퍼블릭 및 하이브리드 클라우드

NetApp Solutions

NetApp
May 10, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/netapp-solutions/ehc/ehc-overview.html on May 10, 2024. Always check docs.netapp.com for the latest.

목차

퍼블릭 및 하이브리드 클라우드

VMware 솔루션을 사용하는 NetApp 하이브리드 멀티 클라우드

VMware - 퍼블릭 클라우드

VMware를 사용하는 NetApp 하이브리드 멀티 클라우드 개요

대부분의 IT 조직은 하이브리드 클라우드 우선 접근 방식을 따릅니다. 전환 단계에 있는 이들 조직은 고객이 현재 IT 환경을 평가한 다음 평가 및 검색 결과를 기반으로 워크로드를 클라우드로 마이그레이션하고 있습니다.

클라우드로 마이그레이션하는 고객의 요인에는 탄력성 및 버스트, 데이터 센터 이탈, 데이터 센터 통합, 수명 종료 시나리오, 인수 합병, 인수 합병 등 이 마이그레이션의 이유는 각 조직 및 각 비즈니스 우선순위에 따라 달라질 수 있습니다. 하이브리드 클라우드로 전환할 때 클라우드 구축과 탄력성의 잠재력을 최대한 활용하려면 클라우드에 적합한 스토리지를 선택하는 것이 매우 중요합니다.

퍼블릭 클라우드의 VMware 클라우드 옵션

이 섹션에서는 각 클라우드 공급자가 해당 퍼블릭 클라우드 오퍼링 내에서 VMware SDDC(Software Defined Data Center) 및/또는 VCF(VMware Cloud Foundation) 스택을 지원하는 방법에 대해 설명합니다.

Azure VMware 솔루션

Azure VMware 솔루션은 Microsoft Azure 퍼블릭 클라우드 내에서 VMware DC를 완벽하게 작동하는 하이브리드 클라우드 서비스입니다. Azure VMware 솔루션은 Microsoft에서 완벽하게 관리 및 지원하는 타사 솔루션으로, Azure 인프라를 활용하는 VMware에서 검증되었습니다. 즉, Azure VMware 솔루션을 구축할 때 고객은 컴퓨팅 가상화를 위한 VMware ESXi, 하이퍼 컨버지드 스토리지를 위한 vSAN을 얻게 됩니다. 네트워킹 및 보안을 위한 NSX는 물론, Microsoft Azure의 세계적인 입지, 동급 최고의 데이터 센터 시설을 활용하고 네이티브 Azure 서비스 및 솔루션의 풍부한 에코시스템에 근접합니다.

AWS 기반 VMware 클라우드

VMware Cloud on AWS는 기본 AWS 서비스에 최적화된 액세스를 통해 VMware의 엔터프라이즈급 SDDC 소프트웨어를 AWS 클라우드에 제공합니다. VMware Cloud Foundation을 기반으로 하는 AWS 기반 VMware Cloud는 VMware의 컴퓨팅, 스토리지 및 네트워크 가상화 제품(VMware vSphere, VMware vSAN 및 VMware NSX)을 VMware vCenter Server 관리 기능과 통합하여 유연하고 전용 베어 메탈 AWS 인프라에서 실행되도록 최적화되었습니다.

Google Cloud VMware 엔진

Google Cloud VMware Engine은 Google Cloud의 고성능 확장형 인프라와 VMware Cloud Foundation 스택(VMware vSphere, vCenter, vSAN 및 NSX-T)을 기반으로 구축된 IaaS(Infrastructure-as-a-Service) 제품입니다 이 서비스를 사용하면 비용, 노력 또는 애플리케이션 재설계 또는 운영 재조정 위험 없이 기존 VMware 워크로드를 온프레미스 환경에서 Google Cloud Platform으로 원활하게 마이그레이션하거나 확장할 수 있습니다. Google에서 판매 및 지원하는 서비스로서 VMware와 긴밀하게 협력하고 있습니다.

SDDC 프라이빗 클라우드 및 NetApp Cloud Volumes 코로케이션을 통해 최소한의 네트워크 지연 시간으로 최상의 성능을 제공합니다.

알고 계셨습니까?

사용된 클라우드에 관계없이 VMware SDDC를 구축할 때 초기 클러스터에 포함되는 제품은 다음과 같습니다.

- 관리를 위해 vCenter Server 어플라이언스를 사용하여 컴퓨팅 가상화를 위한 VMware ESXi 호스트
- VMware vSAN 하이퍼 컨버지드 스토리지는 각 ESXi 호스트의 물리적 스토리지 자산을 통합합니다
- 관리를 위해 NSX Manager 클러스터를 사용하여 가상 네트워킹 및 보안을 위한 VMware NSX

스토리지 구성

스토리지 집약적인 워크로드를 호스팅하거나 클라우드 호스팅 VMware 솔루션에서 스케일아웃하려는 고객의 경우 기본 하이퍼 컨버지드 인프라는 확장이 컴퓨팅 및 스토리지 리소스 모두에 있어야 한다는 것을 나타냅니다.

Azure NetApp Files, Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP(세 가지 주요 하이퍼 스케일러 모두에서 사용 가능) 및 Cloud Volumes Service for Google Cloud와 같은 NetApp Cloud Volumes와 통합함으로써 고객은 이제 스토리지를 개별적으로 확장할 수 있는 옵션을 갖게 됩니다. 필요에 따라 SDDC 클러스터에만 컴퓨팅 노드를 추가할 수 있습니다.

참고:

- VMware는 불균형 클러스터 구성을 권장하지 않습니다. 따라서 스토리지를 확장한다는 것은 더 많은 호스트를 추가해야 한다는 것을 의미하며, 이는 더 많은 TCO를 의미합니다.
- 하나의 vSAN 환경만 가능합니다. 따라서 모든 스토리지 트래픽은 운영 워크로드와 직접 경쟁하게 됩니다.
- 애플리케이션 요구사항, 성능, 비용을 맞추기 위해 여러 성능 계층을 제공하는 옵션은 없습니다.
- 클러스터 호스트 위에 구축된 vSAN의 스토리지 용량 제한에 매우 쉽게 도달할 수 있습니다. NetApp Cloud Volumes를 사용하여 액티브 데이터 세트를 호스트하거나 영구 스토리지로 계층 쿨러 데이터를 계층화하도록 스토리지를 확장할 수 있습니다.

Azure NetApp Files, Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP(세 가지 주요 하이퍼 스케일러 모두에서 사용 가능) 및 Cloud Volumes Service for Google Cloud를 게스트 VM과 함께 사용할 수 있습니다. 이 하이브리드 스토리지 아키텍처는 게스트 운영 체제 및 애플리케이션 바이너리 데이터를 보관하는 vSAN 데이터스토어로 구성됩니다. 애플리케이션 데이터는 각각 NetApp ONTAP용 Amazon FSx, Cloud Volume ONTAP, Azure NetApp Files 및 Google Cloud용 Cloud Volumes Service와 직접 통신하는 게스트 기반 iSCSI 이니시에이터 또는 NFS/SMB 마운트를 통해 VM에 연결됩니다. 이 구성을 사용하면 vSAN과 같이 스토리지 용량과 관련된 문제를 쉽게 해결할 수 있습니다. 사용 가능한 여유 공간은 사용된 여유 공간 및 스토리지 정책에 따라 달라집니다.

AWS의 VMware Cloud에서 3노드 SDDC 클러스터를 살펴보겠습니다.

- 3노드 SDDC의 총 물리적 용량은 31.1TB(각 노드당 약 10TB)입니다.
- 호스트를 추가하기 전에 유지 관리해야 하는 여유 공간 = 25% = (.25 x 31.1TB) = 7.7TB
- 여유 공간 차감 후의 가용 물리적 용량 = 23.4TB
- 사용 가능한 유효 여유 공간은 적용된 스토리지 정책에 따라 달라집니다.

  예를 들면 다음과 같습니다.

  - RAID 0 = 유효 여유 공간 = 23.4TB(사용 가능한 물리적 용량/1)
  - RAID 1 = 유효 여유 공간 = 11.7TB(사용 가능한 물리적 용량/2)
  - RAID 5 = 유효 여유 공간 = 17.5TB(사용 가능한 물리적 용량/1.33)

따라서 NetApp Cloud Volumes를 게스트 연결 스토리지로 사용하면 스토리지를 확장하고 TCO를 최적화하는 동시에 성능 및 데이터 보호 요구사항을 충족할 수 있습니다.

> 이 문서가 작성된 시점에서 게스트 내 저장소가 유일하게 사용 가능한 옵션이었습니다. 보충 NFS 데이터 저장소 지원이 제공되면 추가 설명서를 사용할 수 있습니다 "여기".

기억해야 할 사항

- 하이브리드 스토리지 모델에서는 Tier 1 또는 높은 우선 순위의 워크로드를 vSAN 데이터 저장소에 배치하여 호스트 자체의 일부이고 근접하기 때문에 특정 지연 시간 요구 사항을 처리합니다. 트랜잭션 지연 시간이 허용되는 워크로드 VM에 대해 게스트 내 메커니즘을 사용합니다.
- NetApp SnapMirror ® 기술을 사용하여 온프레미스 ONTAP 시스템에서 Cloud Volumes ONTAP 또는 NetApp ONTAP용 Amazon FSx로 워크로드 데이터를 복제하여 블록 레벨 메커니즘을 사용하여 손쉽게 마이그레이션할 수 있습니다. Azure NetApp Files 및 Cloud Volumes Services에는 적용되지 않습니다. 데이터를 Azure NetApp Files 또는 Cloud Volumes Services로 마이그레이션하는 경우 사용되는 파일 프로토콜에 따라 NetApp XCP, BlueXP Copy and Sync, rysnc 또는 Robocopy를 사용합니다.
- 테스트 결과, 각 SDDC에서 스토리지에 액세스하는 동안 지연 시간이 2-4ms로 더 길어집니다. 스토리지를 매핑할 때 애플리케이션 요구 사항에 이러한 추가 지연 시간을 고려하십시오.
- 테스트 페일오버 및 실제 페일오버 중에 게스트 연결 스토리지를 마운트하려면 iSCSI 이니시에이터가 재구성되고 DNS가 SMB 공유용으로 업데이트되며 NFS 마운트 지점이 fstab에서 업데이트되도록 합니다.
- 게스트 내 Microsoft MPIO(Multipath I/O), 방화벽 및 디스크 시간 초과 레지스트리 설정이 VM 내에서 올바르게 구성되어 있는지 확인합니다.

> 이는 게스트 연결 스토리지에만 적용됩니다.

NetApp 클라우드 스토리지의 이점

NetApp 클라우드 스토리지는 다음과 같은 이점을 제공합니다.

- 컴퓨팅과 상관없이 스토리지를 확장함으로써 컴퓨팅 및 스토리지 간 밀도 향상
- 호스트 수를 줄여 전체 TCO를 줄일 수 있습니다.
- 컴퓨팅 노드 장애는 스토리지 성능에 영향을 주지 않습니다.

- Azure NetApp Files의 볼륨 재구성 및 동적 서비스 수준 기능을 사용하면 안정적인 워크로드 크기를 조정하여 비용을 최적화하고 오버 프로비저닝을 방지할 수 있습니다.
- Cloud Volumes ONTAP의 스토리지 효율성, 클라우드 계층화 및 인스턴스 유형 수정 기능을 사용하면 스토리지를 최적의 방법으로 추가 및 확장할 수 있습니다.
- 필요 시에만 스토리지 리소스의 초과 프로비저닝을 방지합니다.
- 효율적인 스냅샷 복사본 및 복제를 사용하면 성능에 영향을 미치지 않고 복사본을 빠르게 생성할 수 있습니다.
- Snapshot 복사본에서 빠른 복구를 사용하여 랜섬웨어 공격을 해결할 수 있도록 도와줍니다.
- 효율적인 증분 블록 전송 기반 지역 재해 복구 및 여러 지역에 걸쳐 통합된 백업 블록 레벨을 제공하여 RPO 및 RTO가 향상됩니다.

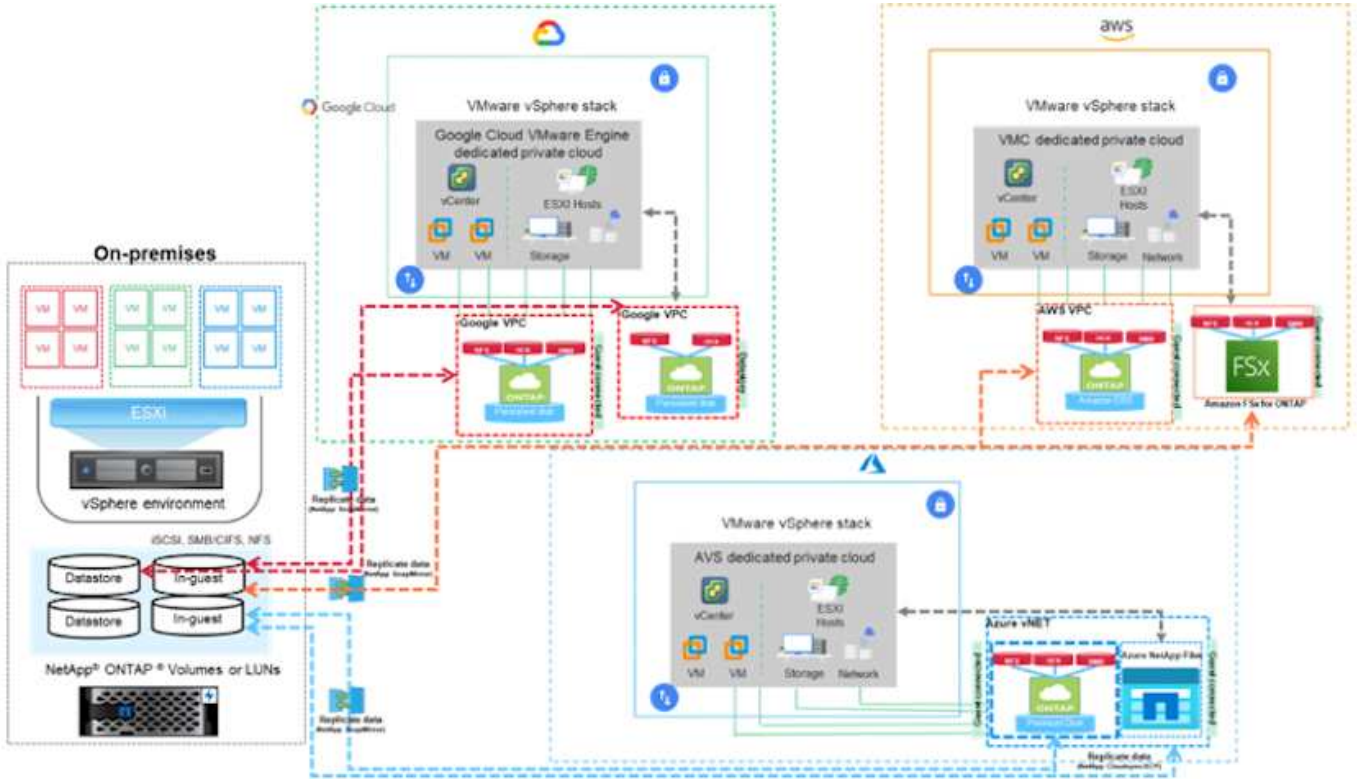
가정

- SnapMirror 기술 또는 기타 관련 데이터 마이그레이션 메커니즘이 사용됩니다. 온프레미스에서 하이퍼스케일러 클라우드에 이르기까지 다양한 연결 옵션이 있습니다. 적절한 경로를 사용하고 관련 네트워킹 팀과 협력하십시오.
- 이 문서가 작성된 시점에서 게스트 내 저장소가 유일하게 사용 가능한 옵션이었습니다. 보충 NFS 데이터 저장소 지원이 제공되면 추가 설명서를 사용할 수 있습니다 "여기".

스토리지 계획 및 사이징과 필요한 호스트 수에 대해서는 NetApp 솔루션 설계자와 각각의 하이퍼스케일러 클라우드 설계자를 설득하십시오. Cloud Volumes ONTAP Sizer를 사용하여 스토리지 인스턴스 유형 또는 적절한 서비스 수준을 최적의 처리량으로 확정하기 전에 스토리지 성능 요구사항을 파악하는 것이 좋습니다.

상세 아키텍처

개략적인 관점에서 볼 때 이 아키텍처(아래 그림에 표시)에서는 NetApp Cloud Volumes ONTAP, Cloud Volumes Service for Google Cloud 및 Azure NetApp Files를 추가 게스트 스토리지 옵션으로 사용하여 여러 클라우드 공급자 간에 하이브리드 멀티 클라우드 연결 및 애플리케이션 이동성을 달성하는 방법을 설명합니다.



하이퍼스케일 솔루션 에서 **VMware**를 위한 **NetApp** 솔루션

NetApp이 게스트 연결 스토리지 장치로 NetApp에서 제공하는 3가지 운영 하이퍼스케일러 또는 보조 NFS 데이터 저장소를 마이그레이션 워크플로우에 전환하여 클라우드, 백업/복원 및 재해 복구를 확장/버스팅 하는 기능에 대해 자세히 알아보십시오.

클라우드를 선택하시면 NetApp에서 나머지 작업을 해 드립니다!

특정 하이퍼스케일러의 기능을 보려면 해당 하이퍼스케일러의 적절한 탭을 클릭하십시오.

다음 옵션 중 하나를 선택하여 원하는 콘텐츠의 섹션으로 이동합니다.

- "하이퍼스케일 구성의 VMware"
- "NetApp 스토리지 옵션"

- "NetApp/VMware 클라우드 솔루션"

하이퍼스케일 구성의 **VMware**

온프레미스에서와 마찬가지로 클라우드 기반 가상화 환경을 계획하는 것은 VM 및 마이그레이션을 생성할 수 있는 성공적인 프로덕션 준비 환경에 매우 중요합니다.

AWS/VMC

이 섹션에서는 AWS SDDC에서 VMware Cloud를 설정 및 관리하고, NetApp 스토리지를 연결하는 데 사용할 수 있는 옵션과 함께 사용하는 방법을 설명합니다.

> 게스트 내 스토리지는 Cloud Volumes ONTAP을 AWS VMC에 연결하는 유일한 지원 방법입니다.

설치 프로세스는 다음 단계로 나눌 수 있습니다.

- VMware Cloud for AWS 구축 및 구성
- VMware Cloud를 FSx ONTAP에 연결합니다

자세한 내용을 확인하십시오 "VMC에 대한 구성 단계".

Azure/AVS

이 섹션에서는 Azure VMware 솔루션을 설정 및 관리하고 NetApp 스토리지를 연결하는 데 사용할 수 있는 옵션과 함께 사용하는 방법을 설명합니다.

> 게스트 내 스토리지는 Cloud Volumes ONTAP를 Azure VMware 솔루션에 연결하는 유일한 지원 방법입니다.

설치 프로세스는 다음 단계로 나눌 수 있습니다.

- 리소스 공급자를 등록하고 프라이빗 클라우드를 생성합니다
- 새 또는 기존 ExpressRoute 가상 네트워크 게이트웨이에 연결합니다
- 네트워크 연결을 확인하고 프라이빗 클라우드에 액세스합니다

자세한 내용을 확인하십시오 "AVS의 구성 단계".

GCP/GCVE

이 섹션에서는 GCVE를 설정 및 관리하고 NetApp 스토리지를 연결하는 데 사용할 수 있는 옵션과 함께 사용하는 방법을 설명합니다.

> 게스트 내 저장소는 Cloud Volumes ONTAP 및 Cloud Volumes Services를 GCVE에 연결하는 유일한 지원 방법입니다.

설치 프로세스는 다음 단계로 나눌 수 있습니다.

- GCVE 배포 및 구성
- GCVE에 대한 개인 액세스를 활성화합니다

자세한 내용을 확인하십시오 "GCVE에 대한 구성 단계".

NetApp 스토리지 옵션

NetApp 스토리지는 세 가지 주요 하이퍼 스케일러 내에서 게스트 연결 또는 보조 NFS 데이터 저장소로 여러 가지 방법으로 활용할 수 있습니다.

를 방문하십시오 "지원되는 NetApp 스토리지 옵션" 를 참조하십시오.

AWS/VMC

AWS는 다음과 같은 구성에서 NetApp 스토리지를 지원합니다.

- FSX ONTAP를 게스트 연결 스토리지로 사용합니다
- CVO(Cloud Volumes ONTAP)를 게스트 연결 스토리지로 사용합니다
- FSX ONTAP는 보조 NFS 데이터 저장소입니다

자세한 내용을 확인하십시오 "VMC에 대한 게스트 연결 스토리지 옵션". 자세한 내용을 확인하십시오 "VMC에 대한 보조 NFS 데이터 저장소 옵션".

Azure/AVS

Azure는 다음과 같은 구성에서 NetApp 스토리지를 지원합니다.

- 게스트 연결 스토리지로서의 Azure NetApp Files(ANF)
- CVO(Cloud Volumes ONTAP)를 게스트 연결 스토리지로 사용합니다
- Azure NetApp Files(ANF)를 보조 NFS 데이터 저장소로 사용합니다

자세한 내용을 확인하십시오 "AVS용 게스트 연결 스토리지 옵션". 자세한 내용을 확인하십시오 "AVS용 보조 NFS 데이터 저장소 옵션".

GCP/GCVE

Google Cloud는 다음과 같은 구성에서 NetApp 스토리지를 지원합니다.

- CVO(Cloud Volumes ONTAP)를 게스트 연결 스토리지로 사용합니다
- CVS(Cloud Volumes Service)를 게스트 연결 스토리지로 사용합니다
- CVS(Cloud Volumes Service)를 보조 NFS 데이터 저장소로 사용

자세한 내용을 확인하십시오 "GCVE에 대한 게스트 연결 저장소 옵션".

에 대해 자세히 알아보십시오 "Google Cloud VMware Engine에 대한 NetApp Cloud Volumes Service 데이터 저장소 지원(NetApp 블로그)" 또는 "NetApp CVS를 Google Cloud VMware Engine용 데이터 저장소로 사용하는 방법(Google 블로그)"

NetApp/VMware 클라우드 솔루션

NetApp 및 VMware 클라우드 솔루션을 사용하면 대부분의 사용 사례를 하이퍼스케일러에서 간편하게 구축할 수 있습니다. VMware는 운영 클라우드 워크로드 사용 사례를 다음과 같이 정의합니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 마이그레이션
- 확장

AWS/VMC

"AWS/VMC용 NetApp 솔루션을 찾아보십시오"

Azure/AVS

"Azure/AVS용 NetApp 솔루션을 찾아보십시오"

GCP/GCVE

"Google Cloud Platform (GCP)/GCVE용 NetApp 솔루션을 찾아보십시오"

VMware를 사용하는 **NetApp** 하이브리드 멀티 클라우드에 지원되는 구성

주요 하이퍼 스케일러에서 NetApp 스토리지 지원 조합을 이해합니다.

	* 게스트 연결됨 *	* 보조 NFS 데이터 저장소 *
* AWS *	CVO FSx ONTAP"세부 정보"	FSX ONTAP"세부 정보"
* Azure *	CVO ANF"세부 정보"	ANF"세부 정보"
* GCP *	CVO CVS"세부 정보"	CV"세부 정보"

클라우드 공급자에서 가상화 환경 구성

지원되는 각 하이퍼 스케일러에서 가상화 환경을 구성하는 방법에 대한 자세한 내용은 여기 를 참조하십시오.

AWS/VMC

이 섹션에서는 AWS SDDC에서 VMware Cloud를 설정 및 관리하고, NetApp 스토리지를 연결하는 데 사용할 수 있는 옵션과 함께 사용하는 방법을 설명합니다.

게스트 내 스토리지는 Cloud Volumes ONTAP을 AWS VMC에 연결하는 유일한 지원 방법입니다.

설치 프로세스는 다음 단계로 나눌 수 있습니다.

- VMware Cloud for AWS 구축 및 구성
- VMware Cloud를 FSx ONTAP에 연결합니다

자세한 내용을 확인하십시오 "VMC에 대한 구성 단계".

Azure/AVS

이 섹션에서는 Azure VMware 솔루션을 설정 및 관리하고 NetApp 스토리지를 연결하는 데 사용할 수 있는 옵션과 함께 사용하는 방법을 설명합니다.

게스트 내 스토리지는 Cloud Volumes ONTAP를 Azure VMware 솔루션에 연결하는 유일한 지원 방법입니다.

설치 프로세스는 다음 단계로 나눌 수 있습니다.

- 리소스 공급자를 등록하고 프라이빗 클라우드를 생성합니다
- 새 또는 기존 ExpressRoute 가상 네트워크 게이트웨이에 연결합니다
- 네트워크 연결을 확인하고 프라이빗 클라우드에 액세스합니다

자세한 내용을 확인하십시오 "AVS의 구성 단계".

GCP/GCVE

이 섹션에서는 GCVE를 설정 및 관리하고 NetApp 스토리지를 연결하는 데 사용할 수 있는 옵션과 함께 사용하는 방법을 설명합니다.

게스트 내 저장소는 Cloud Volumes ONTAP 및 Cloud Volumes Services를 GCVE에 연결하는 유일한 지원 방법입니다.

설치 프로세스는 다음 단계로 나눌 수 있습니다.

- GCVE 배포 및 구성
- GCVE에 대한 개인 액세스를 활성화합니다

자세한 내용을 확인하십시오 "GCVE에 대한 구성 단계".

AWS에서 가상화 환경을 구축하고 구성합니다

사내 환경과 마찬가지로, AWS에서 VMware Cloud를 계획하는 것은 VM과 마이그레이션을

성공적으로 운영 환경에 구축하는 데 매우 중요합니다.

이 섹션에서는 AWS SDDC에서 VMware Cloud를 설정 및 관리하고, NetApp 스토리지를 연결하는 데 사용할 수 있는 옵션과 함께 사용하는 방법을 설명합니다.

현재 CVO(Cloud Volumes ONTAP)를 AWS VMC에 연결하는 유일한 방법은 게스트 내 스토리지 뿐입니다.

설치 프로세스는 다음 단계로 나눌 수 있습니다.

VMware Cloud for AWS 구축 및 구성

"AWS 기반 VMware 클라우드" AWS 에코시스템의 VMware 기반 워크로드에 클라우드 네이티브 경험을 제공합니다. 각 VMware SDDC(소프트웨어 정의 데이터 센터)는 VPC(Amazon Virtual Private Cloud)에서 실행되며 전체 VMware 스택(vCenter Server 포함), NSX-T 소프트웨어 정의 네트워킹, vSAN 소프트웨어 정의 스토리지, 워크로드에 컴퓨팅 및 스토리지 리소스를 제공하는 하나 이상의 ESXi 호스트를 제공합니다.

이 섹션에서는 AWS에서 VMware Cloud를 설정 및 관리하고, 게스트 내 스토리지에서 AWS에서 NetApp ONTAP용 Amazon FSx 및/또는 Cloud Volumes ONTAP와 함께 사용하는 방법에 대해 설명합니다.

> ⓘ 현재 CVO(Cloud Volumes ONTAP)를 AWS VMC에 연결하는 유일한 방법은 게스트 내 스토리지 뿐입니다.

설정 프로세스는 다음 세 부분으로 나눌 수 있습니다.

AWS 계정을 등록하십시오

에 등록하십시오 "아마존 웹 서비스 계정".

이미 생성된 계정이 없는 경우 시작하려면 AWS 계정이 필요합니다. 이 절차의 여러 단계에 대해 새 계정 또는 기존 계정에 관리 권한이 필요합니다. 자세한 내용은 다음을 참조하십시오 "링크" AWS 자격 증명에 대한 자세한 내용은

내 VMware 계정을 등록합니다

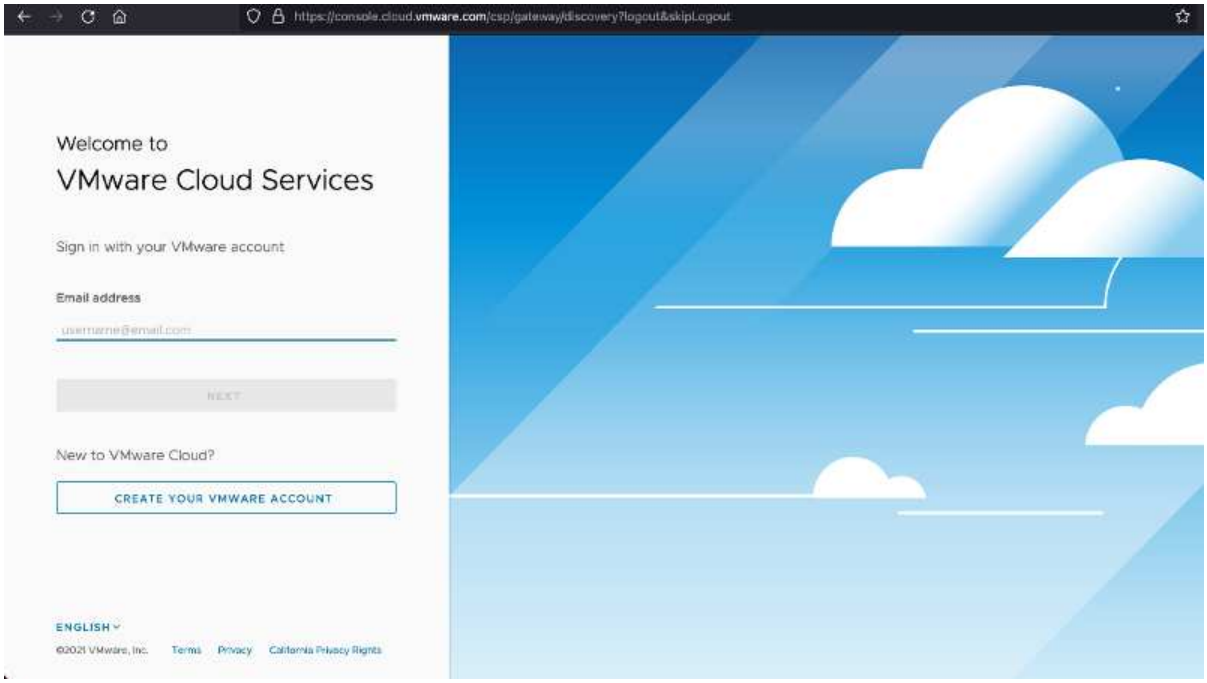
에 등록하십시오 "내 VMware" 계정.

VMware의 클라우드 포트폴리오(AWS의 VMware Cloud 포함)에 액세스하려면 VMware 고객 계정 또는 My VMware 계정이 필요합니다. 아직 생성하지 않은 경우 VMware 계정을 생성합니다 "여기".

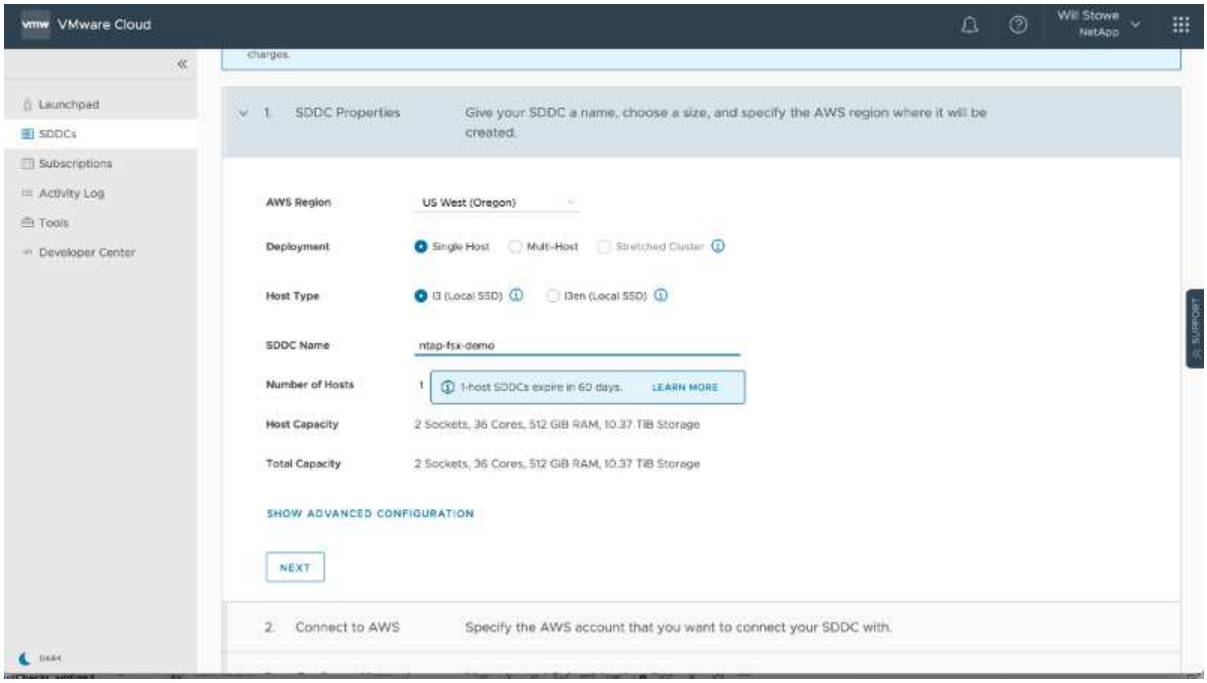
VMware 클라우드에서 **SDDC** 프로비저닝

VMware 계정을 구성하고 적절한 사이징을 수행한 후에는 AWS에서 VMware Cloud 서비스를 사용하기 위한 확실한 다음 단계로 소프트웨어 정의 데이터 센터를 구축할 수 있습니다. SDDC를 생성하려면 호스팅할 AWS 영역을 선택하고 SDDC에 이름을 지정하고 SDDC에 포함할 ESXi 호스트 수를 지정합니다. 아직 AWS 계정이 없는 경우에도 단일 ESXi 호스트를 포함하는 시작 구성 SDDC를 생성할 수 있습니다.

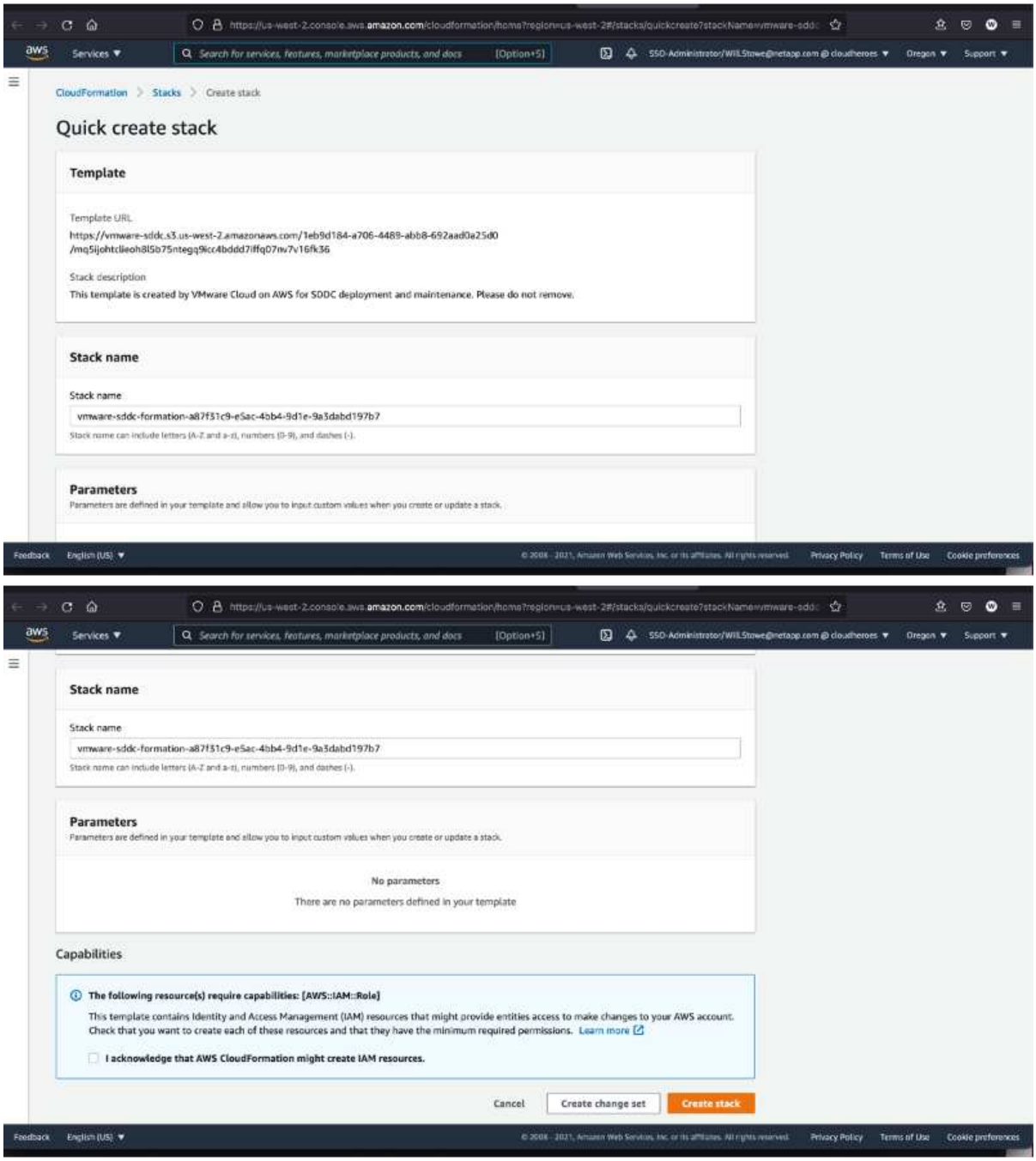
1. 기존 또는 새로 생성한 VMware 자격 증명을 사용하여 VMware Cloud Console에 로그인합니다.

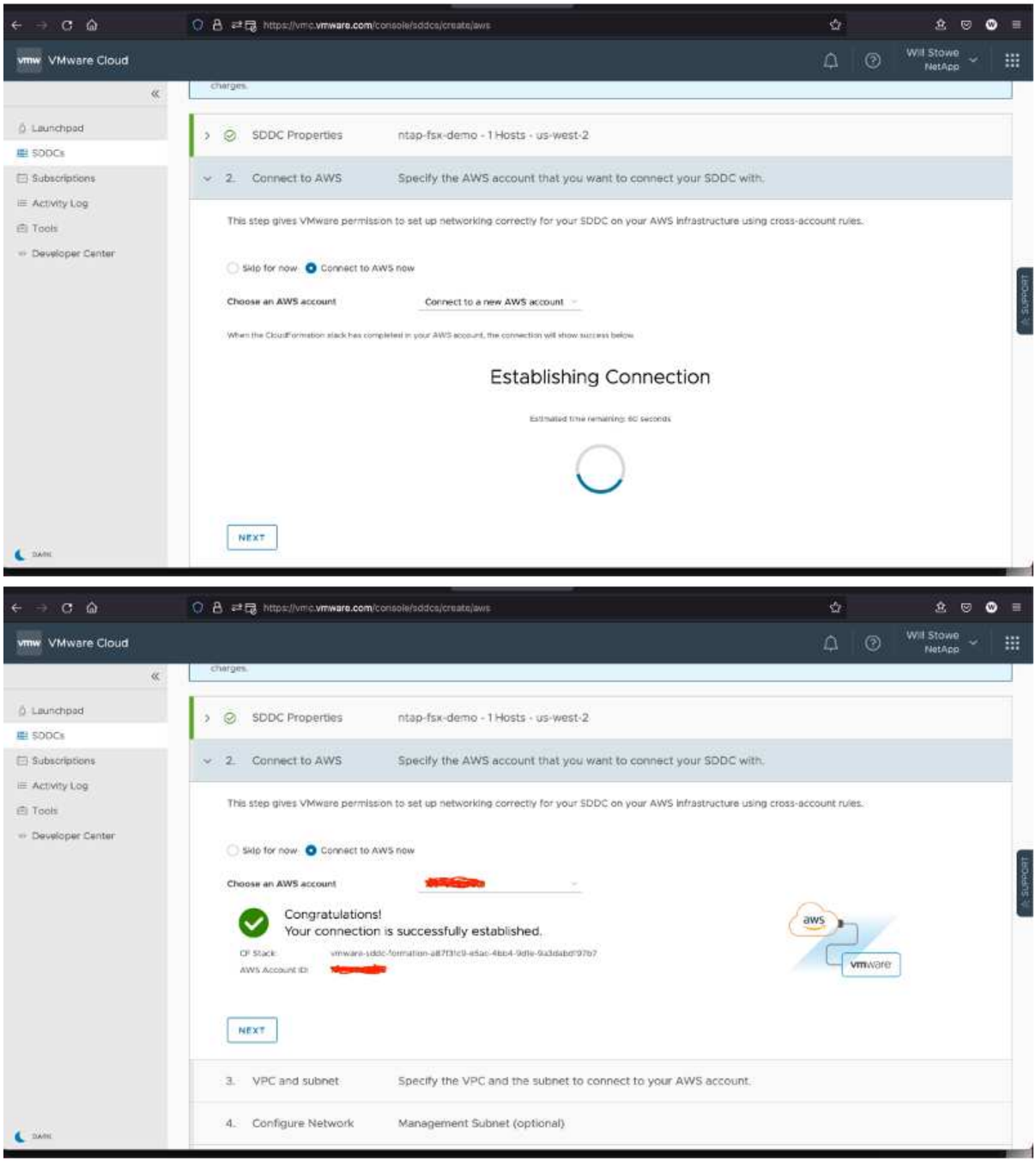


2. AWS 지역, 구축 및 호스트 유형과 SDDC 이름을 구성합니다.



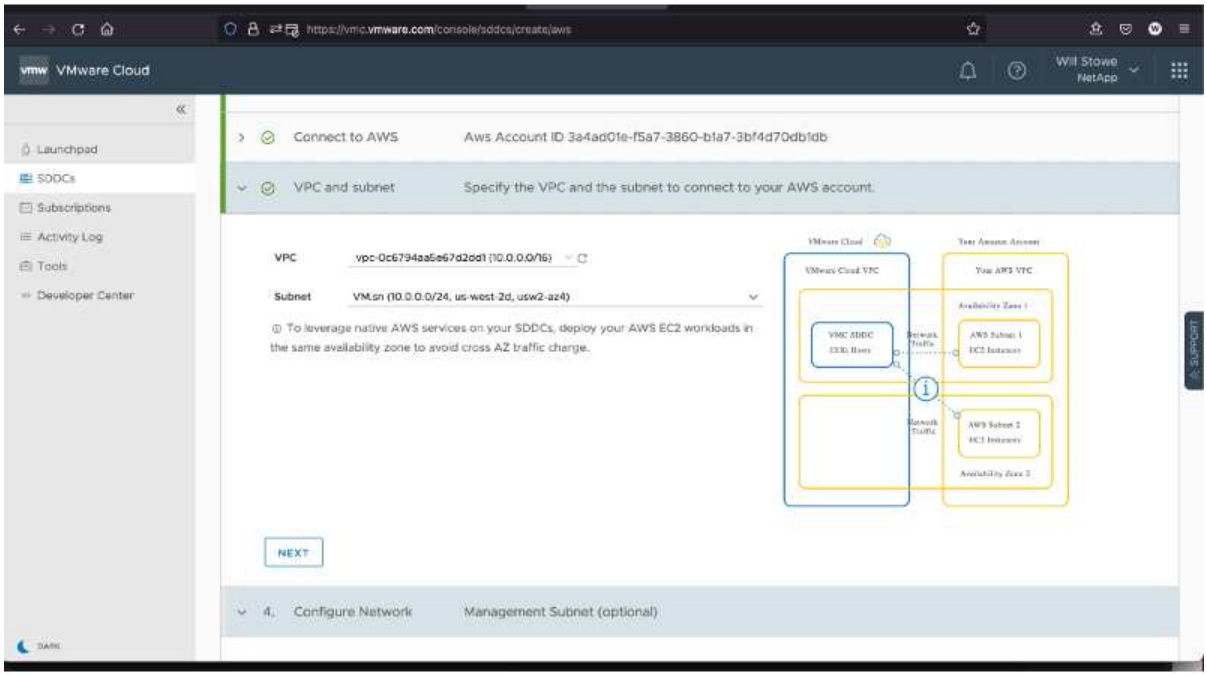
3. 원하는 AWS 계정에 연결하고 AWS Cloud 포메이션 스택을 실행합니다.


CloudFormation > Stacks > Create stack
Quick create stack
Template
Template URL
https://vmware-sddc.s3.us-west-2.amazonaws.com/1eb9d184-a706-4489-abb8-692aad0a25d0/mq5ijohtclieoh8l5b75ntegq9icc4bddd7iffq07nv7v16fk36
Stack description
This template is created by VMware Cloud on AWS for SDDC deployment and maintenance. Please do not remove.
Stack name
Stack name
vmware-sddc-formation-a87f51c9-e5ac-4bb4-9d1e-9a3dabd197b7
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
Stack name
Stack name
vmware-sddc-formation-a87f51c9-e5ac-4bb4-9d1e-9a3dabd197b7
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
No parameters
There are no parameters defined in your template
Capabilities
The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. Learn more
I acknowledge that AWS CloudFormation might create IAM resources.
Cancel
Create change set
Create stack

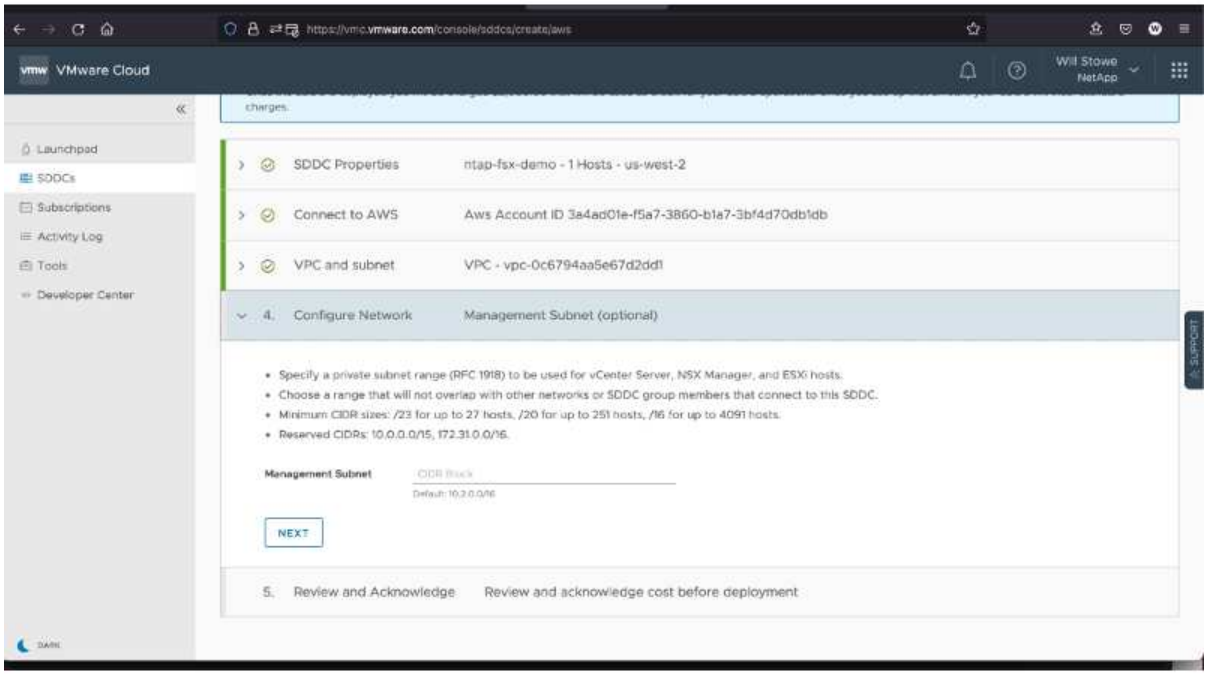


이 검증에는 단일 호스트 구성이 사용됩니다.

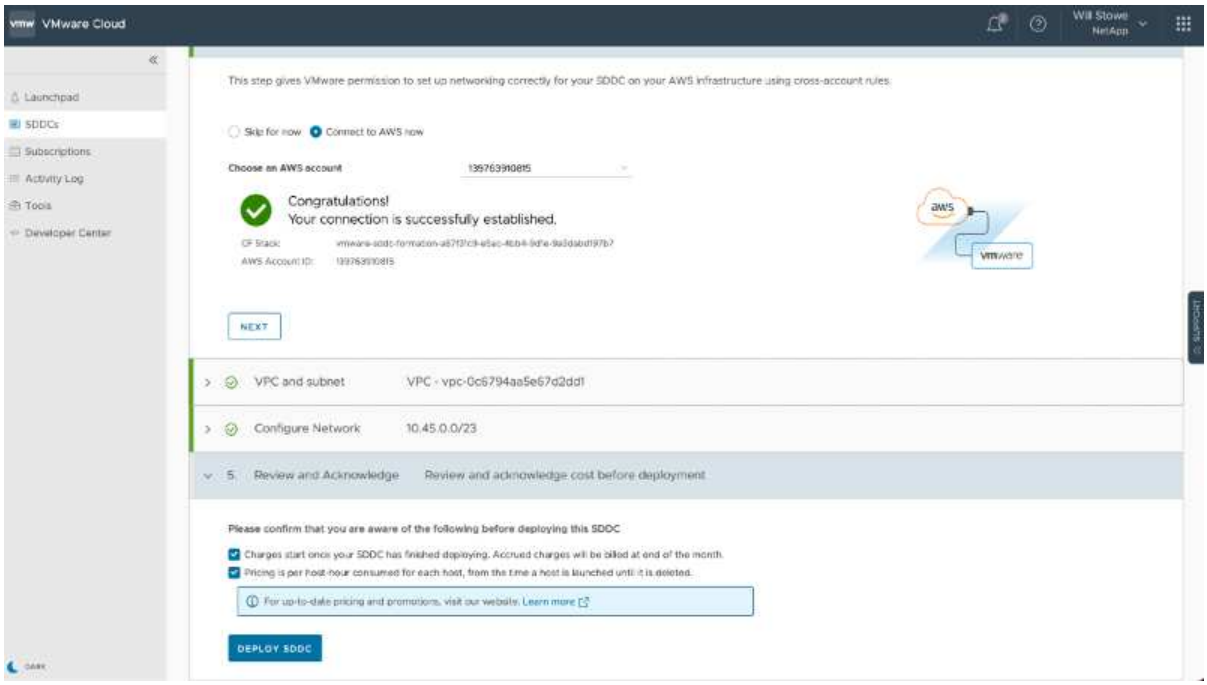
4. 원하는 AWS VPC를 선택하여 VMC 환경을 에 연결합니다.



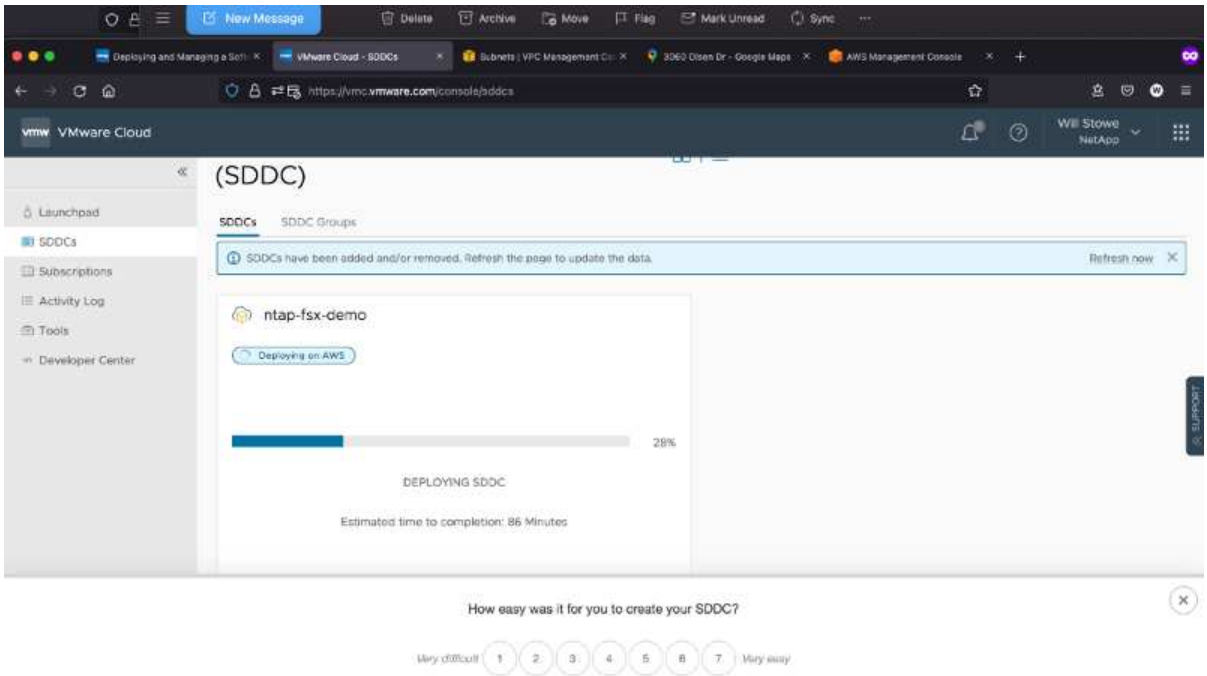
5. VMC 관리 서브넷을 구성합니다. 이 서브넷에는 vCenter, NSX 등과 같은 VMC 관리 서비스가 포함됩니다. SDDC 환경에 대한 연결이 필요한 다른 네트워크와 겹치는 주소 공간을 선택하지 마십시오. 마지막으로 아래에 기입된 CIDR 크기에 대한 권장 사항을 따르십시오.



