를 사용하여 서명된 다이제스트를 해독하여 이미지 파일의 다이제스트를 추출합니다
  - 다운로드한 disk.raw 파일의 다이제스트를 만듭니다
  - 검증을 위해 두 개의 다이제스트 파일을 비교합니다



OpenSSL을 사용하여 **disk.raw** 파일 및 다이제스트 파일 내용을 확인합니다

Google Cloud에서 다운로드한 disk.raw 파일을 을 통해 사용 가능한 다이제스트 파일 내용과 비교하여 확인할 수 있습니다 "NSS" OpenSSL 사용.

이미지의 유효성을 검사하는 OpenSSL 명령은 Linux, Mac OS 및 Windows 시스템과 호환됩니다.

단계

1. OpenSSL을 사용하여 인증서를 확인합니다.

스크립트를 표시하려면 클릭합니다

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
          e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
          22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
          38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
          fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
          bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. 다운로드한 disk.raw 파일, 서명 및 인증서를 디렉터리에 넣습니다.
3. OpenSSL을 사용하여 인증서에서 공개 키를 추출합니다.
4. 추출된 공개 키를 사용하여 서명을 해독하고 다운로드한 disk.raw 파일의 내용을 확인합니다.

스크립트를 표시하려면 클릭합니다

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```