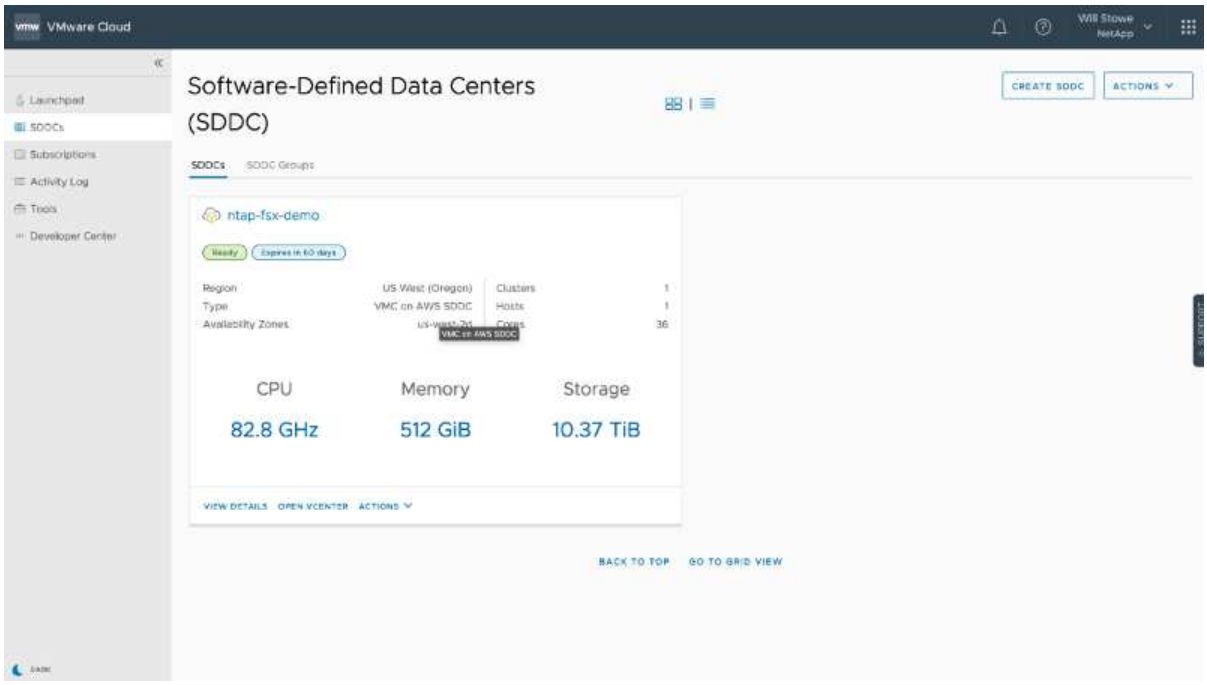
6. SDDC 구성을 검토 및 확인한 다음 SDDC 구축 을 클릭합니다.



일반적으로 구축 프로세스를 완료하는 데 약 2시간이 소요됩니다.



7. 완료되면 SDDC를 사용할 수 있습니다.

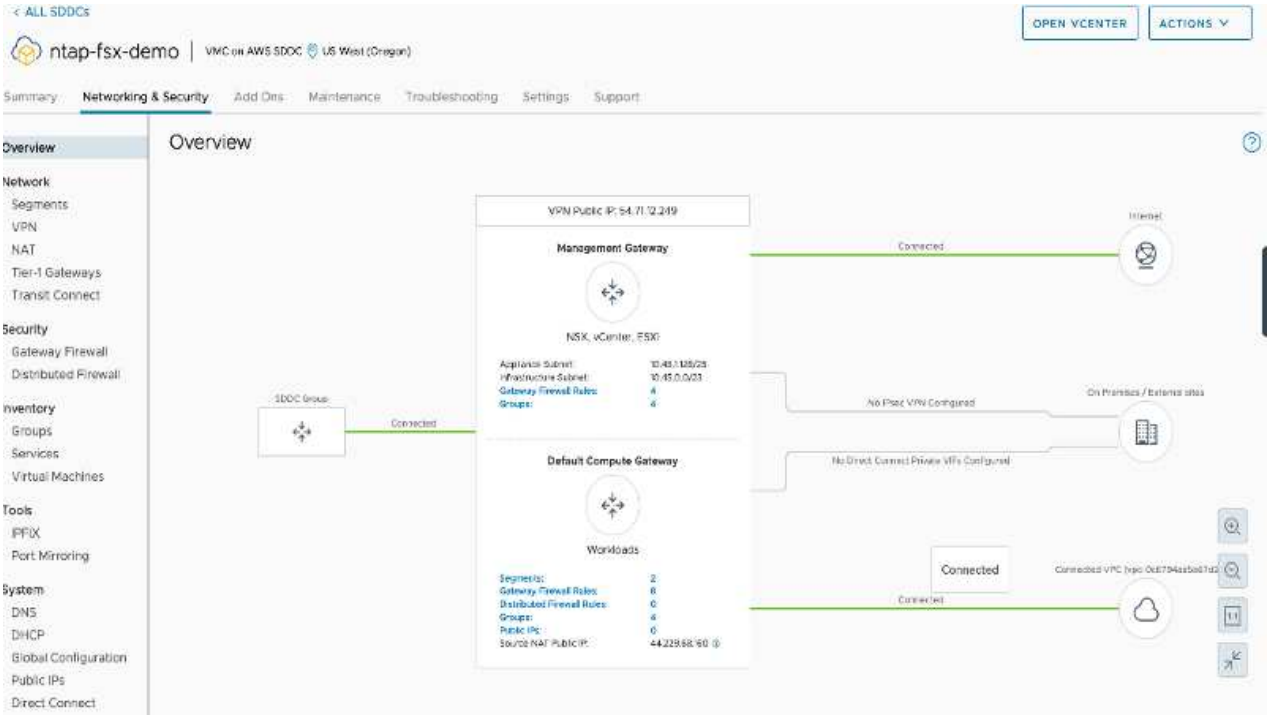


SDDC 구축에 대한 단계별 가이드는 를 참조하십시오 "VMC 콘솔에서 SDDC를 구축합니다".

VMware Cloud를 **FSx ONTAP**에 연결합니다

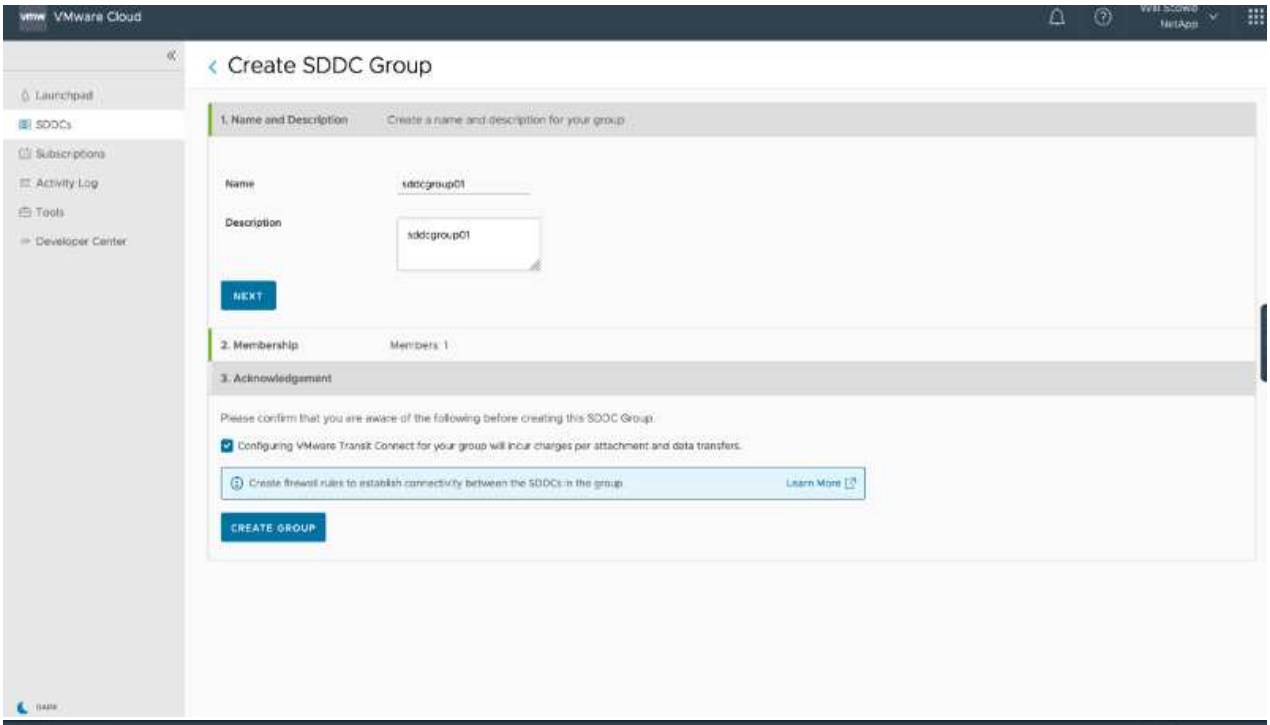
VMware Cloud를 FSx ONTAP에 연결하려면 다음 단계를 수행하십시오.

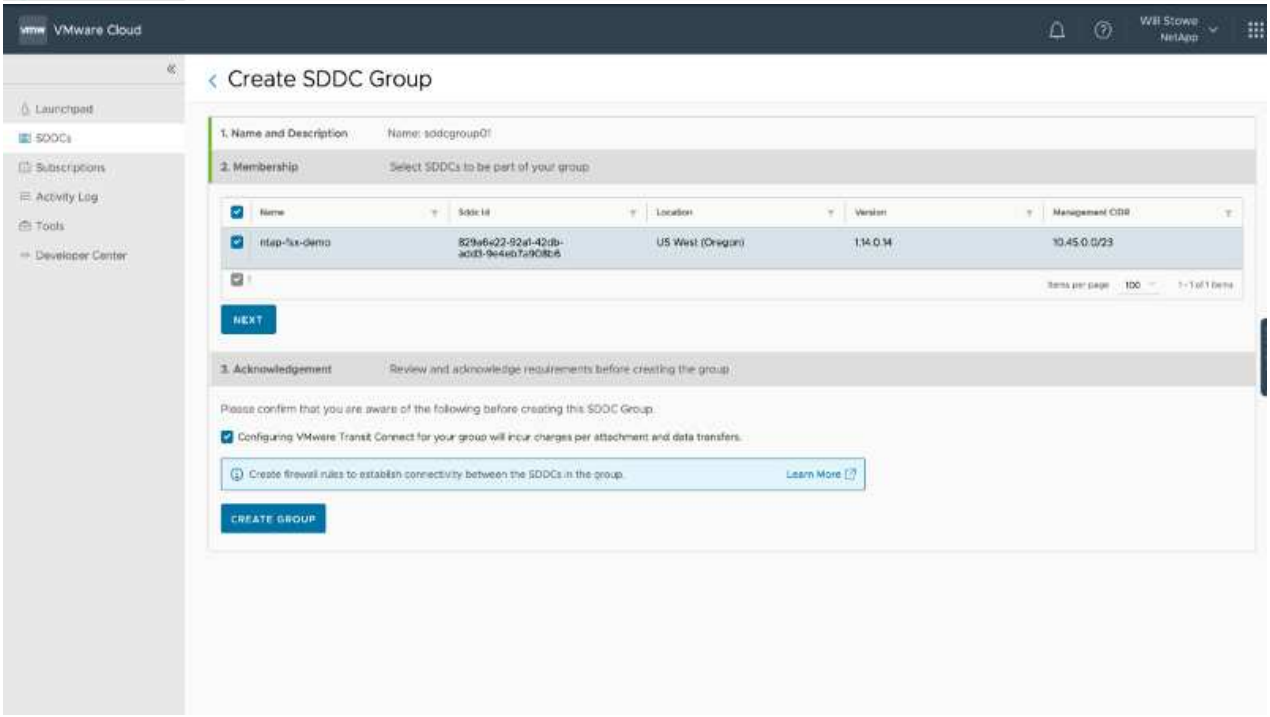
1. VMware 클라우드 구축이 완료되고 AWS VPC에 연결되면 NetApp ONTAP용 Amazon FSx를 원래 연결된 VPC가 아닌 새 VPC에 구축해야 합니다(아래 스크린샷 참조). 연결된 VPC에 FSX(NFS 및 SMB 부동 IP)를 구축하면 FSX에 액세스할 수 없습니다. Cloud Volumes ONTAP와 같은 iSCSI 엔드포인트는 연결된 VPC에서 정상적으로 작동합니다.

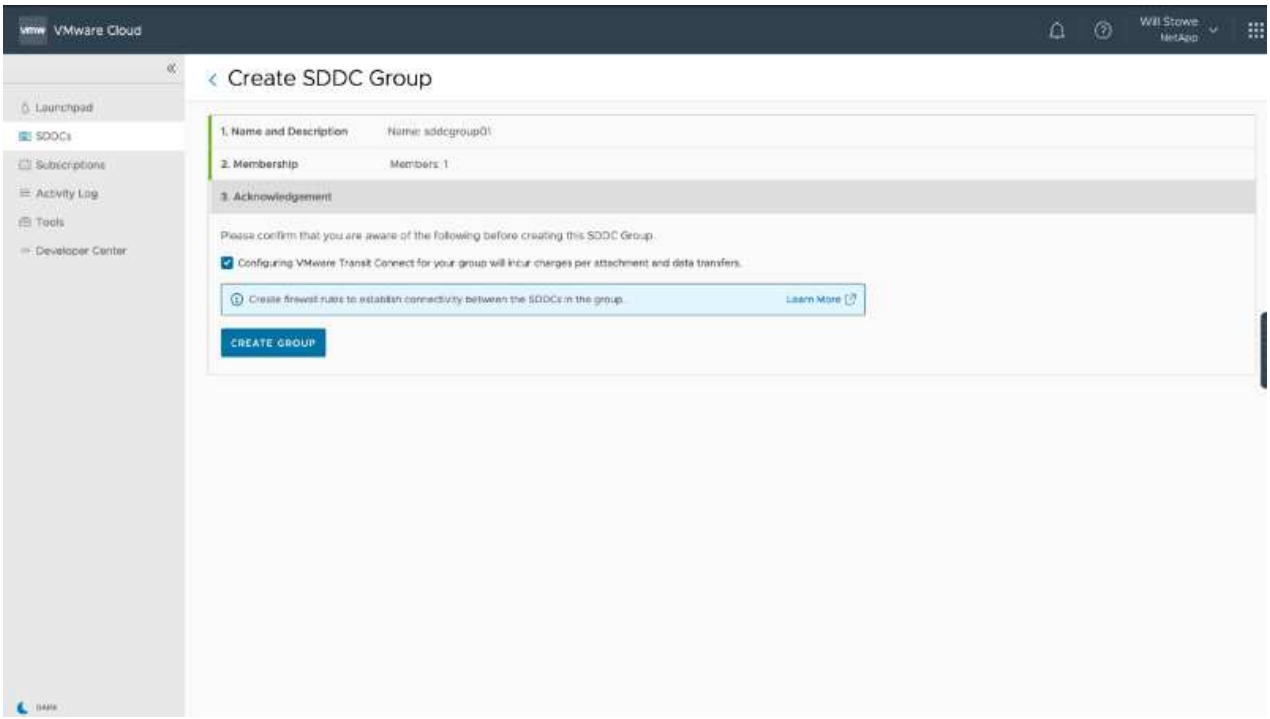


2. 동일한 지역에 추가 VPC를 구축한 다음 NetApp ONTAP용 Amazon FSx를 새 VPC에 구축합니다.

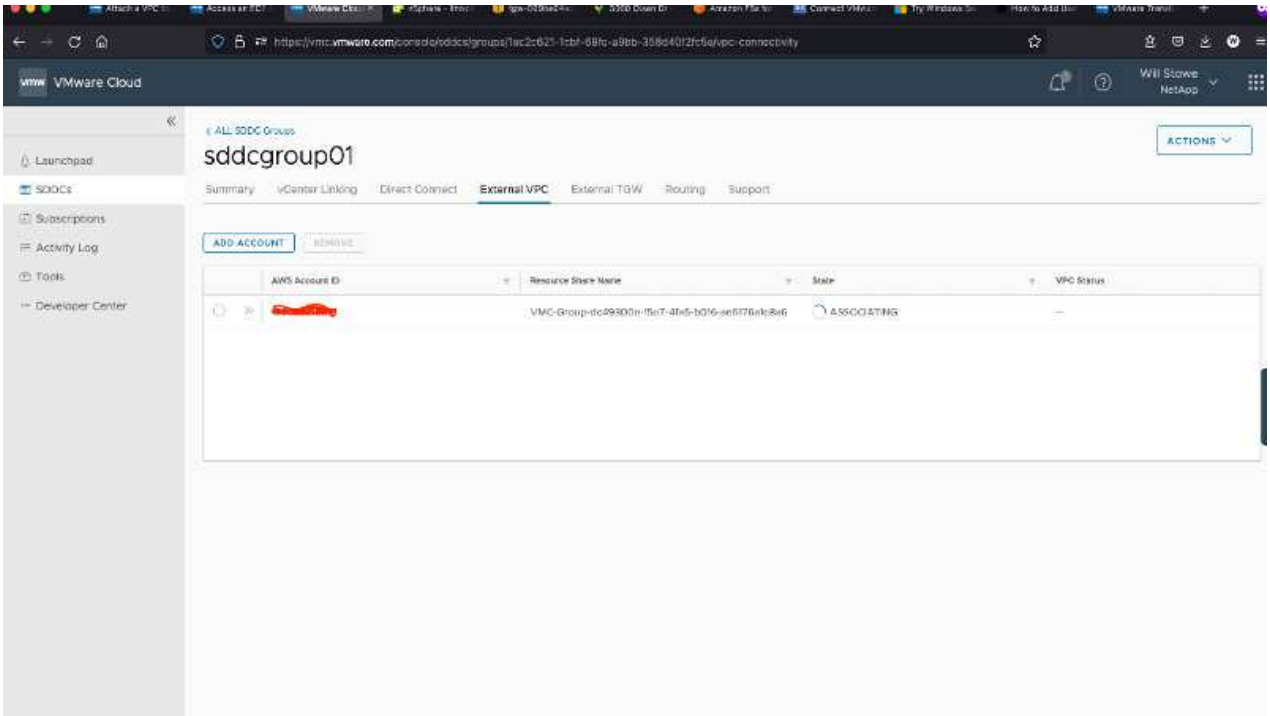
   VMware Cloud Console에서 SDDC 그룹을 구성하면 FSx가 구축된 새 VPC에 연결하는 데 필요한 네트워킹 구성 옵션을 사용할 수 있습니다. 3단계에서 "그룹에 대한 VMware Transit Connect 구성 시 첨부 파일 및 데이터 전송당 비용이 청구됨"이 선택되어 있는지 확인한 다음 그룹 생성 을 선택합니다. 이 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있습니다.

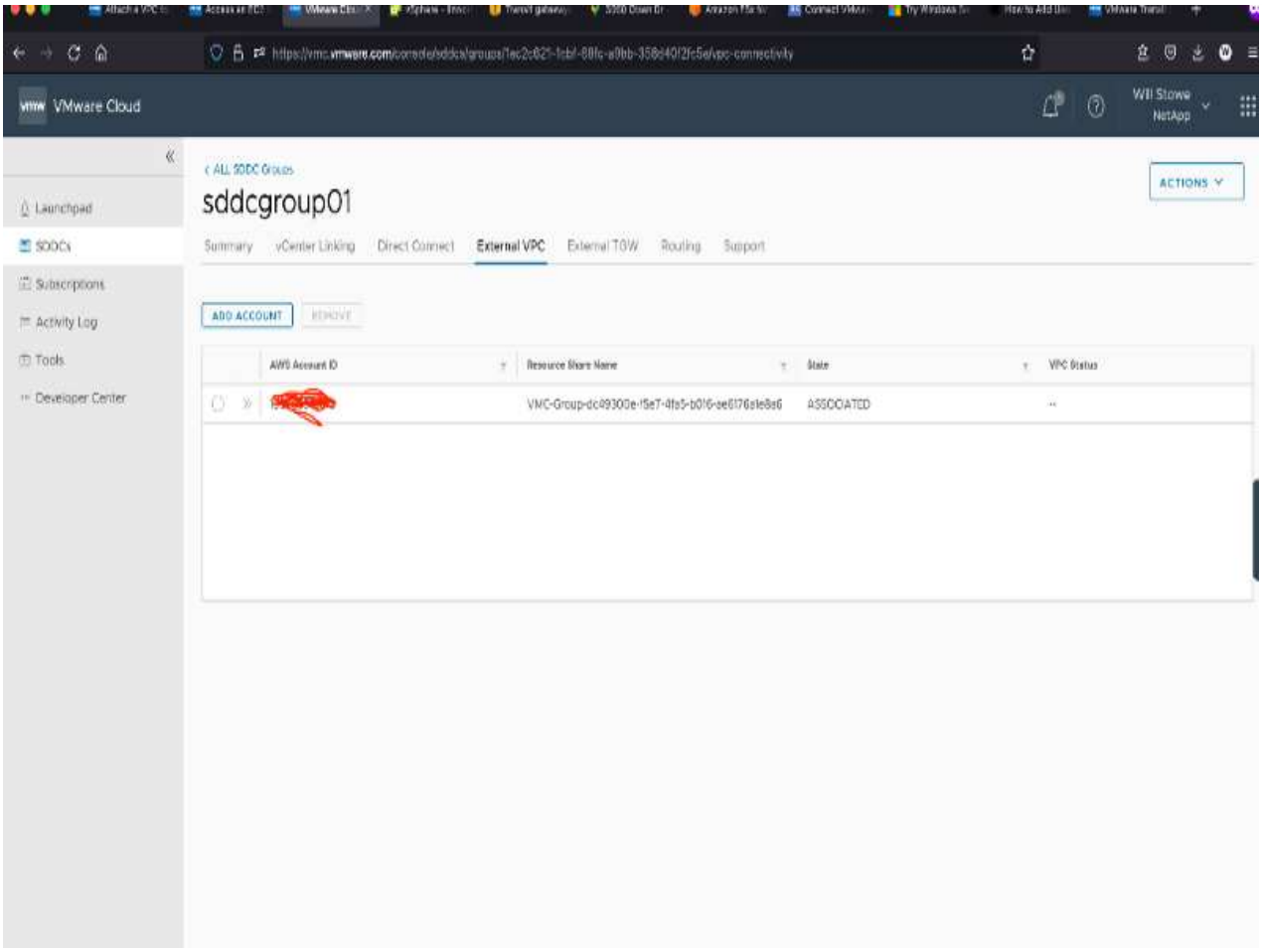

VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Create a name and description for your group
Name
sddcgroup01
Description
sddcgroup01
NEXT
2. Membership
Members: 1
3. Acknowledgement
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP


VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Name: sddcgroup01
2. Membership
Select SDDCs to be part of your group
Name
Sddc Id
Location
Version
Management CIDR
ntap-fsx-demo
829a6e22-92a1-42db-acd3-9e4eb7a908b6
US West (Oregon)
1.14.0.14
10.45.0.0/23
Items per page
100
1 - 1 of 1 items
NEXT
3. Acknowledgement
Review and acknowledge requirements before creating the group
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP

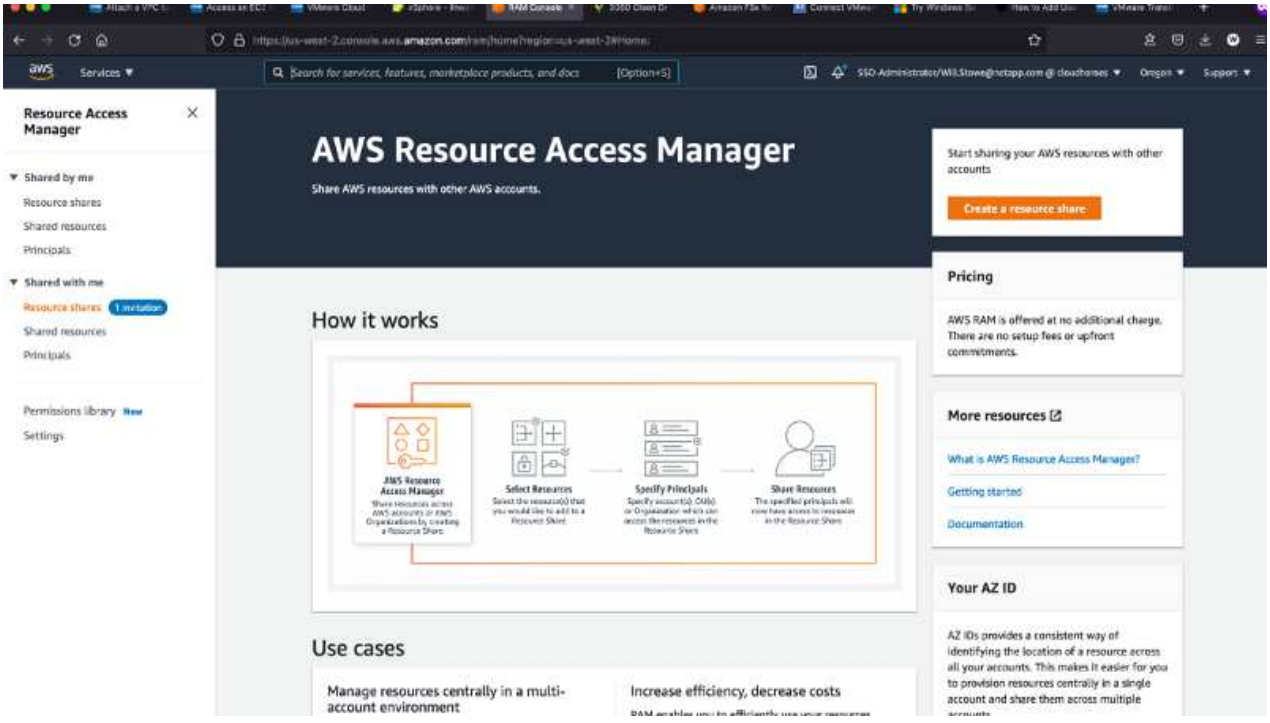


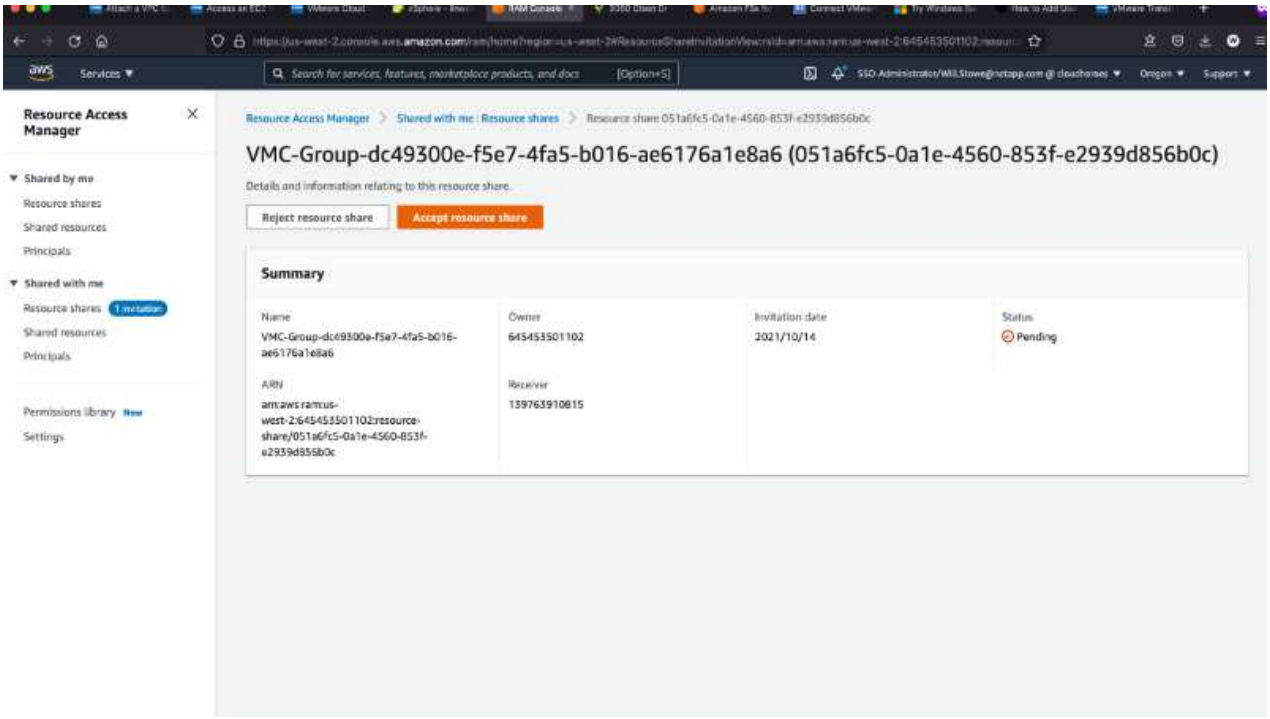
3. 새로 생성된 VPC를 방금 생성된 SDDC 그룹에 연결합니다. External VPC 탭을 선택하고 에 따릅니다 "외부 VPC 연결 지침" 그룹에. 이 프로세스를 완료하는 데 10-15분 정도 걸릴 수 있습니다.



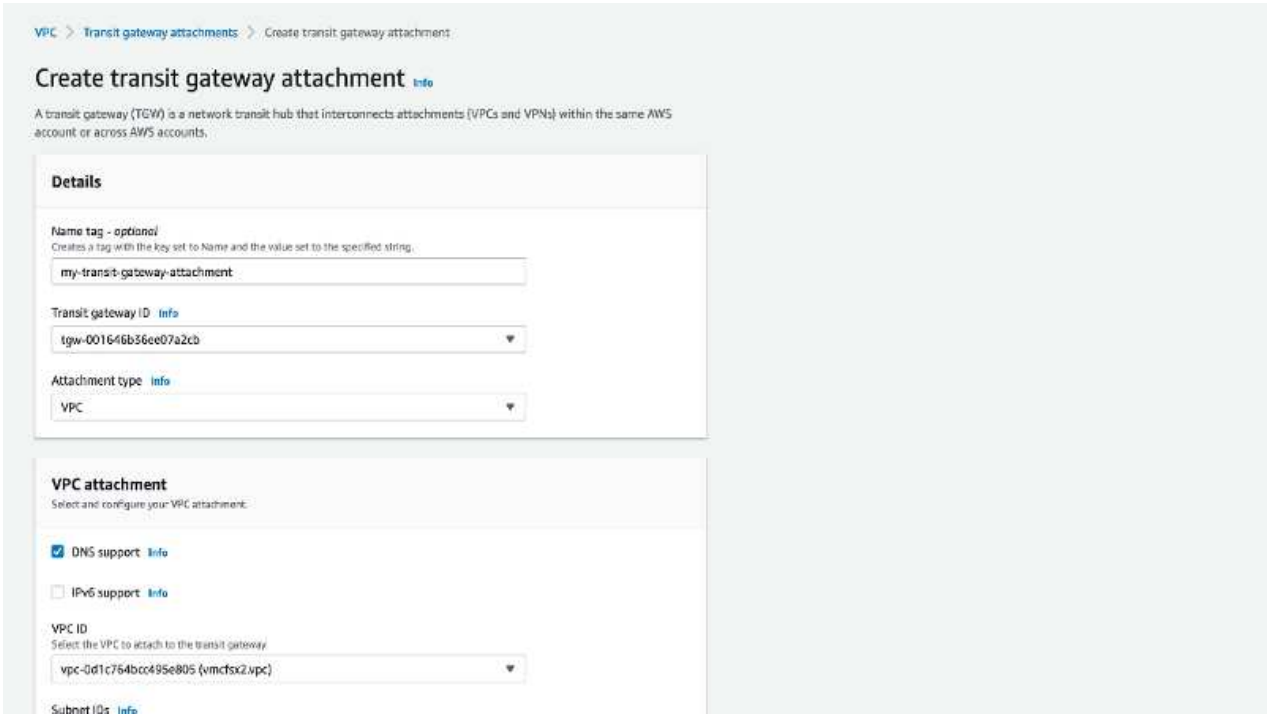


4. 외부 VPC 프로세스의 일환으로, 리소스 액세스 관리자를 통해 AWS 콘솔을 통해 새 공유 리소스에 대한 메시지가 표시됩니다. 공유 리소스는 입니다 "AWS Transit Gateway를 참조하십시오" VMware Transit Connect에서 관리합니다.

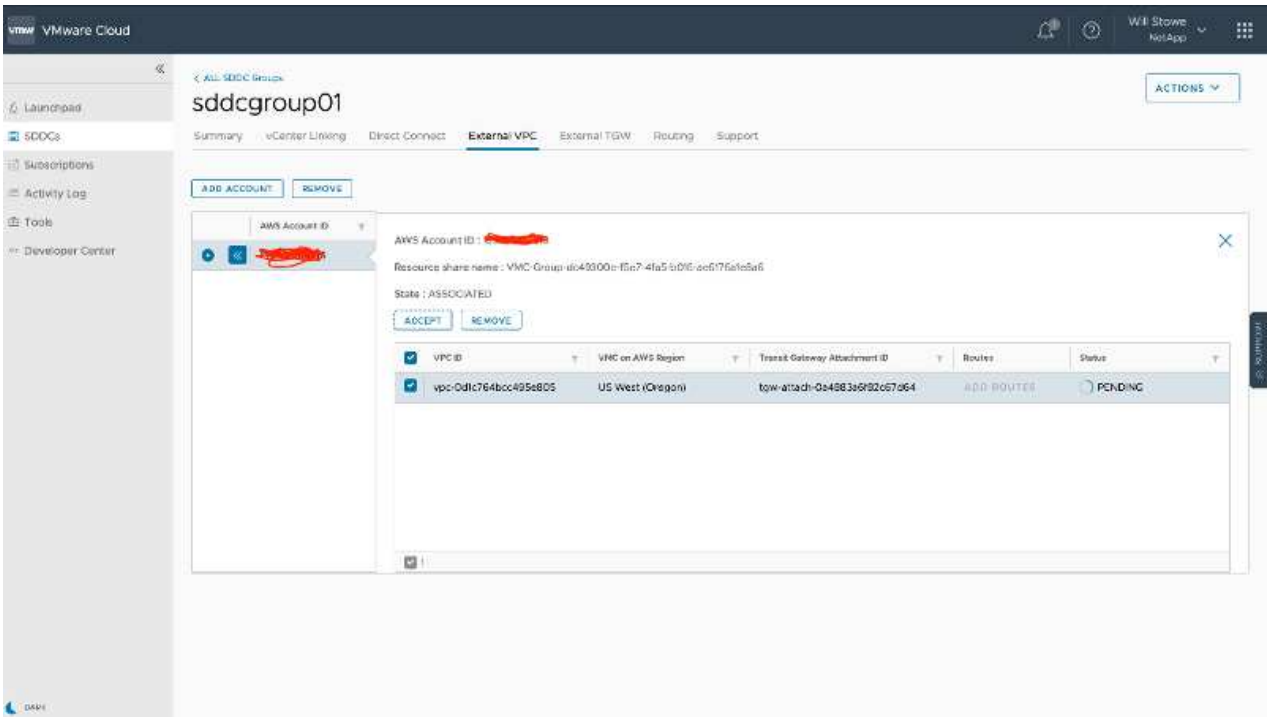




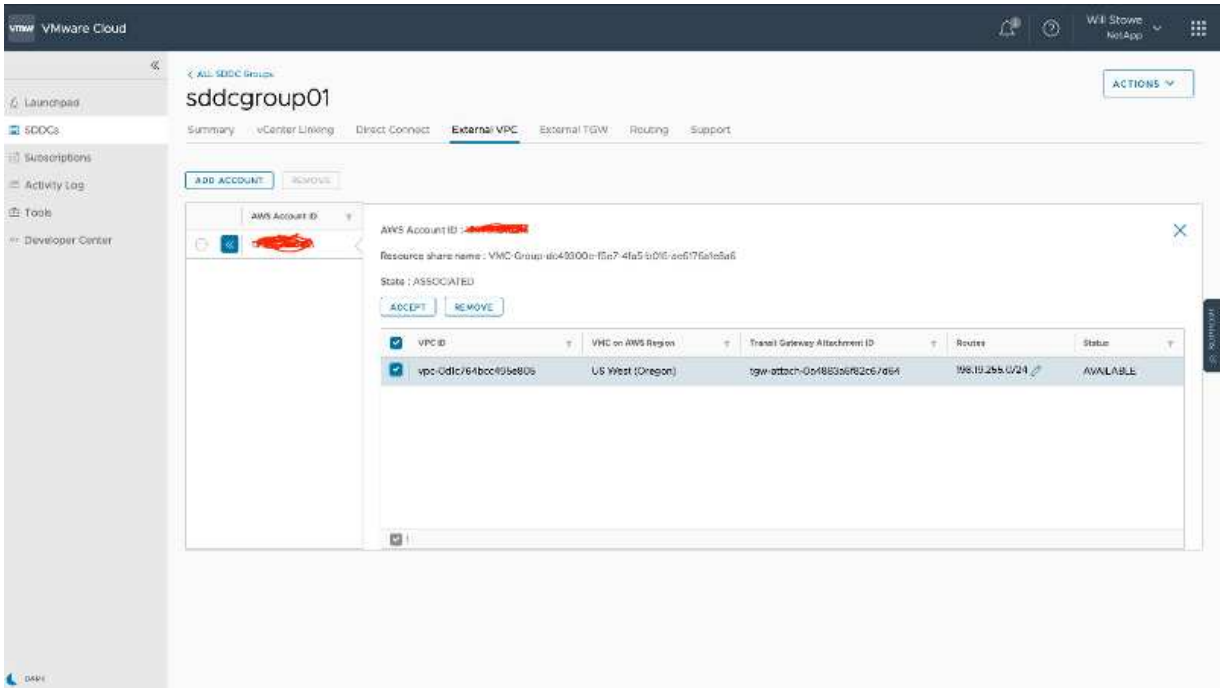
5. Transit Gateway Attachment를 생성합니다.



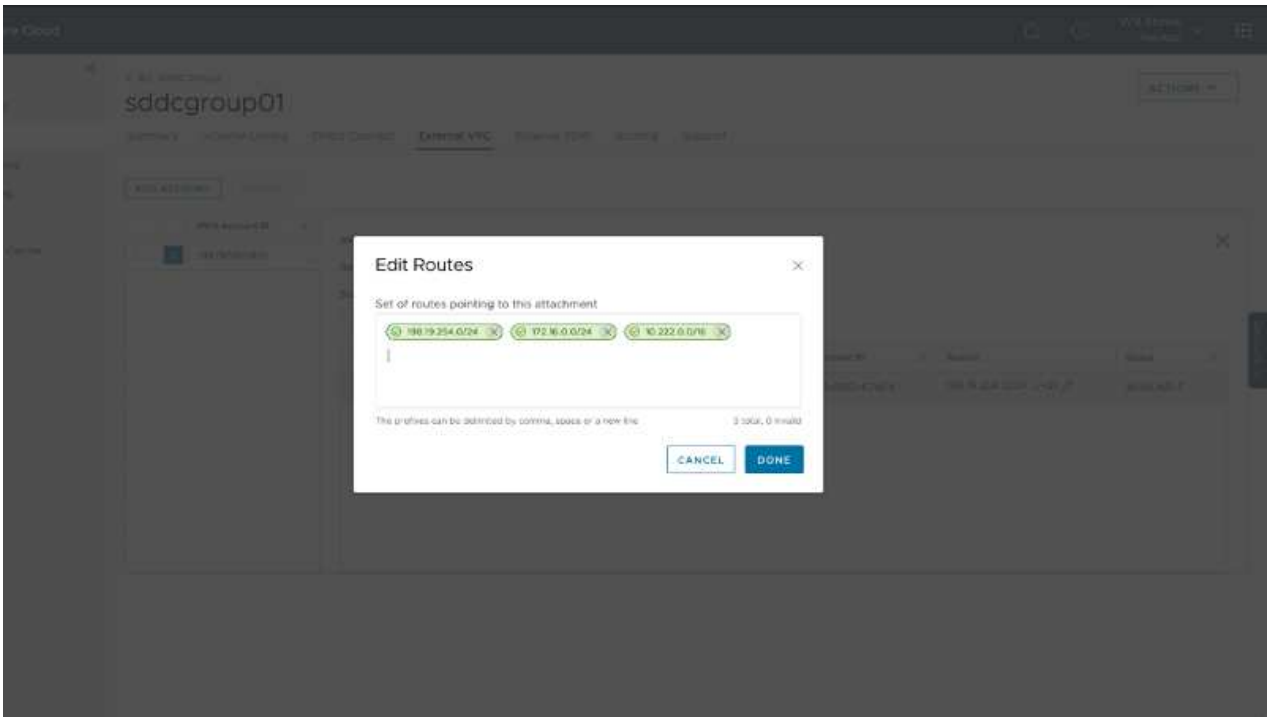
6. VMC 콘솔에서 VPC 첨부 파일을 수락합니다. 이 프로세스를 완료하는 데 약 10분 정도 걸릴 수 있습니다.



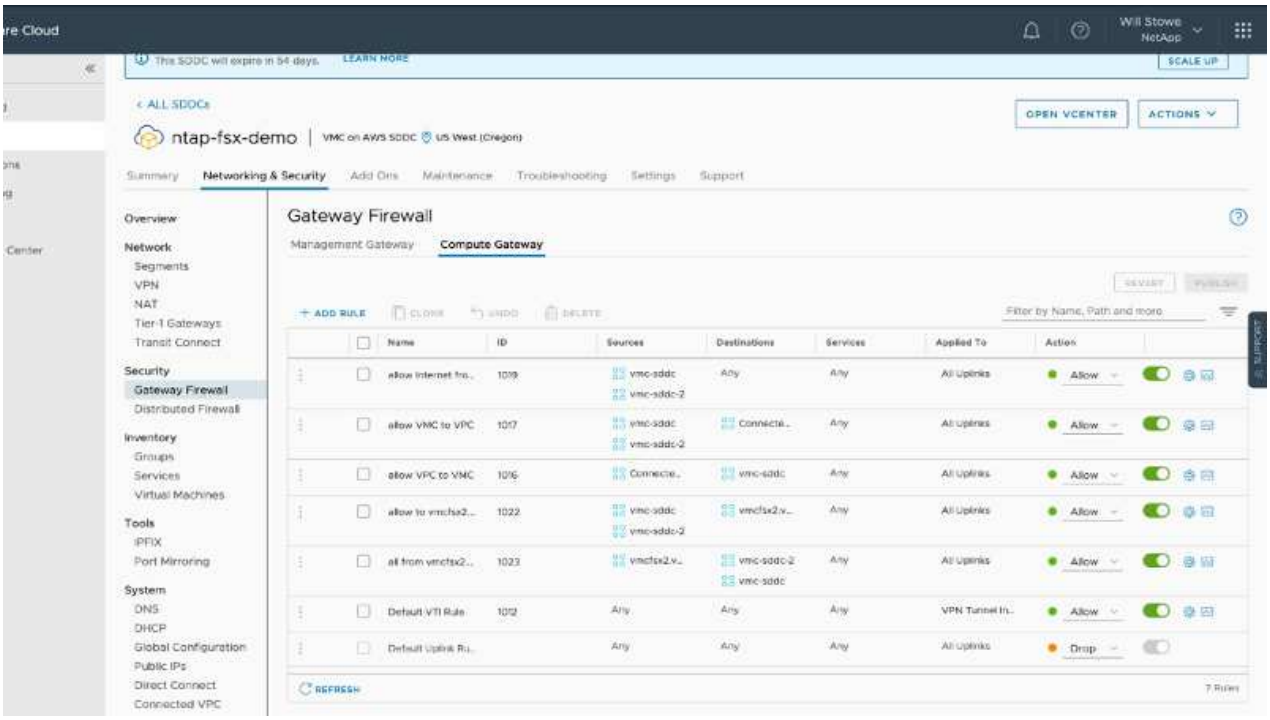
7. External VPC 탭에서 Routes 열의 편집 아이콘을 클릭하고 다음과 같은 필수 경로를 추가합니다.
   - NetApp ONTAP용 Amazon FSx의 부동 IP 범위에 대한 경로입니다 "유동 IP".
   - Cloud Volumes ONTAP의 부동 IP 범위에 대한 라우트입니다(해당하는 경우).
   - 새로 생성된 외부 VPC 주소 공간의 경로입니다.



8. 마지막으로 양방향 트래픽을 허용합니다 "방화벽 규칙" FSx/CVO에 액세스하기 위한 것입니다. 다음 사항을 따르십시오 "세부 단계" SDDC 워크로드 연결을 위한 컴퓨팅 게이트웨이 방화벽 규칙의 경우



9. 방화벽 그룹이 관리 및 컴퓨팅 게이트웨이 모두에 대해 구성된 후에는 다음과 같이 vCenter에 액세스할 수 있습니다.



다음 단계에서는 요구 사항에 따라 Amazon FSx ONTAP 또는 Cloud Volumes ONTAP가 구성되어 있는지, 그리고 구축을 최적화하기 위해 vSAN에서 스토리지 구성 요소를 오프로드하기 위해 볼륨이 프로비저닝되었는지 확인합니다.

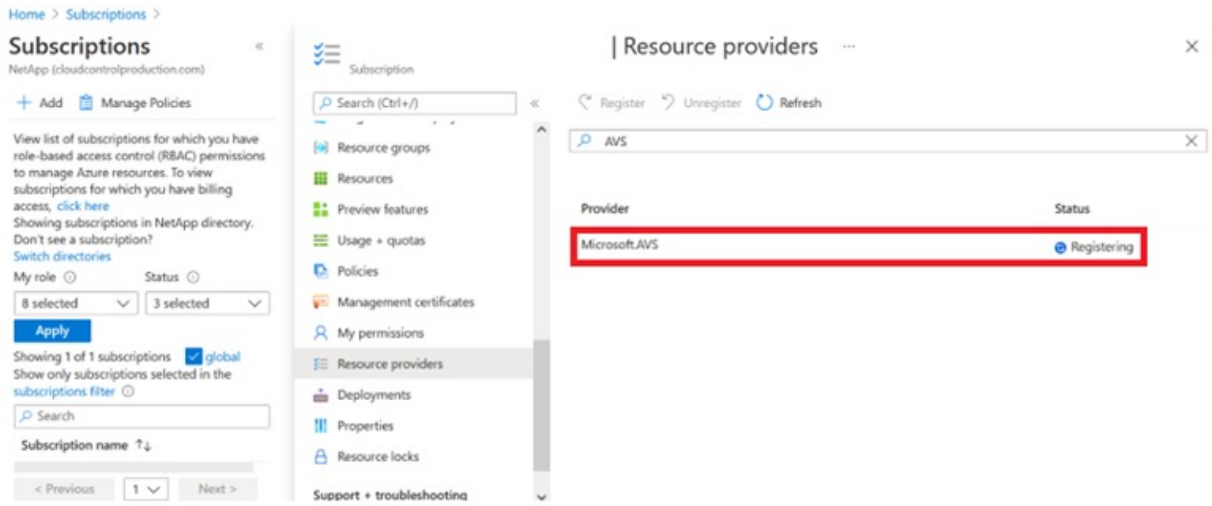
온프레미스와 마찬가지로 Azure VMware 솔루션 계획은 VM 및 마이그레이션을 생성할 수 있는 성공적인 프로덕션 준비 환경에 매우 중요합니다.

이 섹션에서는 Azure VMware 솔루션을 설정 및 관리하고 NetApp 스토리지를 연결하는 데 사용할 수 있는 옵션과 함께 사용하는 방법을 설명합니다.

설치 프로세스는 다음 단계로 나눌 수 있습니다.

Azure VMware 솔루션을 사용하려면 먼저 확인된 구독 내에 리소스 공급자를 등록해야 합니다.

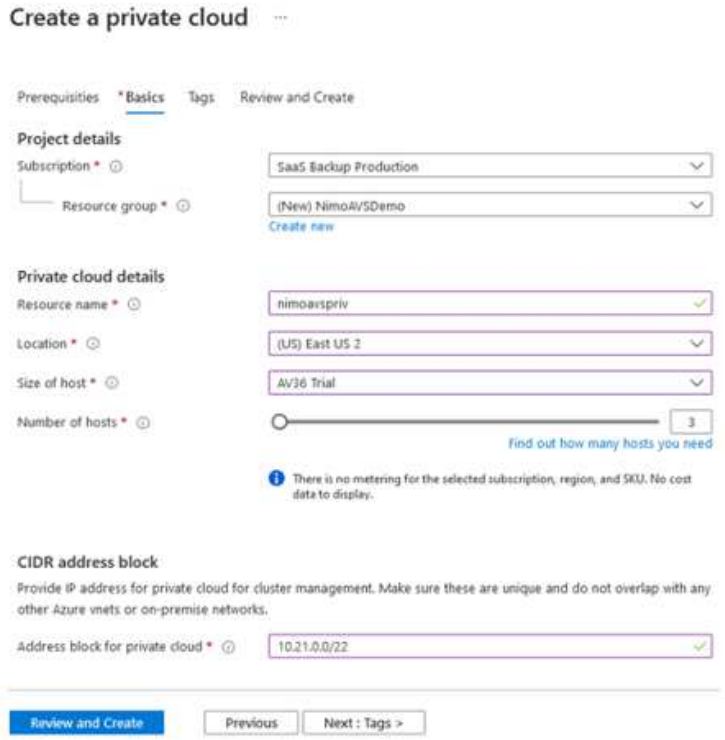
1. Azure 포털에 로그인합니다.
2. Azure 포털 메뉴에서 모든 서비스를 선택합니다.
3. 모든 서비스 대화 상자에서 구독을 입력한 다음 구독 을 선택합니다.
4. 보려면 구독 목록에서 구독을 선택합니다.
5. 리소스 공급자 를 선택하고 검색에 Microsoft.AVS 를 입력합니다.
6. 리소스 공급자가 등록되지 않은 경우 등록 을 선택합니다.



7. 리소스 공급자를 등록한 후 Azure 포털을 사용하여 Azure VMware Solution 프라이빗 클라우드를 생성합니다.
8. Azure 포털에 로그인합니다.
9. 새 리소스 만들기 를 선택합니다.
10. Marketplace 검색 텍스트 상자에 Azure VMware Solution을 입력하고 결과에서 선택합니다.
11. Azure VMware 솔루션 페이지에서 생성 을 선택합니다.
12. 기본 탭에서 필드에 값을 입력하고 검토 + 만들기를 선택합니다.

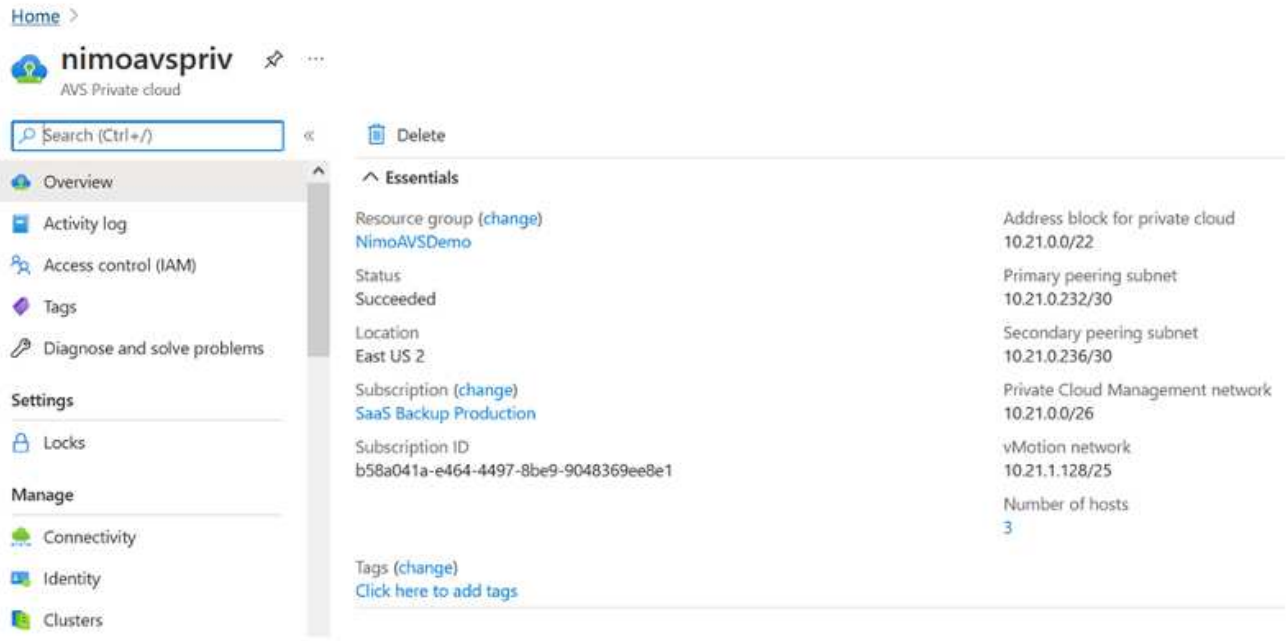
참고:

- 빠른 시작을 위해 계획 단계에서 필요한 정보를 수집합니다.
- 기존 리소스 그룹을 선택하거나 프라이빗 클라우드에 대한 새 리소스 그룹을 생성합니다. 리소스 그룹은 Azure 리소스가 배포 및 관리되는 논리적 컨테이너입니다.
- CIDR 주소가 고유하며 다른 Azure 가상 네트워크 또는 온-프레미스 네트워크와 겹치지 않도록 하십시오. CIDR은 프라이빗 클라우드 관리 네트워크를 나타내며 vCenter Server 및 NSX-T Manager와 같은 클러스터 관리 서비스에 사용됩니다. /22 주소 공간을 사용하는 것이 좋습니다. 이 예에서는 10.21.0.0/22 가 사용됩니다.



프로비저닝 프로세스는 약 4~5시간이 소요됩니다. 프로세스가 완료된 후 Azure 포털에서 프라이빗 클라우드에 액세스하여 성공적으로 배포되었는지 확인합니다. 구축이 완료되면 성공 상태가 표시됩니다.

Azure VMware 솔루션 프라이빗 클라우드에는 Azure 가상 네트워크가 필요합니다. Azure VMware 솔루션은 사내 vCenter를 지원하지 않으므로 기존 사내 환경과 통합하려면 추가 단계가 필요합니다. 또한 ExpressRoute 회로 및 가상 네트워크 게이트웨이를 설정해야 합니다. 클러스터 프로비저닝이 완료될 때까지 기다리는 동안 새 가상 네트워크를 생성하거나 기존 가상 네트워크를 사용하여 Azure VMware 솔루션에 연결합니다.



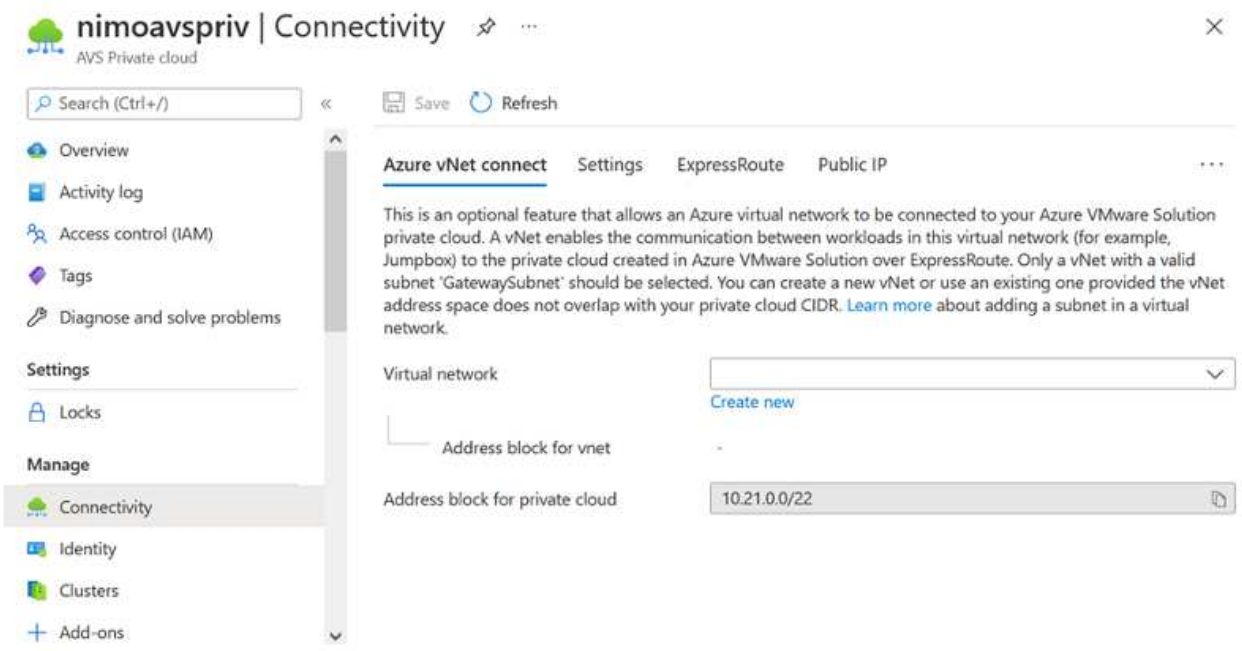
새 또는 기존 **ExpressRoute** 가상 네트워크 게이트웨이에 연결합니다

새 Azure VNet(Virtual Network)을 생성하려면 Azure VNET Connect 탭을 선택합니다. 또는 가상 네트워크 생성 마법사를 사용하여 Azure 포털에서 수동으로 생성할 수도 있습니다.

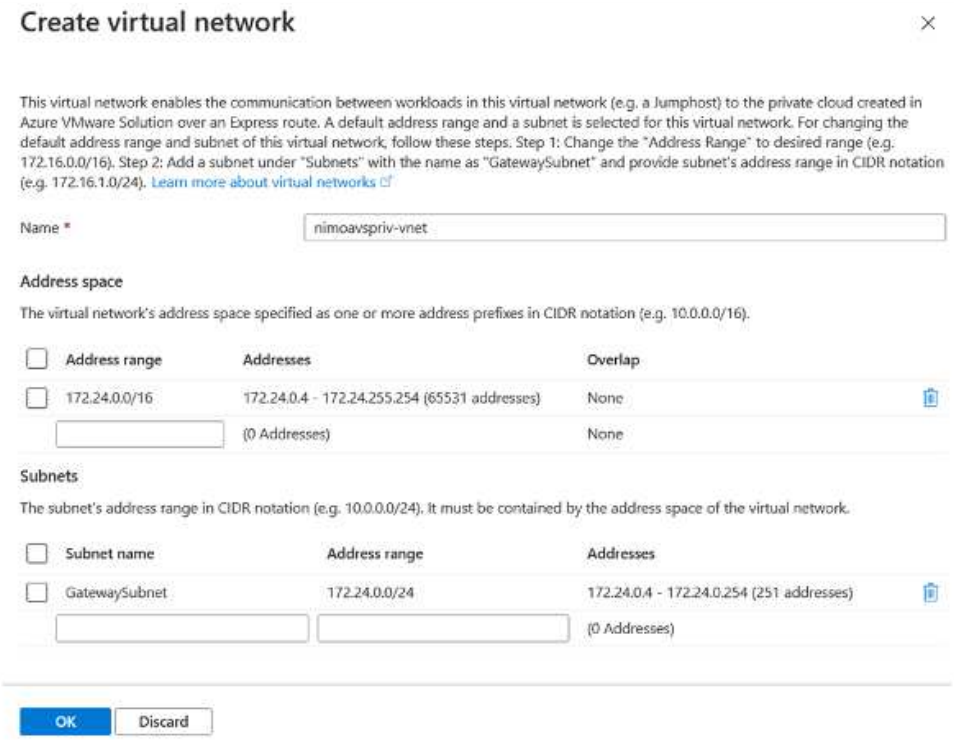
1. Azure VMware Solution 프라이빗 클라우드로 이동하고 관리 옵션 아래에서 접속 구성에 액세스합니다.
2. Azure VNET Connect를 선택합니다.
3. 새 VNET를 생성하려면 Create New 옵션을 선택합니다.

   이 기능을 사용하면 VNET를 Azure VMware Solution 프라이빗 클라우드에 연결할 수 있습니다. VNET는 Azure VMware Solution에서 ExpressRoute를 통해 생성된 프라이빗 클라우드에 필요한 구성 요소(예: 점프 박스, Azure NetApp Files와 같은 공유 서비스, 클라우드 볼륨 ONTAP)를 자동으로 생성하여 이 가상 네트워크의 워크로드 간 통신을 지원합니다.

   ◦ 참고: * VNET 주소 공간은 사설 클라우드 CIDR과 겹치지 않아야 합니다.



4. 새 VNET에 대한 정보를 제공하거나 업데이트하고 OK(확인) 를 선택합니다.

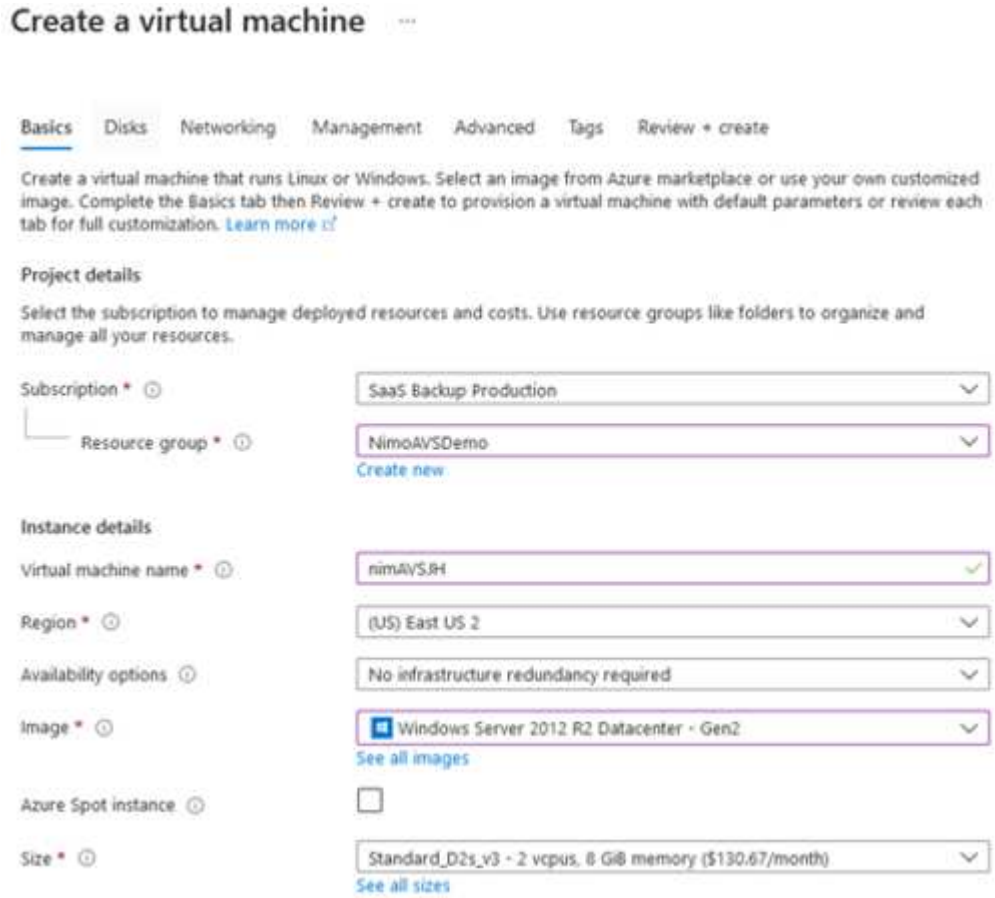


제공된 주소 범위 및 게이트웨이 서브넷이 있는 VNET는 지정된 가입 및 리소스 그룹에 생성됩니다.

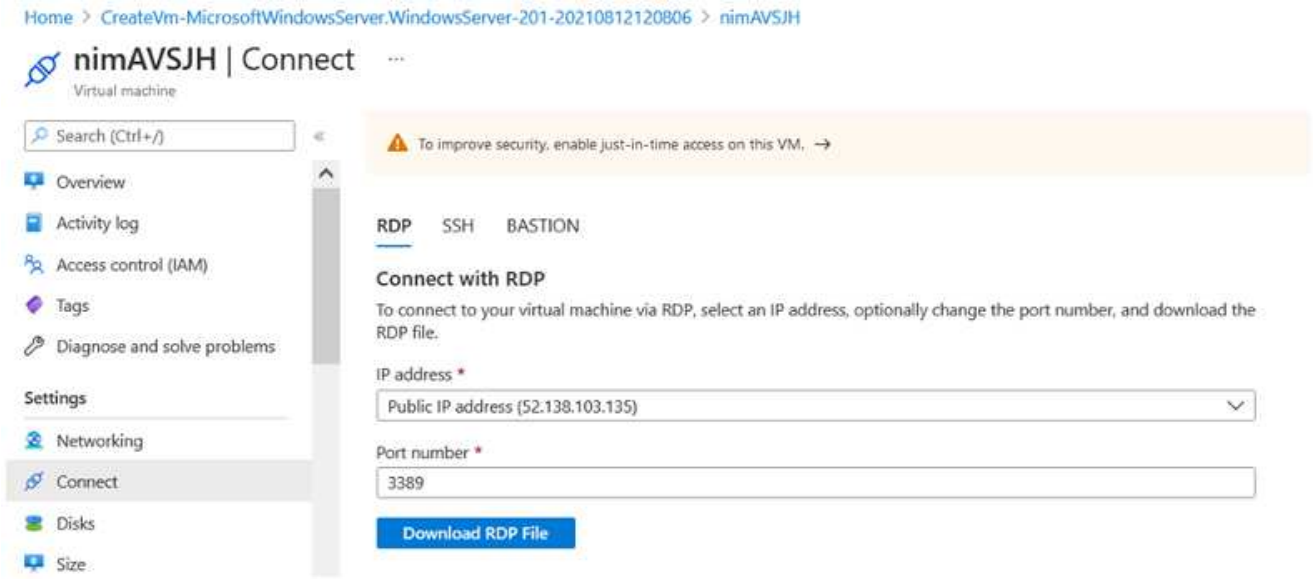
VNET를 수동으로 생성하는 경우 해당 SKU와 ExpressRoute를 게이트웨이 유형으로 사용하여 가상 네트워크 게이트웨이를 생성합니다. 구축이 완료되면 인증 키를 사용하여 Azure VMware Solution 프라이빗 클라우드가 포함된 가상 네트워크 게이트웨이에 ExpressRoute 연결을 연결합니다. 자세한 내용은 을 참조하십시오 "Azure에서 VMware 프라이빗 클라우드에 대한 네트워킹을 구성합니다".

Azure VMware Solution 프라이빗 클라우드에 대한 네트워크 연결 및 액세스 검증

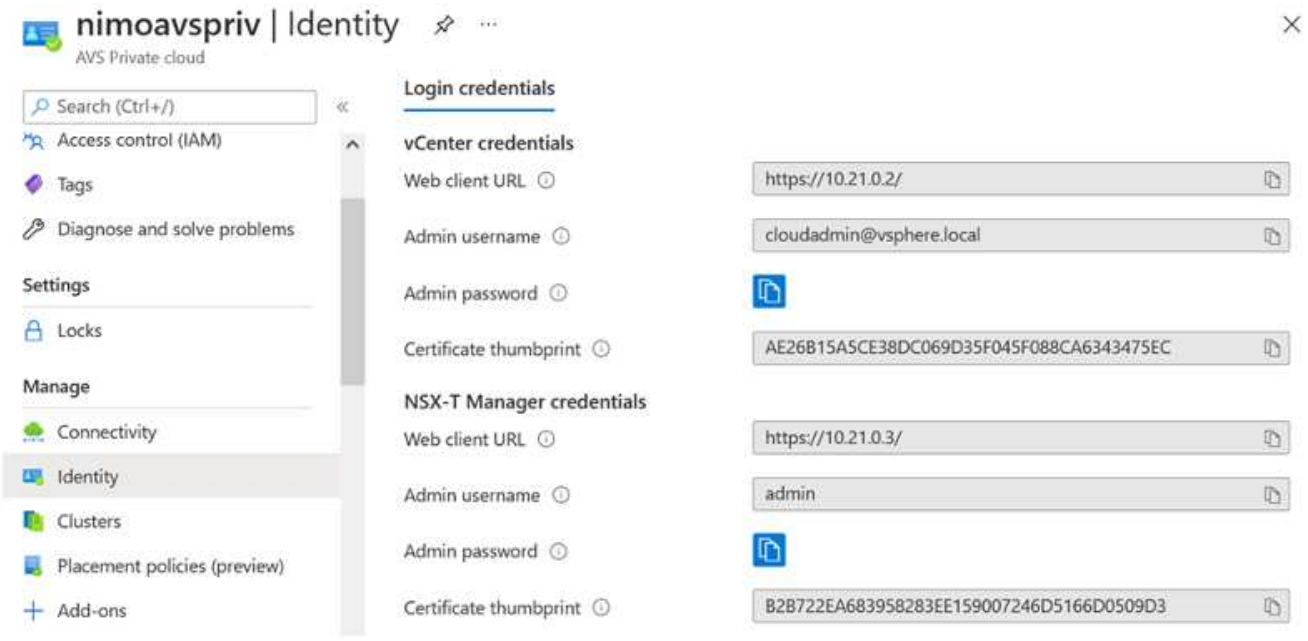
Azure VMware 솔루션에서는 사내 VMware vCenter를 통해 프라이빗 클라우드를 관리할 수 없습니다. 대신, 점프 호스트는 Azure VMware Solution vCenter 인스턴스에 연결하는 데 필요합니다. 지정된 리소스 그룹에 점프 호스트를 생성하고 Azure VMware Solution vCenter에 로그인합니다. 이 점프 호스트는 연결을 위해 생성된 동일한 가상 네트워크의 Windows VM이고 vCenter 및 NSX Manager에 대한 액세스를 제공해야 합니다.



가상 시스템을 프로비저닝한 후에는 연결 옵션을 사용하여 RDP에 액세스합니다.

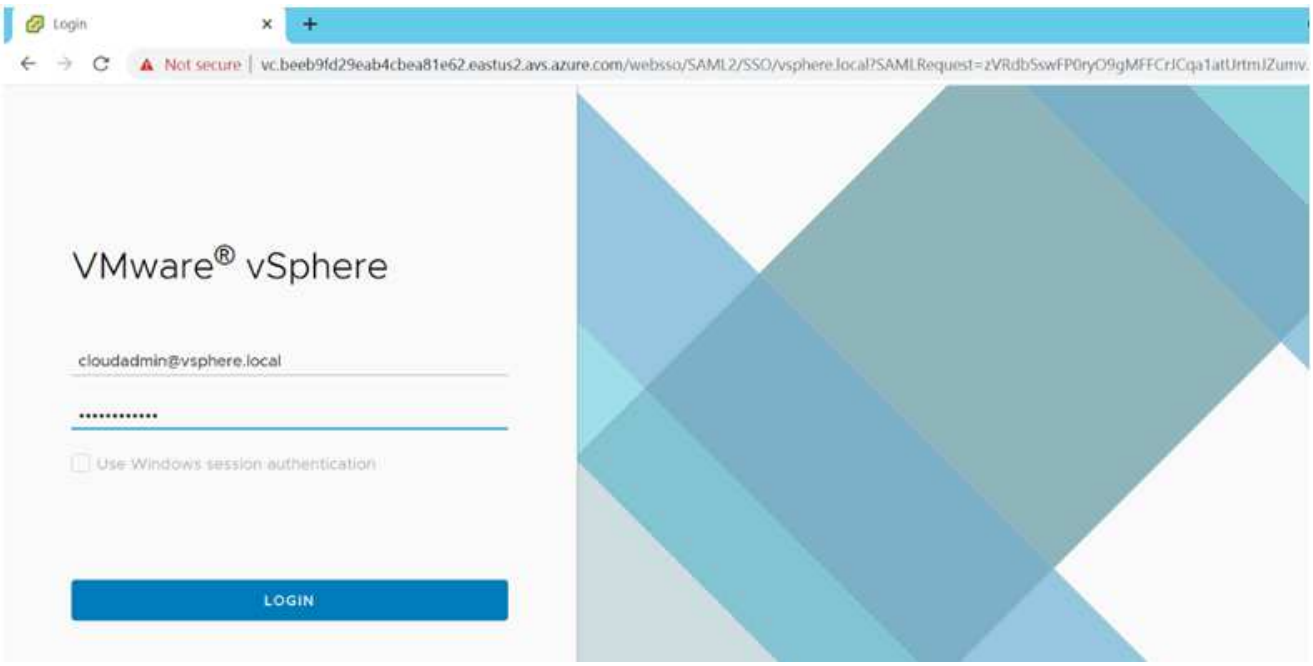


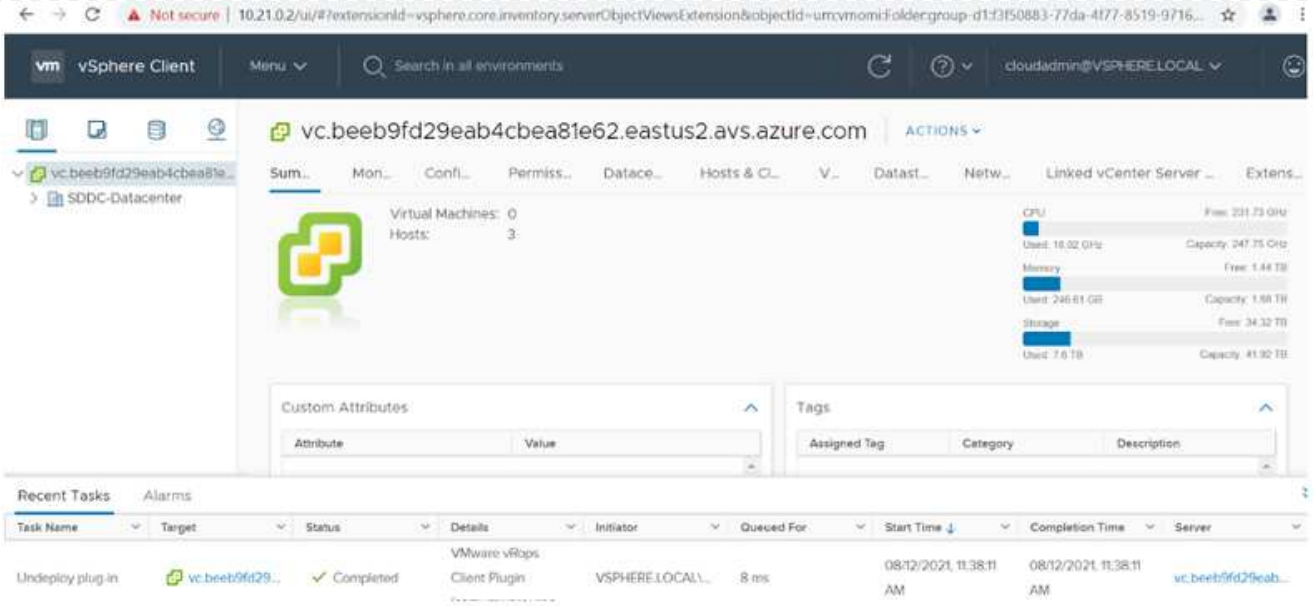
새로 생성된 이 점프 호스트 가상 머신에서 클라우드 관리자 사용자를 사용하여 vCenter에 로그인합니다. 자격 증명에 액세스하려면 Azure 포털로 이동하여 ID로 이동합니다(프라이빗 클라우드 내의 관리 옵션 아래). 프라이빗 클라우드 vCenter 및 NSX-T Manager의 URL 및 사용자 자격 증명은 여기에서 복사할 수 있습니다.



Windows 가상 머신에서 브라우저를 열고 vCenter 웹 클라이언트 URL로 이동합니다 관리자 사용자 이름을 * cloudadmin@vsphere.loca l * 로 사용하고 복사한 암호를 붙여 넣습니다. 마찬가지로 웹 클라이언트 URL을 사용하여 NSX-T Manager에 액세스할 수도 있습니다 관리자 사용자 이름을 사용하여 복사한 암호를 붙여 넣어 새 세그먼트를 만들거나 기존 계층 게이트웨이를 수정합니다.

웹 클라이언트 URL은 프로비저닝된 각 SDDC에 따라 다릅니다.





이제 Azure VMware Solution SDDC가 구축 및 구성되었습니다. ExpressRoute Global Reach를 활용하여 사내 환경을 Azure VMware 솔루션 프라이빗 클라우드에 연결합니다. 자세한 내용은 을 참조하십시오 "온프레미스 환경을 Azure VMware 솔루션에 대해 알아보십시오".

Google Cloud Platform(GCP)에서 가상화 환경 구축 및 구성

온프레미스에서와 마찬가지로, VM 및 마이그레이션을 생성하기 위한 성공적인 프로덕션 준비 환경을 위해서는 Google Cloud VMware Engine(GCVE)을 계획하는 것이 매우 중요합니다.

이 섹션에서는 GCVE를 설정 및 관리하고 NetApp 스토리지를 연결하는 데 사용할 수 있는 옵션과 함께 사용하는 방법을 설명합니다.

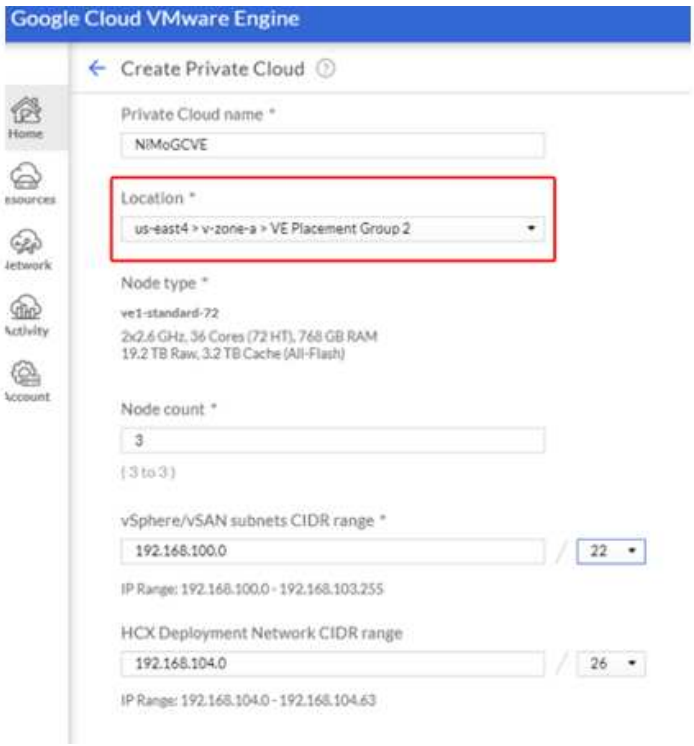
설치 프로세스는 다음 단계로 나눌 수 있습니다.

GCP에서 GCVE 환경을 구성하려면 GCP 콘솔에 로그인하고 VMware Engine 포털에 액세스합니다.

"새 사설 클라우드" 버튼을 클릭하고 GCVE 프라이빗 클라우드에 대해 원하는 구성을 입력합니다. "위치"에서 CVS/CVO가 배포된 동일한 지역/영역에 프라이빗 클라우드를 배포하여 최상의 성능과 최저 지연 시간을 보장해야 합니다.

전제 조건:

- VMware Engine Service Admin IAM 역할을 설정합니다
- "VMware Engine API 액세스 및 노드 할당량을 설정합니다"
- CIDR 범위가 온-프레미스 또는 클라우드 서브넷과 겹치지 않도록 하십시오. CIDR 범위는 /27 이상이어야 합니다.



참고: 프라이빗 클라우드를 생성하는 데 30분에서 2시간까지 걸릴 수 있습니다.

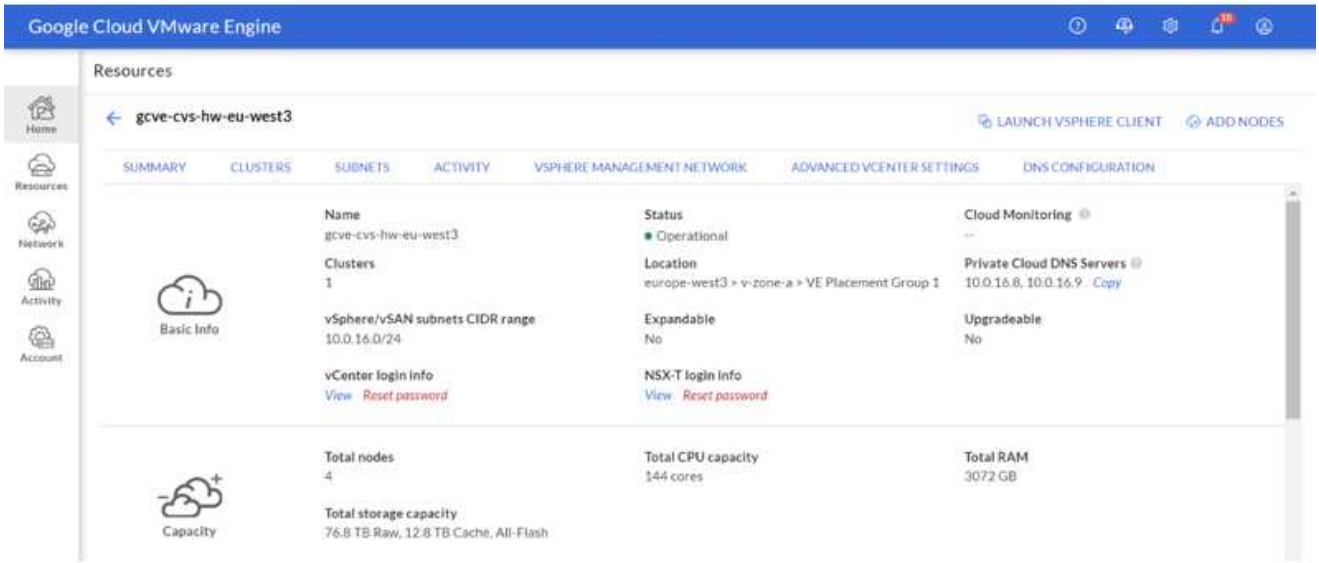
GCVE에 대한 개인 액세스를 활성화합니다

프라이빗 클라우드가 프로비저닝되면 높은 처리량과 짧은 지연 시간의 데이터 경로 연결을 위해 프라이빗 클라우드에 대한 프라이빗 액세스를 구성합니다.

이렇게 하면 Cloud Volumes ONTAP 인스턴스가 실행 중인 VPC 네트워크가 GCVE 프라이빗 클라우드와 통신할 수 있습니다. 이렇게 하려면 를 따르십시오 "GCP 문서". 클라우드 볼륨 서비스의 경우 테넌트 호스트 프로젝트 간에 일회성 피어링을 수행하여 VMware 엔진과 Cloud Volumes Service 간에 연결을 설정합니다. 자세한 단계는 다음과 같습니다 "링크".

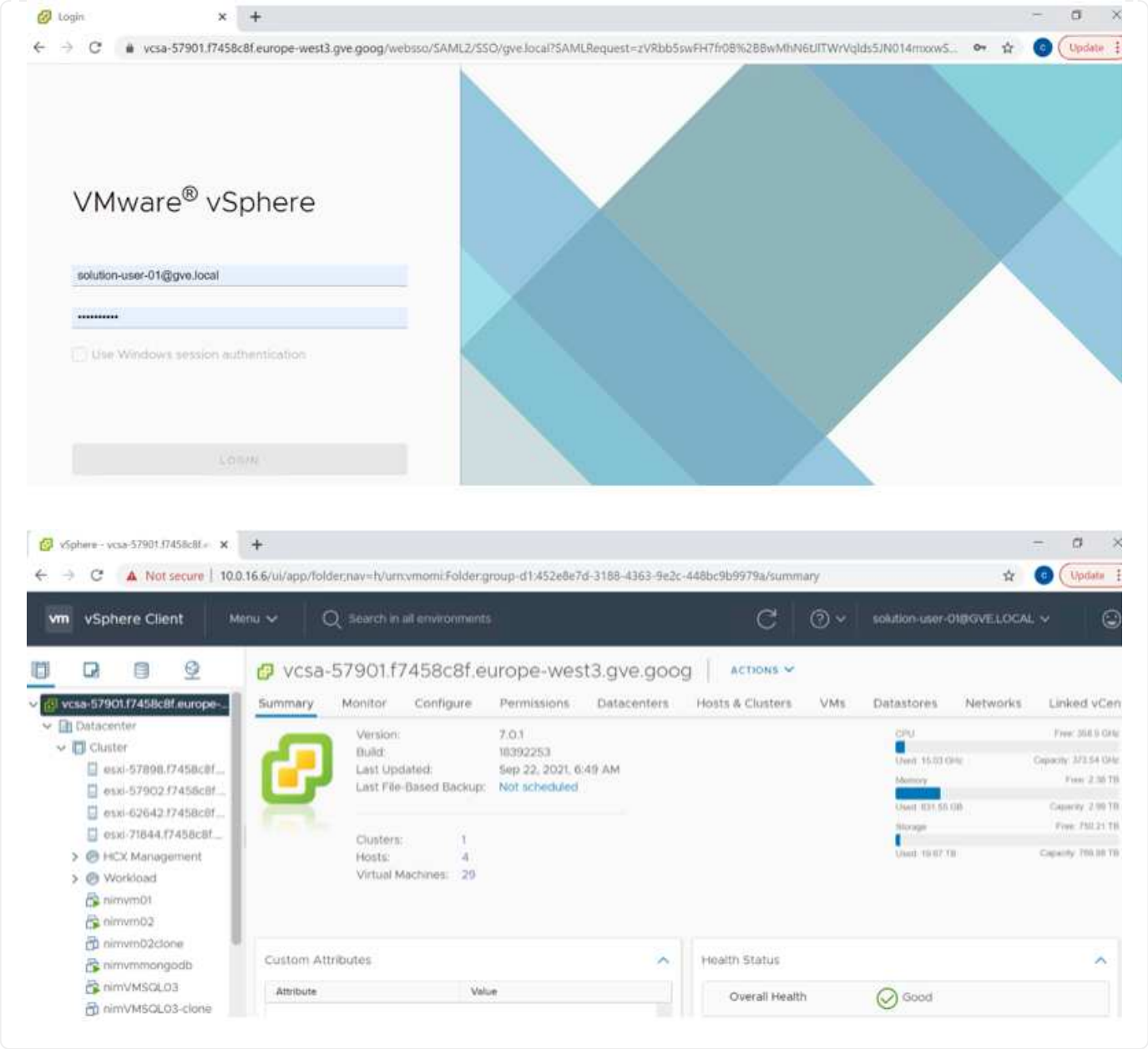
Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

CloudOwner@gve.loca I 사용자를 사용하여 vCenter에 로그인합니다. 자격 증명을 액세스하려면 VMware Engine 포털로 이동하여 리소스 로 이동한 다음 적절한 프라이빗 클라우드를 선택합니다. 기본 정보 섹션에서 vCenter 로그인 정보(vCenter Server, HCX Manager) 또는 NSX-T 로그인 정보(NSX Manager)에 대한 보기 링크를 클릭합니다.



Windows 가상 머신에서 브라우저를 열고 vCenter 웹 클라이언트 URL로 이동합니다 admin 사용자 이름을 CloudOwner@gve.loca I 로 사용하여 복사한 암호를 붙여 넣습니다. 마찬가지로 웹 클라이언트 URL을 사용하여 NSX-T Manager에 액세스할 수도 있습니다 관리자 사용자 이름을 사용하여 복사한 암호를 붙여 넣어 새 세그먼트를 만들거나 기존 계층 게이트웨이를 수정합니다.

사내 네트워크에서 VMware Engine 프라이빗 클라우드로 연결하려면 클라우드 VPN 또는 Cloud Interconnect를 활용하여 적절한 연결을 설정하고 필요한 포트가 열려 있는지 확인합니다. 자세한 단계는 다음과 같습니다 "링크".



NetApp Cloud Volume Service 보조 데이터 저장소를 **GCVE**에 배포합니다

을 참조하십시오 "NetApp CVS to GCVE를 사용하여 보조 NFS 데이터 저장소를 배포하는 절차"

퍼블릭 클라우드 공급자를 위한 **NetApp** 스토리지 옵션

세 가지 주요 하이퍼 스케일러의 스토리지로서의 NetApp 옵션에 대해 알아보십시오.

AWS/VMC

AWS는 다음과 같은 구성에서 NetApp 스토리지를 지원합니다.

- FSX ONTAP를 게스트 연결 스토리지로 사용합니다
- CVO(Cloud Volumes ONTAP)를 게스트 연결 스토리지로 사용합니다
- FSX ONTAP는 보조 NFS 데이터 저장소입니다

자세한 내용을 확인하십시오 "VMC에 대한 게스트 연결 스토리지 옵션". 자세한 내용을 확인하십시오 "VMC에 대한 보조 NFS 데이터 저장소 옵션".

Azure/AVS

Azure는 다음과 같은 구성에서 NetApp 스토리지를 지원합니다.

- 게스트 연결 스토리지로서의 Azure NetApp Files(ANF)
- CVO(Cloud Volumes ONTAP)를 게스트 연결 스토리지로 사용합니다
- Azure NetApp Files(ANF)를 보조 NFS 데이터 저장소로 사용합니다

자세한 내용을 확인하십시오 "AVS용 게스트 연결 스토리지 옵션". 자세한 내용을 확인하십시오 "AVS용 보조 NFS 데이터 저장소 옵션".

GCP/GCVE

Google Cloud는 다음과 같은 구성에서 NetApp 스토리지를 지원합니다.

- CVO(Cloud Volumes ONTAP)를 게스트 연결 스토리지로 사용합니다
- CVS(Cloud Volumes Service)를 게스트 연결 스토리지로 사용합니다
- CVS(Cloud Volumes Service)를 보조 NFS 데이터 저장소로 사용

자세한 내용을 확인하십시오 "GCVE에 대한 게스트 연결 저장소 옵션".

에 대해 자세히 알아보십시오 "Google Cloud VMware Engine에 대한 NetApp Cloud Volumes Service 데이터 저장소 지원(NetApp 블로그)" 또는 "NetApp CVS를 Google Cloud VMware Engine용 데이터 저장소로 사용하는 방법(Google 블로그)"

TR-4938: AWS에서 **VMware Cloud**를 사용하여 **ONTAP**용 **Amazon FSx**를 **NFS** 데이터 저장소로 마운트합니다

Niyaz Mohamed, NetApp

소개

성공적인 모든 조직은 혁신과 현대화의 길을 따라 있습니다. 이 프로세스의 일환으로, 기업은 일반적으로 기존 VMware 투자를 사용하여 클라우드의 이점을 활용하고 가능한 한 원활하게 프로세스에 대한 재해 복구를 마이그레이션, 버스트, 확장 및 제공하는 방법을 모색합니다. 클라우드로 마이그레이션하는 고객은 탄력성 및 폭발적 사용 사례, 데이터 센터 종료, 데이터 센터 통합, 수명 종료 시나리오, 인수 합병 인수 합병 등

대부분의 고객은 VMware Cloud on AWS를 통해 고유한 하이브리드 기능을 제공할 수 있기 때문에 이 옵션을 선호하지만, 제한된 기본 스토리지 옵션으로 인해 스토리지 집약적인 워크로드를 사용하는 조직에는 유용성이 제한되었습니다. 스토리지가 호스트에 직접 연결되어 있으므로 스토리지를 확장하는 유일한 방법은 호스트를 추가하는

것입니다. 이렇게 하면 스토리지 집약적인 워크로드에서 비용이 35-40% 이상 증가할 수 있습니다. 이러한 워크로드는 추가 성능이 아닌 추가 스토리지 및 분리된 성능을 필요로 하며, 이는 추가 호스트에 대한 비용을 지불한다는 것을 의미합니다. 이 부분에서 가 사용됩니다 "최신 통합" ONTAP용 FSx는 AWS 기반의 VMware Cloud를 통해 스토리지 및 성능 집약적인 워크로드에 매우 유용합니다.

다음과 같은 시나리오를 생각해 보겠습니다. 고객은 마력(vCPU/vmem)을 위해 8개의 호스트를 필요로 하지만 스토리지에 대한 요구 사항도 상당히 있습니다. 평가를 기준으로 이 고객은 스토리지 요구사항을 충족하기 위해 16개의 호스트를 필요로 합니다. 이렇게 하면 실제로 필요한 모든 것이 더 많은 스토리지일 때 마력을 추가로 구입해야 하기 때문에 전체 TCO가 증가합니다. 마이그레이션, 재해 복구, 사용 급증, 개발/테스트, 등.

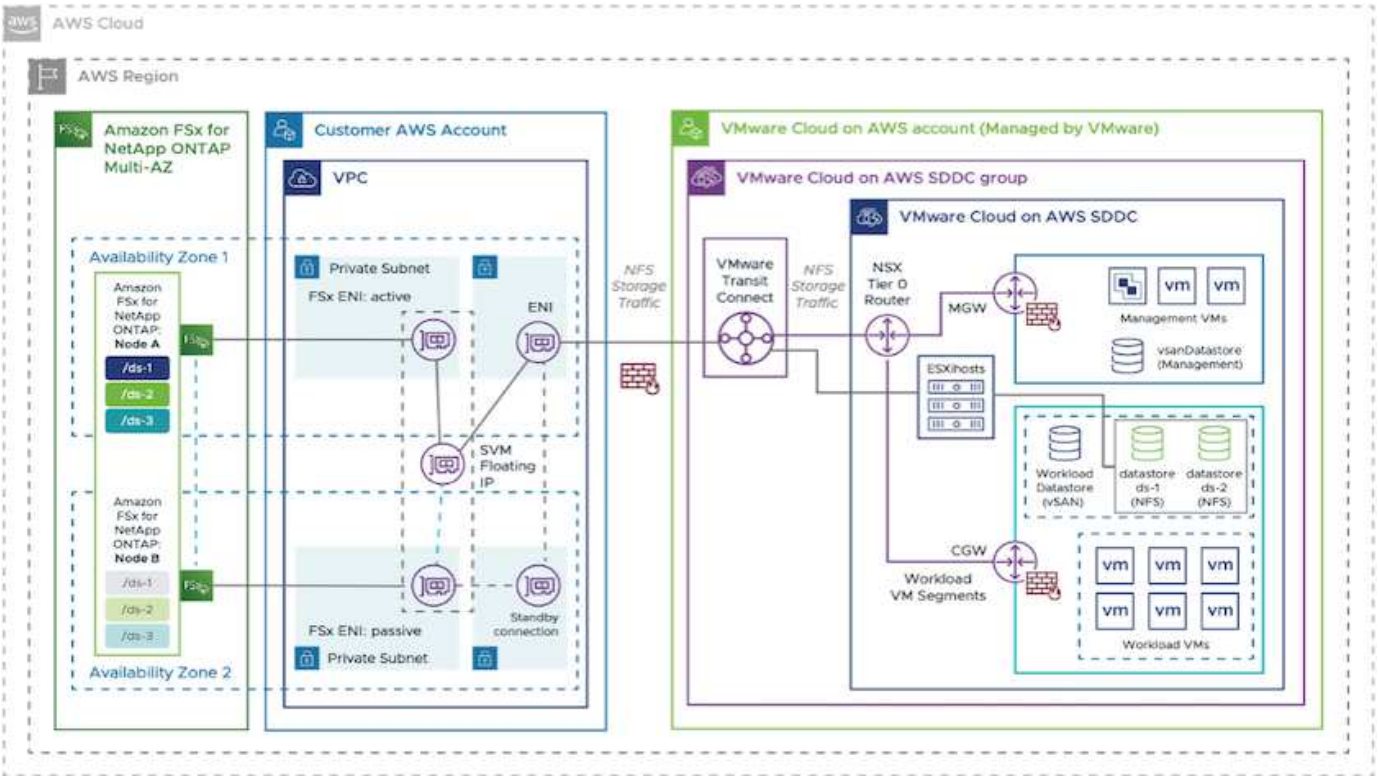
이 문서에서는 ONTAP용 FSx를 AWS의 VMware Cloud용 NFS 데이터 저장소로 프로비저닝하고 연결하는 데 필요한 단계를 안내합니다.

> 이 솔루션은 VMware에서도 사용할 수 있습니다. 를 방문하십시오 "VMware 클라우드 기술 영역" 를 참조하십시오.

연결 옵션

> AWS 기반 VMware Cloud는 ONTAP용 FSx의 다중 AZ 및 단일 AZ 구축을 모두 지원합니다.

이 섹션에서는 고속 접속 아키텍처와 추가 호스트 추가 없이 SDDC 클러스터의 스토리지를 확장하는 솔루션을 구축하는 데 필요한 단계에 대해 설명합니다.



고급 배포 단계는 다음과 같습니다.

1. 새로 지정된 VPC에서 ONTAP용 Amazon FSx를 생성합니다.
2. SDDC 그룹을 만듭니다.
3. VMware Transit Connect 및 TGW 접속 장치를 생성합니다.

4. 라우팅(AWS VPC 및 SDDC) 및 보안 그룹을 구성합니다.
5. NFS 볼륨을 SDDC 클러스터에 데이터 저장소로 연결합니다.

ONTAP용 FSx를 NFS 데이터 저장소로 프로비저닝하고 연결하려면 먼저 클라우드 SDDC 환경에서 VMware를 설정하거나 기존 SDDC를 v1.20 이상으로 업그레이드해야 합니다. 자세한 내용은 를 참조하십시오 "AWS 기반 VMware Cloud 시작하기".

ONTAP용 FSX는 현재 확장 클러스터에서 지원되지 않습니다.

결론

이 문서에서는 AWS에서 VMware 클라우드를 사용하여 ONTAP용 Amazon FSx를 구성하는 데 필요한 단계를 설명합니다. ONTAP용 Amazon FSx는 파일 서비스와 함께 애플리케이션 워크로드를 배포 및 관리하는 탁월한 옵션을 제공하는 동시에 애플리케이션 계층에 대한 데이터 요구 사항을 원활하게 만들어 TCO를 절감합니다. 어떤 사용 사례에서든 AWS 기반 VMware Cloud와 Amazon FSx for ONTAP를 함께 사용하여 클라우드의 이점, 일관된 인프라, 그리고 사내 스토리지에서 AWS로 이르는 운영, 워크로드의 양방향 이동성, 엔터프라이즈급 용량 및 성능을 빠르게 실현할 수 있습니다. 스토리지 연결에 사용되는 것과 동일한 친숙한 프로세스 및 절차입니다. 이는 새로운 이름과 함께 변경된 데이터의 위치일 뿐입니다. 도구와 프로세스는 모두 동일하며 ONTAP용 Amazon FSx는 전체 구축을 최적화하는 데 도움이 됩니다.

이 프로세스에 대해 자세히 알아보려면 자세한 단계별 안내 비디오를 참조하십시오.

Amazon FSx for ONTAP VMware Cloud를 참조하십시오

AWS를 위한 **NetApp** 게스트 연결 스토리지 옵션

AWS는 네이티브 FSx 서비스(FSx ONTAP) 또는 Cloud Volumes ONTAP(CVO)를 사용하여 게스트로 연결된 NetApp 스토리지를 지원합니다.

FSX ONTAP

NetApp ONTAP용 Amazon FSx는 NetApp의 인기 있는 ONTAP 파일 시스템을 기반으로 구축된 매우 안정적이고 확장 가능하며 고성능 및 다양한 기능을 갖춘 파일 스토리지를 제공하는 완전 관리형 서비스입니다. ONTAP용 FSX는 NetApp 파일 시스템의 친숙한 기능, 성능, 기능 및 API 작업을 완벽하게 관리되는 AWS 서비스의 민첩성, 확장성 및 간편성과 결합합니다.

ONTAP용 FSX는 AWS 또는 사내에서 실행되는 Linux, Windows 및 macOS 컴퓨팅 인스턴스에서 광범위하게 액세스할 수 있는 다양한 기능을 갖춘 빠르고 유연한 공유 파일 스토리지를 제공합니다. ONTAP용 FSX는 밀리초 미만의 지연 시간으로 고성능 SSD(Solid State Drive) 스토리지를 제공합니다. ONTAP용 FSx를 사용하면 SSD 스토리지 비용을 절감하면서 작업 부하에 대한 SSD 수준의 성능을 달성할 수 있습니다. 단, 데이터의 일부만이 가능합니다.

ONTAP용 FSx를 사용하면 버튼 클릭 한 번으로 파일을 스냅샷, 클론 생성 및 복제할 수 있으므로 데이터 관리가 더욱 쉬워집니다. 또한, ONTAP용 FSx는 데이터를 비용이 저렴하고 탄력적인 스토리지에 자동으로 계층화하므로 용량을 할당하거나 관리할 필요가 없습니다.

또한 ONTAP용 FSX는 완벽하게 관리되는 백업과 지역 간 재해 복구를 지원하는 고가용성의 내구성 스토리지를 제공합니다. 데이터를 보다 쉽게 보호하고 보안을 유지할 수 있도록 ONTAP용 FSx는 널리 사용되는 데이터 보안 및 바이러스 백신 응용 프로그램을 지원합니다.

FSX ONTAP를 게스트 연결 스토리지로 사용합니다

AWS에서 VMware Cloud를 사용하여 NetApp ONTAP용 Amazon FSx를 구성합니다

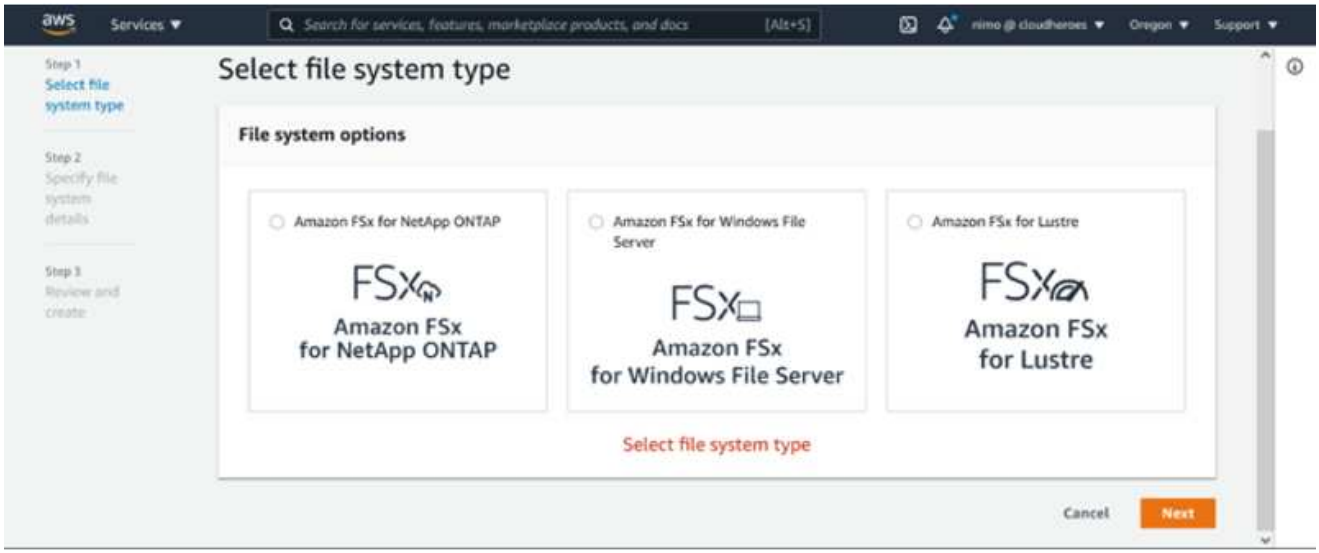
NetApp ONTAP용 Amazon FSx 파일 공유 및 LUN은 AWS의 VMware Cloud에서 VMware SDDC 환경 내에 생성된 VM에서 마운트할 수 있습니다. Linux 클라이언트에도 볼륨을 마운트하고 NFS 또는 SMB 프로토콜을 사용하여 Windows 클라이언트에 매핑할 수 있으며, iSCSI를 통해 마운트하면 Linux 또는 Windows 클라이언트에서 LUN에 블록 디바이스로 액세스할 수 있습니다. NetApp ONTAP 파일 시스템용 Amazon FSx는 다음 단계를 통해 빠르게 설정할 수 있습니다.

AWS 기반 NetApp ONTAP 및 VMware Cloud용 Amazon FSx는 더 나은 성능을 달성하고 가용성 영역 간의 데이터 전송 비용을 방지하려면 동일한 가용성 영역에 있어야 합니다.

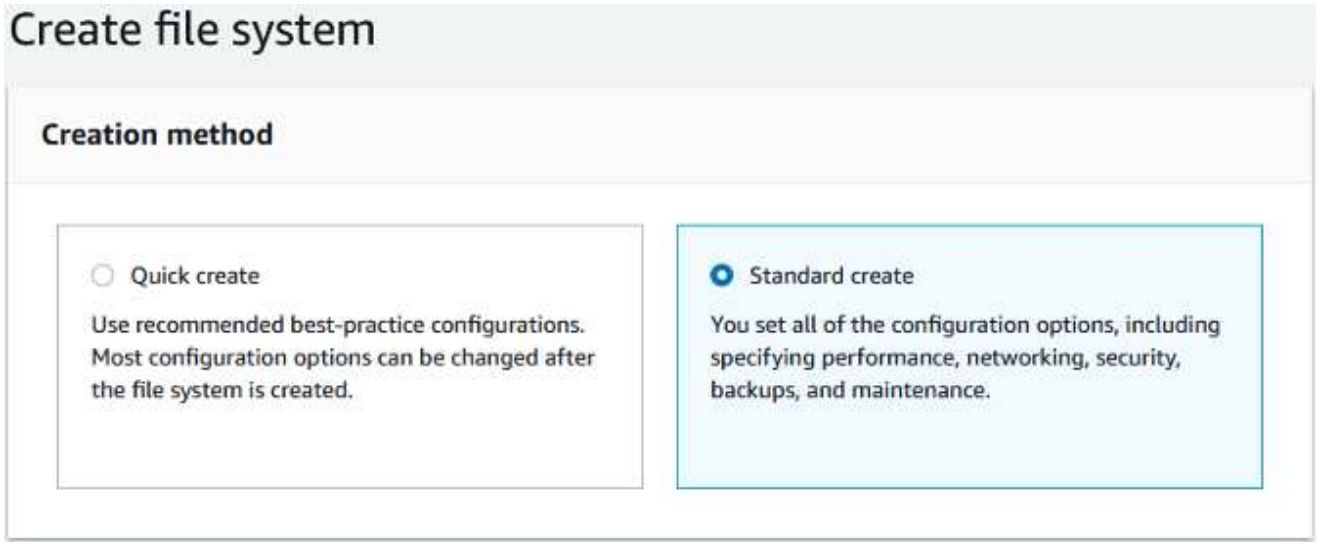
ONTAP 볼륨용 Amazon FSx를 생성하고 마운트합니다

NetApp ONTAP 파일 시스템용 Amazon FSx를 생성하고 마운트하려면 다음 단계를 완료하십시오.

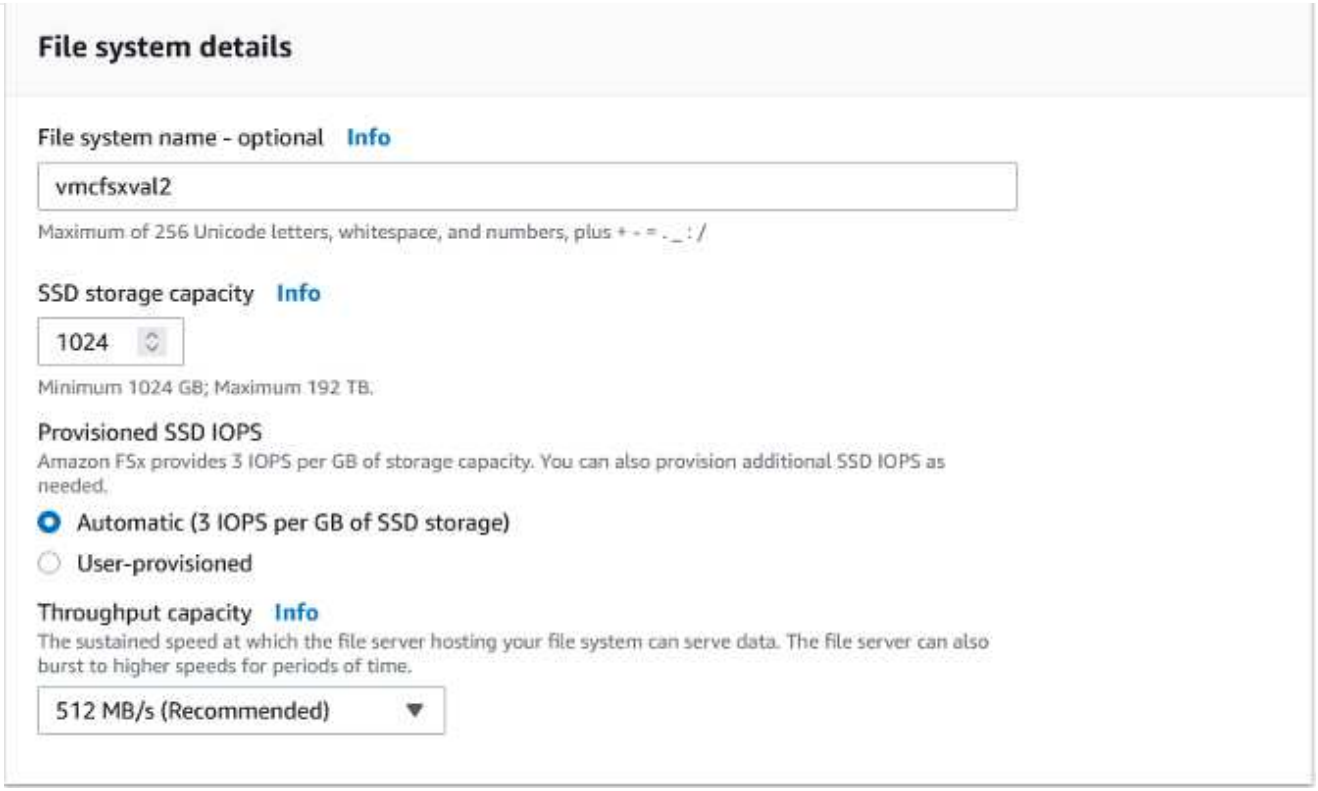
1. 를 엽니다 "Amazon FSx 콘솔" 파일 시스템 생성 마법사를 시작하려면 파일 시스템 생성 을 선택합니다.
2. 파일 시스템 유형 선택 페이지에서 NetApp ONTAP용 Amazon FSx 를 선택하고 다음 을 선택합니다. 파일 시스템 생성 페이지가 나타납니다.



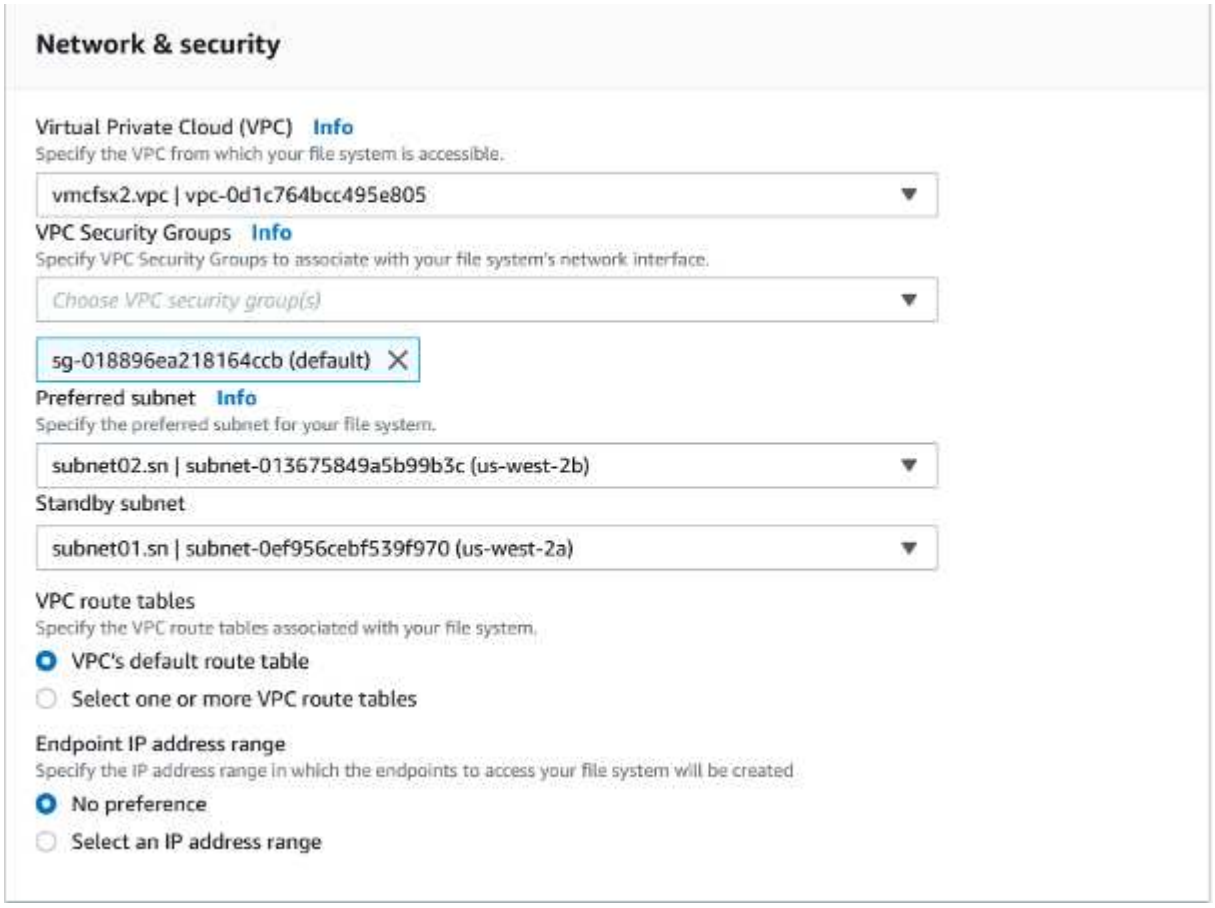
1. 네트워킹 섹션의 VPC(가상 프라이빗 클라우드)에서 경로 테이블과 함께 적절한 VPC 및 기본 서브넷을 선택합니다. 이 경우 드롭다운에서 vmcfsx2.vpc가 선택됩니다.



1. 생성 방법의 경우 표준 작성을 선택합니다. 빠른 만들기를 선택할 수도 있지만 이 문서에서는 표준 만들기 옵션을 사용합니다.

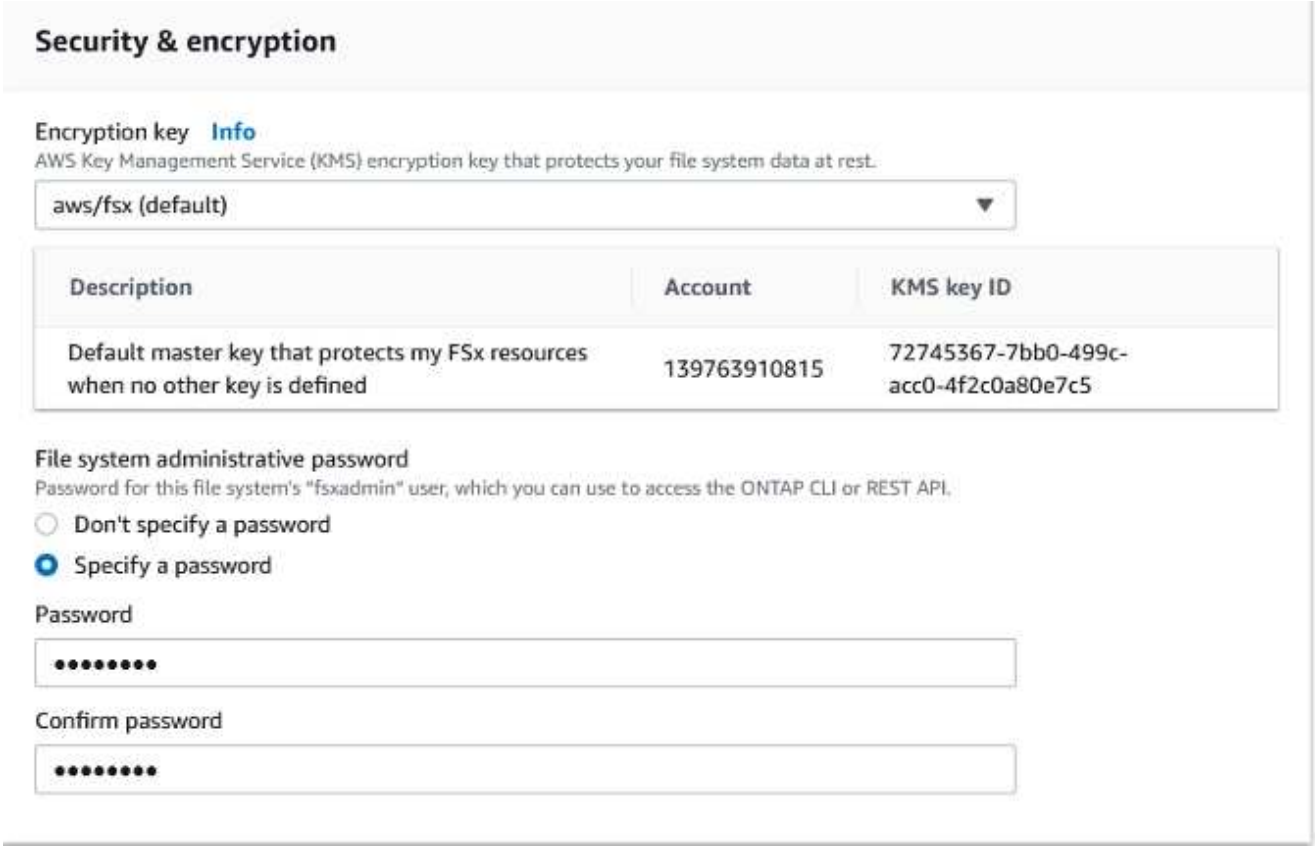


1. 네트워킹 섹션의 VPC(가상 프라이빗 클라우드)에서 경로 테이블과 함께 적절한 VPC 및 기본 서브넷을 선택합니다. 이 경우 드롭다운에서 vmcfsx2.vpc가 선택됩니다.

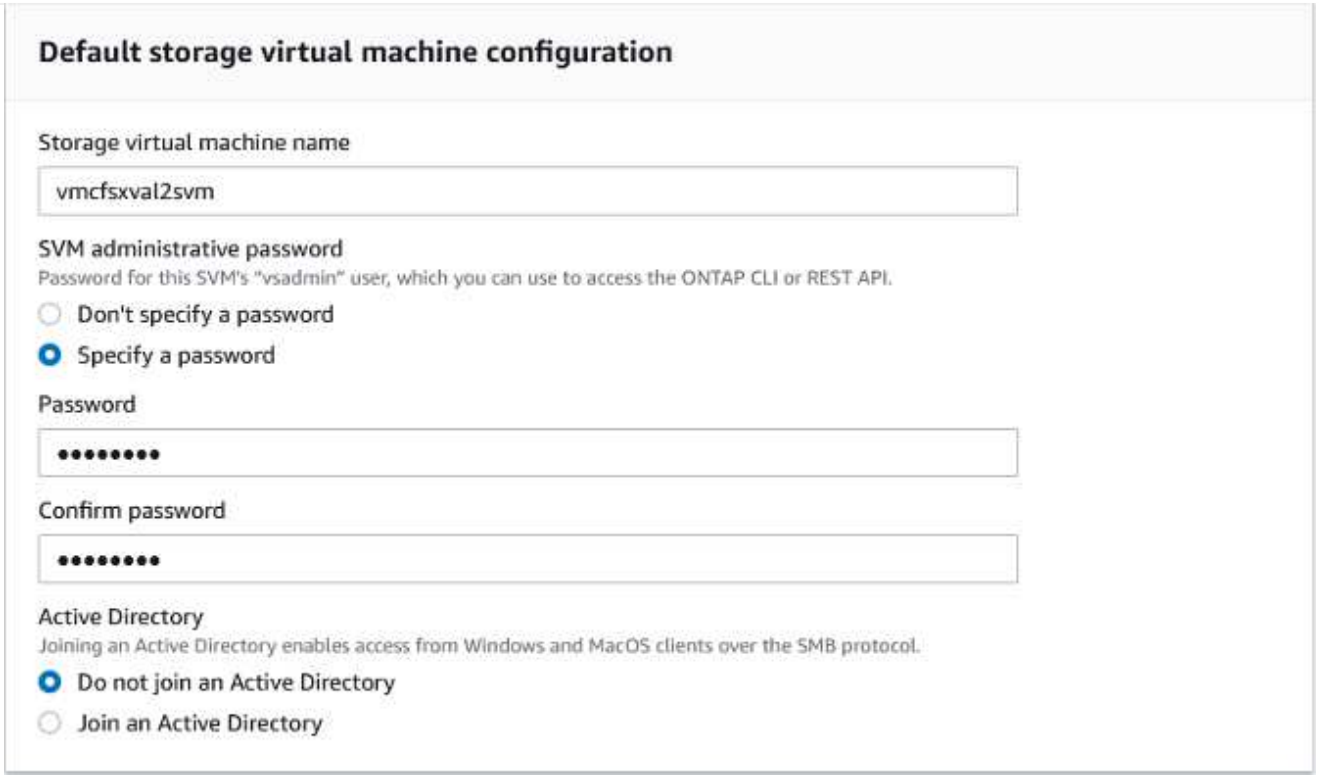


네트워킹 섹션의 VPC(가상 프라이빗 클라우드)에서 경로 테이블과 함께 적절한 VPC 및 기본 서브넷을 선택합니다. 이 경우 드롭다운에서 vmcfsx2.vpc가 선택됩니다.

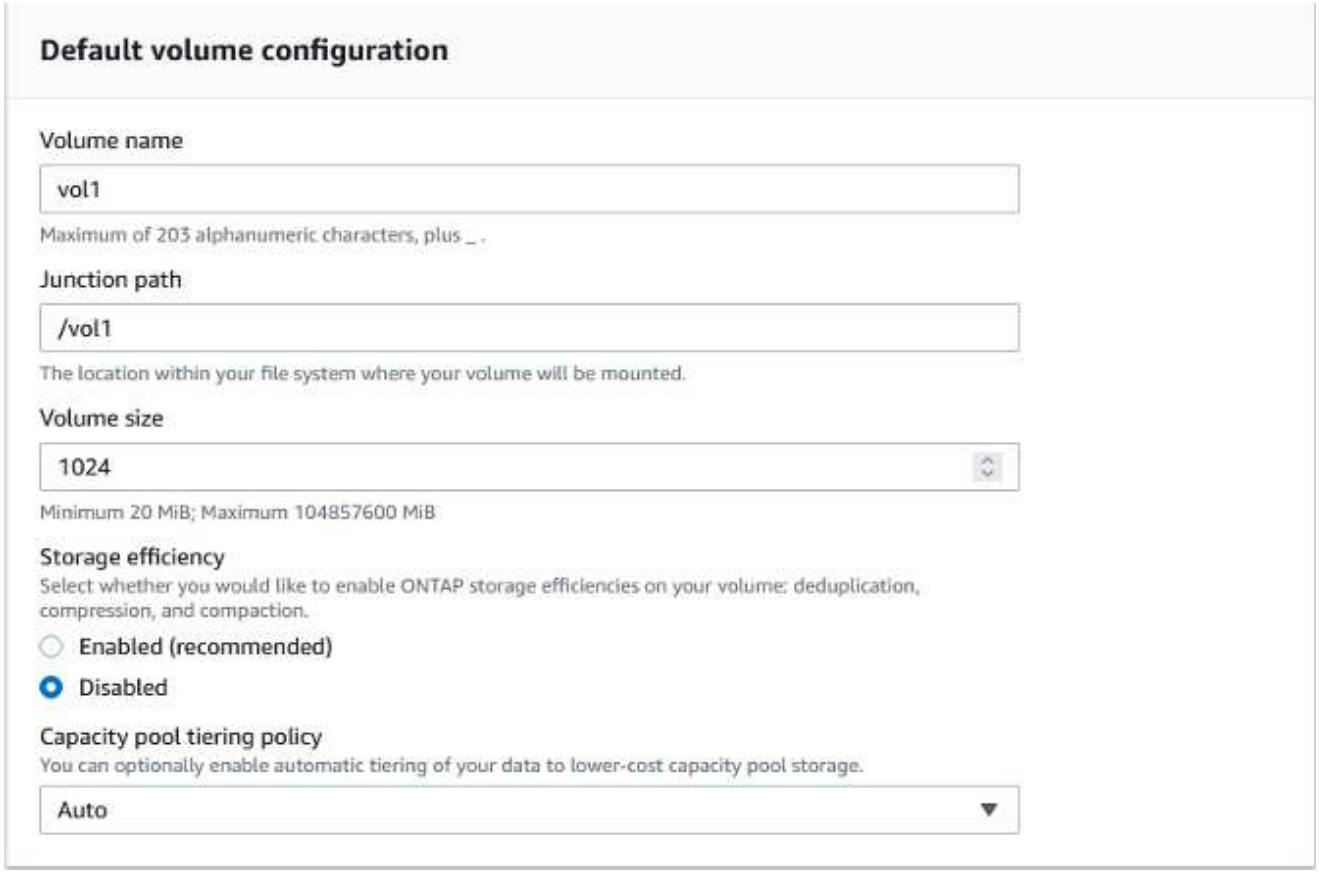
1. 보안 및 암호화 섹션의 암호화 키에 대해 파일 시스템의 유휴 데이터를 보호하는 AWS KMS(Key Management Service) 암호화 키를 선택합니다. 파일 시스템 관리 암호에 fsxadmin 사용자의 보안 암호를 입력합니다.



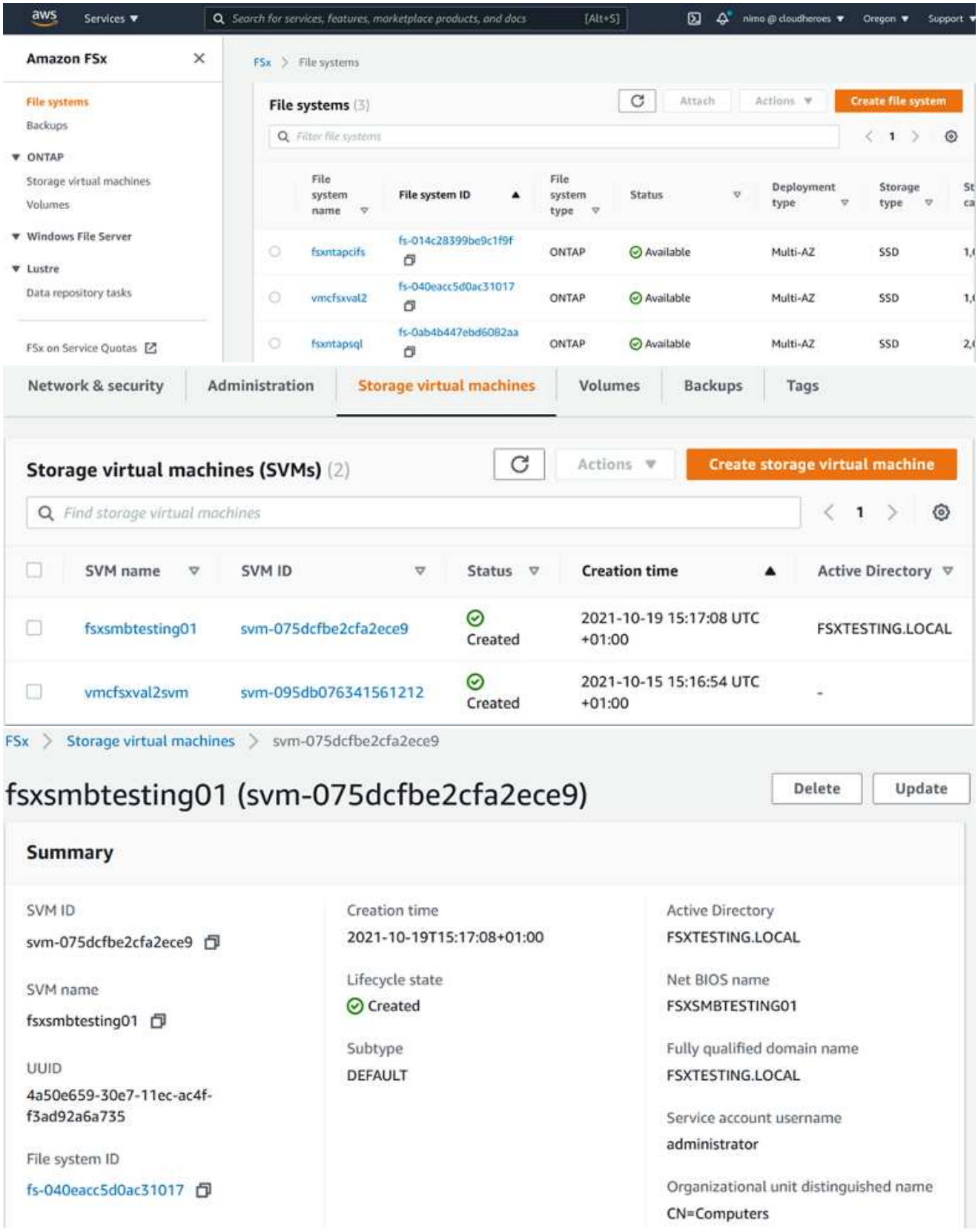
1. 가상 시스템에서 REST API 또는 CLI를 사용하여 ONTAP를 관리하는 데 vsadmin과 함께 사용할 암호를 지정합니다. 암호를 지정하지 않으면 fsxadmin 사용자를 SVM 관리에 사용할 수 있습니다. Active Directory 섹션에서 Active Directory를 SVM에 가입하여 SMB 공유를 프로비저닝해야 합니다. 기본 스토리지 가상 머신 구성 섹션에서 이 검증에 사용할 스토리지의 이름을 제공합니다. SMB 공유는 자체 관리되는 Active Directory 도메인을 사용하여 프로비저닝됩니다.



1. 기본 볼륨 구성 섹션에서 볼륨 이름 및 크기를 지정합니다. NFS 볼륨입니다. 스토리지 효율성의 경우 사용 을 선택하여 ONTAP 스토리지 효율성 기능(압축, 중복제거, 컴팩션)을 사용하도록 설정하거나 해제 를 선택하여 해제합니다.



1. 파일 시스템 생성 페이지에 표시된 파일 시스템 구성을 검토합니다.
2. 파일 시스템 생성 을 클릭합니다.

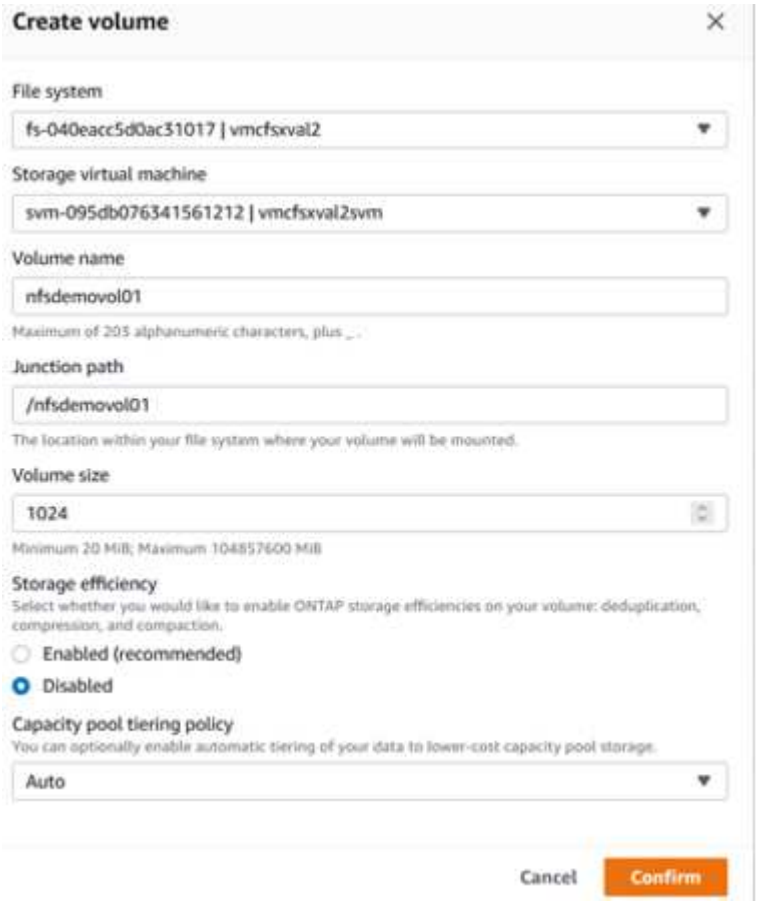


자세한 내용은 을 참조하십시오 "NetApp ONTAP용 Amazon FSx 시작하기".

위와 같이 파일 시스템을 생성한 후 필요한 크기와 프로토콜을 사용하여 볼륨을 생성합니다.

1. 를 엽니다 "Amazon FSx 콘솔".
2. 왼쪽 탐색 창에서 파일 시스템 을 선택한 다음 볼륨을 생성할 ONTAP 파일 시스템을 선택합니다.
3. Volumes 탭을 선택합니다.
4. Create Volume 탭을 선택합니다.
5. 볼륨 생성 대화 상자가 나타납니다.

이 섹션에서는 데모용으로 NFS 볼륨을 생성하여 AWS의 VMware 클라우드에서 실행되는 VM에 손쉽게 마운트할 수 있습니다. nfsdemovol01은 아래 그림과 같이 생성됩니다.



이전 단계에서 생성한 FSx ONTAP 볼륨을 마운트합니다. AWS SDDC의 VMC 내에 있는 Linux VM에서 다음 단계를 완료합니다.

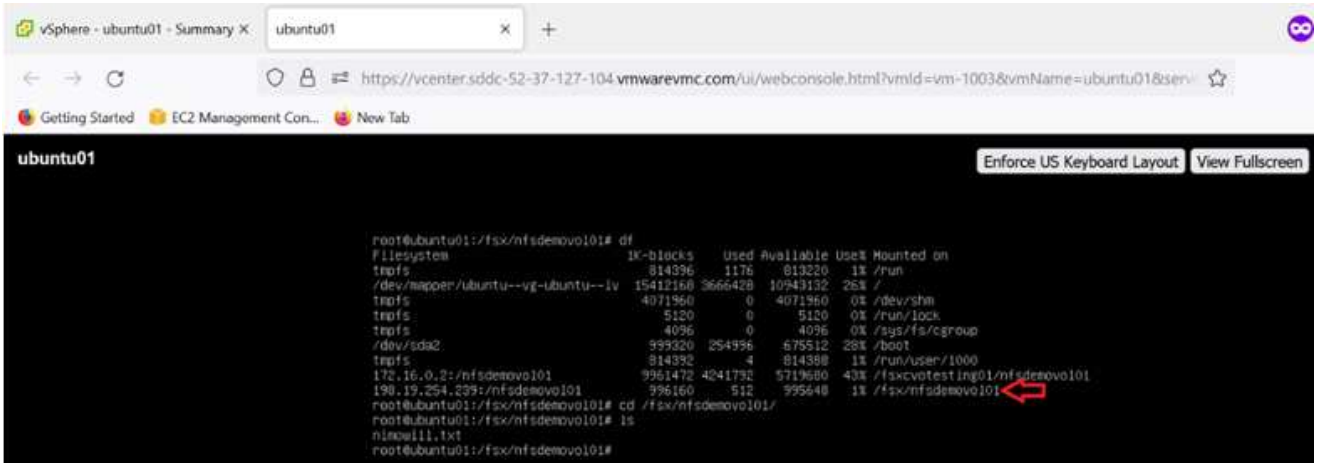
1. 지정된 Linux 인스턴스에 연결합니다.
2. SSH(Secure Shell)를 사용하여 인스턴스의 터미널을 열고 적절한 자격 증명을 사용하여 로그인합니다.
3. 다음 명령을 사용하여 볼륨의 마운트 지점에 대한 디렉토리를 만듭니다.

```
 $ sudo mkdir /fsx/nfsdemovol01
. NetApp ONTAP NFS 볼륨용 Amazon FSx를 이전 단계에서 생성한 디렉토리에 마운트합니다.
```

```
sudo mount -t nfs nfsvers=4.1,198.19.254.239:/nfsdemovol01 /fsx/nfsdemovol01
```

```
root@ubuntu01:/fsx/nfsdemovol01# mount -t nfs 198.19.254.239:/nfsdemovol01 /fsx/nfsdemovol01
```

1. 실행된 후 df 명령을 실행하여 마운트를 확인합니다.

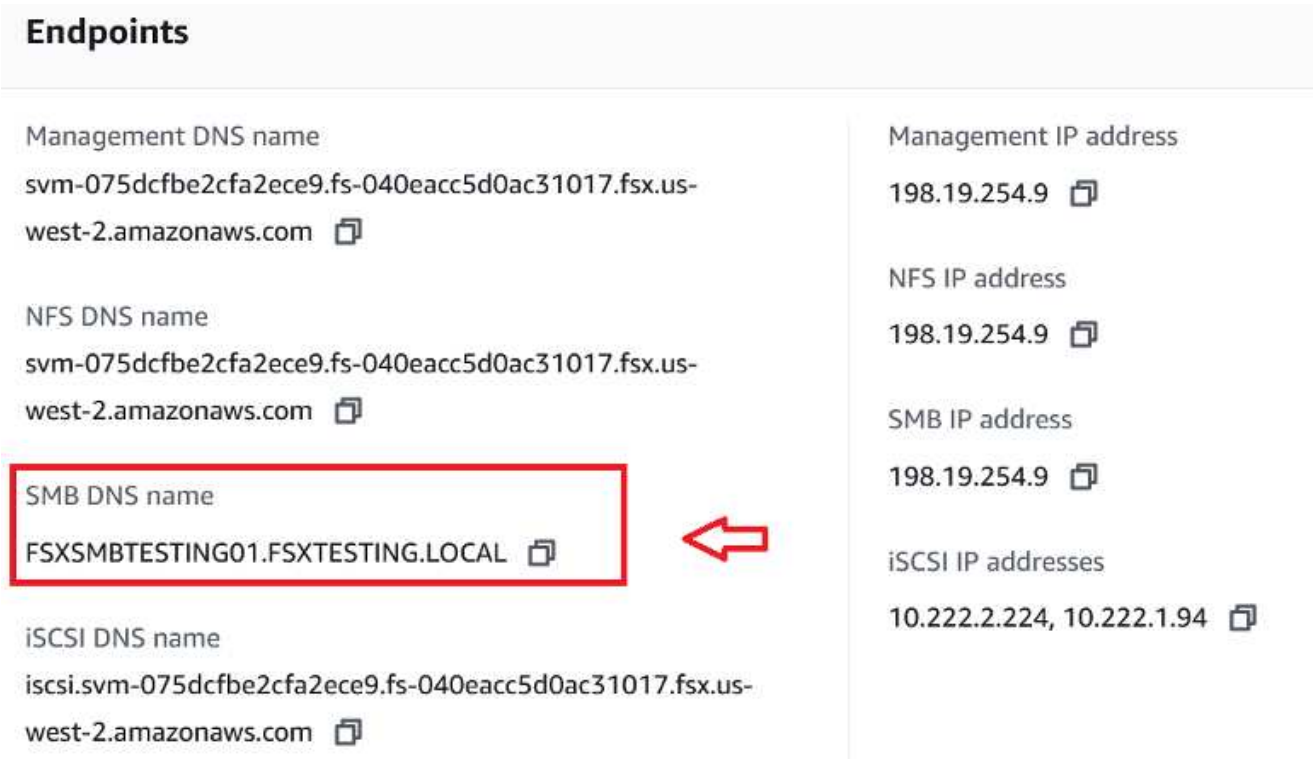


Linux 클라이언트에 FSx ONTAP 볼륨을 마운트합니다

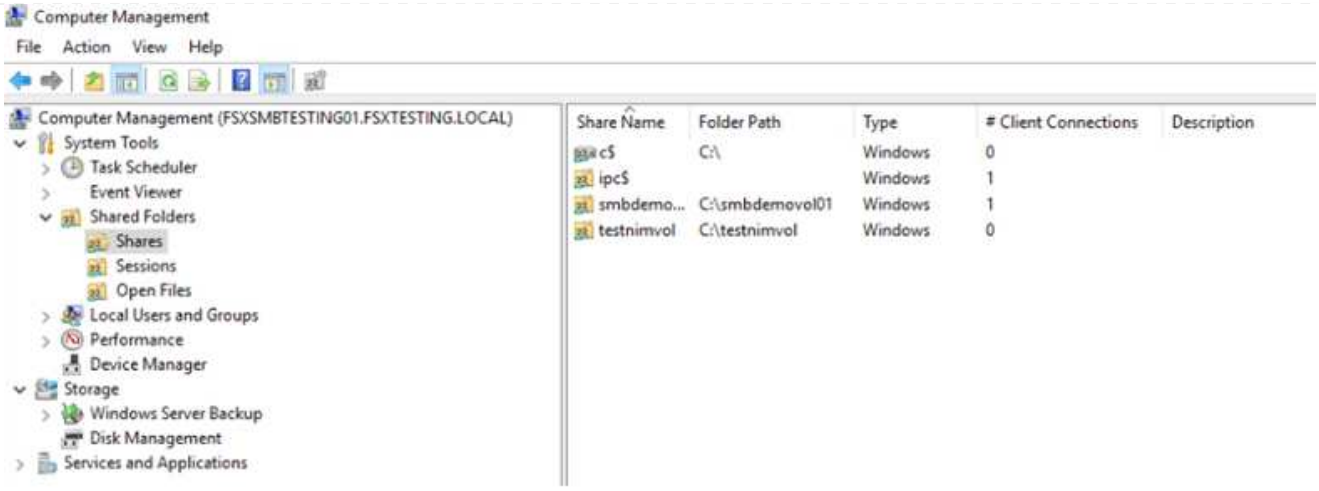
Amazon FSx 파일 시스템에서 파일 공유를 관리 및 매핑하려면 공유 폴더 GUI를 사용해야 합니다.

1. 시작 메뉴를 열고 관리자 권한으로 실행 을 사용하여 fsmgmt.msc 를 실행합니다. 이렇게 하면 공유 폴더 GUI 도구가 열립니다.
2. 작업 > 모든 작업 을 클릭하고 다른 컴퓨터에 연결 을 선택합니다.
3. 다른 컴퓨터의 경우 SVM(스토리지 가상 머신)의 DNS 이름을 입력합니다. 예를 들어, FSXSMBTESTING01.FSXTESTING.LOCAL이 이 예제에서 사용됩니다.

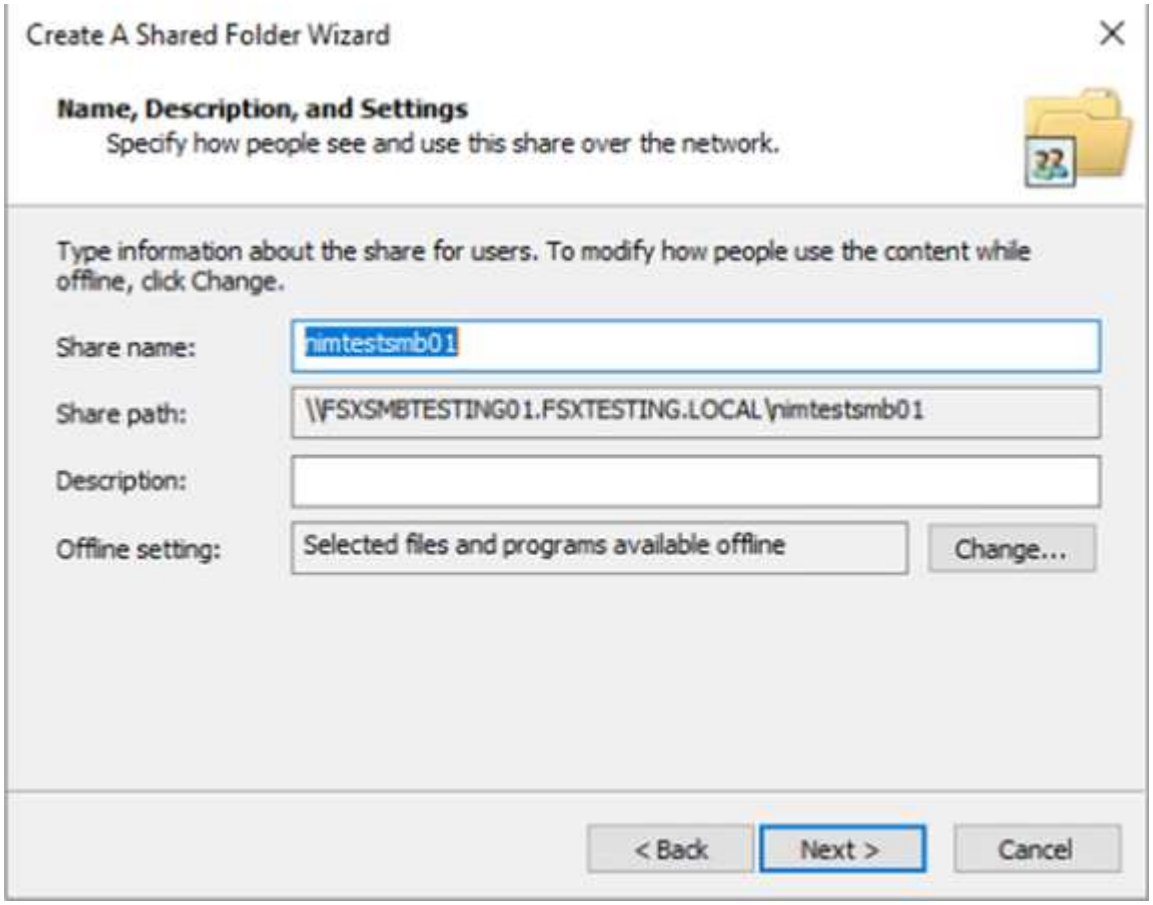
TP는 Amazon FSx 콘솔에서 SVM의 DNS 이름을 찾아 Storage Virtual Machines를 선택하고 SVM을 선택한 다음 Endpoints로 스크롤하여 SMB DNS 이름을 찾습니다. 확인 을 클릭합니다. 공유 폴더 목록에 Amazon FSx 파일 시스템이 나타납니다.



1. 공유 폴더 도구의 왼쪽 창에서 공유 를 선택하여 Amazon FSx 파일 시스템에 대한 활성 공유를 표시합니다.

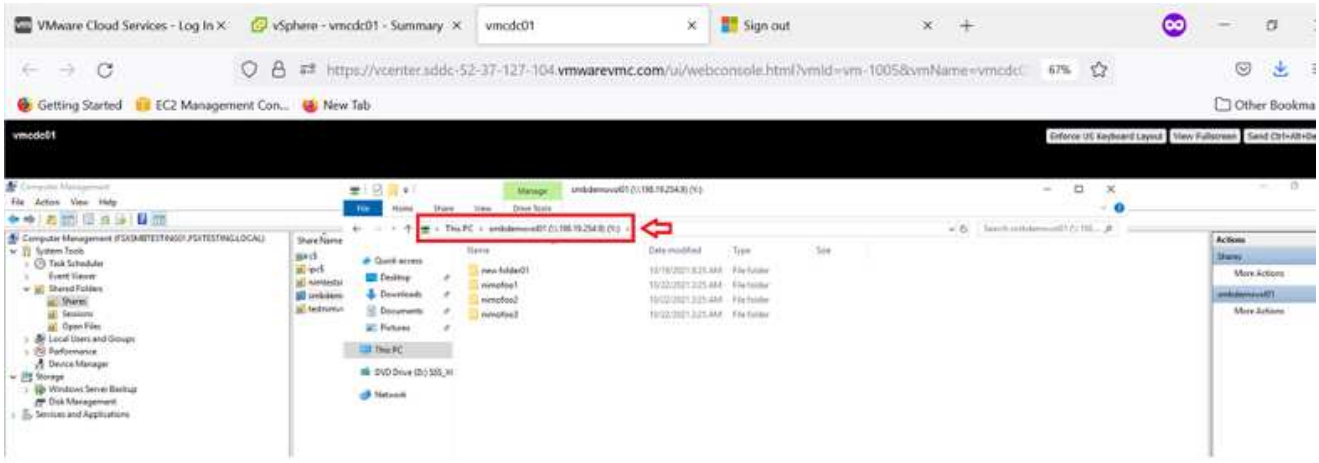


1. 이제 새 공유를 선택하고 공유 폴더 생성 마법사를 완료합니다.



Amazon FSx 파일 시스템에서 SMB 공유를 생성 및 관리하는 방법에 대한 자세한 내용은 를 참조하십시오 "SMB 공유 생성".

1. 접속이 완료되면 SMB 공유를 연결하고 애플리케이션 데이터에 사용할 수 있습니다. 이 작업을 수행하려면 공유 경로를 복사하고 네트워크 드라이브 매핑 옵션을 사용하여 AWS SDDC의 VMware Cloud에서 실행되는 VM에 볼륨을 마운트합니다.



NetApp ONTAP LUN용 FSx를 iSCSI를 사용하여 호스트에 연결합니다

FSx의 iSCSI 트래픽은 이전 섹션에 제공된 경로를 통해 VMware Transit Connect/AWS Transit Gateway를 통과합니다. NetApp ONTAP용 Amazon FSx에서 LUN을 구성하려면 찾은 문서를 따르십시오 "여기".

Linux 클라이언트에서 iSCSI 데몬이 실행되고 있는지 확인합니다. LUN을 프로비저닝한 후 Ubuntu를 사용한 iSCSI 구성에 대한 자세한 지침을 참조하십시오(예:). "여기".

이 문서에서는 iSCSI LUN을 Windows 호스트에 연결하는 방법을 설명합니다.

NetApp ONTAP용 FSx에서 LUN 프로비저닝:

1. ONTAP 파일 시스템용 FSx의 관리 포트를 사용하여 NetApp ONTAP CLI에 액세스합니다.
2. 사이징 출력에 표시된 대로 필요한 크기의 LUN을 생성합니다.

```
FsxId040eacc5d0ac31017::> lun create -vserver vmcfsxval2svm -volume
nimfsxscsivol -lun nimofsxlun01 -size 5gb -ostype windows -space
-reserve enabled
```

이 예에서는 5G 크기의 LUN(5368709120)을 생성했습니다.

1. 특정 LUN에 액세스할 수 있는 호스트를 제어하는 데 필요한 igroup을 생성합니다.

```
FsxId040eacc5d0ac31017::> igroup create -vserver vmcfsxval2svm -igroup
winIG -protocol iscsi -ostype windows -initiator iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local

FsxId040eacc5d0ac31017::> igroup show

Vserver   Igroup       Protocol OS Type  Initiators

--------- ------------ -------- --------
-------------------------------------

vmcfsxval2svm

          ubuntu01     iscsi    linux    iqn.2021-
10.com.ubuntu:01:initiator01

vmcfsxval2svm

          winIG        iscsi    windows  iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local
```

두 개의 항목이 표시되었습니다.

1. 다음 명령을 사용하여 LUN을 igroup에 매핑합니다.

```
FsxId040eacc5d0ac31017::> lun map -vserver vmcfsxval2svm -path
/vol/nimfsxscsivol/nimofsxlun01 -igroup winIG

FsxId040eacc5d0ac31017::> lun show

Vserver   Path                            State   Mapped   Type
Size

--------- ------------------------------- ------- -------- --------
--------

vmcfsxval2svm

          /vol/blocktest01/lun01          online  mapped   linux
5GB

vmcfsxval2svm

          /vol/nimfsxscsivol/nimofsxlun01 online  mapped   windows
5GB
```

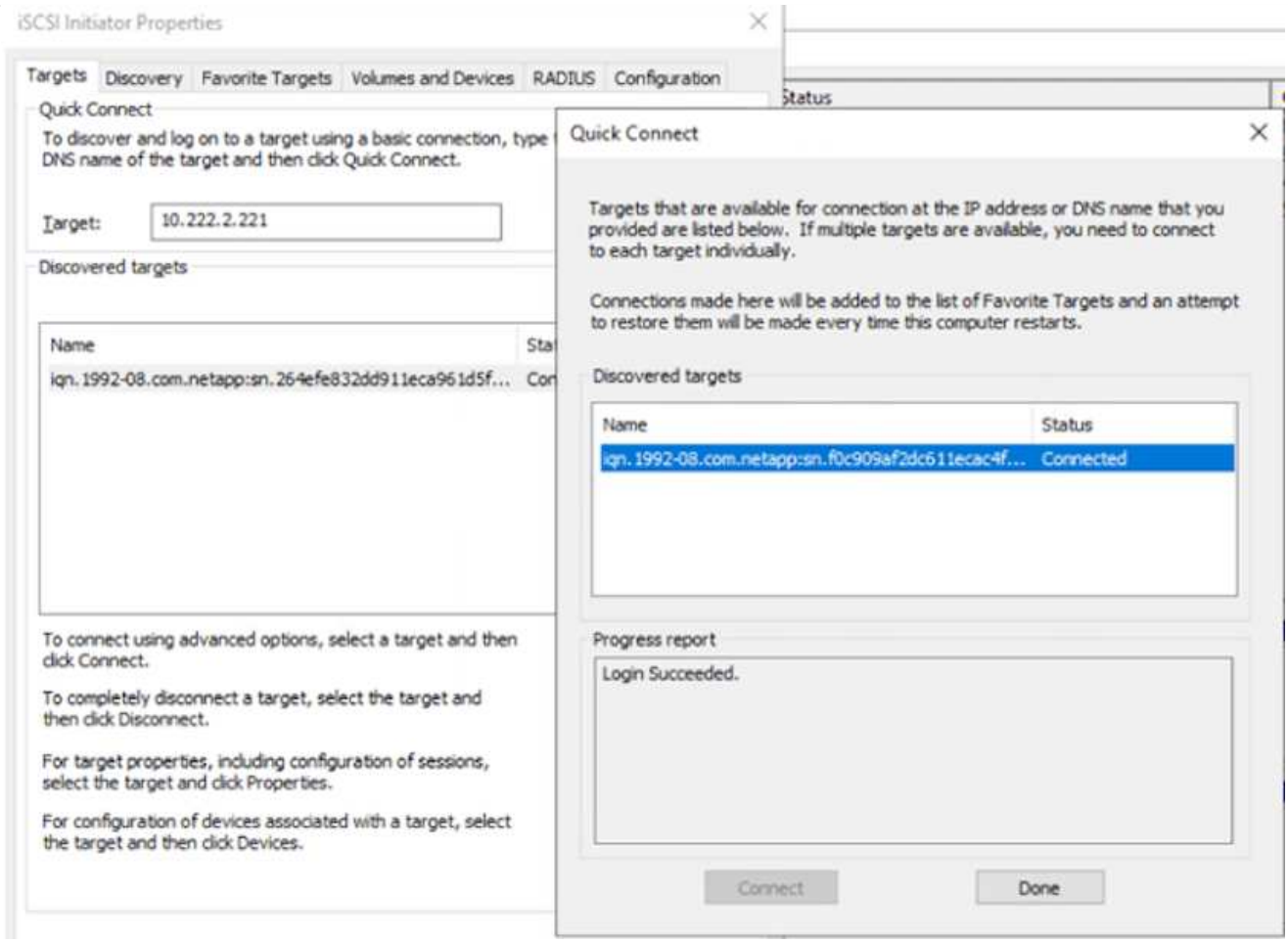
두 개의 항목이 표시되었습니다.

1. 새로 프로비저닝된 LUN을 Windows VM에 연결합니다.

새 LUN을 AWS SDDC의 VMware 클라우드에 있는 Windows 호스트에 연결하려면 다음 단계를 수행하십시오.

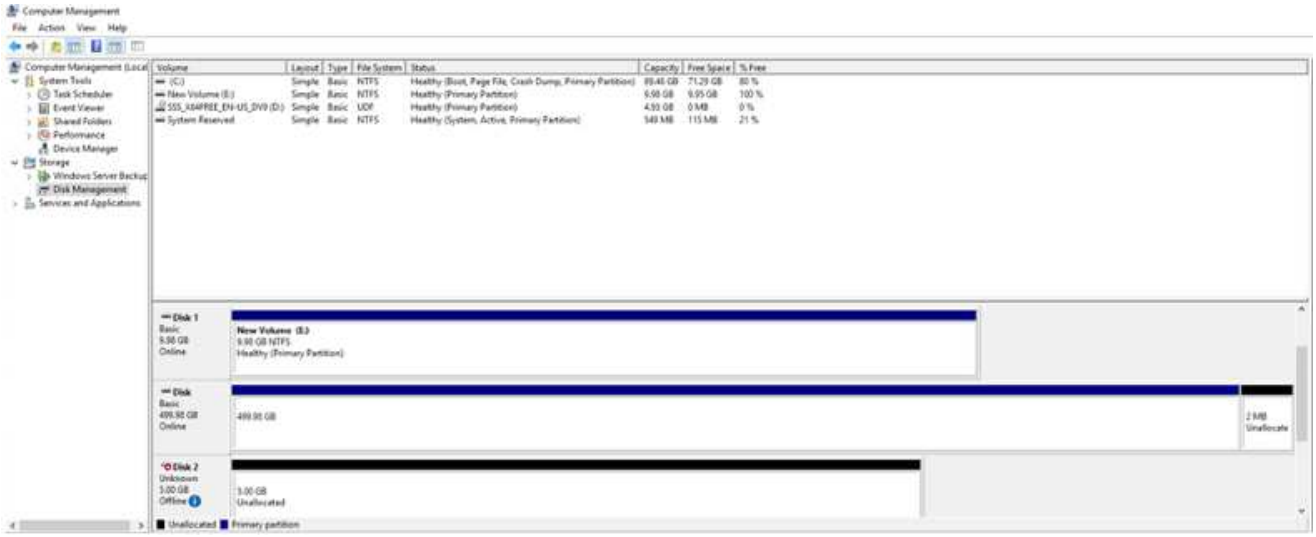
1. AWS SDDC 기반 VMware 클라우드에서 호스팅되는 Windows VM에 대한 RDP
2. Server Manager > Dashboard > Tools > iSCSI Initiator로 이동하여 iSCSI Initiator Properties 대화 상자를 엽니다.
3. 검색 탭에서 포털 검색 또는 포털 추가 를 클릭한 다음 iSCSI 대상 포트의 IP 주소를 입력합니다.
4. 대상 탭에서 검색된 대상을 선택한 다음 로그온 또는 연결을 클릭합니다.
5. 다중 경로 사용을 선택한 다음 “컴퓨터를 시작할 때 이 연결 자동 복원” 또는 “즐겨찾는 대상 목록에 이 연결 추가”를 선택합니다. 고급 을 클릭합니다.

Windows 호스트에는 클러스터의 각 노드에 대한 iSCSI 연결이 있어야 합니다. 기본 DSM은 가장 적합한 경로를 선택합니다.



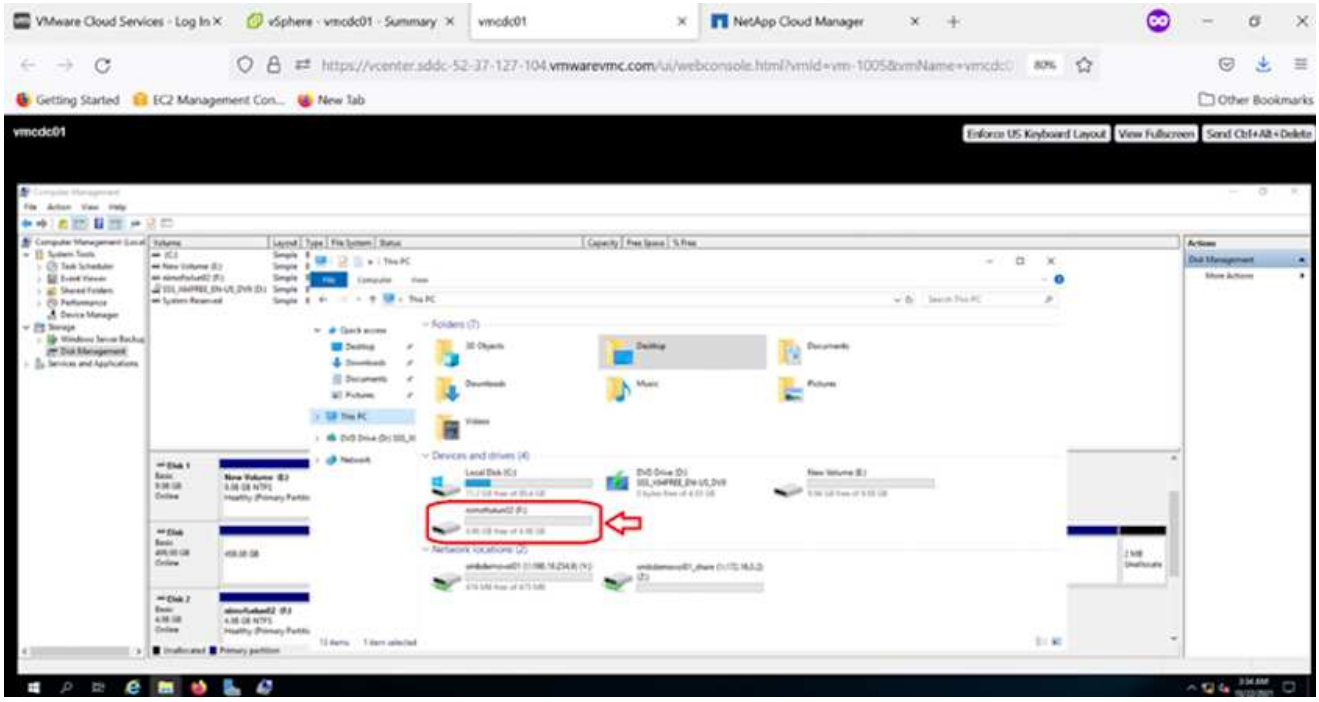
SVM(스토리지 가상 머신)의 LUN은 Windows 호스트에 디스크로 표시됩니다. 추가된 새 디스크는 호스트에서 자동으로 검색되지 않습니다. 수동 재검색을 트리거하여 다음 단계를 수행하여 디스크를 검색합니다.

1. 시작 > 관리 도구 > 컴퓨터 관리를 차례로 클릭하여 Windows 컴퓨터 관리 유틸리티를 엽니다.
2. 탐색 트리에서 스토리지 노드를 확장합니다.
3. 디스크 관리를 클릭합니다.
4. 작업 > 디스크 다시 검사 를 클릭합니다.



Windows 호스트에서 새 LUN을 처음 액세스할 때 파티션이나 파일 시스템이 없습니다. LUN을 초기화하고 필요에 따라 다음 단계를 완료하여 파일 시스템으로 LUN을 포맷합니다.

1. Windows 디스크 관리를 시작합니다.
2. LUN을 마우스 오른쪽 버튼으로 클릭한 다음 필요한 디스크 또는 파티션 유형을 선택합니다.
3. 마법사의 지침을 따릅니다. 이 예에서는 드라이브 F:가 마운트되었습니다.



CVO(Cloud Volumes ONTAP)

Cloud Volumes ONTAP, 즉 CVO는 NetApp의 ONTAP 스토리지 소프트웨어를 기반으로 하는 업계 최고의 클라우드 데이터 관리 솔루션으로, AWS(Amazon Web Services), Microsoft Azure 및 GCP(Google Cloud Platform)에서 기본적으로 제공됩니다.

ONTAP의 소프트웨어 정의 버전이며 클라우드 네이티브 스토리지를 사용합니다. 따라서 클라우드와 사내에서 동일한 스토리지 소프트웨어를 사용할 수 있으므로 데이터를 관리하는 새로운 방법을 통해 IT 직원을 재교육할 필요가 없습니다.

CVO를 사용하면 데이터를 에지에서 데이터 센터, 클라우드로 원활하게 이동하고 다시 가져올 수 있습니다. 또한 단일 창 관리 콘솔인 NetApp Cloud Manager를 사용하여 하이브리드 클라우드를 통합할 수 있습니다.

설계상 CVO는 최고 성능과 고급 데이터 관리 기능을 제공하여 클라우드에서 가장 까다로운 애플리케이션도 충족합니다

CVO(Cloud Volumes ONTAP)를 게스트 연결 스토리지로 사용합니다

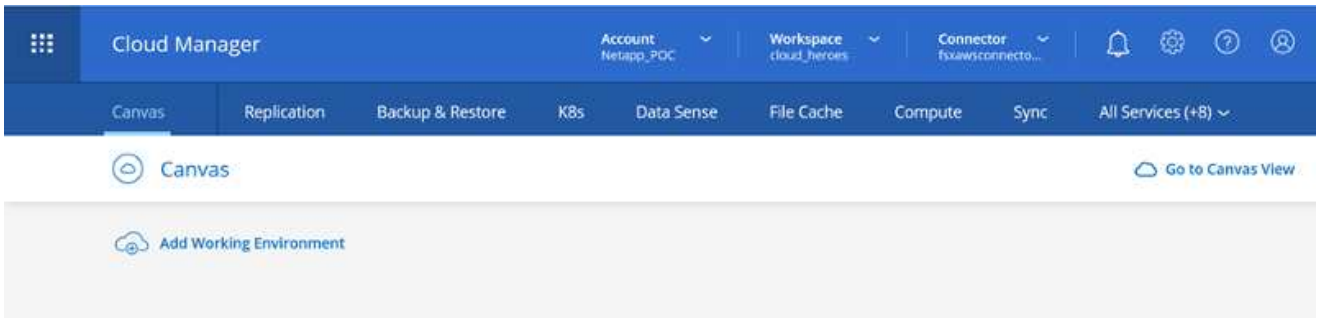
AWS에 새로운 **Cloud Volumes ONTAP** 인스턴스 구축(직접 구현)

Cloud Volumes ONTAP 공유 및 LUN은 AWS SDDC 환경의 VMware 클라우드에서 생성된 VM에서 마운트할 수 있습니다. 또한 볼륨은 네이티브 AWS VM Linux Windows 클라이언트에 마운트할 수 있으며, Cloud Volumes ONTAP는 iSCSI, SMB 및 NFS 프로토콜을 지원하므로 iSCSI를 통해 마운트할 때 Linux 또는 Windows 클라이언트에서 LUN에 블록 디바이스로 액세스할 수 있습니다. Cloud Volumes ONTAP 볼륨은 몇 가지 간단한 단계를 통해 설정할 수 있습니다.

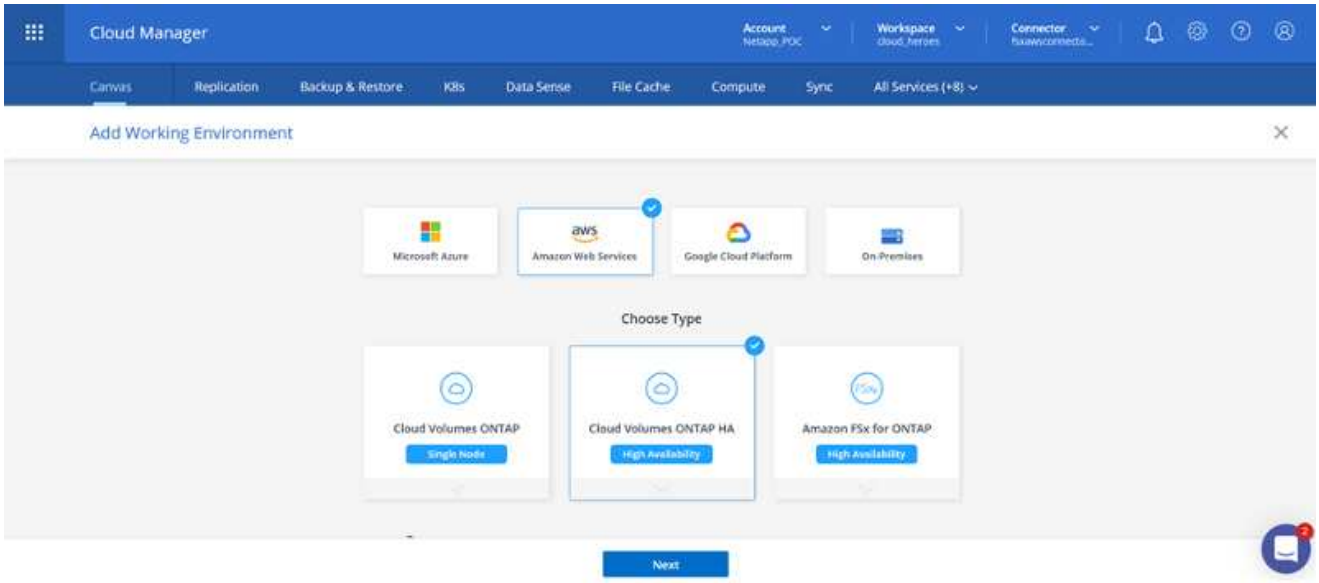
재해 복구 또는 마이그레이션을 위해 사내 환경에서 클라우드로 볼륨을 복제하려면 사이트 간 VPN 또는 DirectConnect를 사용하여 AWS에 대한 네트워크 연결을 설정합니다. 사내의 데이터를 Cloud Volumes ONTAP로 복제하는 작업은 이 문서의 범위를 벗어납니다. 사내 시스템과 Cloud Volumes ONTAP 시스템 간에 데이터를 복제하려면 을 참조하십시오 "시스템 간 데이터 복제 설정".

를 사용합니다 "Cloud Volumes ONTAP Sizer" Cloud Volumes ONTAP 인스턴스의 크기를 정확하게 지정합니다. 또한, Cloud Volumes ONTAP Sizer에서 입력으로 사용할 온프레미스 성능을 모니터링합니다.

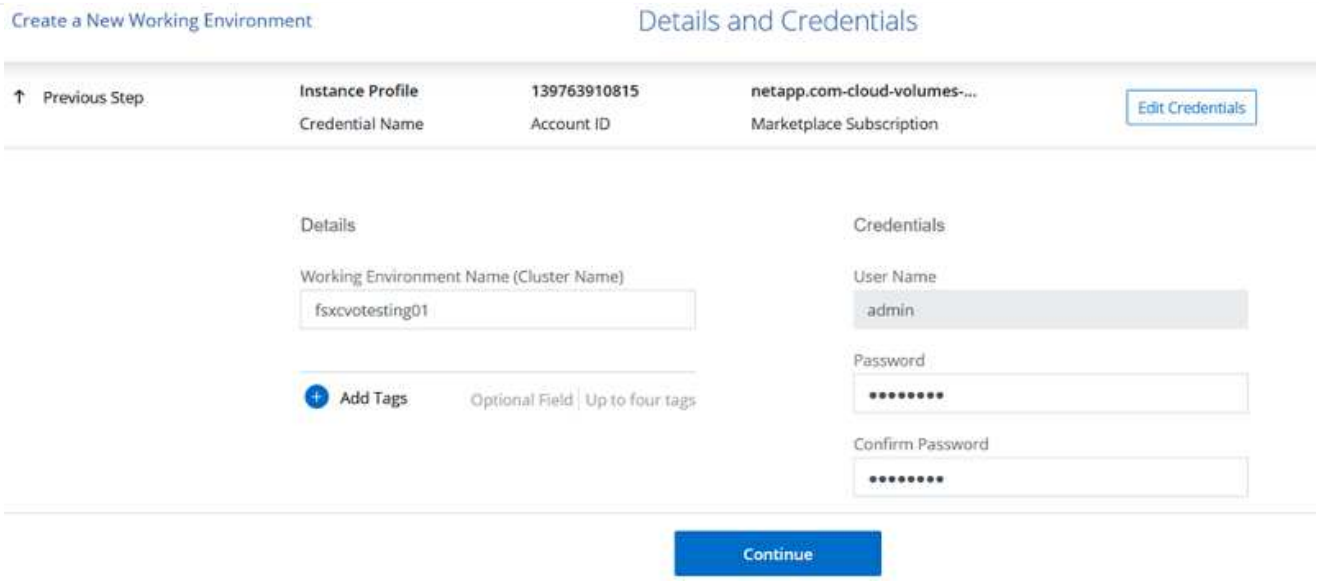
1. NetApp Cloud Central에 로그인하면 Fabric View 화면이 표시됩니다. Cloud Volumes ONTAP 탭을 찾아 Cloud Manager로 이동 을 선택합니다. 로그인하면 Canvas 화면이 표시됩니다.



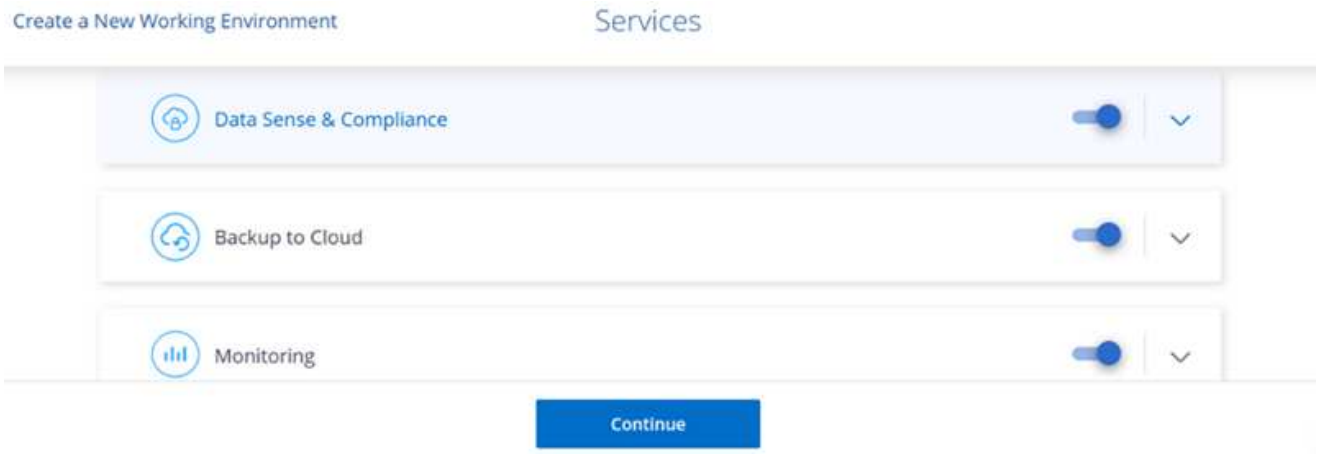
1. Cloud Manager 홈 페이지에서 작업 환경 추가를 클릭한 다음 AWS를 클라우드로 선택하고 시스템 구성의 유형을 선택합니다.



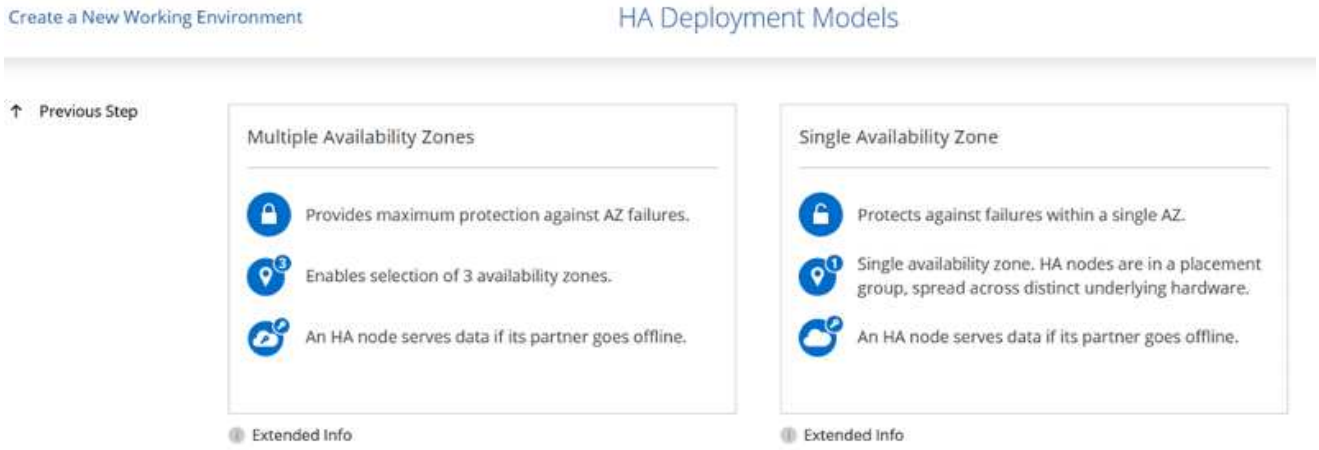
1. 환경 이름 및 관리자 자격 증명을 비롯하여 생성할 환경에 대한 세부 정보를 제공합니다. 계속 을 클릭합니다.



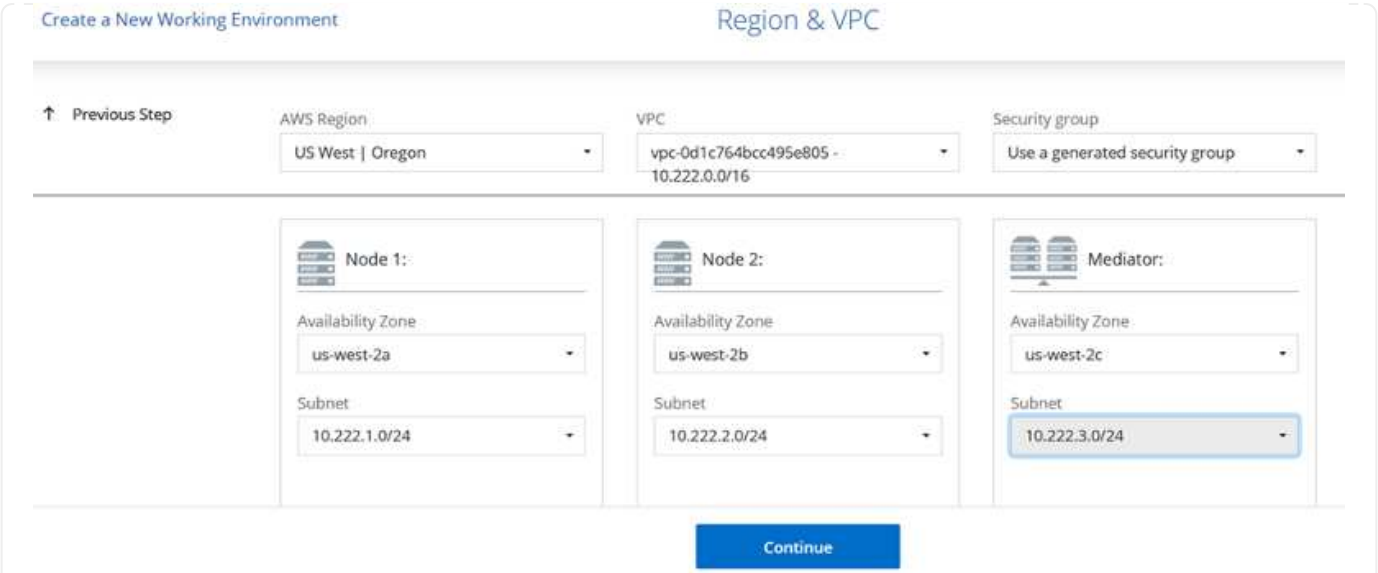
1. BlueXP 분류, BlueXP 백업 및 복구, Cloud Insights를 비롯하여 Cloud Volumes ONTAP 구축을 위한 애드온 서비스를 선택하십시오. 계속 을 클릭합니다.



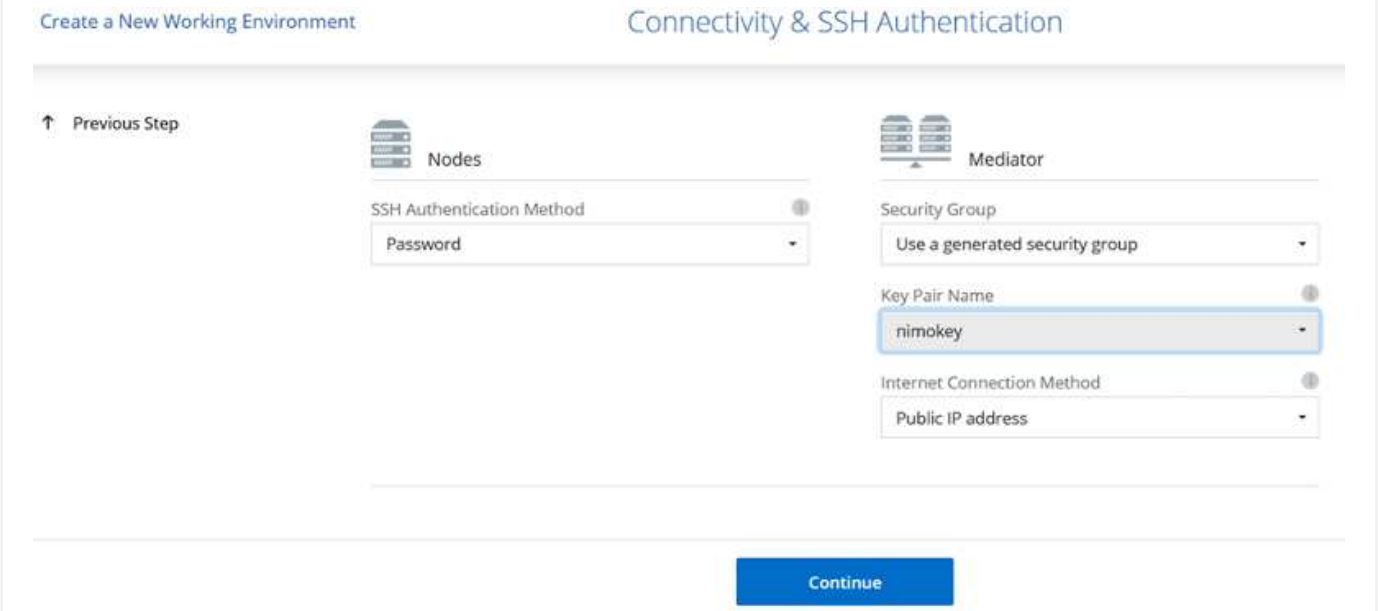
1. HA 배포 모델 페이지에서 여러 가용성 영역 구성을 선택합니다.



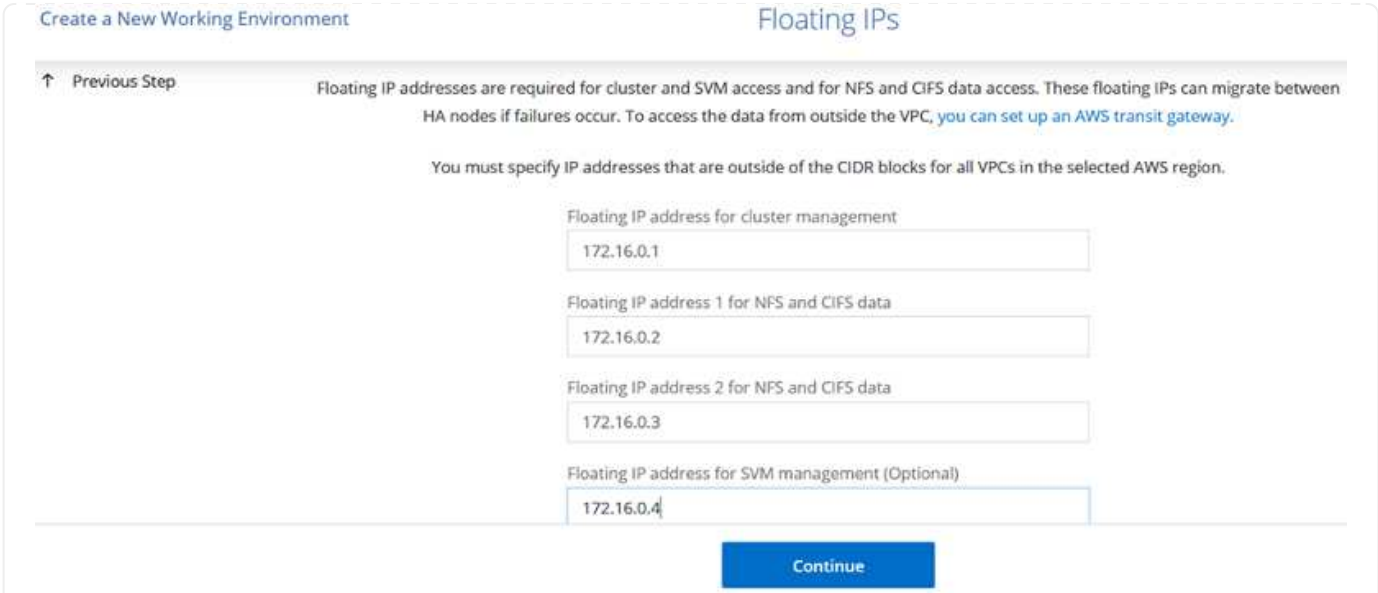
1. 지역 및 VPC 페이지에서 네트워크 정보를 입력한 다음 계속 을 클릭합니다.



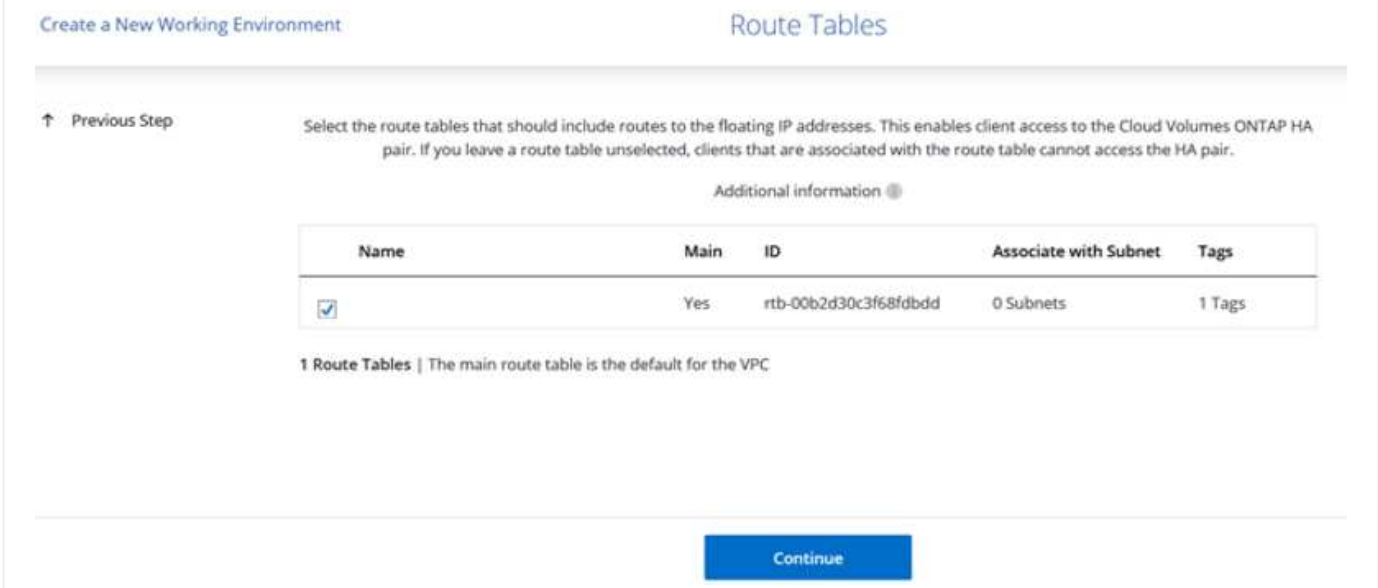
1. 연결 및 SSH 인증 페이지에서 HA 쌍의 연결 방법과 중재자를 선택합니다.



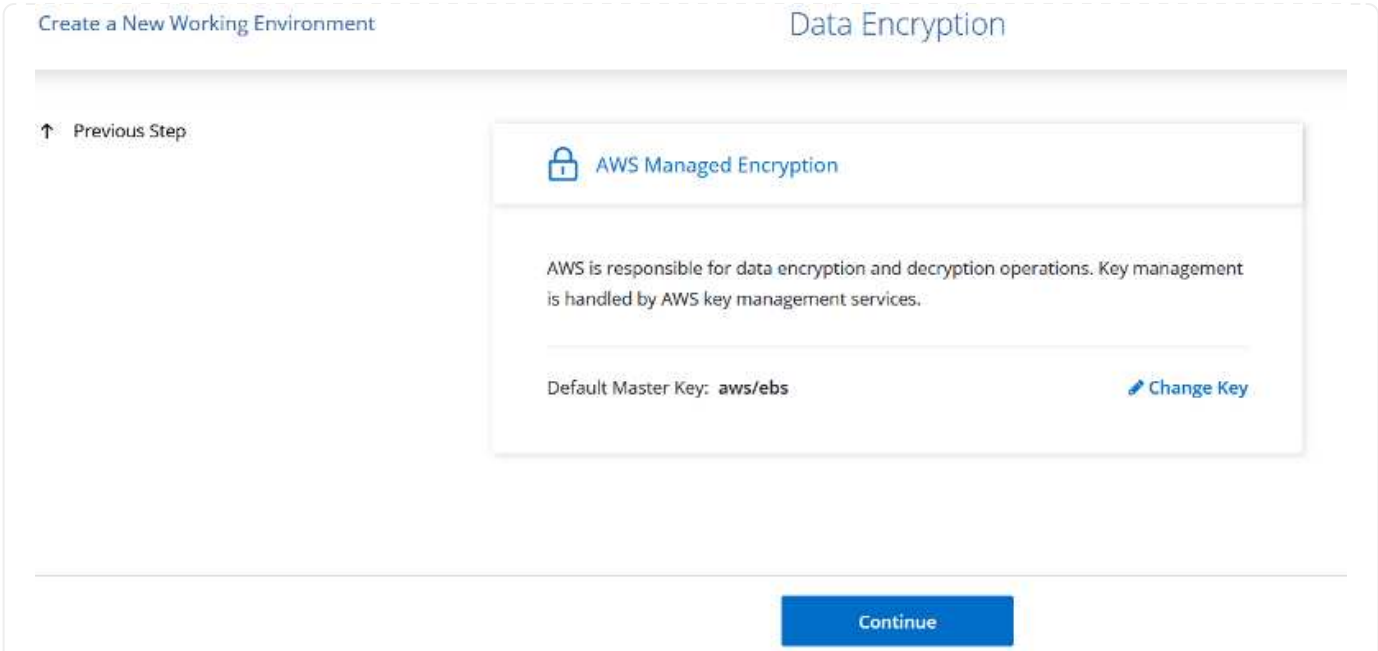
1. 부동 IP 주소를 지정하고 계속 을 클릭합니다.



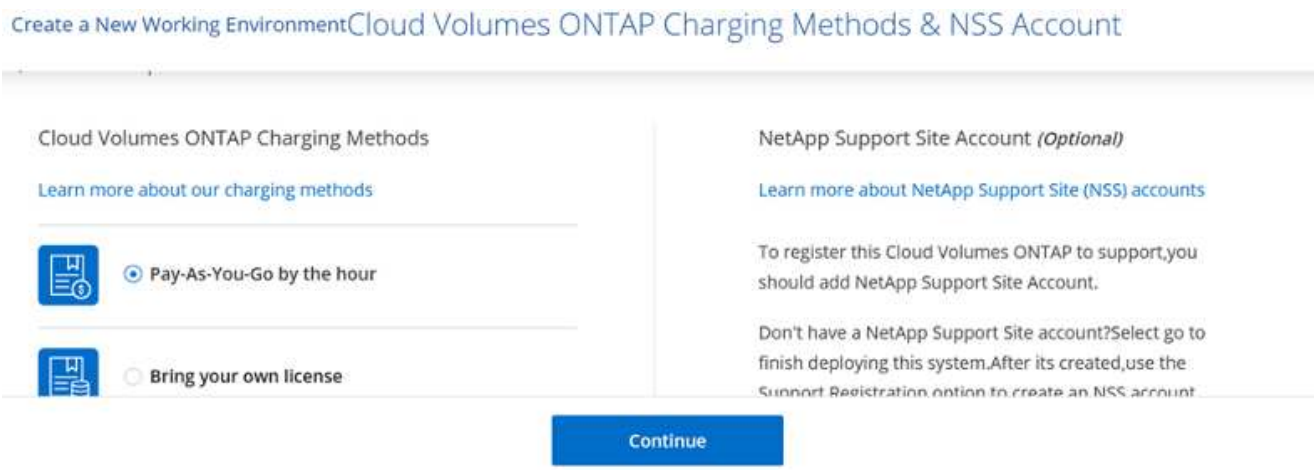
1. 부동 IP 주소에 대한 라우트를 포함할 적절한 라우트 테이블을 선택한 다음 계속 을 클릭합니다.



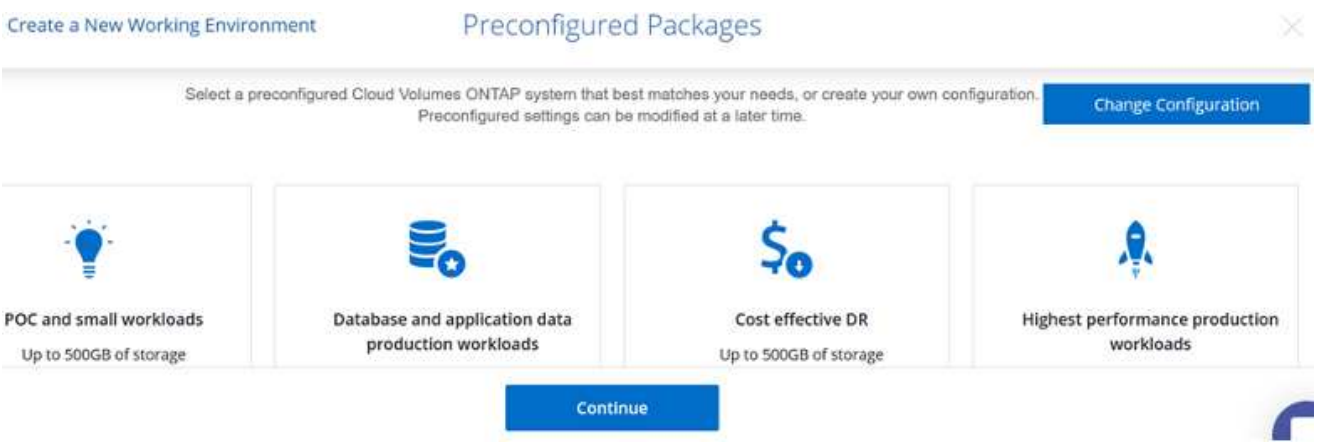
1. 데이터 암호화 페이지에서 AWS 관리 암호화 를 선택합니다.



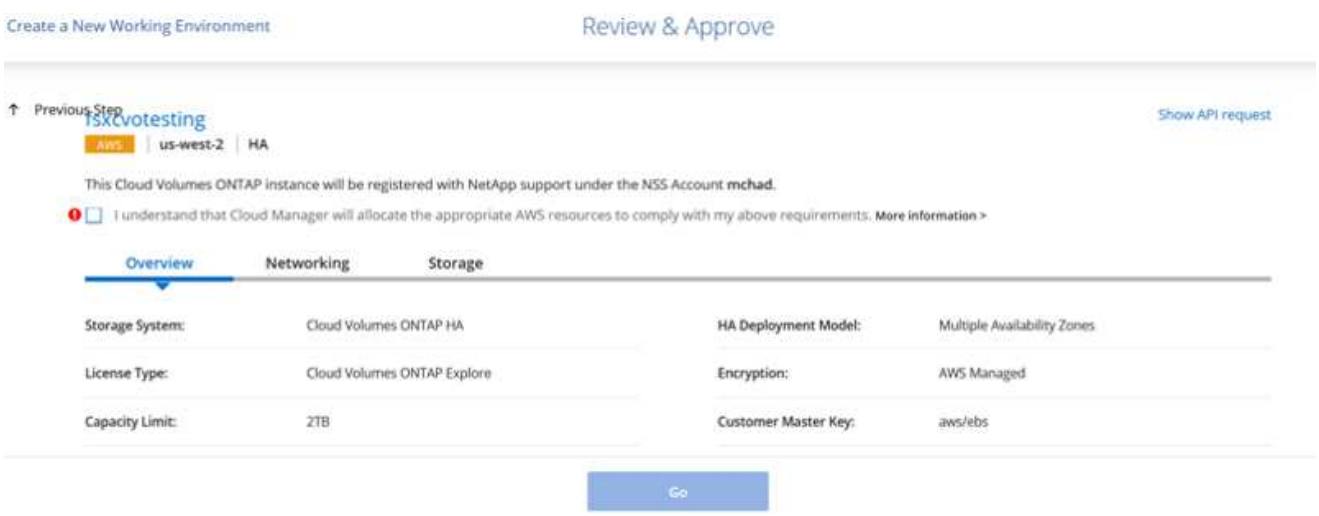
1. 라이센스 옵션 선택: 사용한 만큼만 지불 또는 BYOL 방식으로 기존 라이센스 사용 이 예에서는 pay-as-you-go 옵션을 사용합니다.



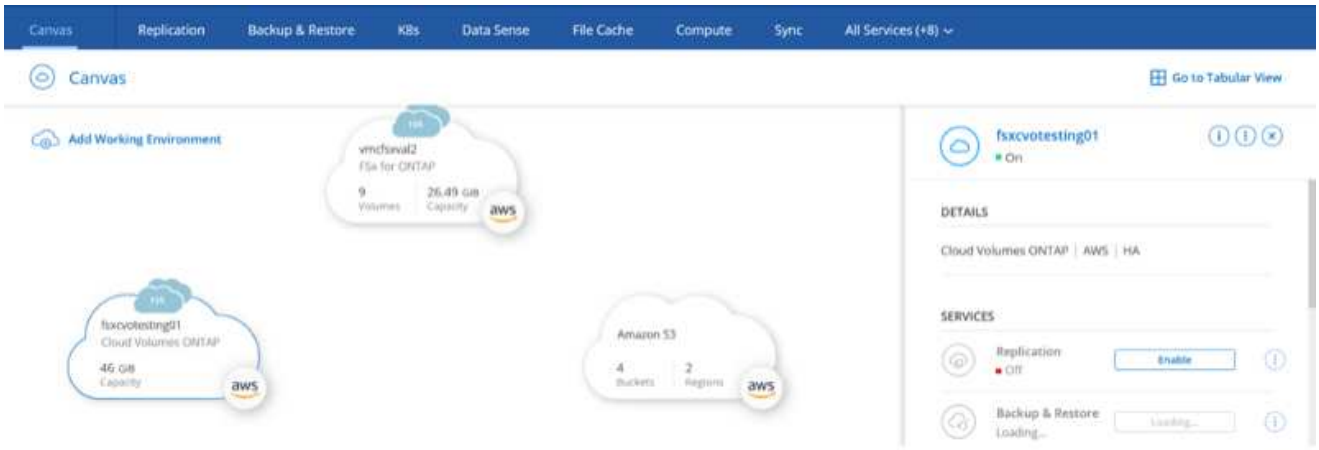
1. AWS SDDC 기반 VMware 클라우드에서 실행되는 VM에 구축할 워크로드 유형을 기반으로 사용할 수 있는 사전 구성된 패키지 몇 개 중 하나를 선택합니다.



1. 검토 및 승인 페이지에서 선택 항목을 검토하고 확인합니다. Cloud Volumes ONTAP 인스턴스를 만들려면 이동을 클릭합니다.

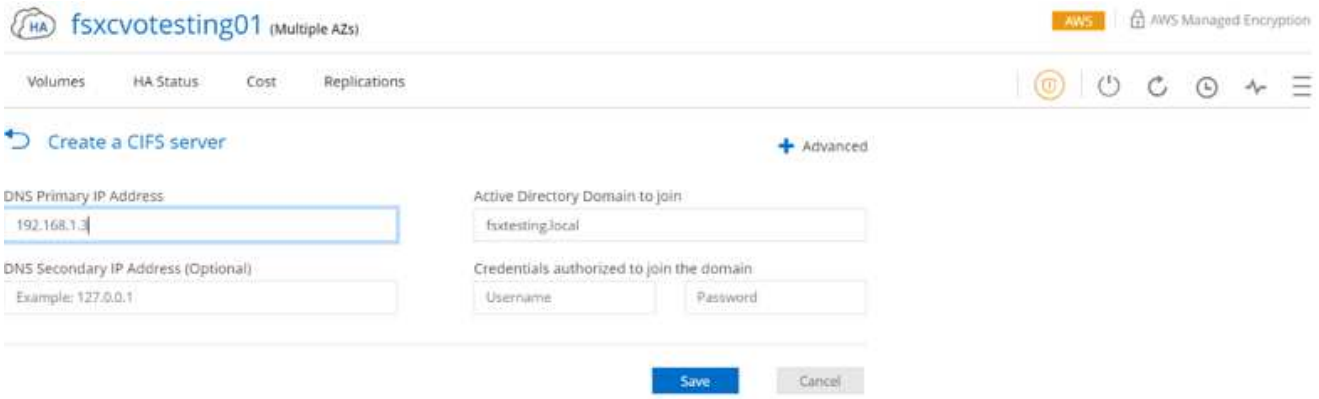


1. Cloud Volumes ONTAP를 프로비저닝하면 Canvas 페이지의 작업 환경에 나열됩니다.

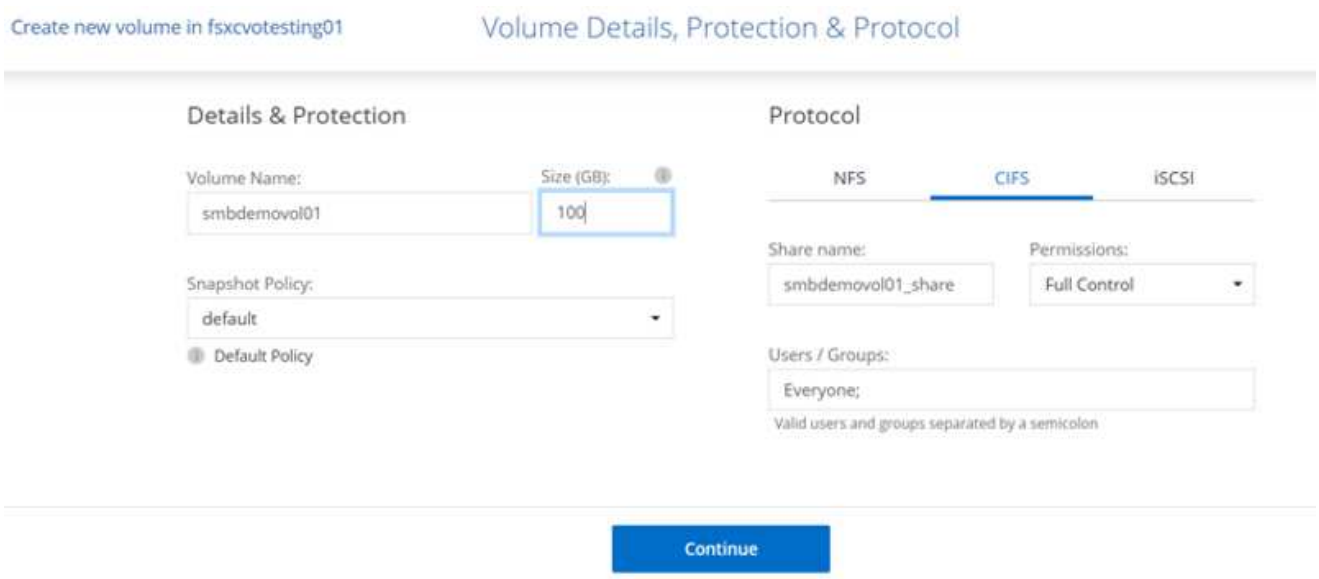


SMB 볼륨을 위한 추가 구성

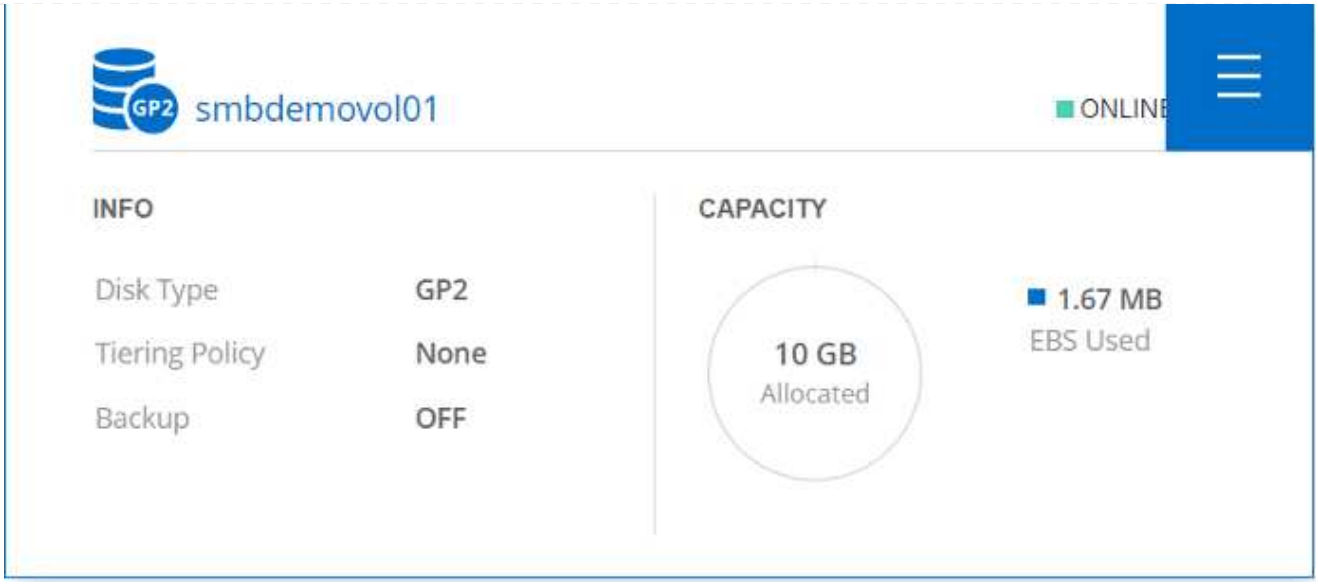
1. 작업 환경이 준비되면 CIFS 서버가 적절한 DNS 및 Active Directory 구성 매개 변수로 구성되어 있는지 확인합니다. 이 단계는 SMB 볼륨을 생성하기 전에 필요합니다.



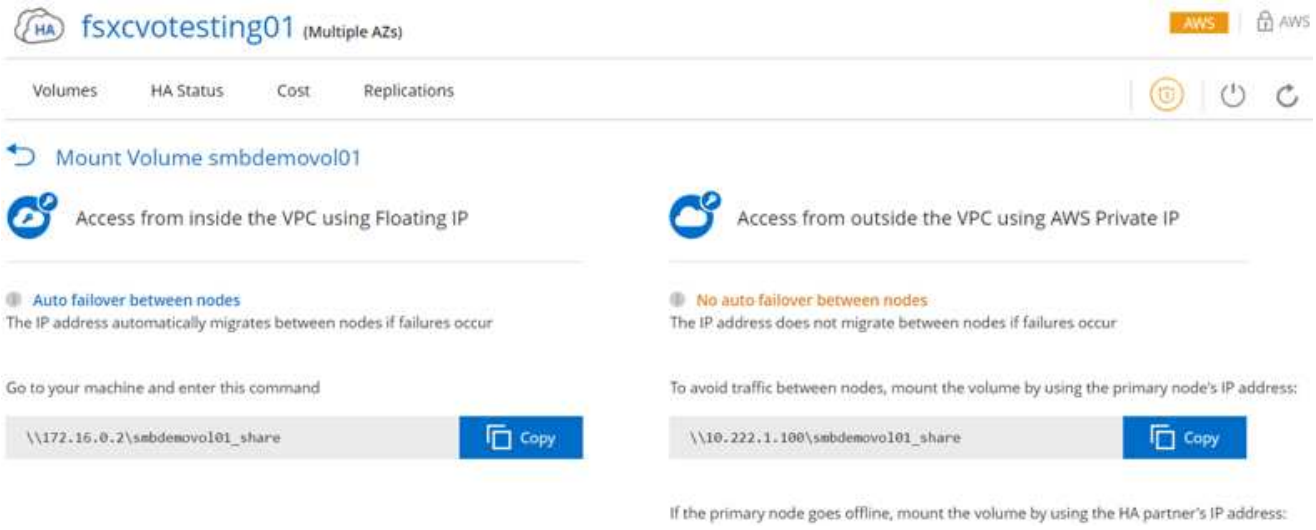
1. CVO 인스턴스를 선택하여 볼륨을 생성하고 Create Volume 옵션을 클릭합니다. 적절한 크기를 선택하고 클라우드 관리자가 포함하는 애그리게이트를 선택하거나, 고급 할당 메커니즘을 사용하여 특정 애그리게이트에 배치할 수 있습니다. 이 데모에서는 SMB가 프로토콜로 선택됩니다.

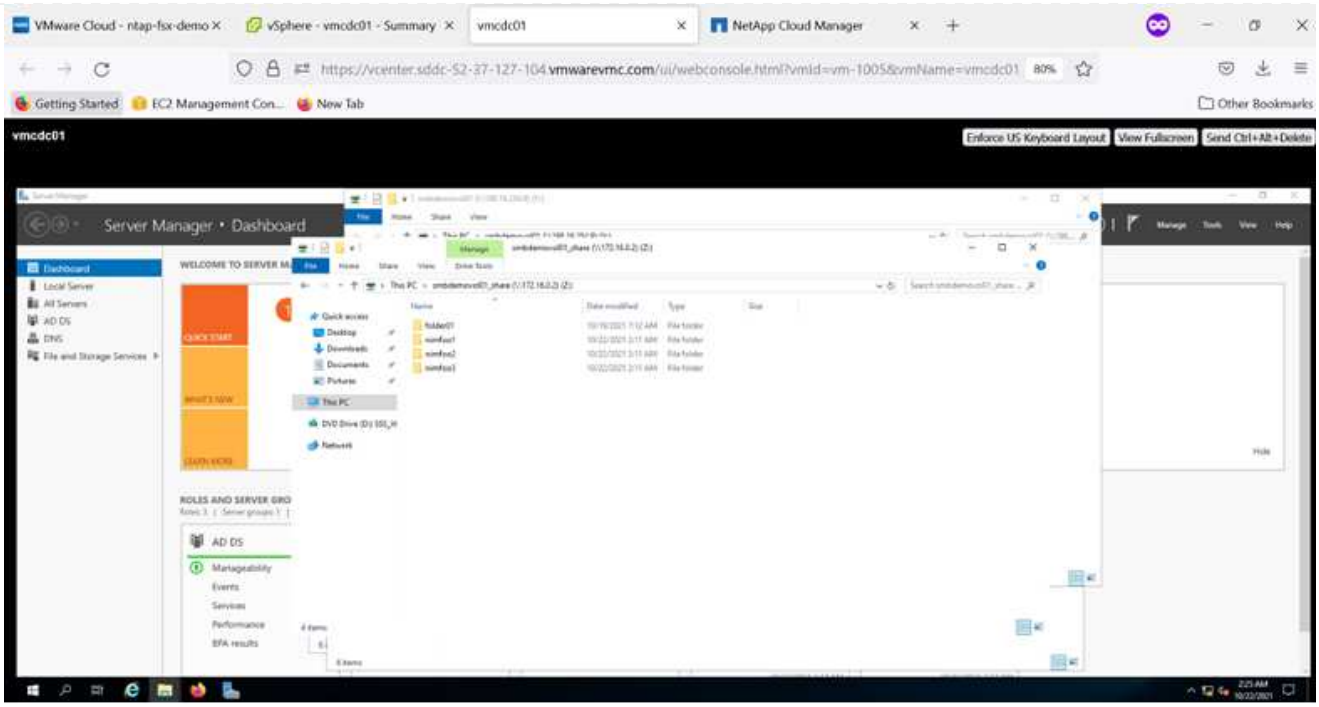


1. 볼륨 용량 할당 후 볼륨 창 아래에서 사용할 수 있습니다. CIFS 공유가 프로비저닝되므로 사용자나 그룹에 파일 및 폴더에 대한 권한을 제공하고 해당 사용자가 공유를 액세스하고 파일을 생성할 수 있는지 확인해야 합니다.



1. 볼륨을 생성한 후 mount 명령을 사용하여 AWS SDDC 호스트의 VMware Cloud에서 실행되는 VM에서 공유에 접속합니다.
2. 다음 경로를 복사하고 Map Network Drive 옵션을 사용하여 AWS SDDC의 VMware Cloud에서 실행되는 VM에 볼륨을 마운트합니다.

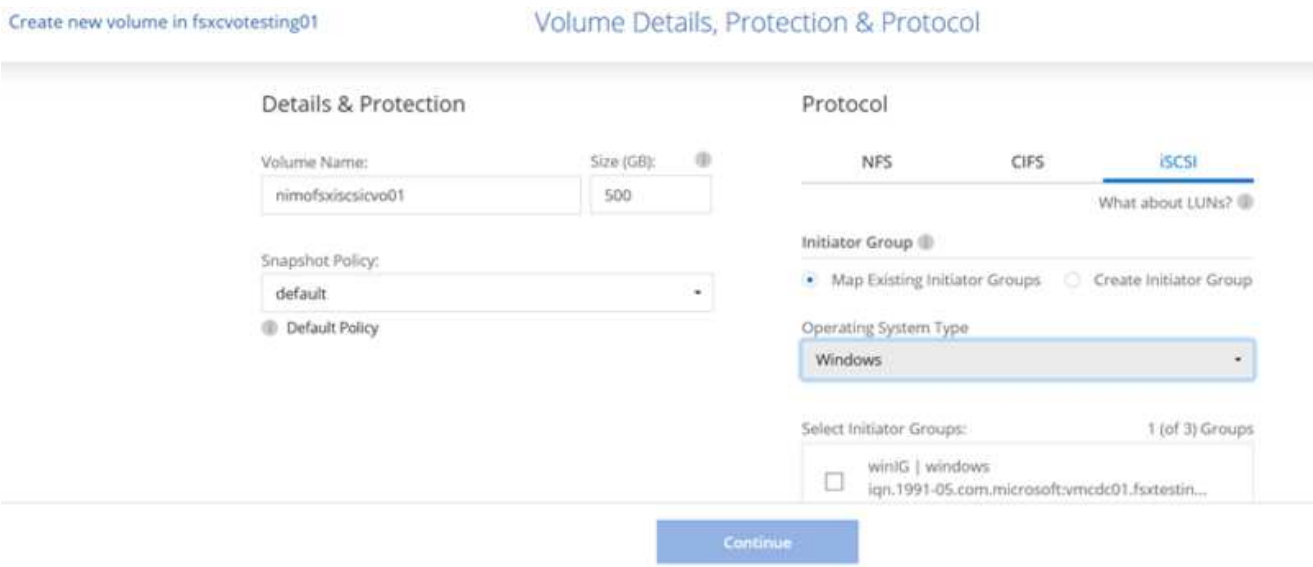


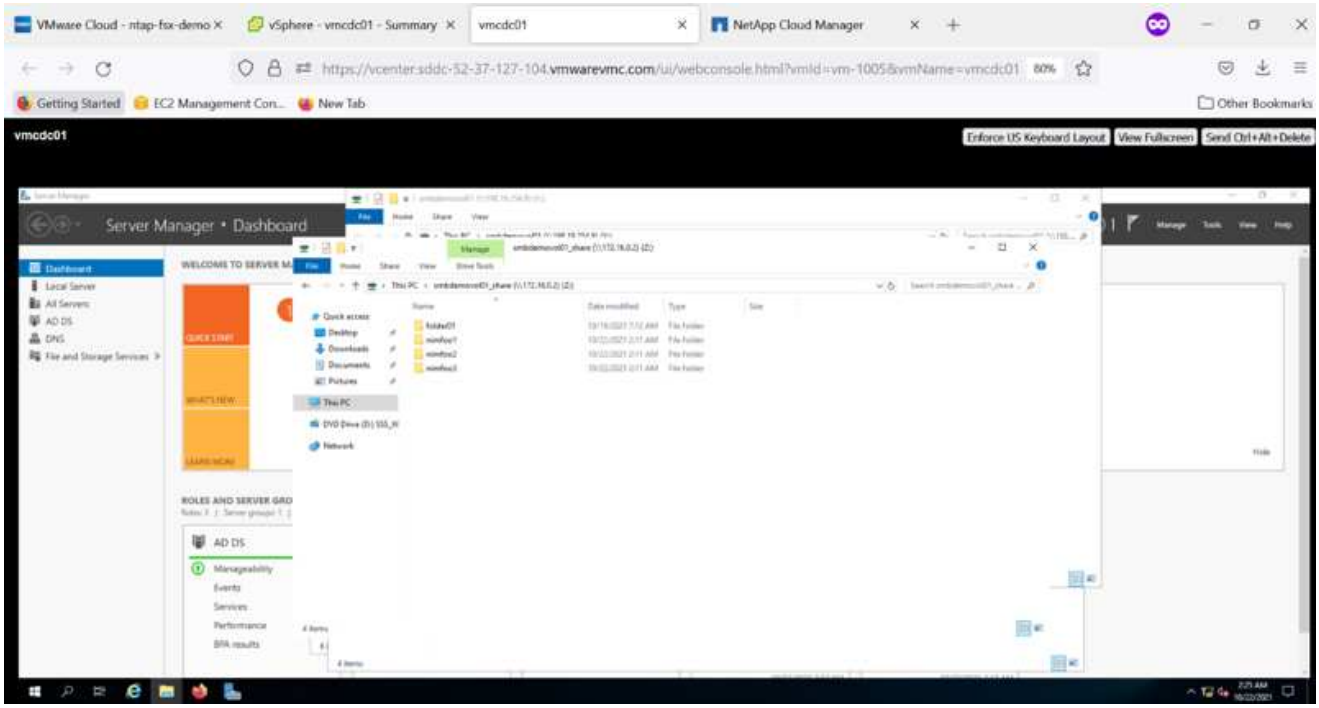

VMware Cloud - ntap-fsx-demo
vSphere - vmcdc01 - Summary
vmcdc01
NetApp Cloud Manager
https://vcenter.sddc-52-37-127-104.vmwarevmc.com/ui/webconsole.html?vmId=vm-1005&vmName=vmcdc01
Getting Started
EC2 Management Con...
New Tab
Other Bookmarks
vmcdc01
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Server Manager • Dashboard

LUN을 호스트에 연결합니다

Cloud Volumes ONTAP LUN을 호스트에 연결하려면 다음 단계를 수행하십시오.

1. Cloud Manager Canvas 페이지에서 Cloud Volumes ONTAP 작업 환경을 두 번 클릭하여 볼륨을 생성하고 관리합니다.
2. 볼륨 추가 > 새 볼륨 을 클릭하고 iSCSI 를 선택한 다음 이니시에이터 그룹 생성 을 클릭합니다. 계속 을 클릭합니다.





1. 볼륨이 프로비저닝되면 볼륨을 선택한 다음 대상 IQN을 클릭합니다. IQN(iSCSI Qualified Name)을 복사하려면 Copy(복사)를 클릭합니다. 호스트에서 LUN으로의 iSCSI 접속을 설정합니다.

AWS SDDC의 VMware Cloud에 있는 호스트에 대해 동일한 작업을 수행하려면 다음 단계를 수행하십시오.

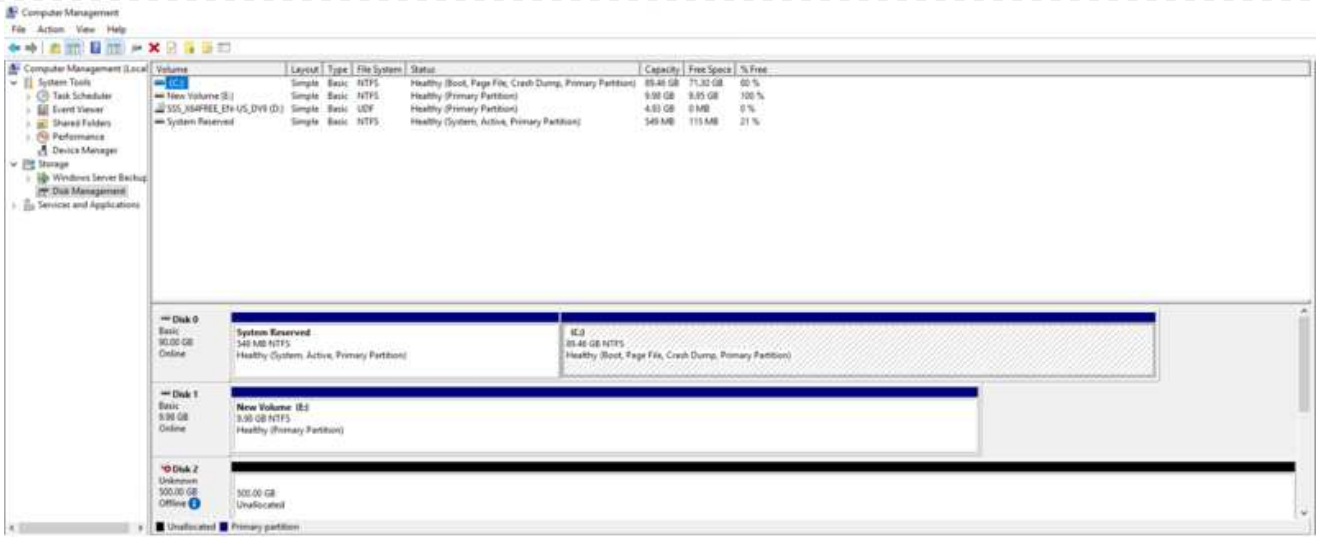
1. RDP를 AWS의 VMware 클라우드에서 호스팅되는 VM에 대한 것입니다.

2. iSCSI 초기자 속성 대화 상자(서버 관리자 > 대시보드 > 도구 > iSCSI 초기자)를 엽니다.
3. 검색 탭에서 포털 검색 또는 포털 추가 를 클릭한 다음 iSCSI 대상 포트의 IP 주소를 입력합니다.
4. 대상 탭에서 검색된 대상을 선택한 다음 로그온 또는 연결을 클릭합니다.
5. 다중 경로 사용 을 선택한 다음 컴퓨터가 시작될 때 이 연결 자동 복원 또는 즐겨찾기 대상 목록에 이 연결 추가 를 선택합니다. 고급 을 클릭합니다.

Windows 호스트에는 클러스터의 각 노드에 대한 iSCSI 연결이 있어야 합니다. 기본 DSM은 가장 적합한 경로를 선택합니다.

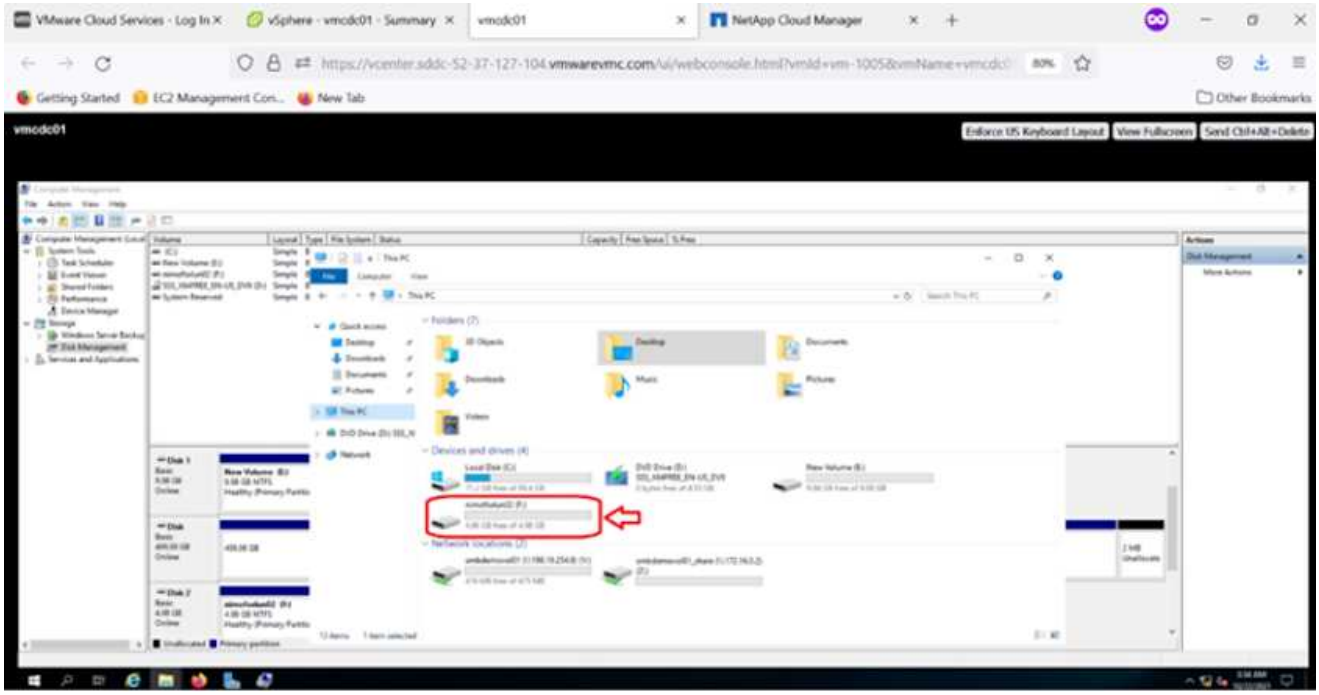
SVM의 LUN은 Windows 호스트에 디스크로 표시됩니다. 추가된 새 디스크는 호스트에서 자동으로 검색되지 않습니다. 수동 재검색을 트리거하여 다음 단계를 수행하여 디스크를 검색합니다.

1. 시작 > 관리 도구 > 컴퓨터 관리를 차례로 클릭하여 Windows 컴퓨터 관리 유틸리티를 엽니다.
2. 탐색 트리에서 스토리지 노드를 확장합니다.
3. 디스크 관리를 클릭합니다.
4. 작업 > 디스크 다시 검사 를 클릭합니다.



Windows 호스트에서 새 LUN을 처음 액세스할 때 파티션이나 파일 시스템이 없습니다. LUN을 초기화하고 필요에 따라 다음 단계를 완료하여 파일 시스템으로 LUN을 포맷합니다.

1. Windows 디스크 관리를 시작합니다.
2. LUN을 마우스 오른쪽 버튼으로 클릭한 다음 필요한 디스크 또는 파티션 유형을 선택합니다.
3. 마법사의 지침을 따릅니다. 이 예에서는 드라이브 F:가 마운트되었습니다.



Linux 클라이언트에서 iSCSI 데몬이 실행되고 있는지 확인합니다. LUN을 프로비저닝한 후에는 Linux 배포용 iSCSI 구성에 대한 자세한 지침을 참조하십시오. 예를 들어 Ubuntu iSCSI 구성을 찾을 수 있습니다 "여기". 확인하려면 셸에서 lsblk cmd 를 실행합니다.

Linux 클라이언트에 **Cloud Volumes ONTAP NFS** 볼륨을 마운트합니다

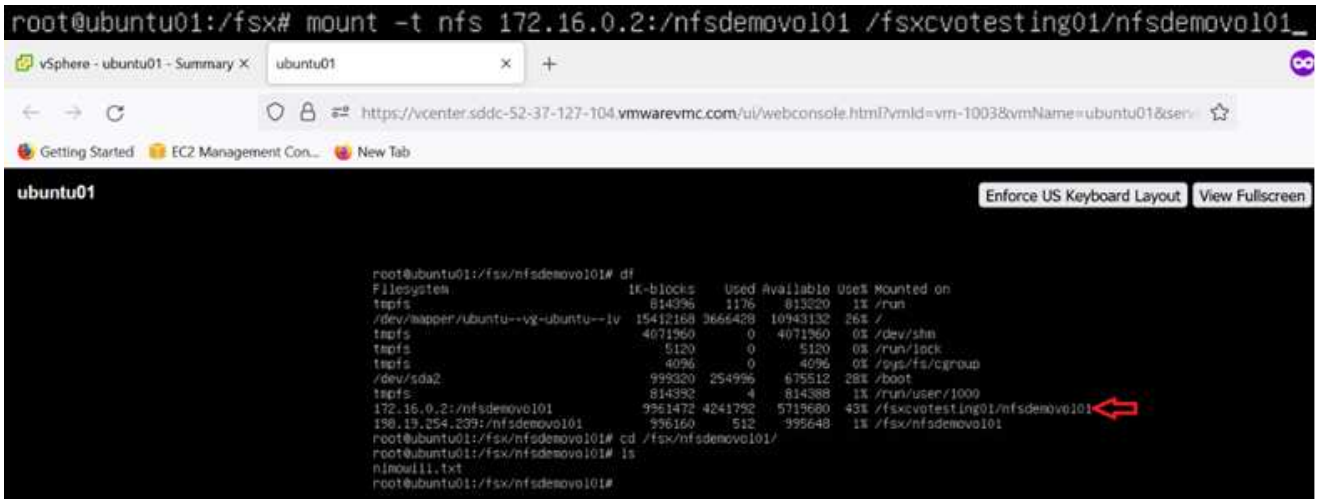
AWS SDDC의 VMC 내에서 DIY(Cloud Volumes ONTAP) 파일 시스템을 VM에서 마운트하려면 다음 단계를 수행하십시오.

1. 지정된 Linux 인스턴스에 연결합니다.
2. SSH(Secure Shell)를 사용하여 인스턴스의 터미널을 열고 적절한 자격 증명을 사용하여 로그인합니다.
3. 다음 명령을 사용하여 볼륨의 마운트 지점에 대한 디렉토리를 만듭니다.

```
 $ sudo mkdir /fsxcvotesting01/nfsdemovol01
```

. NetApp ONTAP NFS 볼륨용 Amazon FSx를 이전 단계에서 생성한 디렉토리에 마운트합니다.

```
sudo mount -t nfs nfsvers=4.1,172.16.0.2:/nfsdemovol01
/fsxcvotesting01/nfsdemovol01
```



ANF 데이터 저장소 솔루션 개요

성공적인 모든 조직은 혁신과 현대화의 길을 따라 있습니다. 이 프로세스의 일환으로, 기업은 일반적으로 기존 VMware 투자를 활용하는 동시에 클라우드의 이점을 활용하고 마이그레이션, 버스트, 확장 및 재해 복구 프로세스를 최대한 원활하게 만드는 방법을 모색합니다. 클라우드로 마이그레이션하는 고객은 탄력성 및 폭발적 문제, 데이터 센터 이탈, 데이터 센터 통합, 수명 종료 시나리오, 인수 합병 등을 평가해야 합니다. 각 조직에서 채택한 접근 방식은 각 비즈니스 우선순위에 따라 다를 수 있습니다. 클라우드 기반 운영을 선택할 때 적절한 성능과 최소 장애 요인을 갖춘 저렴한 모델을 선택하는 것이 중요한 목표입니다. 적합한 플랫폼을 선택할 뿐만 아니라, 스토리지 및 워크플로우 오케스트레이션은 클라우드의 강력한 기능과 탄력성을 최대한 활용하는 데 특히 중요합니다.

사용 사례

Azure VMware 솔루션은 고객에게 고유한 하이브리드 기능을 제공하지만, 제한된 기본 스토리지 옵션으로 스토리지 집약적인 워크로드를 사용하는 조직의 유용성이 제한됩니다. 스토리지가 호스트에 직접 연결되어 있으므로 스토리지를 확장하는 유일한 방법은 호스트를 추가하는 것입니다. 이렇게 하면 스토리지 집약적인 워크로드에서 비용이 35-40% 이상 증가할 수 있습니다. 이러한 워크로드는 추가 처리 능력이 아니라 추가 스토리지를 필요로 합니다. 즉, 추가 호스트에 대한 비용을 지불해야 합니다.

다음 시나리오를 고려해 보겠습니다. 고객은 마력(vCPU/vmem)을 위해 6개의 호스트를 필요로 하지만 스토리지에 대한 요구 사항도 상당히 있습니다. 평가를 기준으로 볼 때 스토리지 요구사항을 충족하기 위해 12개의 호스트가 필요합니다. 이렇게 하면 실제로 필요한 모든 것이 더 많은 스토리지일 때 마력을 추가로 구입해야 하기 때문에 전체 TCO가 증가합니다. 마이그레이션, 재해 복구, 사용 급증, 개발/테스트, 등.

Azure VMware 솔루션의 또 다른 일반적인 사용 사례는 DR(재해 복구)입니다. 대부분의 조직은 재해 복구 전략이 없거나 DR을 위한 고스트 데이터 센터의 실행을 정당화하는 데 어려움을 겪을 수 있습니다. 관리자는 파일럿 라이트 클러스터 또는 온디맨드 클러스터를 통해 설치 공간이 필요 없는 DR 옵션을 탐색할 수 있습니다. 그런 다음 호스트를 추가하지 않고 스토리지를 확장할 수 있으므로 매력적인 옵션이 될 수 있습니다.

요약하자면, 사용 사례는 다음 두 가지 방법으로 분류할 수 있습니다.

- ANF 데이터 저장소를 사용하여 스토리지 용량을 확장합니다
- 소프트웨어 정의 데이터 센터(SDDC) 간의 사내 또는 Azure 지역 내에서 비용 최적화된 복구 워크플로를 위해 ANF 데이터 저장소를 재해 복구 타겟으로 사용합니다. 이 가이드에서는 Azure NetApp Files를 사용하여 데이터 저장소에 최적화된 스토리지(현재 공개 미리 보기)를 제공하는 방법에 대해 설명합니다. Azure VMware 솔루션에서 동급 최고의 데이터 보호 및 DR 기능을 제공하므로 vSAN 스토리지에서 스토리지 용량을 오프로드할 수 있습니다.

ANF 데이터 저장소 사용에 대한 자세한 내용은 해당 지역의 NetApp 또는 Microsoft 솔루션 설계자에게 문의하십시오.

Azure의 **VMware** 클라우드 옵션

Azure VMware 솔루션

Azure VMware 솔루션(AVS)은 Microsoft Azure 퍼블릭 클라우드 내에서 완벽하게 작동하는 VMware SDDC를 제공하는 하이브리드 클라우드 서비스입니다. AVS는 Microsoft에서 완벽하게 관리 및 지원하고 Azure 인프라를 사용하는 VMware에서 검증한 최초의 솔루션입니다. 따라서 고객은 컴퓨팅 가상화를 위한 VMware ESXi, 하이퍼 컨버지드 스토리지를 위한 vSAN 및 네트워킹 및 보안을 위한 NSX를 얻는 동시에 Microsoft Azure의 세계적인 입지, 동급 최고의 데이터 센터 시설 및 네이티브 Azure 서비스 및 솔루션의 풍부한 에코시스템에 근접할 수 있는 이점을 누릴 수 있습니다. Azure VMware 솔루션 SDDC와 Azure NetApp Files를 함께 사용하면 네트워크 지연 시간을 최소화하면서 최상의 성능을 얻을 수 있습니다.

사용된 클라우드에 관계없이 VMware SDDC를 구축할 때 초기 클러스터에 포함되는 구성 요소는 다음과 같습니다.

- 관리를 위해 vCenter Server 어플라이언스를 사용하여 컴퓨팅 가상화를 위한 VMware ESXi 호스트
- VMware vSAN 하이퍼 컨버지드 스토리지는 각 ESXi 호스트의 물리적 스토리지 자산을 통합합니다.
- 관리를 위해 NSX Manager 클러스터를 사용하여 가상 네트워킹 및 보안을 위한 VMware NSX

결론

All-Cloud와 하이브리드 클라우드 중 무엇을 목표로 하고 있든 Azure NetApp Files는 애플리케이션 계층과 함께 애플리케이션 워크로드를 구축하고 관리하는 탁월한 옵션을 제공하는 한편 데이터 요구사항을 애플리케이션 계층으로

원활하게 충족하여 TCO를 줄여줍니다. 어떤 사용 사례에서든 Azure NetApp Files와 함께 Azure VMware 솔루션을 선택하면 클라우드의 이점, 일관된 인프라, 온프레미스 및 멀티 클라우드 전반의 운영, 워크로드의 양방향 이동성, 엔터프라이즈급 용량 및 성능을 빠르게 실현할 수 있습니다. 스토리지를 연결하는 데 사용되는 것과 동일한 친숙한 프로세스 및 절차입니다. 이는 새로운 이름과 함께 변경된 데이터의 위치일 뿐입니다. 도구 및 프로세스는 모두 동일하며 Azure NetApp Files는 전체 배포를 최적화하는 데 도움이 됩니다.

이점

이 문서의 핵심 사항은 다음과 같습니다.

- 이제 AVS SDDC에서 Azure NetApp Files를 데이터 저장소로 사용할 수 있습니다.
- 애플리케이션 응답 시간을 단축하고 가용성을 높여 필요할 때 언제 어디서나 액세스 워크로드 데이터를 제공합니다.
- 간단하고 즉각적인 크기 조정 기능을 통해 vSAN 스토리지의 전반적인 복잡성을 단순화합니다.
- 동적 재구성 기능을 사용하여 미션 크리티컬 워크로드의 성능 보장
- Azure VMware 솔루션 클라우드가 그 목적이라면 Azure NetApp Files는 최적의 구축을 위한 최적의 스토리지 솔루션입니다.

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 웹 사이트 링크를 참조하십시오.

- Azure VMware 솔루션 설명서

  "https://docs.microsoft.com/en-us/azure/azure-vmware/"

- Azure NetApp Files 설명서

  "https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- Azure NetApp Files 데이터 저장소를 Azure VMware 솔루션 호스트에 연결(Preview)

  https://docs.microsoft.com/en-us/azure/azure-vmware/attach-azure-netapp-files-to-azure-vmware-solution-hosts?tabs=azure-portal/

Azure용 **NetApp** 게스트 연결 스토리지 옵션

Azure는 기본 Azure NetApp Files(ANF) 서비스 또는 CVO(Cloud Volumes ONTAP)를 통해 게스트 연결 NetApp 스토리지를 지원합니다.

Azure NetApp Files(ANF)

Azure NetApp Files는 Azure에 엔터프라이즈급 데이터 관리 및 스토리지를 제공하므로 워크로드와 애플리케이션을 쉽게 관리할 수 있습니다. 워크로드를 클라우드로 마이그레이션하여 성능 저하 없이 실행할 수 있습니다.

Azure NetApp Files가 장애를 제거하므로 모든 파일 기반 애플리케이션을 클라우드로 이동할 수 있습니다. 따라서 애플리케이션을 재설계할 필요가 없으며 애플리케이션용 영구 스토리지를 간편하게 확보할 수 있습니다.

이 서비스는 Microsoft Azure Portal을 통해 제공되므로 사용자는 Microsoft 기업 계약의 일부로 완벽하게 관리되는 서비스를 이용할 수 있습니다. Microsoft에서 관리하는 세계 최고 수준의 지원을 통해 안심하고 사용할 수 있습니다. 단일 솔루션으로 멀티프로토콜 워크로드를 빠르고 쉽게 추가할 수 있습니다. 레거시 환경에서도 Windows 및 Linux

파일 기반 애플리케이션을 모두 구축하여 배포할 수 있습니다.

게스트 연결 스토리지로서의 **Azure NetApp Files(ANF)**

AVS(Azure VMware Solution)를 사용하여 **Azure NetApp Files** 구성

Azure NetApp Files 공유는 Azure VMware SDDC 솔루션 환경에서 생성된 VM에서 마운트할 수 있습니다. Azure NetApp Files는 SMB 및 NFS 프로토콜을 지원하므로 Linux 클라이언트에 볼륨을 마운트하고 Windows 클라이언트에 매핑할 수도 있습니다. Azure NetApp Files 볼륨은 간단한 5단계를 통해 설정할 수 있습니다.

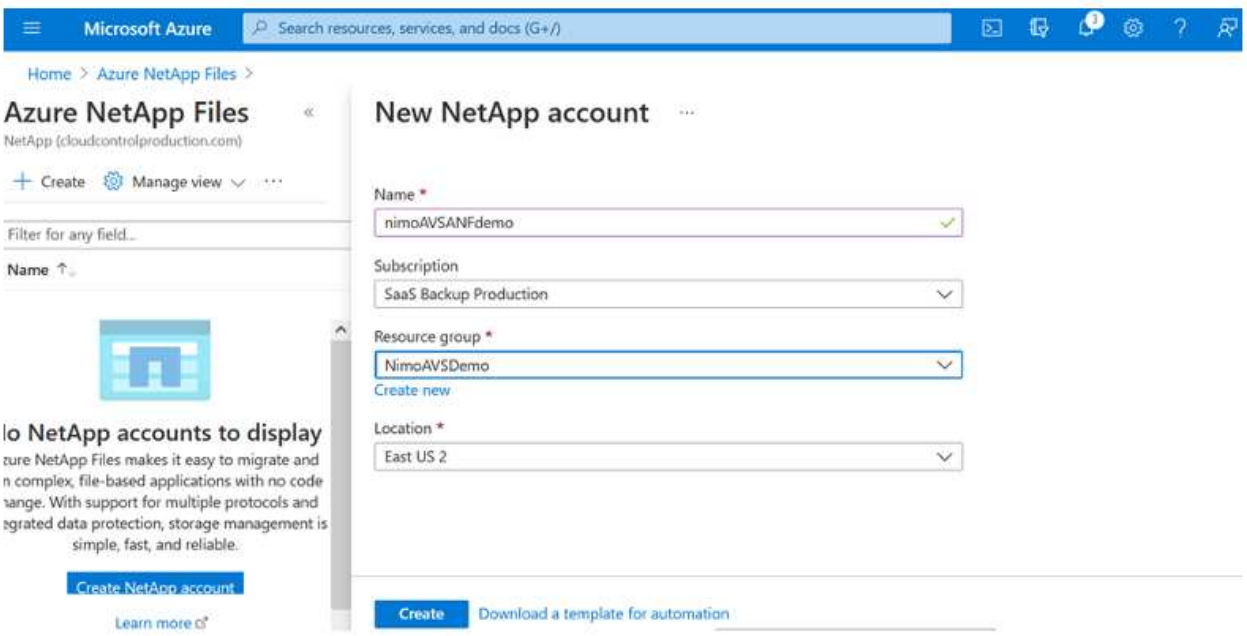
Azure NetApp Files 및 Azure VMware 솔루션은 동일한 Azure 지역에 있어야 합니다.

Azure NetApp Files 볼륨을 생성하고 마운트합니다

Azure NetApp Files 볼륨을 생성 및 마운트하려면 다음 단계를 수행하십시오.

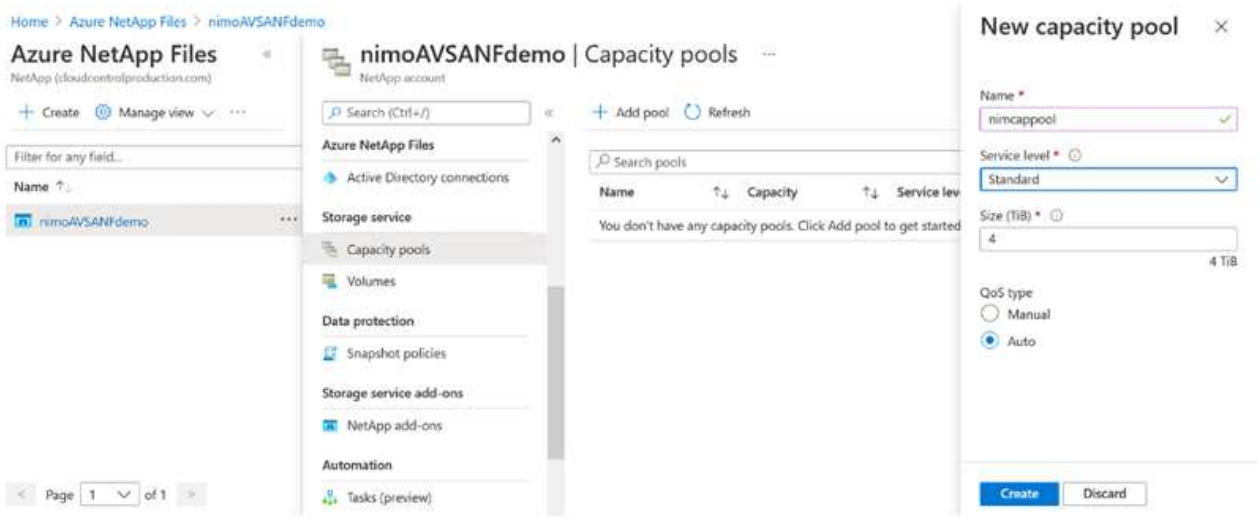
1. Azure 포털에 로그인하고 Azure NetApp Files에 액세스합니다. Azure NetApp Files 서비스에 대한 액세스를 확인하고 _az 공급자 레지스터—namespace Microsoft.NetApp –wait_명령을 사용하여 Azure NetApp Files 리소스 공급자를 등록합니다. 등록이 완료되면 NetApp 계정을 생성합니다.

   자세한 단계는 을 참조하십시오 "Azure NetApp Files 공유". 이 페이지에서는 단계별 프로세스를 안내합니다.

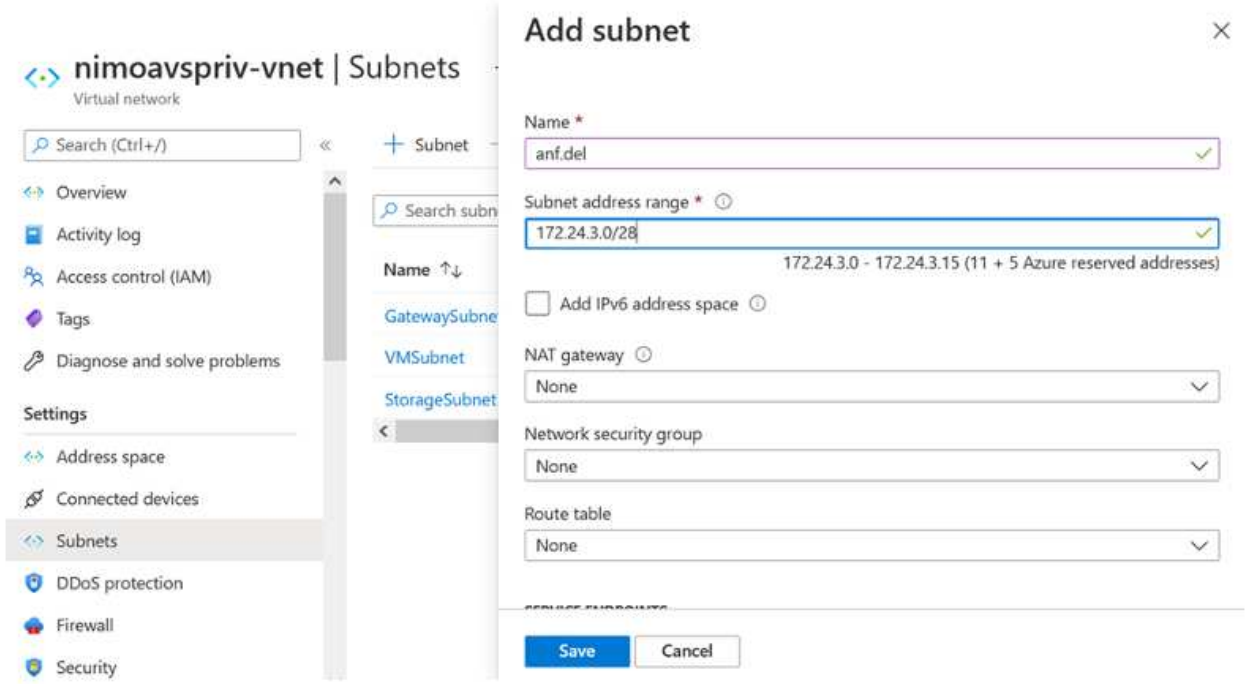


2. NetApp 계정을 생성한 후 필요한 서비스 수준과 크기로 용량 풀을 설정합니다.

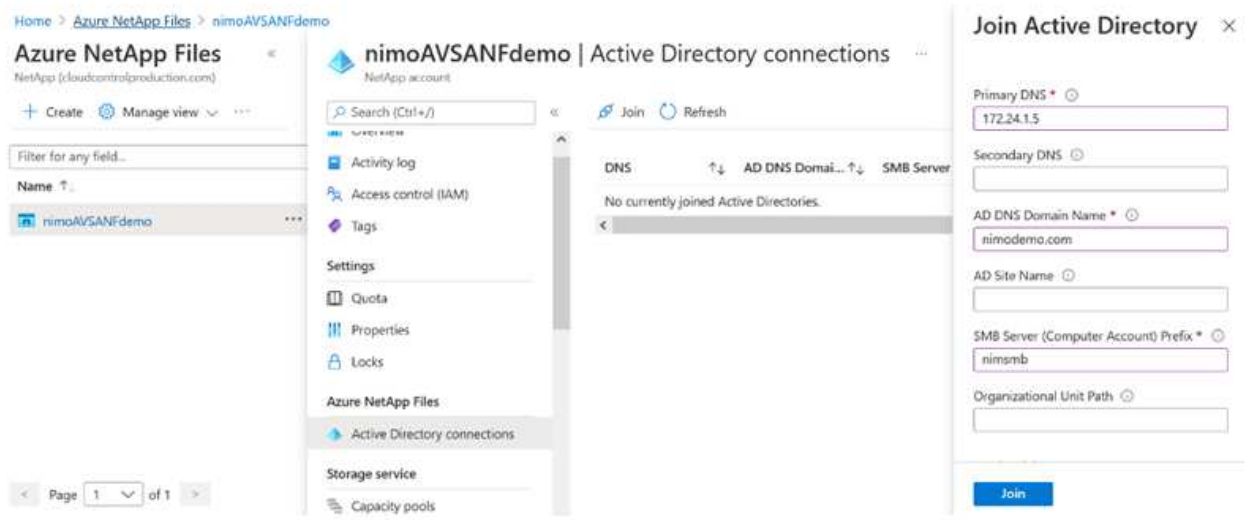
   자세한 내용은 을 참조하십시오 "용량 풀을 설정합니다".



3. Azure NetApp Files에 대해 위임된 서브넷을 구성하고 볼륨을 생성하는 동안 이 서브넷을 지정합니다. 위임된 서브넷을 생성하는 자세한 단계는 을 참조하십시오 "Azure NetApp Files에 서브넷 위임".

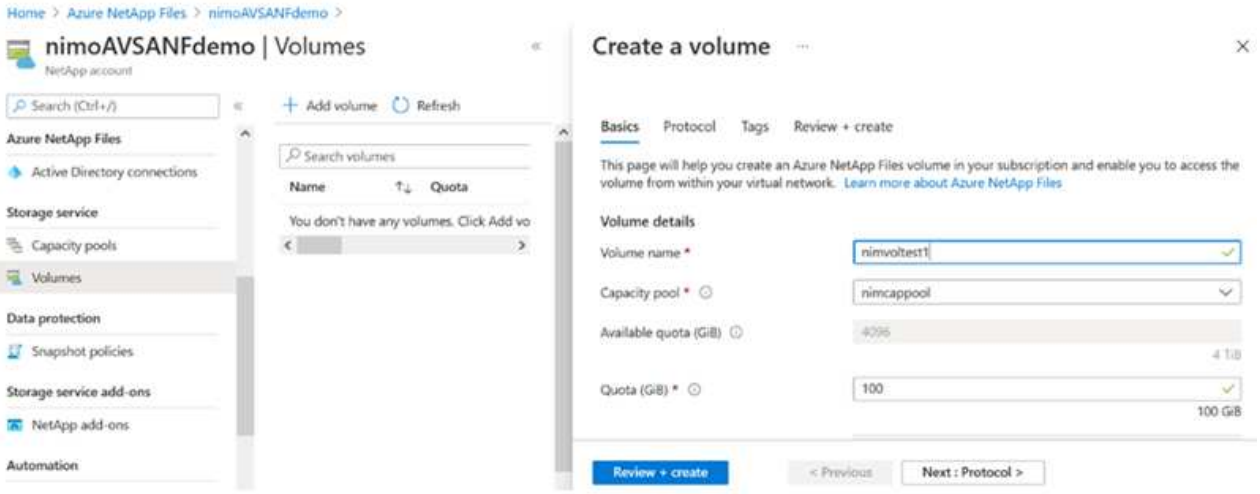


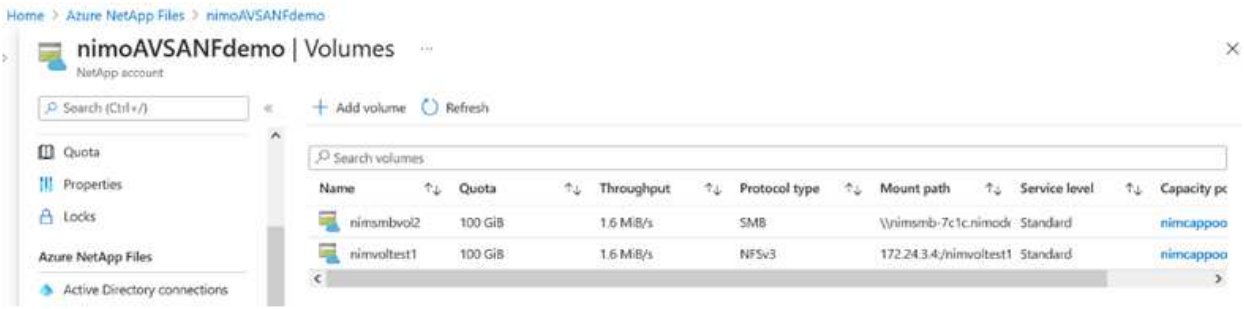
4. Capacity Pools 블레이드 아래의 Volumes 블레이드를 사용하여 SMB 볼륨을 추가합니다. SMB 볼륨을 생성하기 전에 Active Directory 커넥터가 구성되어 있는지 확인합니다.



5. 검토 + 생성 을 클릭하여 SMB 볼륨을 생성합니다.

   애플리케이션이 SQL Server인 경우 SMB의 지속적인 가용성을 설정합니다.

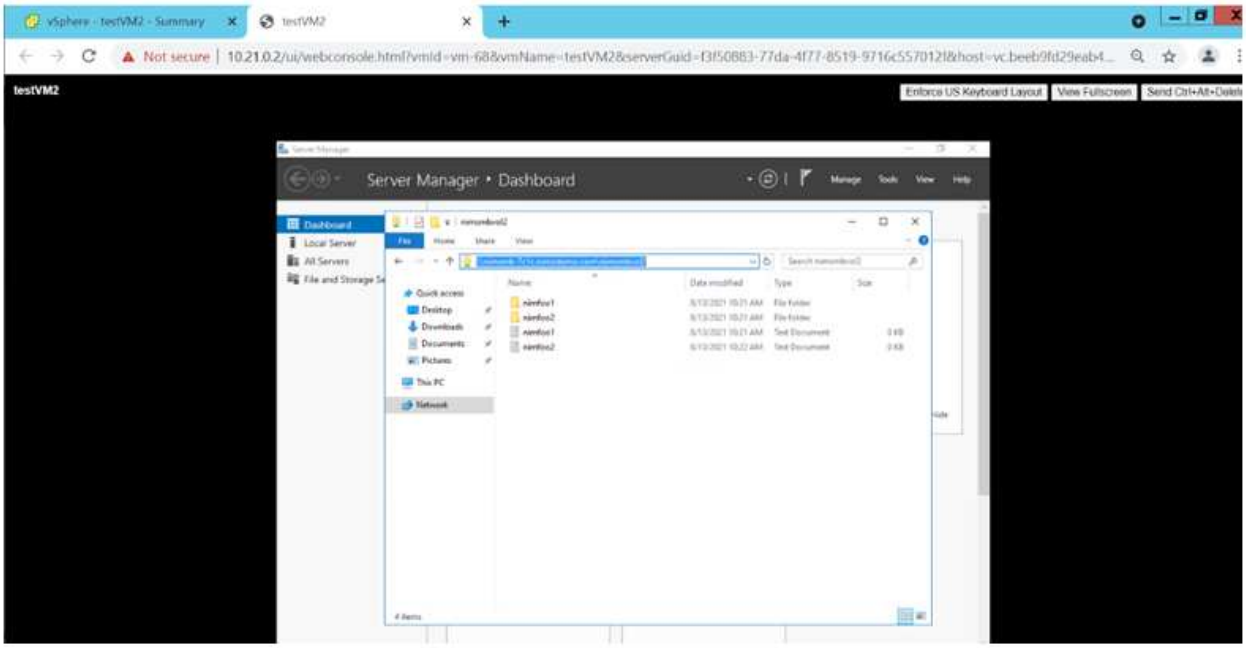


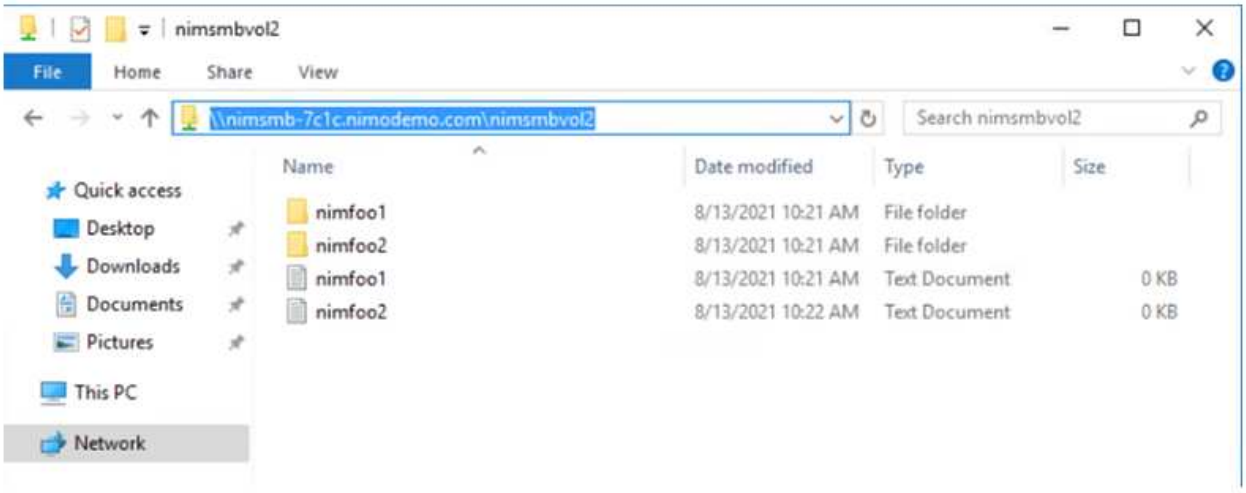


크기 또는 할당량별 Azure NetApp Files 볼륨 성능에 대한 자세한 내용은 을 참조하십시오 "Azure NetApp Files에 대한 성능 고려 사항".

6. 연결이 완료되면 볼륨을 마운트하여 애플리케이션 데이터에 사용할 수 있습니다.

   이를 수행하려면 Azure 포털에서 볼륨 블레이드를 클릭한 다음 마운트할 볼륨을 선택하고 마운트 지침을 액세스합니다. 경로를 복사하고 Map Network Drive 옵션을 사용하여 Azure VMware Solution SDDC에서 실행되는 VM에 볼륨을 마운트합니다.





7. Azure VMware Solution SDDC에서 실행되는 Linux VM에 NFS 볼륨을 마운트하려면 이 프로세스를 사용합니다. 볼륨 재구성 또는 동적 서비스 수준 기능을 사용하여 워크로드 요구 사항을 충족합니다.

```
nimoadmin@nimoadmin-virtual-machine:~$ sudo mount -t nfs -o rw,hard,tcp 172.24.
3.4:/nimodemonfsv1 /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$ df
Filesystem                  1K-blocks     Used Available Use% Mounted on
udev                          8168112        0   8168112   0% /dev
tmpfs                         1639548     1488   1638060   1% /run
/dev/sda5                    50824704  7902752  40310496  17% /
tmpfs                         8197728        0   8197728   0% /dev/shm
tmpfs                            5120        0      5120   0% /run/lock
tmpfs                         8197728        0   8197728   0% /sys/fs/cgroup
/dev/loop0                      56832    56832         0 100% /snap/core18/2128
/dev/loop2                      66688    66688         0 100% /snap/gtk-common-the
mes/1515
/dev/loop1                     224256   224256         0 100% /snap/gnome-3-34-180
4/72
/dev/loop3                      52224    52224         0 100% /snap/snap-store/547
/dev/loop4                      33152    33152         0 100% /snap/snapd/12704
/dev/sda1                      523248        4    523244   1% /boot/efi
tmpfs                         1639544       52   1639492   1% /run/user/1000
/dev/sr0                        54738    54738         0 100% /media/nimoadmin/VMw
are Tools
172.24.3.4:/nimodemonfsv1 104857600        0 104857600   0% /home/nimoadmin/nimo
demo11
nimoadmin@nimoadmin-virtual-machine:~$
```

자세한 내용은 을 참조하십시오 "볼륨의 서비스 수준을 동적으로 변경합니다".

CVO(Cloud Volumes ONTAP)

Cloud Volumes ONTAP, 즉 CVO는 NetApp의 ONTAP 스토리지 소프트웨어를 기반으로 하는 업계 최고의 클라우드 데이터 관리 솔루션으로, AWS(Amazon Web Services), Microsoft Azure 및 GCP(Google Cloud Platform)에서 기본적으로 제공됩니다.

ONTAP의 소프트웨어 정의 버전이며 클라우드 네이티브 스토리지를 사용합니다. 따라서 클라우드와 사내에서 동일한 스토리지 소프트웨어를 사용할 수 있으므로 데이터를 관리하는 새로운 방법을 통해 IT 직원을 재교육할 필요가

없습니다.

CVO를 사용하면 데이터를 에지에서 데이터 센터, 클라우드로 원활하게 이동하고 다시 가져올 수 있습니다. 또한 단일 창 관리 콘솔인 NetApp Cloud Manager를 사용하여 하이브리드 클라우드를 통합할 수 있습니다.

설계상 CVO는 최고 성능과 고급 데이터 관리 기능을 제공하여 클라우드에서 가장 까다로운 애플리케이션도 충족합니다

CVO(Cloud Volumes ONTAP)를 게스트 연결 스토리지로 사용합니다

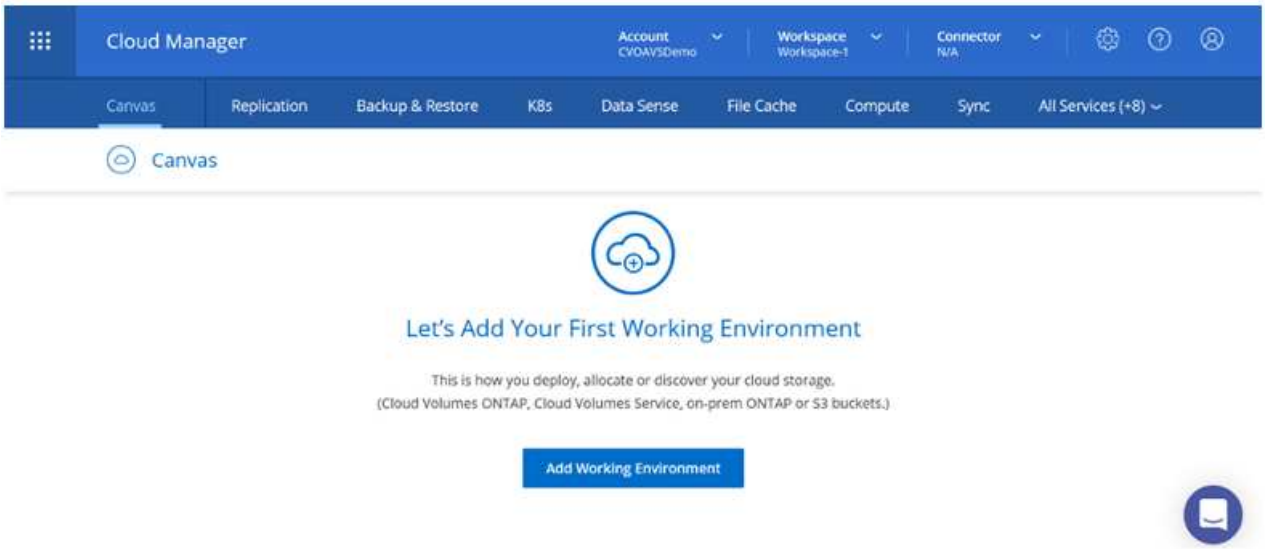
Azure에 새로운 Cloud Volumes ONTAP 구축

Cloud Volumes ONTAP 공유 및 LUN은 Azure VMware Solution SDDC 환경에서 생성된 VM에서 마운트할 수 있습니다. Cloud Volumes ONTAP는 iSCSI, SMB 및 NFS 프로토콜을 지원하므로 Linux 클라이언트와 Windows 클라이언트에도 볼륨을 마운트할 수 있습니다. Cloud Volumes ONTAP 볼륨은 몇 가지 간단한 단계를 통해 설정할 수 있습니다.

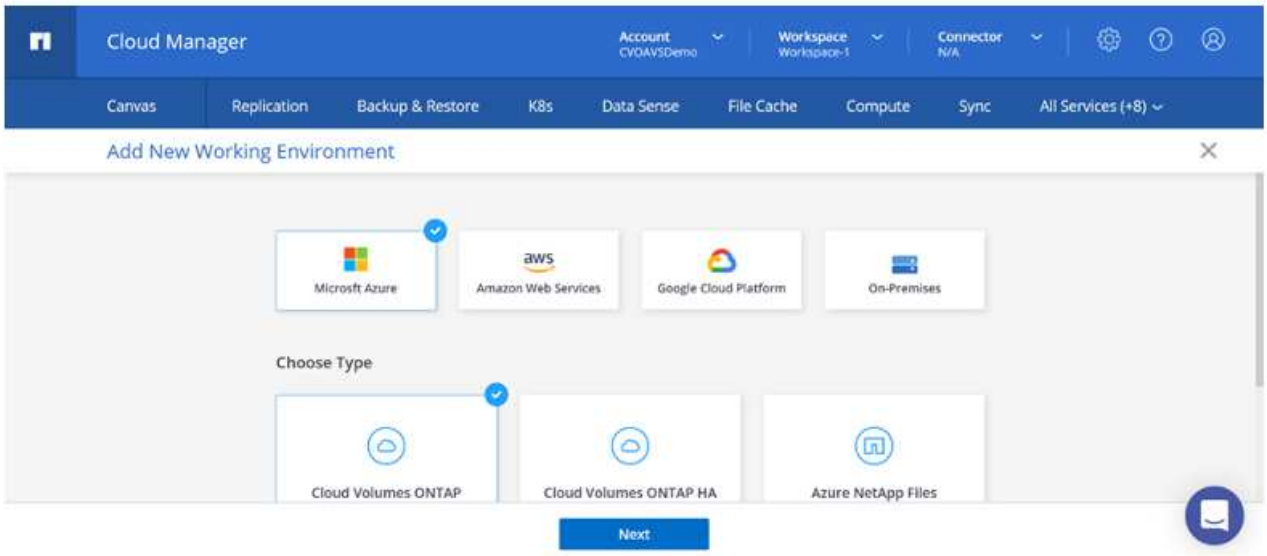
재해 복구 또는 마이그레이션을 위해 사내 환경에서 클라우드로 볼륨을 복제하려면 사이트 간 VPN 또는 ExpressRoute를 사용하여 Azure에 대한 네트워크 연결을 설정합니다. 사내의 데이터를 Cloud Volumes ONTAP로 복제하는 작업은 이 문서의 범위를 벗어납니다. 사내 시스템과 Cloud Volumes ONTAP 시스템 간에 데이터를 복제하려면 을 참조하십시오 "시스템 간 데이터 복제 설정".

사용 "Cloud Volumes ONTAP Sizer" Cloud Volumes ONTAP 인스턴스의 크기를 정확하게 지정합니다. 또한 Cloud Volumes ONTAP Sizer에서 입력으로 사용할 온프레미스 성능을 모니터링합니다.

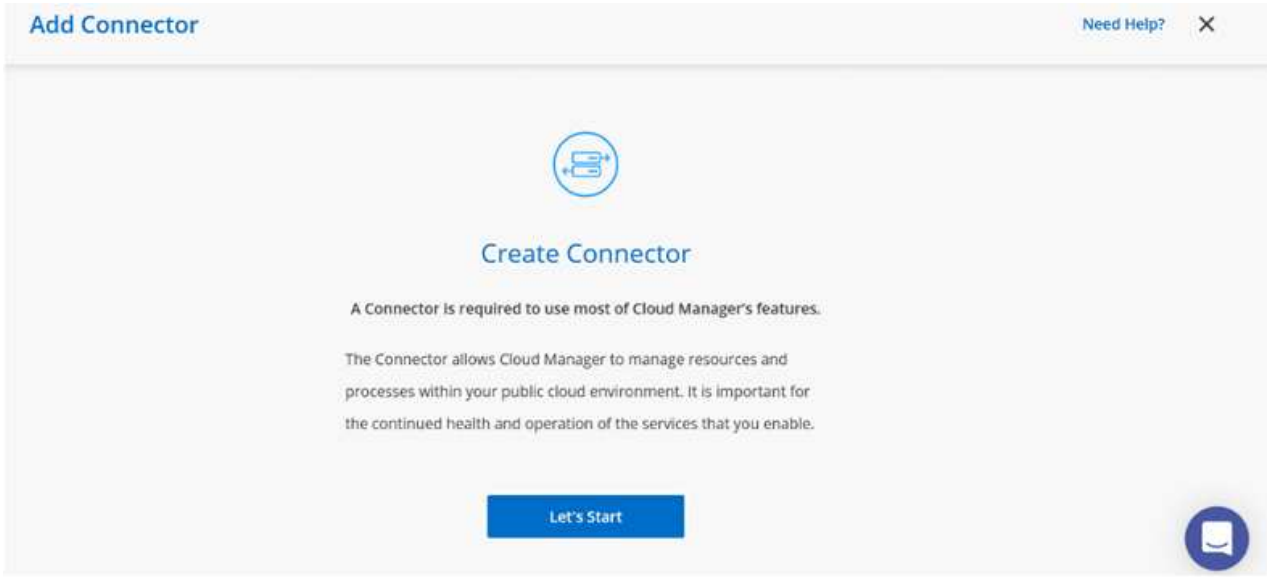
1. NetApp Cloud Central에 로그인 - 패브릭 보기 화면이 표시됩니다. Cloud Volumes ONTAP 탭을 찾아 Cloud Manager로 이동 을 선택합니다. 로그인하면 Canvas 화면이 표시됩니다.



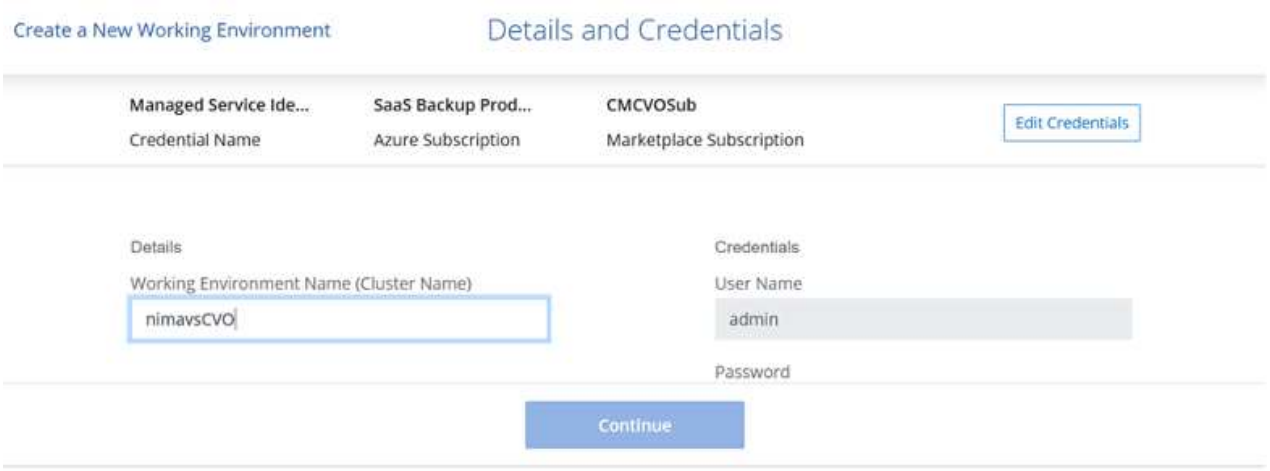
2. Cloud Manager 홈 페이지에서 작업 환경 추가를 클릭한 다음 클라우드로 Microsoft Azure를 선택하고 시스템 구성의 유형을 선택합니다.



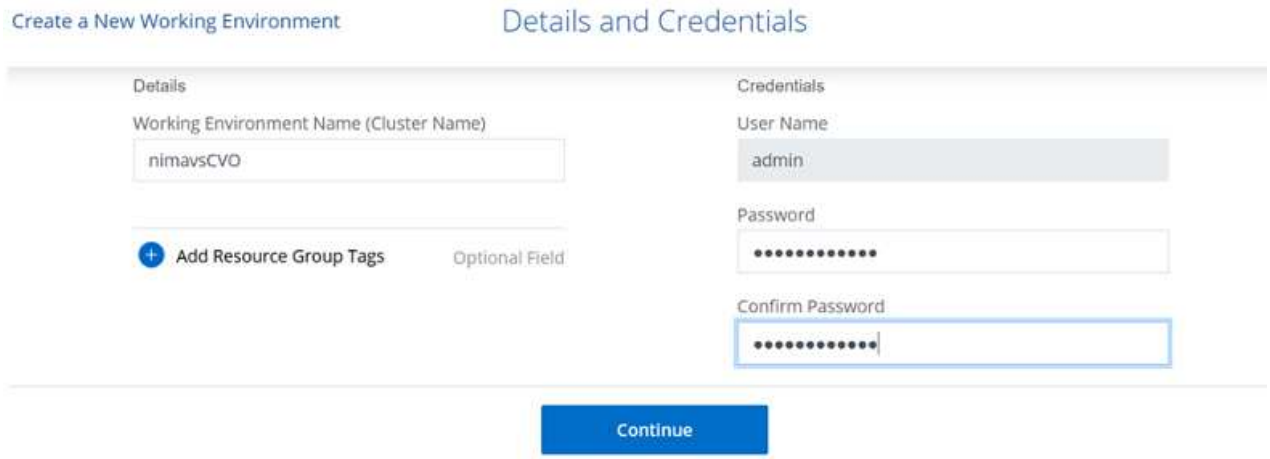
3. 첫 번째 Cloud Volumes ONTAP 작업 환경을 생성할 때 Cloud Manager에서 커넥터를 배포하라는 메시지를 표시합니다.



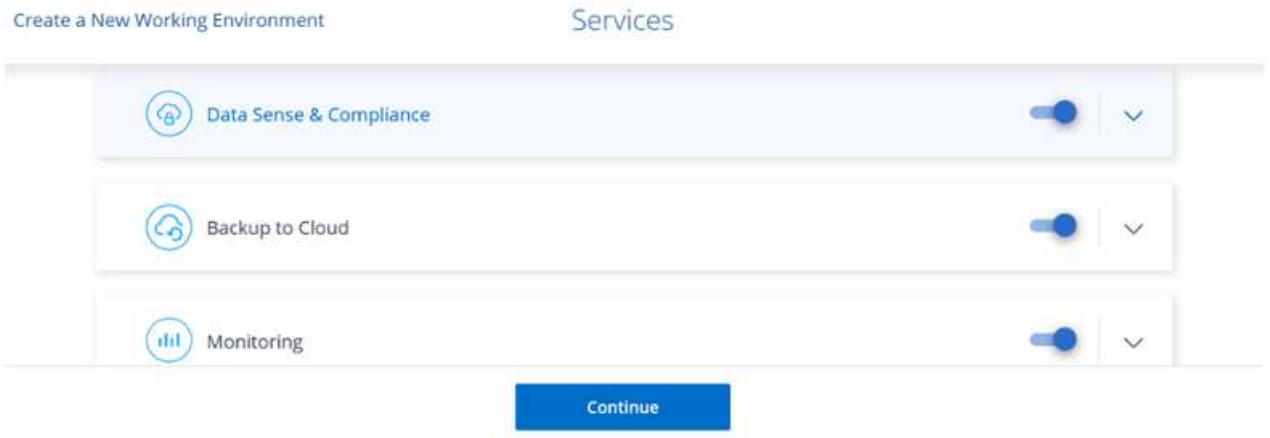
4. 커넥터가 생성되면 세부 정보 및 자격 증명 필드를 업데이트합니다.



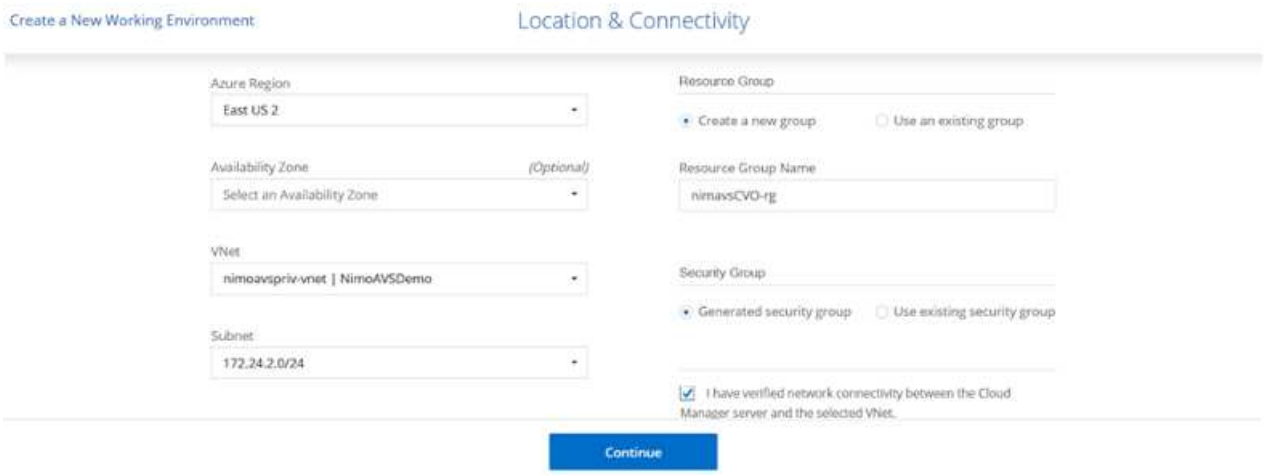
5. 환경 이름 및 관리자 자격 증명을 비롯하여 생성할 환경에 대한 세부 정보를 제공합니다. Azure 환경의 리소스 그룹 태그를 선택적 매개 변수로 추가합니다. 작업을 마친 후 계속 을 클릭합니다.



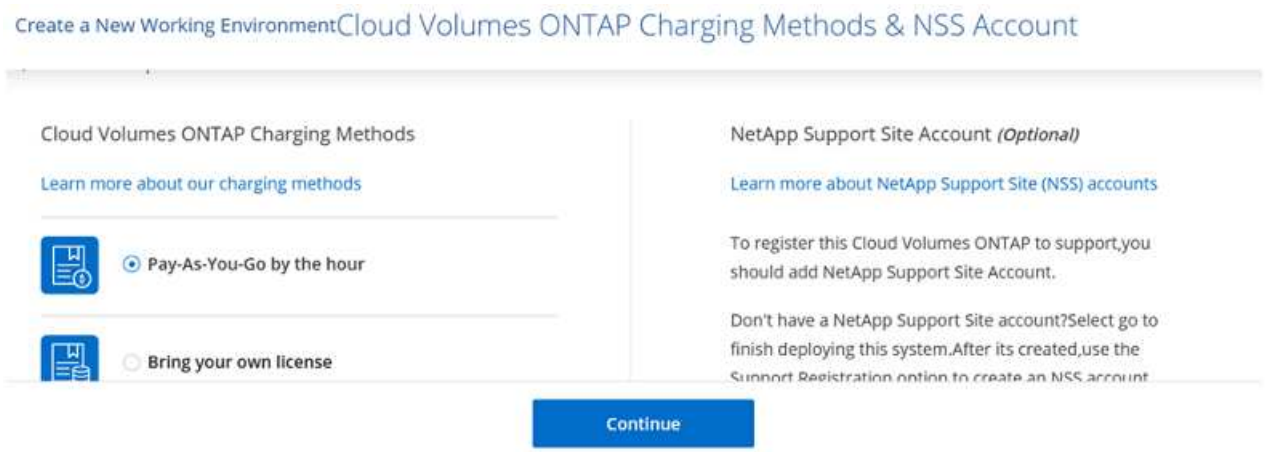
6. BlueXP 분류, BlueXP 백업 및 복구, Cloud Insights를 비롯하여 Cloud Volumes ONTAP 구축을 위한 애드온 서비스를 선택하십시오. 서비스를 선택한 다음 계속 을 클릭합니다.



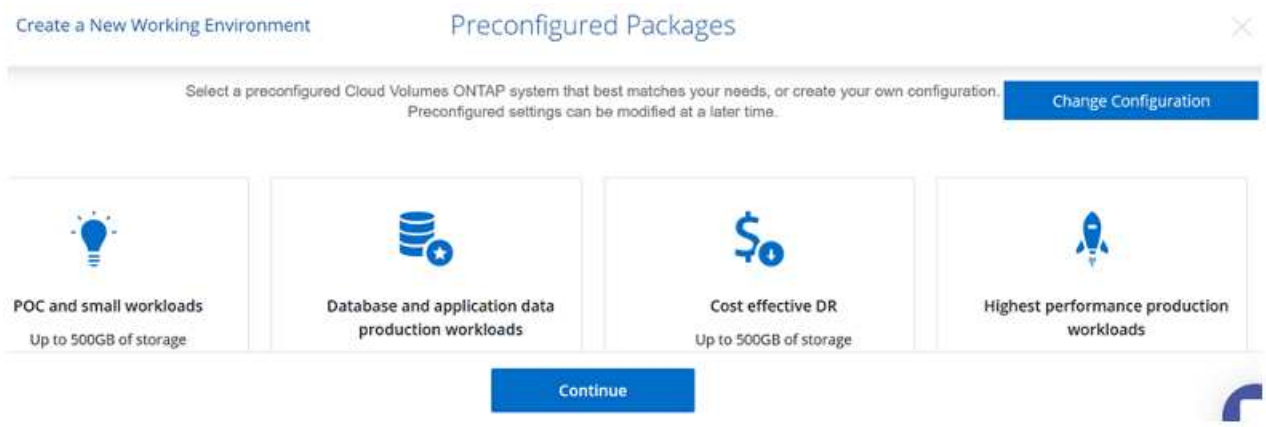
7. Azure 위치 및 연결을 구성합니다. 사용할 Azure 지역, 리소스 그룹, VNET 및 서브넷을 선택합니다.



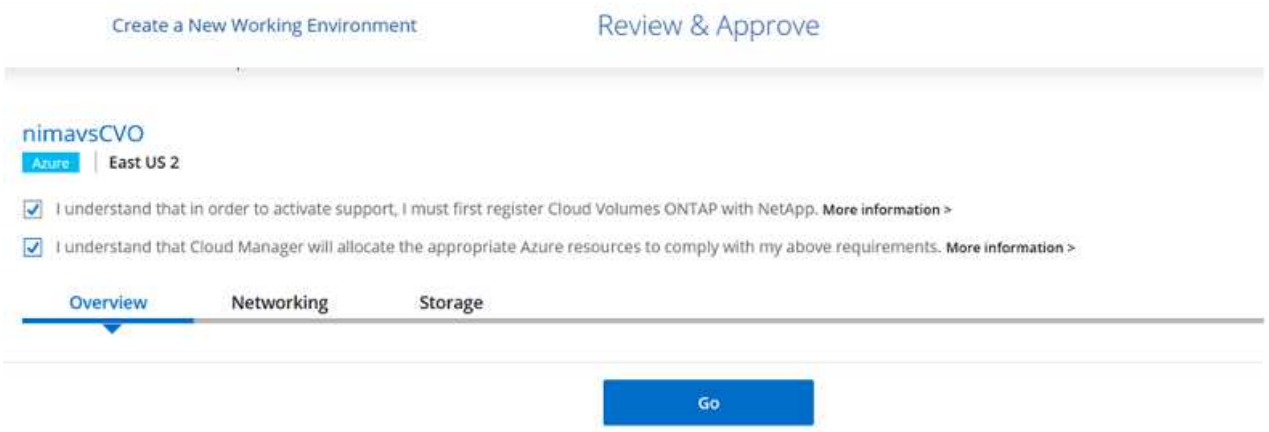
8. 라이센스 옵션 선택: 사용한 만큼만 지불 또는 BYOL 방식으로 기존 라이센스 사용 이 예에서는 pay-as-you-go 옵션을 사용합니다.



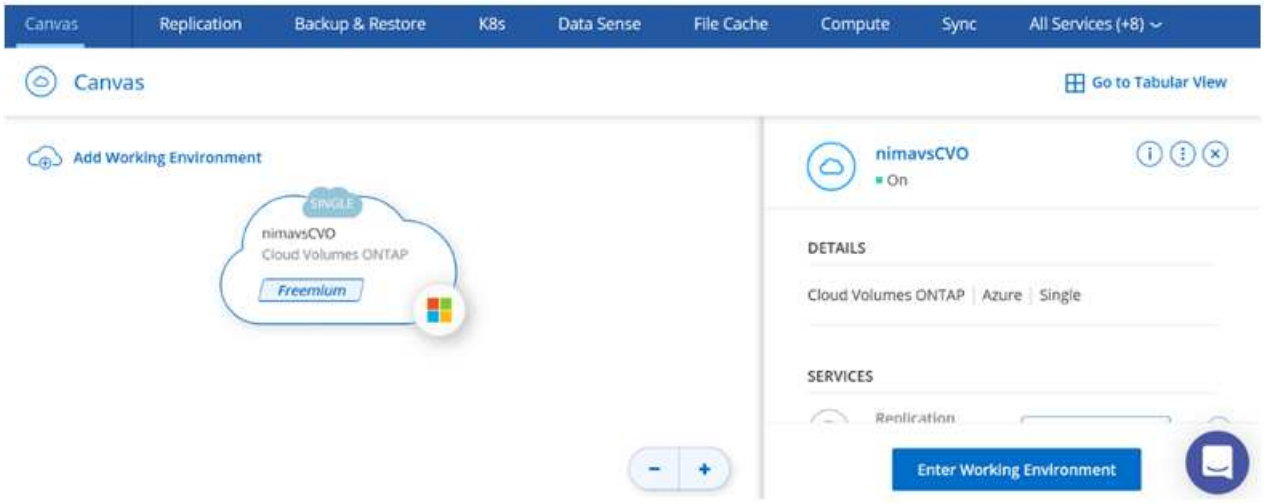
9. 다양한 유형의 워크로드에 사용할 수 있는 사전 구성된 여러 패키지 중 하나를 선택합니다.



10. Azure 리소스의 활성화 및 할당과 관련된 두 가지 계약에 동의합니다. Cloud Volumes ONTAP 인스턴스를 만들려면 이동을 클릭합니다.

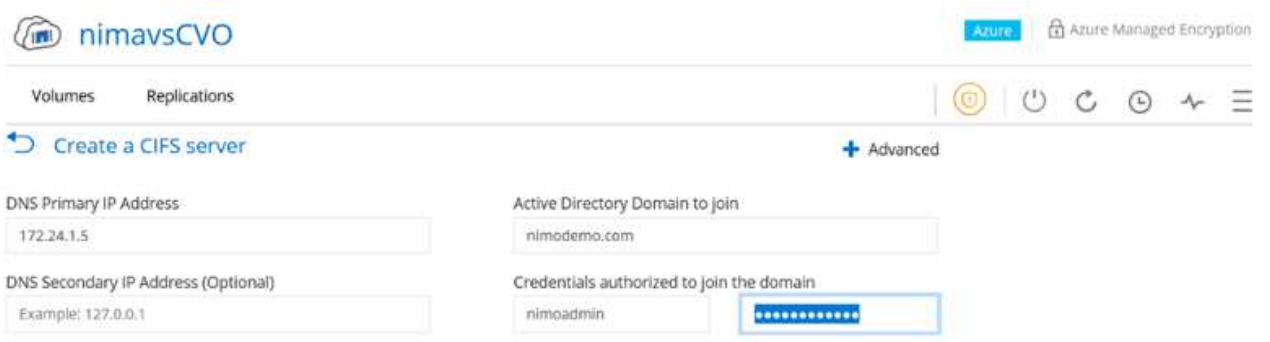


11. Cloud Volumes ONTAP를 프로비저닝하면 Canvas 페이지의 작업 환경에 나열됩니다.

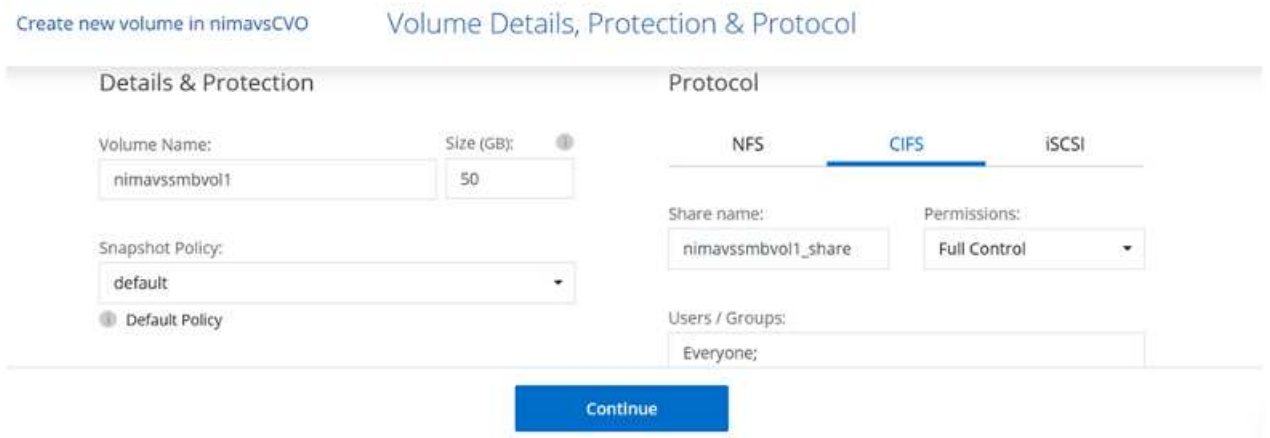


SMB 볼륨을 위한 추가 구성

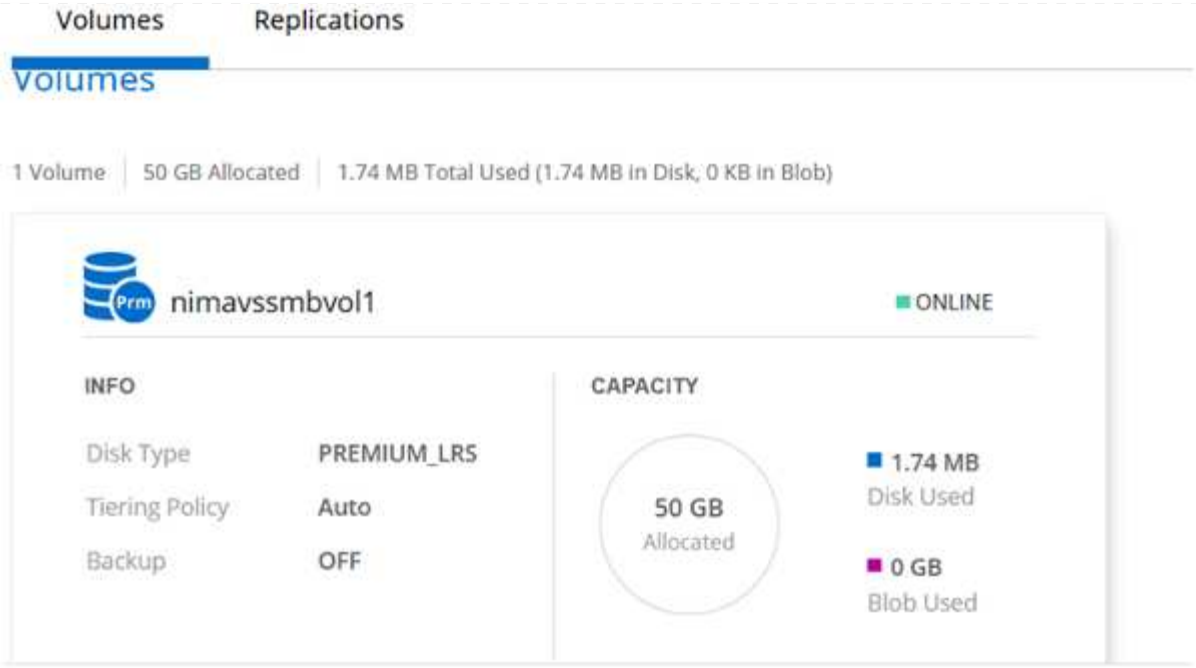
1. 작업 환경이 준비되면 CIFS 서버가 적절한 DNS 및 Active Directory 구성 매개 변수로 구성되어 있는지 확인합니다. 이 단계는 SMB 볼륨을 생성하기 전에 필요합니다.



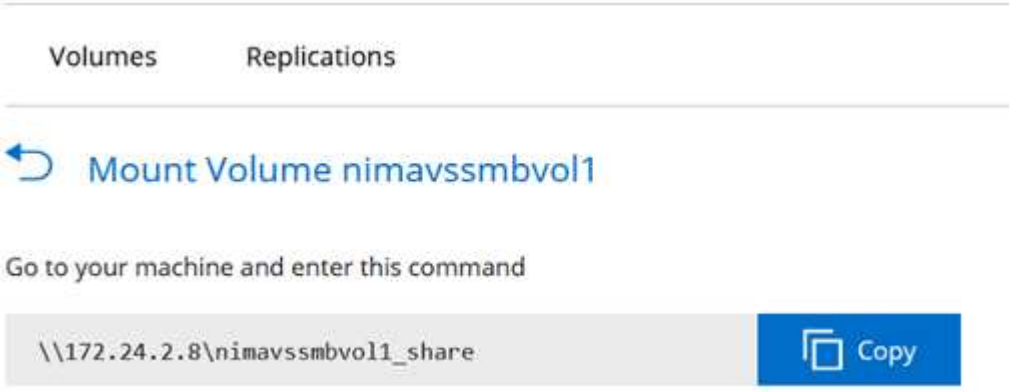
2. SMB 볼륨을 생성하는 것은 쉬운 프로세스입니다. CVO 인스턴스를 선택하여 볼륨을 생성하고 Create Volume 옵션을 클릭합니다. 적절한 크기를 선택하고 클라우드 관리자가 포함하는 애그리게이트를 선택하거나, 고급 할당 메커니즘을 사용하여 특정 애그리게이트에 배치할 수 있습니다. 이 데모에서는 SMB가 프로토콜로 선택됩니다.

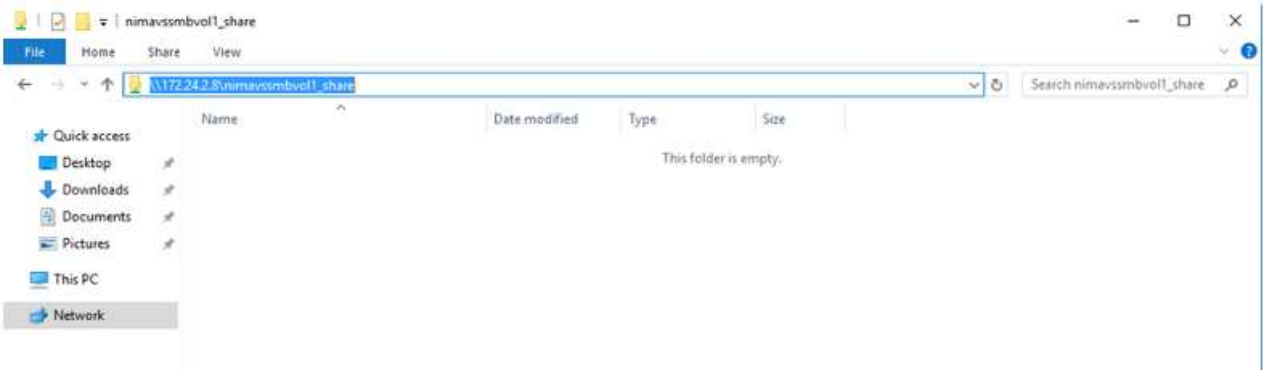


3. 볼륨 용량 할당 후 볼륨 창 아래에서 사용할 수 있습니다. CIFS 공유가 프로비저닝되므로 사용자 또는 그룹에 파일 및 폴더에 대한 권한을 제공하고 해당 사용자가 공유를 액세스하고 파일을 생성할 수 있는지 확인합니다. 파일 및 폴더 권한이 모두 SnapMirror 복제의 일부로 유지되므로 볼륨이 사내 환경에서 복제된 경우에는 이 단계가 필요하지 않습니다.



4. 볼륨을 생성한 후 mount 명령을 사용하여 Azure VMware Solution SDDC 호스트에서 실행 중인 VM에서 공유에 연결합니다.
5. 다음 경로를 복사하고 Map Network Drive 옵션을 사용하여 Azure VMware Solution SDDC에서 실행되는 VM에 볼륨을 마운트합니다.

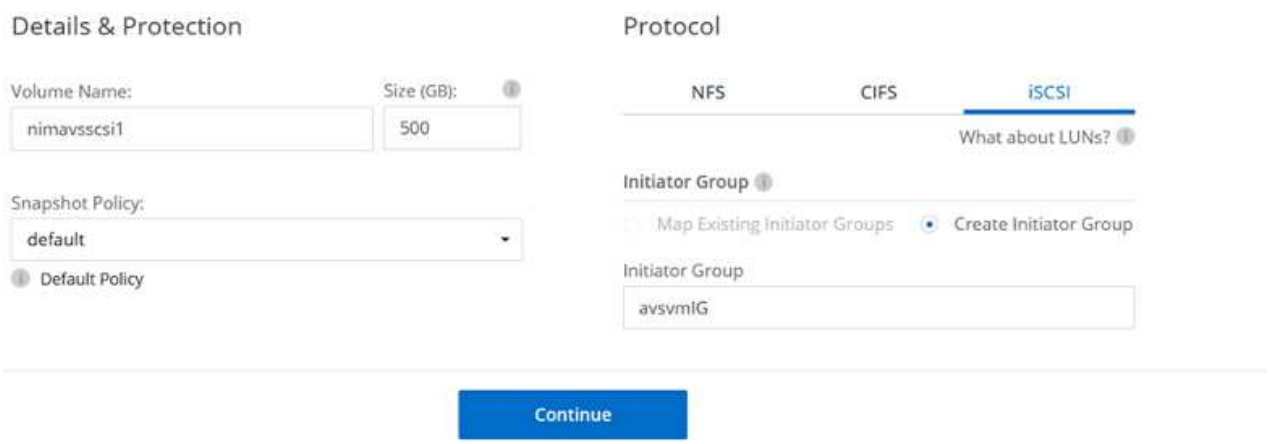




LUN을 호스트에 연결합니다

LUN을 호스트에 연결하려면 다음 단계를 수행하십시오.

1. Canvas 페이지에서 Cloud Volumes ONTAP 작업 환경을 두 번 클릭하여 볼륨을 생성하고 관리합니다.
2. 볼륨 추가 > 새 볼륨 을 클릭하고 iSCSI 를 선택한 다음 이니시에이터 그룹 생성 을 클릭합니다. 계속 을 클릭합니다.



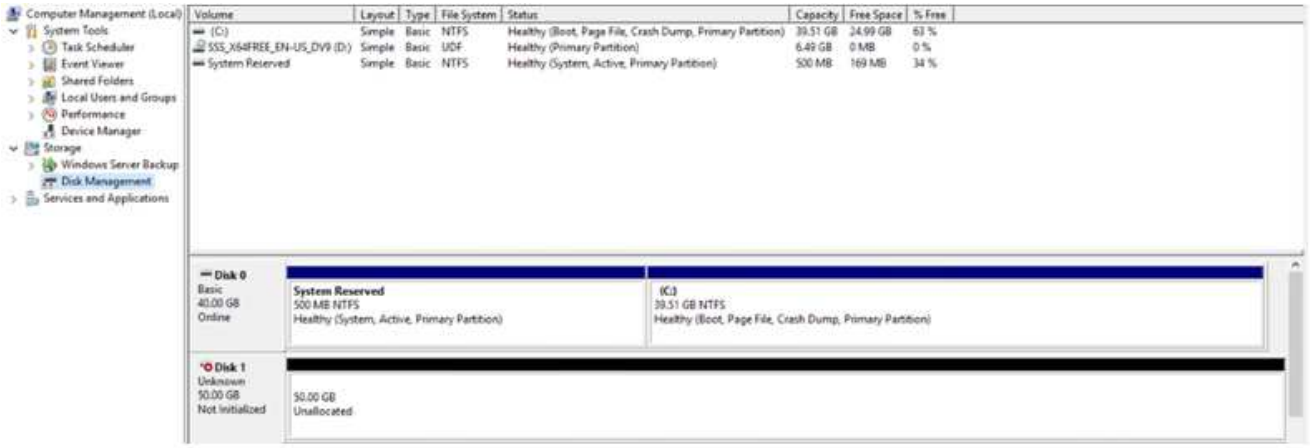
3. 볼륨이 프로비저닝되면 볼륨을 선택한 다음 대상 IQN을 클릭합니다. IQN(iSCSI Qualified Name)을 복사하려면 Copy(복사)를 클릭합니다. 호스트에서 LUN으로의 iSCSI 접속을 설정합니다.

   Azure VMware Solution SDDC에 있는 호스트에 대해 동일한 작업을 수행하려면 다음을 수행합니다.

   a. Azure VMware Solution SDDC에서 호스팅되는 VM에 대한 RDP
   b. iSCSI 초기자 속성 대화 상자(서버 관리자 > 대시보드 > 도구 > iSCSI 초기자)를 엽니다.
   c. 검색 탭에서 포털 검색 또는 포털 추가 를 클릭한 다음 iSCSI 대상 포트의 IP 주소를 입력합니다.
   d. 대상 탭에서 검색된 대상을 선택한 다음 로그온 또는 연결을 클릭합니다.
   e. 다중 경로 활성화 를 선택한 다음 컴퓨터가 시작될 때 이 연결 자동 복원 또는 즐겨찾기 대상 목록에 이 연결 추가 를 선택합니다. 고급 을 클릭합니다.
      - 참고: * Windows 호스트에는 클러스터의 각 노드에 대한 iSCSI 연결이 있어야 합니다. 기본 DSM은 가장 적합한 경로를 선택합니다.

SVM(스토리지 가상 머신)의 LUN은 Windows 호스트에 디스크로 표시됩니다. 추가된 새 디스크는 호스트에서 자동으로 검색되지 않습니다. 수동 재검색을 트리거하여 다음 단계를 수행하여 디스크를 검색합니다.

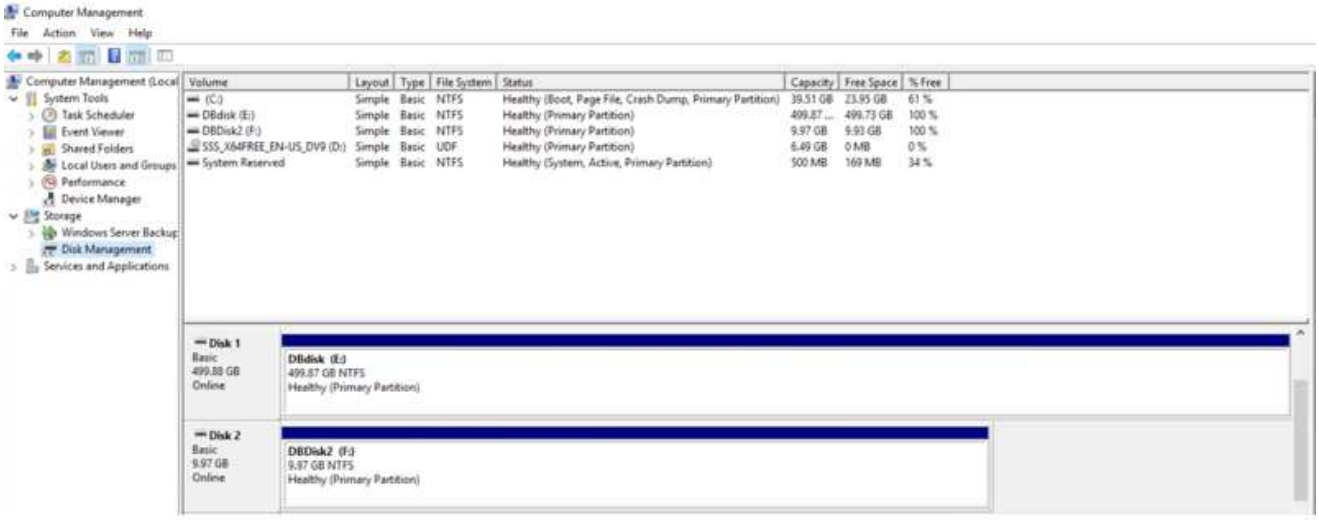
1. 시작 > 관리 도구 > 컴퓨터 관리를 차례로 클릭하여 Windows 컴퓨터 관리 유틸리티를 엽니다.
2. 탐색 트리에서 스토리지 노드를 확장합니다.
3. 디스크 관리를 클릭합니다.
4. 작업 > 디스크 다시 검사 를 클릭합니다.

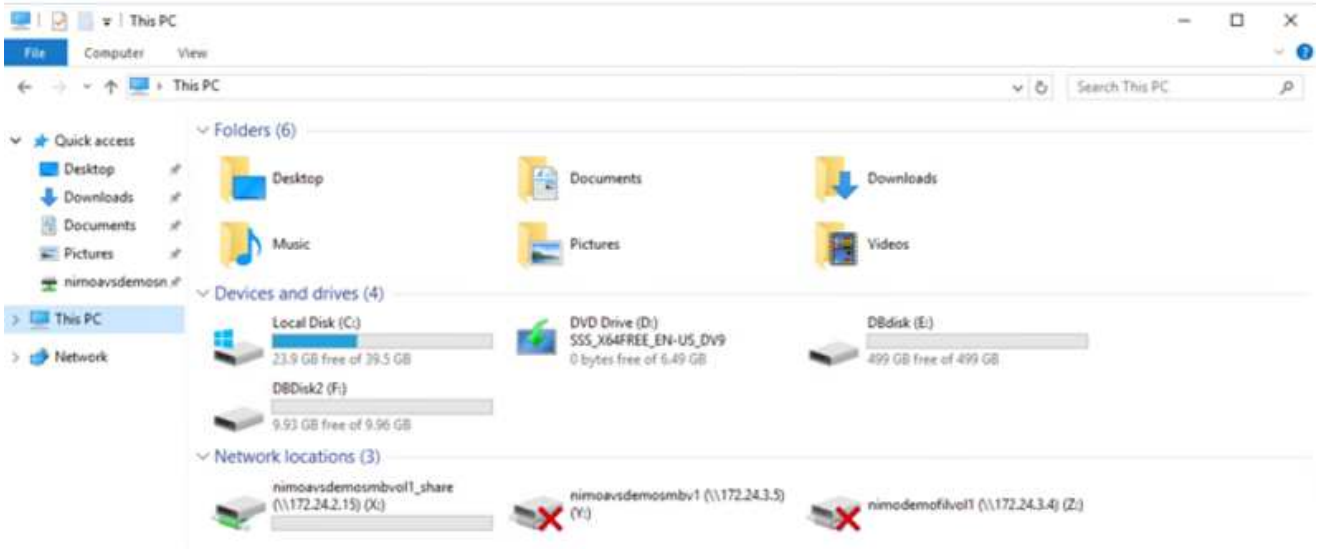


Windows 호스트에서 새 LUN을 처음 액세스할 때 파티션이나 파일 시스템이 없습니다. LUN을 초기화하고 필요에 따라 다음 단계를 완료하여 파일 시스템으로 LUN을 포맷합니다.

1. Windows 디스크 관리를 시작합니다.

2. LUN을 마우스 오른쪽 버튼으로 클릭한 다음 필요한 디스크 또는 파티션 유형을 선택합니다.
3. 마법사의 지침을 따릅니다. 이 예에서는 드라이브 E:가 마운트되었습니다



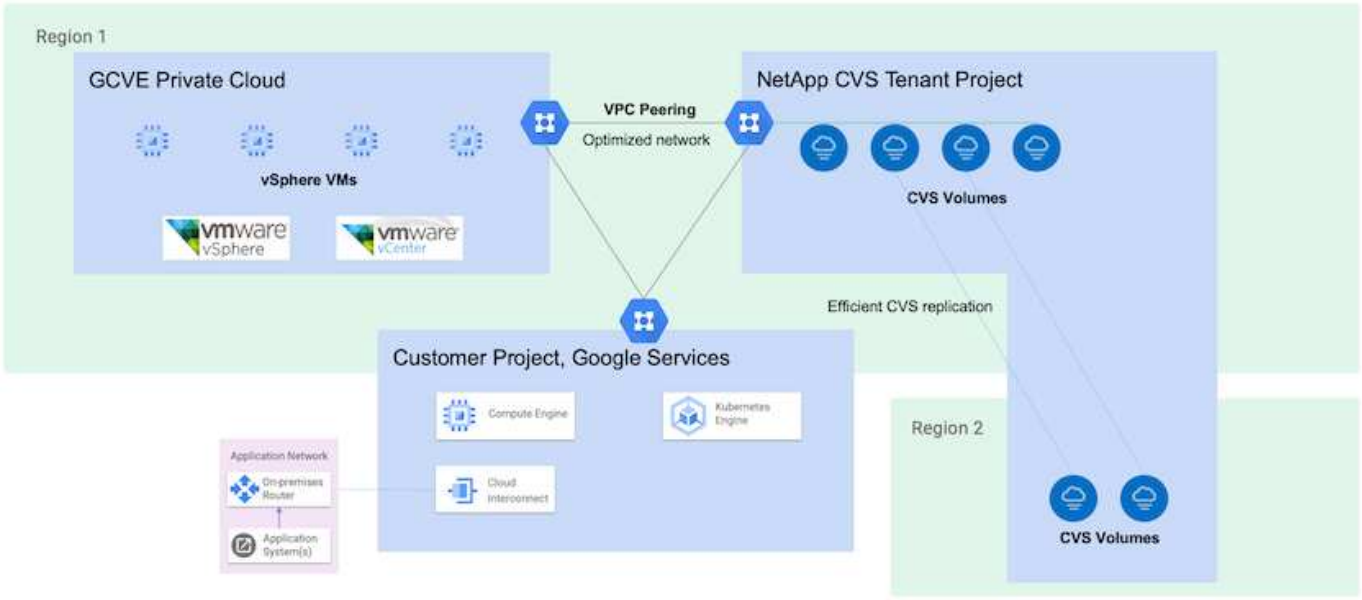


Google Cloud VMware Engine NetApp 클라우드 볼륨 서비스 기반 **NFS** 데이터 저장소를 보완해 줍니다

개요

저자: NetApp Suesh Thoppay

Google Cloud VMware Engine(GCVE) 환경에서 추가 스토리지 용량이 필요한 고객은 NetApp Cloud Volume Service를 활용하여 보조 NFS 데이터 저장소로 마운트할 수 있습니다.
NetApp Cloud Volume Service에 데이터를 저장하면 고객이 지역 간에 데이터를 복제하여 디aster를 보호할 수 있습니다.



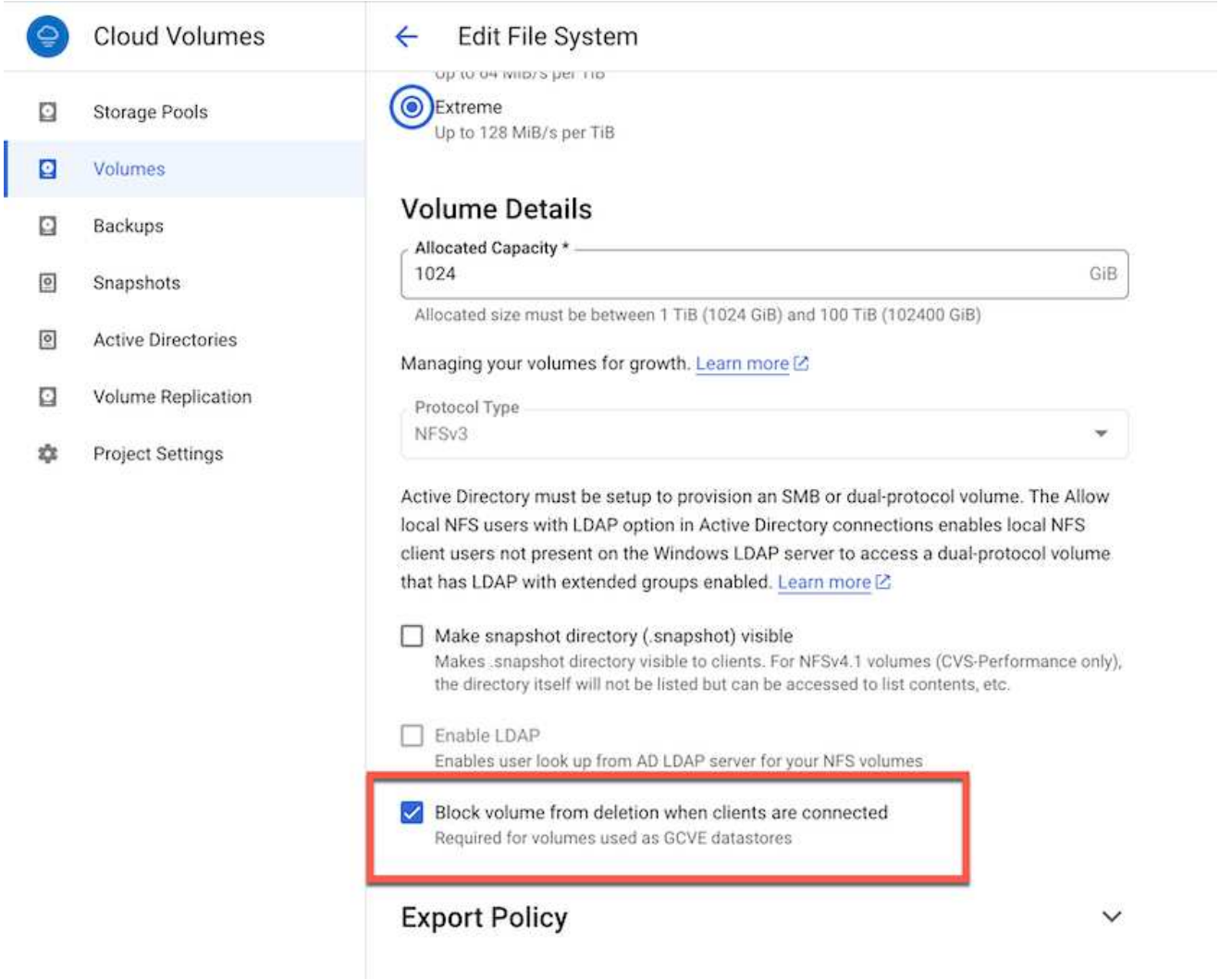
GCVE에서 **NetApp CVS**에서 **NFS** 데이터 저장소를 마운트하는 배포 단계

프로비저닝 **CVS -** 성능 볼륨

NetApp 클라우드 볼륨 서비스 볼륨은 에서 프로비저닝할 수 있습니다
"Google Cloud Console 사용"
"NetApp BlueXP 포털 또는 API 사용"

CVS 볼륨을 삭제할 수 없는 것으로 표시합니다

VM이 실행되는 동안 실수로 볼륨이 삭제되는 것을 방지하려면 아래 스크린샷과 같이 볼륨이 삭제할 수 없는 것으로 표시되어 있는지 확인합니다.



자세한 내용은 을 참조하십시오 "NFS 볼륨 생성 중" 문서화:

NetApp CVS 테넌트 **VPC**용 **GCVE**에 대한 개인 연결이 있는지 확인합니다**.**

NFS 데이터 저장소를 마운트하려면 GCVE와 NetApp CVS 프로젝트 사이에 전용 연결이 있어야 합니다. 자세한 내용은 을 참조하십시오 "개인 서비스 액세스를 설정하는 방법"

NFS 데이터 저장소를 마운트합니다

GCVE에서 NFS 데이터 저장소를 마운트하는 방법에 대한 자세한 내용은 을 참조하십시오 "NetApp CVS를 사용하여 NFS 데이터 저장소를 생성하는 방법"

vSphere 호스트가 Google에서 관리되기 때문에 NFS VAAI(vSphere API for Array Integration) VIB(vSphere 설치 번들)를 설치할 액세스 권한이 없습니다.
VVOL(가상 볼륨)에 대한 지원이 필요한 경우 알려주십시오.
점보 프레임을 사용하려면 을 참조하십시오 "GCP에서 지원되는 최대 MTU 크기입니다"

NetApp 클라우드 볼륨 서비스로 절감

GCVE에 대한 저장소 요구에 대해 NetApp 클라우드 볼륨 서비스를 통해 절감할 수 있는 잠재력에 대해 자세히 알아보려면 을(를) 확인하십시오 "NetApp ROI 계산기"

참조 링크

- "Google 블로그 - NetApp CVS를 Google Cloud VMware Engine용 데이터 저장소로 사용하는 방법"
- "NetApp 블로그 - 스토리지가 풍부한 앱을 Google 클라우드로 마이그레이션하는 더 나은 방법입니다"

GCP용 **NetApp** 스토리지 옵션

GCP는 CVO(Cloud Volumes ONTAP) 또는 CVS(Cloud Volumes Service)를 통해 게스트 연결 NetApp 스토리지를 지원합니다.

CVO(Cloud Volumes ONTAP)

Cloud Volumes ONTAP, 즉 CVO는 NetApp의 ONTAP 스토리지 소프트웨어를 기반으로 하는 업계 최고의 클라우드 데이터 관리 솔루션으로, AWS(Amazon Web Services), Microsoft Azure 및 GCP(Google Cloud Platform)에서 기본적으로 제공됩니다.

ONTAP의 소프트웨어 정의 버전이며 클라우드 네이티브 스토리지를 사용합니다. 따라서 클라우드와 사내에서 동일한 스토리지 소프트웨어를 사용할 수 있으므로 데이터를 관리하는 새로운 방법을 통해 IT 직원을 재교육할 필요가 없습니다.

CVO를 사용하면 데이터를 에지에서 데이터 센터, 클라우드로 원활하게 이동하고 다시 가져올 수 있습니다. 또한 단일 창 관리 콘솔인 NetApp Cloud Manager를 사용하여 하이브리드 클라우드를 통합할 수 있습니다.

설계상 CVO는 최고 성능과 고급 데이터 관리 기능을 제공하여 클라우드에서 가장 까다로운 애플리케이션도 충족합니다

CVO(Cloud Volumes ONTAP)를 게스트 연결 스토리지로 사용합니다

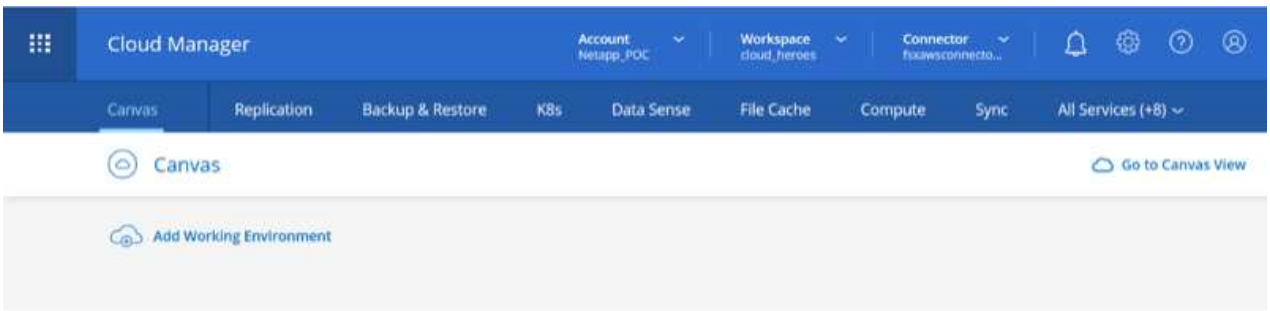
Google Cloud에 Cloud Volumes ONTAP 배포(직접 수행)

Cloud Volumes ONTAP 공유 및 LUN은 GCVE 프라이빗 클라우드 환경에서 생성된 VM에서 마운트할 수 있습니다. Cloud Volumes ONTAP는 iSCSI, SMB 및 NFS 프로토콜을 지원하기 때문에 iSCSI를 통해 마운트할 때 Linux 또는 Windows 클라이언트에서 볼륨을 Linux 클라이언트 및 Windows 클라이언트에 블록 디바이스로 마운트할 수 있습니다. Cloud Volumes ONTAP 볼륨은 몇 가지 간단한 단계를 통해 설정할 수 있습니다.

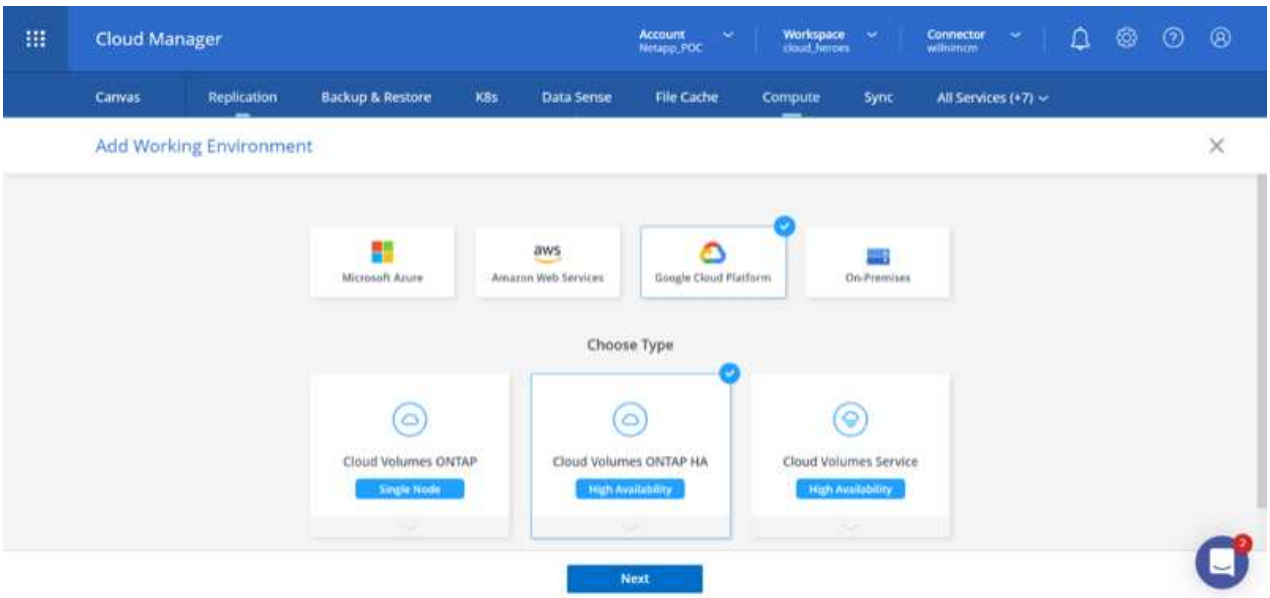
재해 복구 또는 마이그레이션을 위해 사내 환경에서 클라우드로 볼륨을 복제하려면 사이트 간 VPN 또는 Cloud Interconnect를 사용하여 Google Cloud에 대한 네트워크 연결을 설정합니다. 사내의 데이터를 Cloud Volumes ONTAP로 복제하는 작업은 이 문서의 범위를 벗어납니다. 사내 시스템과 Cloud Volumes ONTAP 시스템 간에 데이터를 복제하려면 을 참조하십시오 xref:./ehc/"시스템 간 데이터 복제 설정".

사용 "Cloud Volumes ONTAP Sizer" Cloud Volumes ONTAP 인스턴스의 크기를 정확하게 지정합니다. 또한 Cloud Volumes ONTAP Sizer에서 입력으로 사용할 온프레미스 성능을 모니터링합니다.

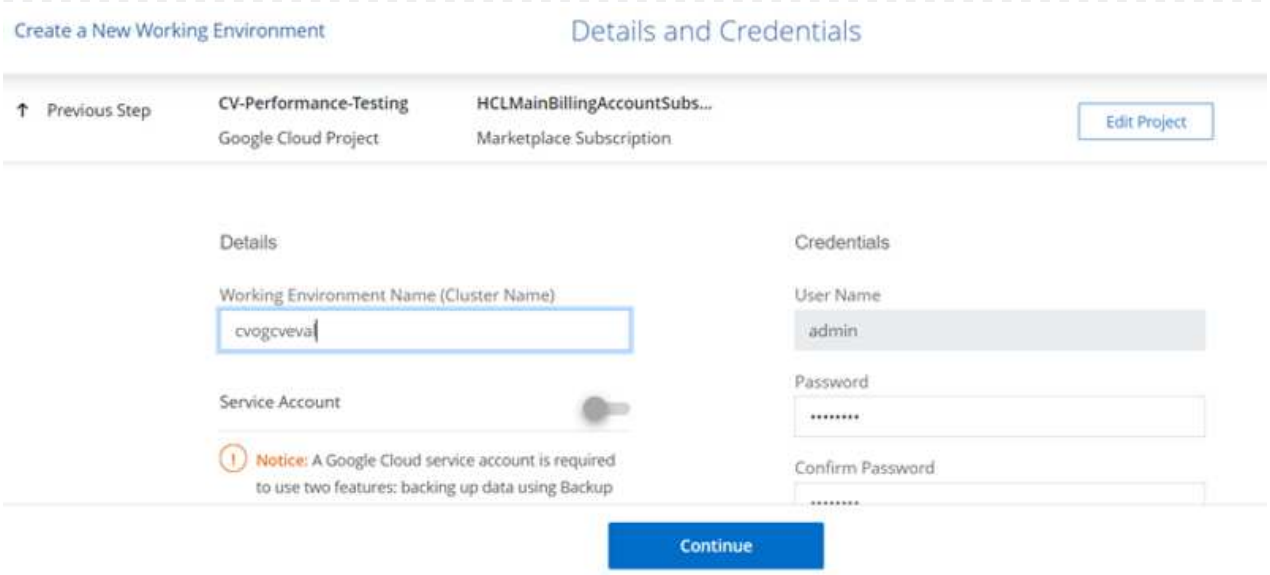
1. NetApp Cloud Central에 로그인 - 패브릭 보기 화면이 표시됩니다. Cloud Volumes ONTAP 탭을 찾아 Cloud Manager로 이동 을 선택합니다. 로그인하면 Canvas 화면이 표시됩니다.



2. Cloud Manager Canvas 탭에서 작업 환경 추가를 클릭한 다음 Google Cloud Platform을 클라우드로 선택하고 시스템 구성 유형을 선택합니다. 다음 을 클릭합니다.

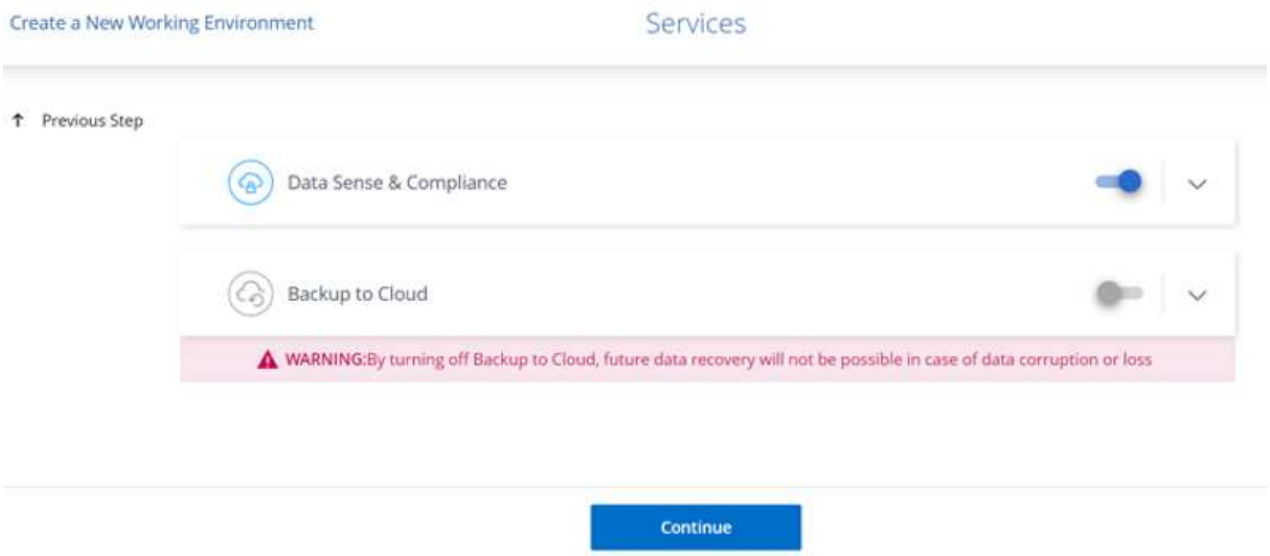


3. 환경 이름 및 관리자 자격 증명을 비롯하여 생성할 환경에 대한 세부 정보를 제공합니다. 작업을 마친 후 계속 을 클릭합니다.

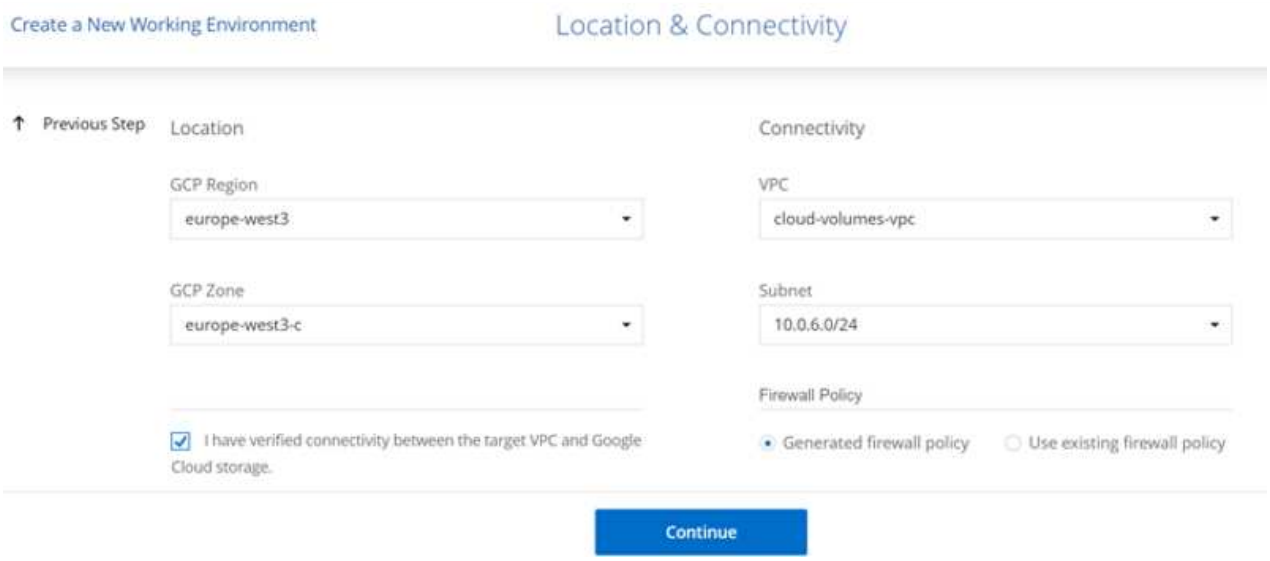


4. 데이터 감지 및 규정 준수, 클라우드 백업 등 Cloud Volumes ONTAP 구축을 위한 추가 서비스 를 선택하거나 선택 취소합니다. 그런 다음 계속 을 클릭합니다.

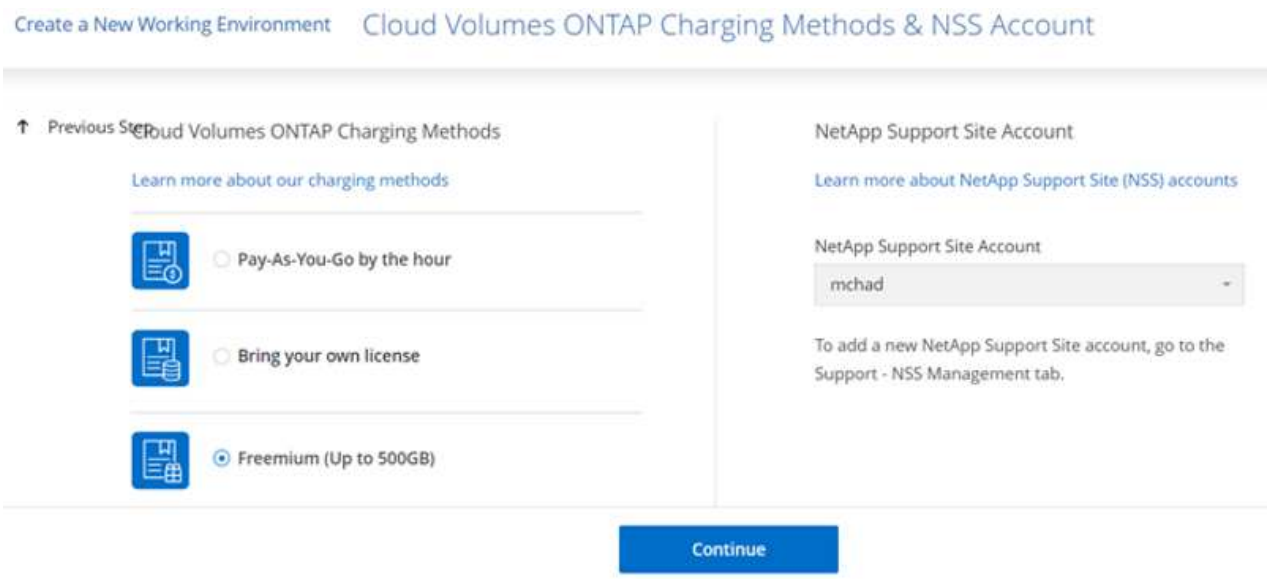
   힌트: 추가 서비스를 비활성화할 때 확인 팝업 메시지가 표시됩니다. 추가 서비스는 CVO 배포 후 추가/제거할 수 있습니다. 비용을 피하기 위해 처음부터 필요하지 않은 경우 선택을 취소하십시오.



5. 위치를 선택하고 방화벽 정책을 선택한 다음 확인란을 선택하여 Google Cloud 스토리지에 대한 네트워크 연결을 확인합니다.

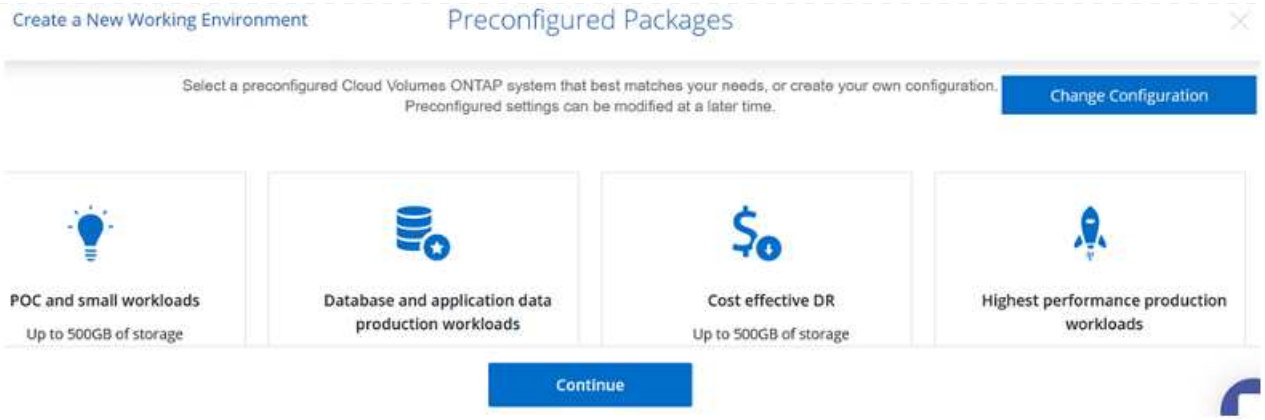


6. 라이센스 옵션 선택: 사용한 만큼만 지불 또는 BYOL 방식으로 기존 라이센스 사용 이 예제에서는 Freemium 옵션을 사용합니다. 그런 다음 계속 을 클릭합니다.

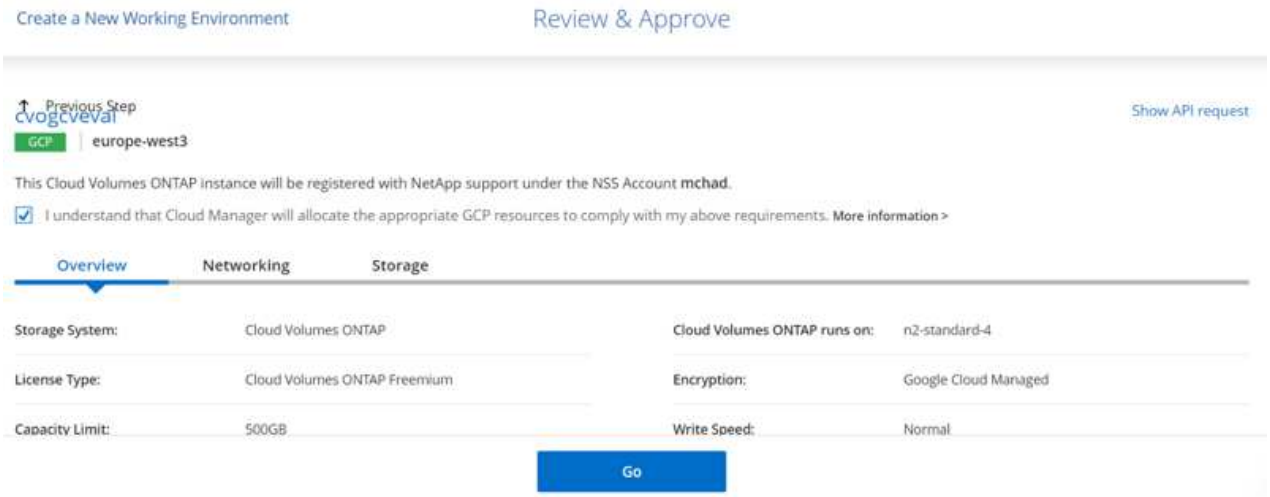


7. AWS SDDC 기반 VMware 클라우드에서 실행되는 VM에 구축할 워크로드의 유형에 따라 사용할 수 있는 사전 구성된 패키지 몇 개 중 하나를 선택합니다.

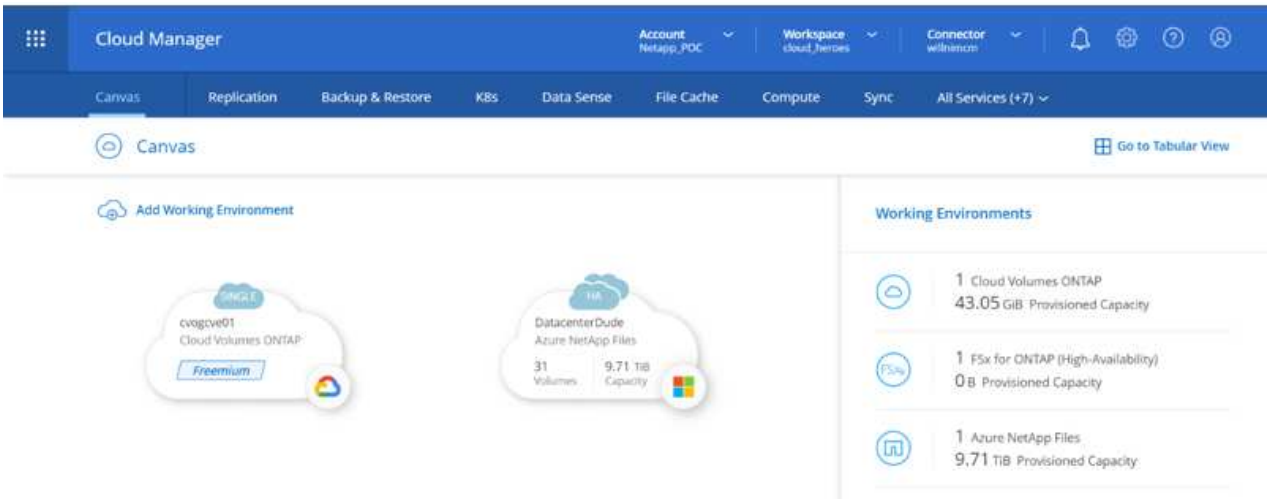
   힌트: 타일 위로 마우스를 가져가 세부 정보를 보거나 구성 변경 을 클릭하여 CVO 구성 요소 및 ONTAP 버전을 사용자 지정합니다.



8. 검토 및 승인 페이지에서 선택 항목을 검토하고 확인합니다. Cloud Volumes ONTAP 인스턴스를 만들려면 이동을 클릭합니다.



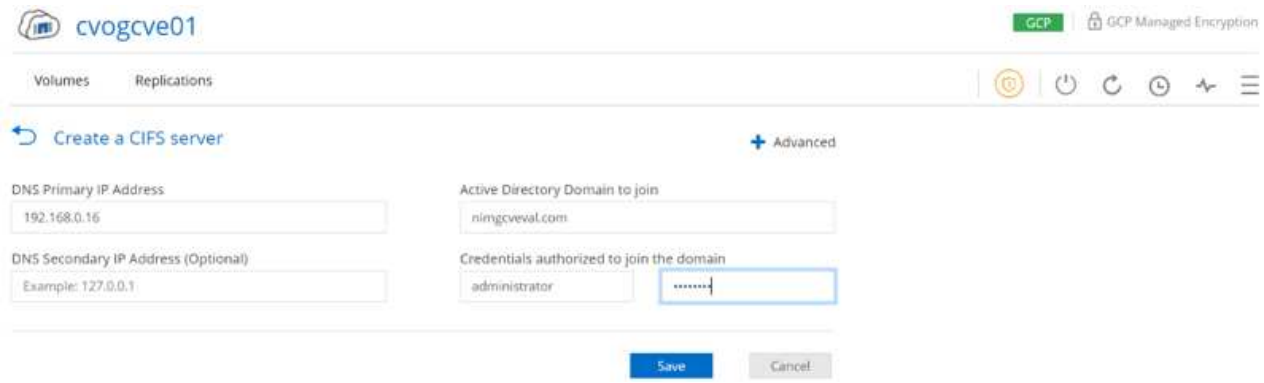
9. Cloud Volumes ONTAP를 프로비저닝하면 Canvas 페이지의 작업 환경에 나열됩니다.



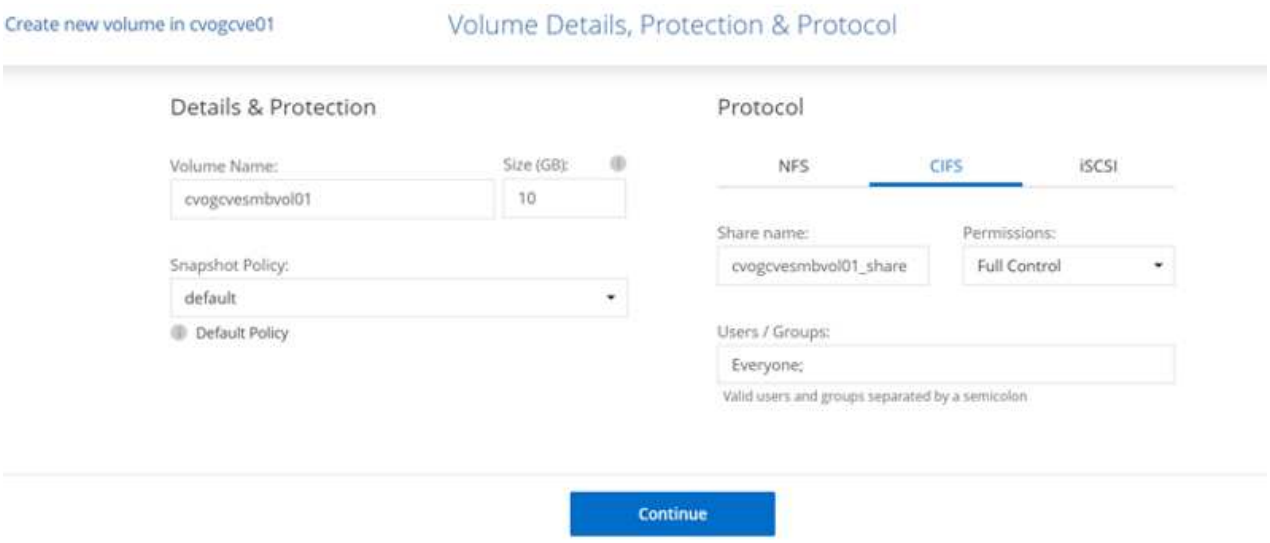
SMB 볼륨을 위한 추가 구성

1. 작업 환경이 준비되면 CIFS 서버가 적절한 DNS 및 Active Directory 구성 매개 변수로 구성되어 있는지 확인합니다. 이 단계는 SMB 볼륨을 생성하기 전에 필요합니다.

   힌트: 메뉴 아이콘(º)을 클릭하고 고급을 선택하여 더 많은 옵션을 표시하고 CIFS 설정을 선택합니다.



2. SMB 볼륨을 생성하는 것은 쉬운 프로세스입니다. Canvas에서 Cloud Volumes ONTAP 작업 환경을 두 번 클릭하여 볼륨을 생성 및 관리하고 볼륨 생성 옵션을 클릭합니다. 적절한 크기를 선택하고 클라우드 관리자가 포함하는 애그리게이트를 선택하거나, 고급 할당 메커니즘을 사용하여 특정 애그리게이트에 배치할 수 있습니다. 이 데모에서는 CIFS/SMB가 프로토콜로 선택됩니다.

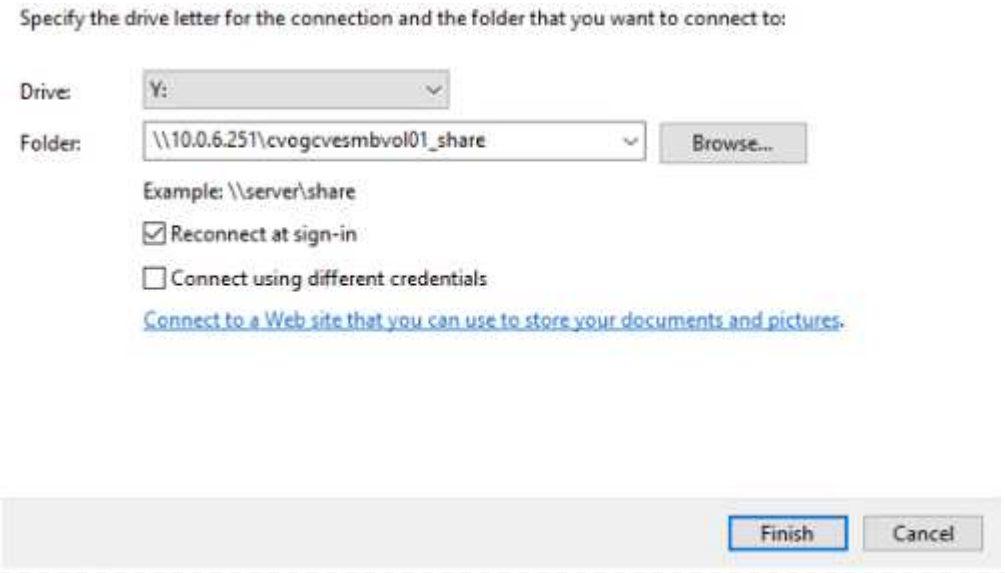


3. 볼륨 용량 할당 후 볼륨 창 아래에서 사용할 수 있습니다. CIFS 공유가 프로비저닝되므로 사용자 또는 그룹에 파일 및 폴더에 대한 권한을 제공하고 해당 사용자가 공유를 액세스하고 파일을 생성할 수 있는지 확인합니다. 파일 및 폴더 권한이 모두 SnapMirror 복제의 일부로 유지되므로 볼륨이 사내 환경에서 복제된 경우에는 이 단계가 필요하지 않습니다.

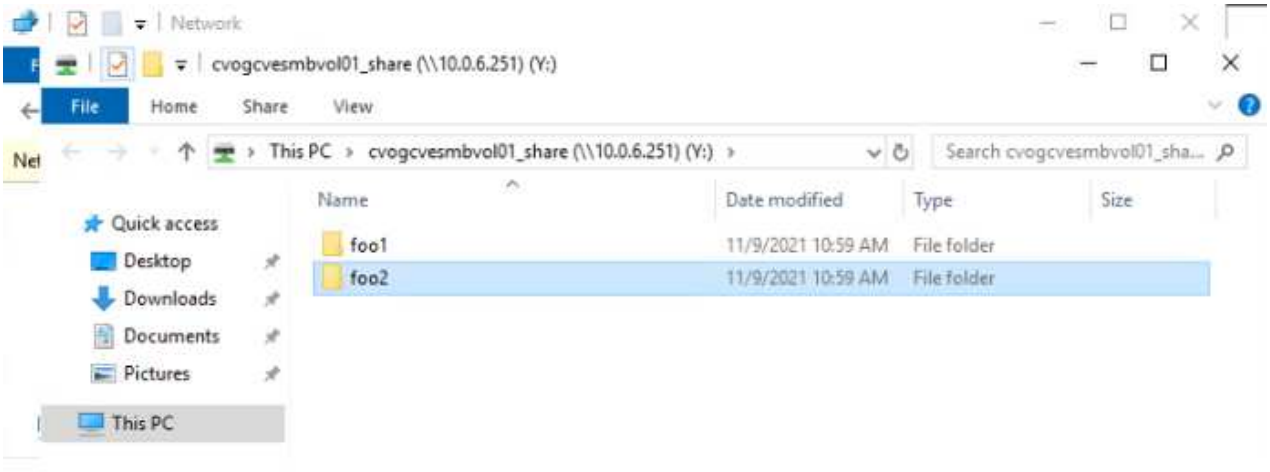
   힌트: 볼륨 메뉴(º)를 클릭하여 옵션을 표시합니다.

4. 볼륨을 생성한 후 mount 명령을 사용하여 볼륨 연결 지침을 표시한 다음 Google Cloud VMware Engine의 VM에서 공유에 연결합니다.

5. 다음 경로를 복사하고 네트워크 드라이브 매핑 옵션을 사용하여 Google Cloud VMware Engine에서 실행 중인 VM에 볼륨을 마운트합니다.



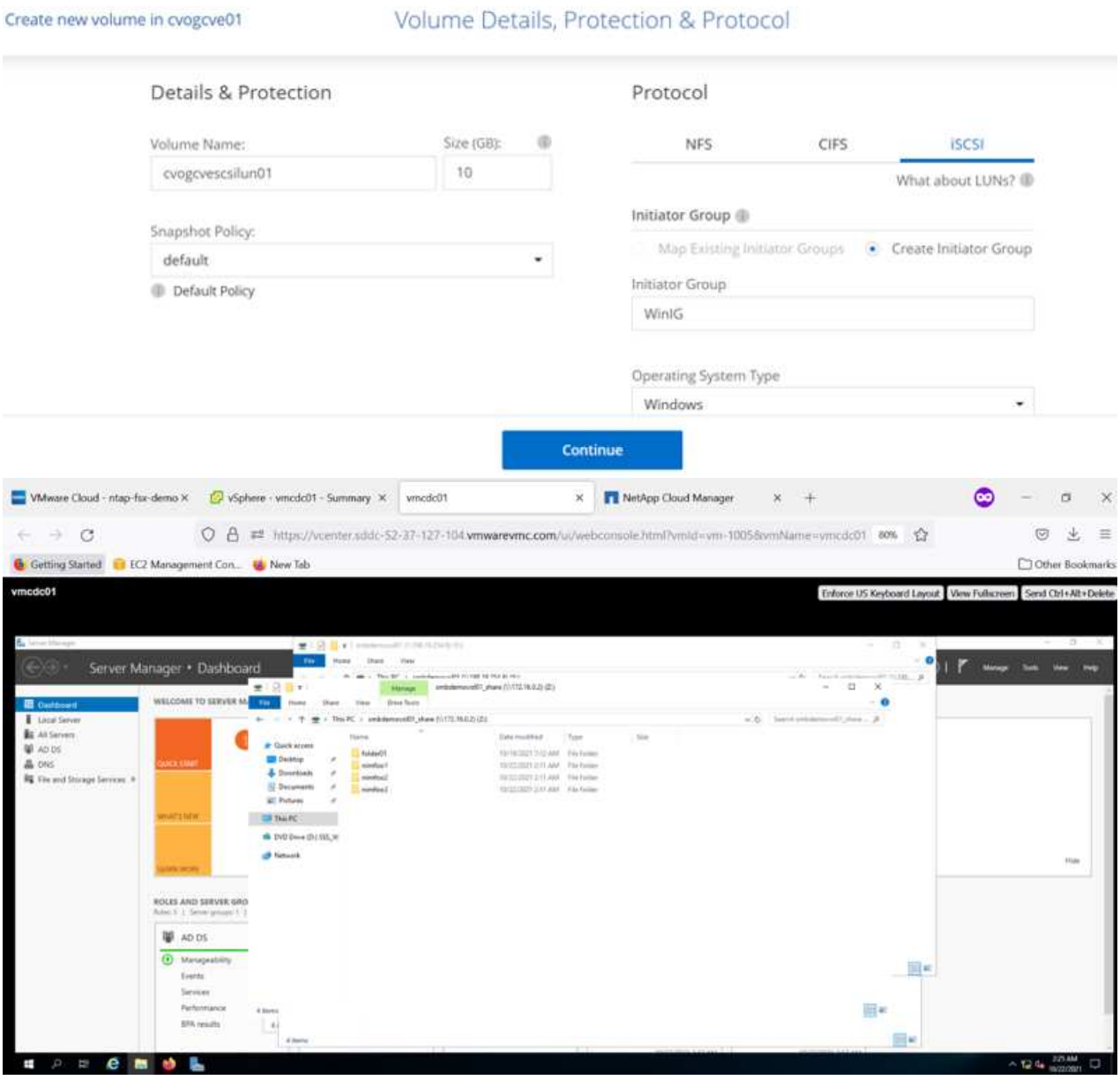
매핑되면 쉽게 액세스할 수 있으며 NTFS 권한을 적절하게 설정할 수 있습니다.



Cloud Volumes ONTAP의 **LUN**을 호스트에 연결합니다

Cloud Volumes ONTAP LUN을 호스트에 연결하려면 다음 단계를 수행하십시오.

1. Canvas 페이지에서 Cloud Volumes ONTAP 작업 환경을 두 번 클릭하여 볼륨을 생성하고 관리합니다.
2. 볼륨 추가 > 새 볼륨 을 클릭하고 iSCSI 를 선택한 다음 이니시에이터 그룹 생성 을 클릭합니다. 계속 을 클릭합니다.



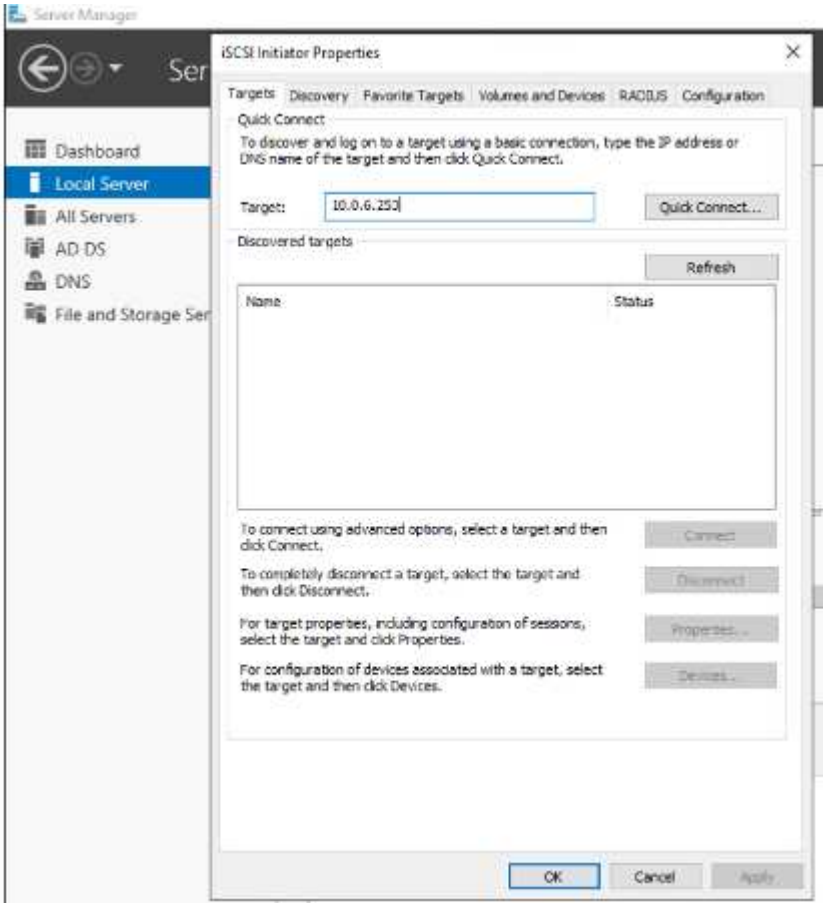
3. 볼륨이 프로비저닝되면 볼륨 메뉴(⁰)를 선택한 다음 대상 IQN을 클릭합니다. IQN(iSCSI Qualified Name)을 복사하려면 Copy(복사)를 클릭합니다. 호스트에서 LUN으로의 iSCSI 접속을 설정합니다.

Google Cloud VMware Engine에 상주하는 호스트에 대해 동일한 작업을 수행하려면 다음을 수행합니다.

1. Google Cloud VMware Engine에서 호스팅되는 VM에 대한 RDP
2. iSCSI 초기자 속성 대화 상자(서버 관리자 > 대시보드 > 도구 > iSCSI 초기자)를 엽니다.

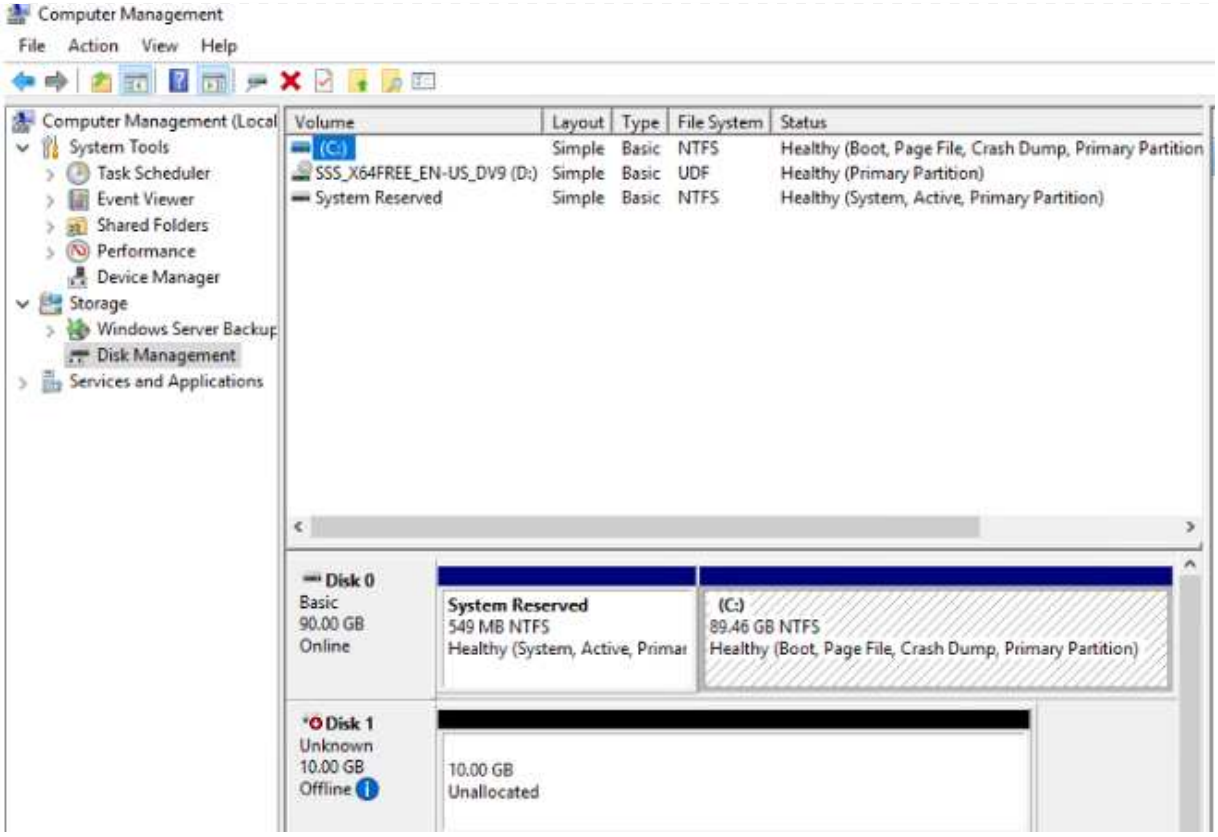
3. 검색 탭에서 포털 검색 또는 포털 추가 를 클릭한 다음 iSCSI 대상 포트의 IP 주소를 입력합니다.
4. 대상 탭에서 검색된 대상을 선택한 다음 로그온 또는 연결을 클릭합니다.
5. 다중 경로 활성화 를 선택한 다음 컴퓨터가 시작될 때 이 연결 자동 복원 또는 즐겨찾기 대상 목록에 이 연결 추가 를 선택합니다. 고급 을 클릭합니다.

> Windows 호스트에는 클러스터의 각 노드에 대한 iSCSI 연결이 있어야 합니다. 기본 DSM은 가장 적합한 경로를 선택합니다.



SVM(스토리지 가상 머신)의 LUN은 Windows 호스트에 디스크로 표시됩니다. 추가된 새 디스크는 호스트에서 자동으로 검색되지 않습니다. 수동 재검색을 트리거하여 다음 단계를 수행하여 디스크를 검색합니다.

a. 시작 > 관리 도구 > 컴퓨터 관리를 차례로 클릭하여 Windows 컴퓨터 관리 유틸리티를 엽니다.
b. 탐색 트리에서 스토리지 노드를 확장합니다.
c. 디스크 관리를 클릭합니다.
d. 작업 > 디스크 다시 검사 를 클릭합니다.

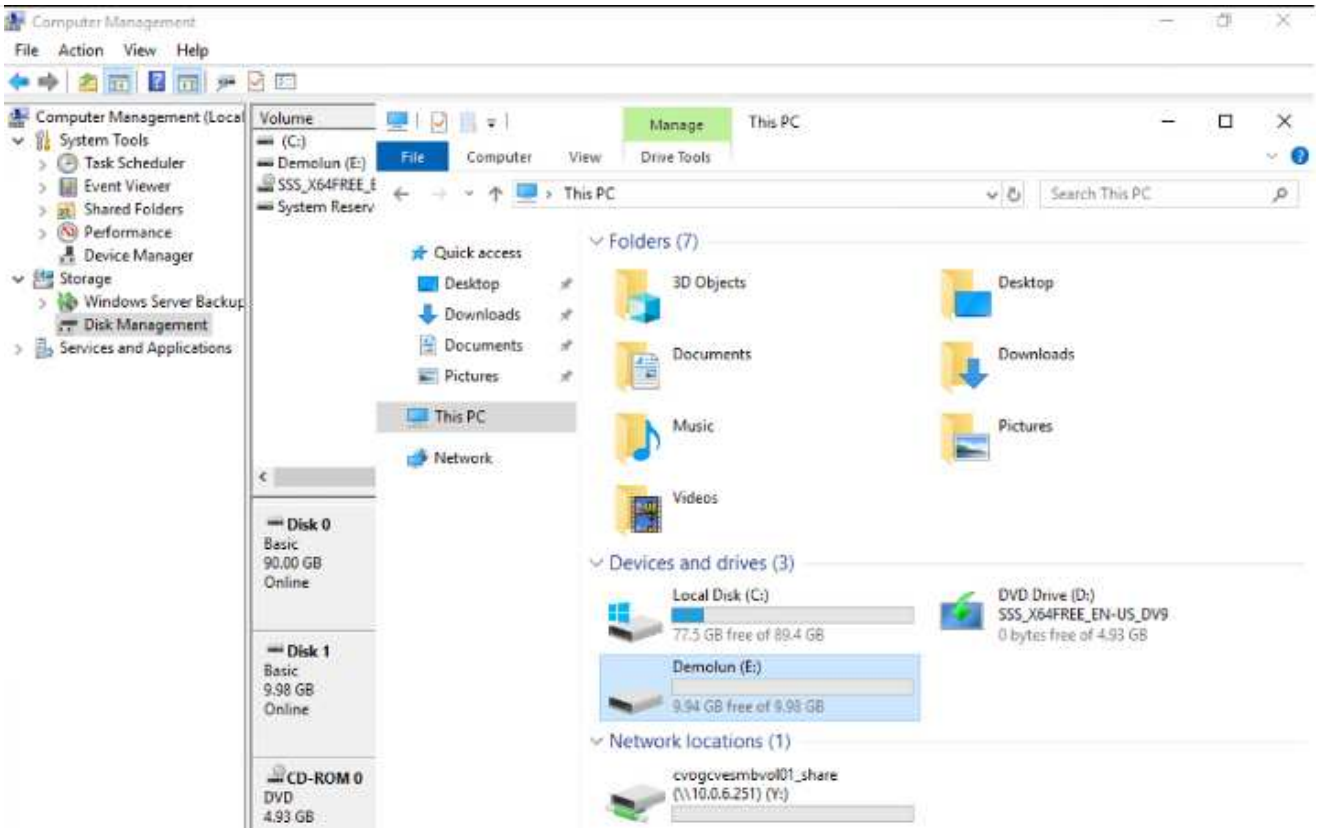


Windows 호스트에서 새 LUN을 처음 액세스할 때 파티션이나 파일 시스템이 없습니다. LUN을 초기화하고 필요에 따라 다음 단계를 완료하여 파일 시스템으로 LUN을 포맷합니다.

a. Windows 디스크 관리를 시작합니다.

b. LUN을 마우스 오른쪽 버튼으로 클릭한 다음 필요한 디스크 또는 파티션 유형을 선택합니다.

c. 마법사의 지침을 따릅니다. 이 예에서는 드라이브 F:가 마운트되었습니다.



Linux 클라이언트에서 iSCSI 데몬이 실행되고 있는지 확인합니다. LUN을 프로비저닝한 후에는 여기에서 Ubuntu를 사용한 iSCSI 구성에 대한 자세한 지침을 참조하십시오. 확인하려면 셸에서 lsblk cmd 를 실행합니다.

```
niyaz@nimubu01:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 55.4M  1 loop /snap/core18/2128
loop1    7:1    0  219M  1 loop /snap/gnome-3-34-1804/72
loop2    7:2    0 65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0   51M  1 loop /snap/snap-store/547
loop4    7:4    0 32.3M  1 loop /snap/snapd/12704
loop5    7:5    0 32.5M  1 loop /snap/snapd/13640
loop6    7:6    0 55.5M  1 loop /snap/core18/2246
loop7    7:7    0    4K  1 loop /snap/bare/5
loop8    7:8    0 65.2M  1 loop /snap/gtk-common-themes/1519
sda      8:0    0   16G  0 disk
├─sda1   8:1    0  512M  0 part /boot/efi
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0 15.5G  0 part /
sdb      8:16   0    1G  0 disk
```

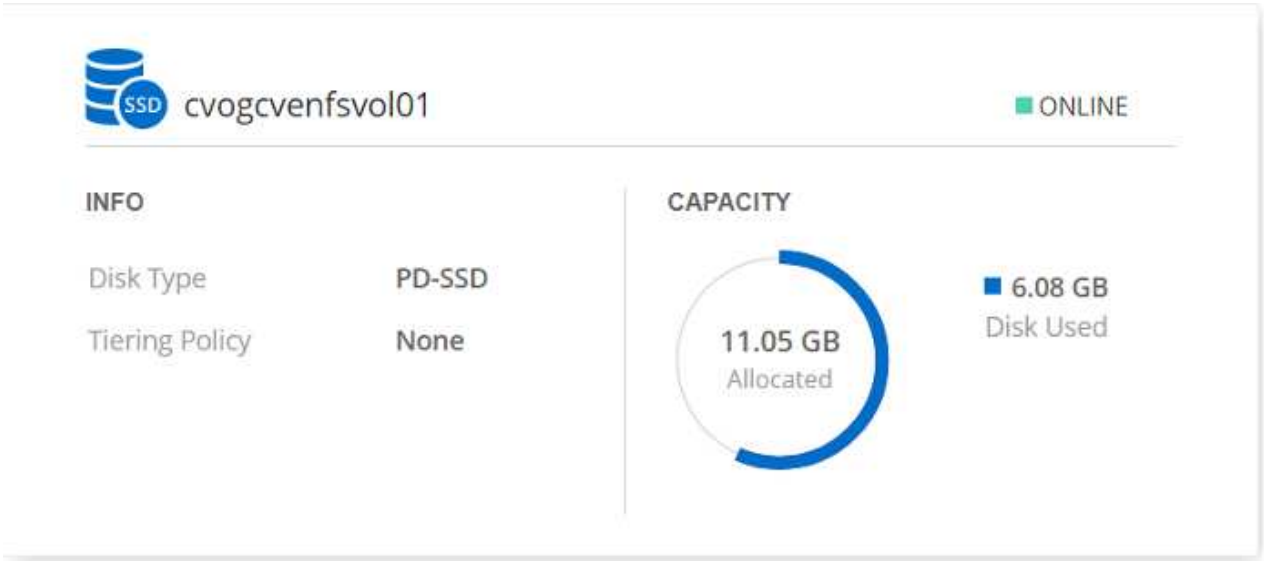
```
niyaz@nimubu01:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           394M  1.5M  392M   1% /run
/dev/sda5        16G  7.6G  6.9G  53% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1      219M  219M     0 100% /snap/gnome-3-34-1804/72
/dev/loop2       66M   66M     0 100% /snap/gtk-common-themes/1515
/dev/loop3       51M   51M     0 100% /snap/snap-store/547
/dev/loop0       56M   56M     0 100% /snap/core18/2128
/dev/loop4       33M   33M     0 100% /snap/snapd/12704
/dev/sda1       511M  4.0K  511M   1% /boot/efi
tmpfs           394M   64K  394M   1% /run/user/1000
/dev/loop5       33M   33M     0 100% /snap/snapd/13640
/dev/loop6       56M   56M     0 100% /snap/core18/2246
/dev/loop7      128K  128K     0 100% /snap/bare/5
/dev/loop8       66M   66M     0 100% /snap/gtk-common-themes/1519
/dev/sdb        976M  2.6M  907M   1% /mnt
```

Linux 클라이언트에 **Cloud Volumes ONTAP NFS** 볼륨을 마운트합니다

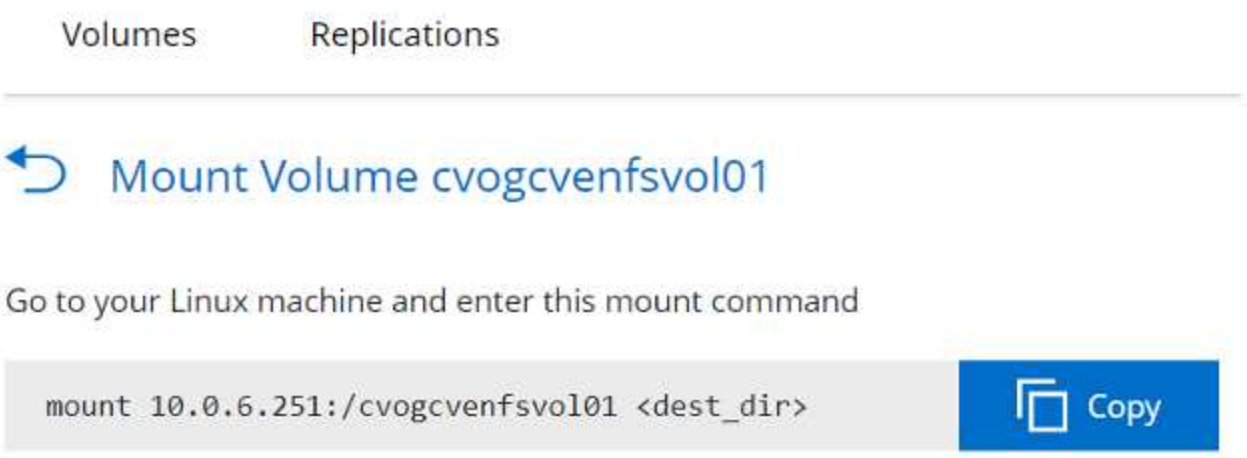
Google Cloud VMware Engine 내의 VM에서 DIY(Cloud Volumes ONTAP) 파일 시스템을 마운트하려면 다음 단계를 수행하십시오.

아래 단계에 따라 볼륨을 프로비저닝합니다

1. 볼륨 탭에서 새 볼륨 생성 을 클릭합니다.
2. 새 볼륨 생성 페이지에서 볼륨 유형을 선택합니다.



3. 볼륨 탭에서 마우스 커서를 볼륨 위에 놓고 메뉴 아이콘(°)을 선택한 다음 Mount Command를 클릭합니다.



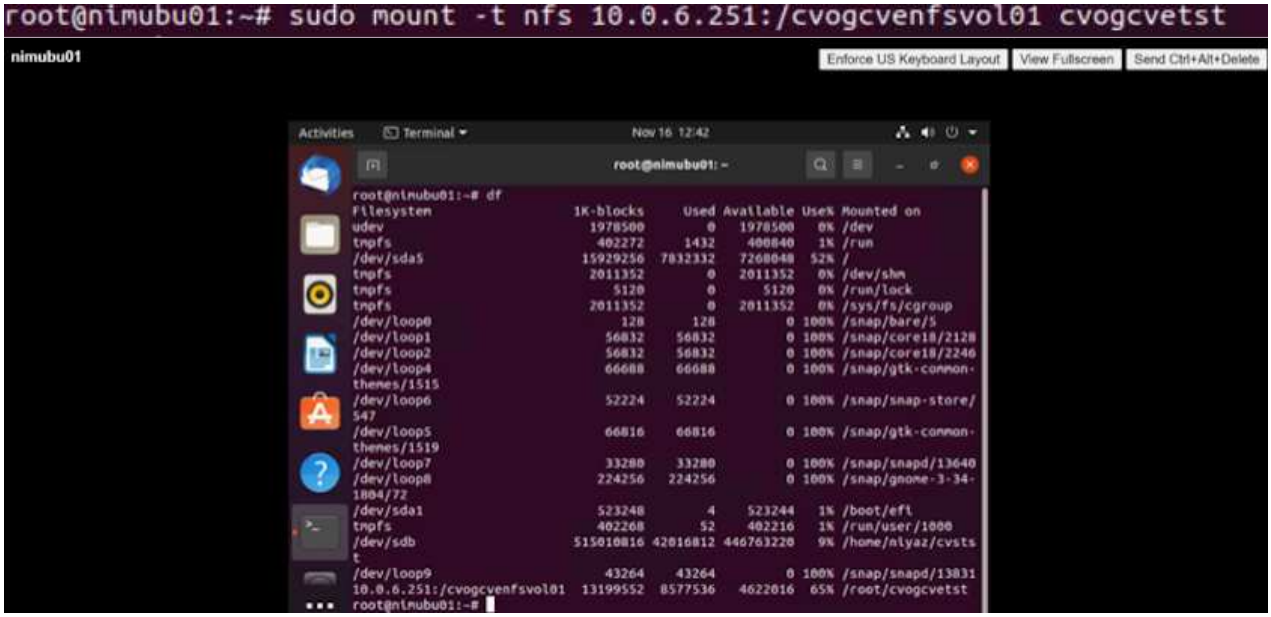
4. 복사를 클릭합니다.
5. 지정된 Linux 인스턴스에 연결합니다.
6. SSH(Secure Shell)를 사용하여 인스턴스의 터미널을 열고 적절한 자격 증명을 사용하여 로그인합니다.
7. 다음 명령을 사용하여 볼륨의 마운트 지점에 대한 디렉토리를 만듭니다.

```
$ sudo mkdir /cvogcvetst
```

```
root@nimubu01:~# sudo mkdir cvogcvetst
```

8. 이전 단계에서 생성한 디렉토리에 Cloud Volumes ONTAP NFS 볼륨을 마운트합니다.

```
sudo mount 10.0.6.251:/cvogcvenfsvol01 /cvogcvetst
```



CVS(Cloud Volumes Service)

CVS(Cloud Volumes Services)는 고급 클라우드 솔루션을 제공하는 완벽한 데이터 서비스 포트폴리오입니다. Cloud Volumes Services는 주요 클라우드 공급자를 위한 여러 파일 액세스 프로토콜(NFS 및 SMB 지원)을 지원합니다.

그 밖의 이점 및 기능: Snapshot을 통한 데이터 보호 및 복원, 온프레미스 또는 클라우드의 데이터 대상을 복제, 동기화, 마이그레이션할 수 있는 특별한 기능, 전용 플래시 스토리지 시스템 레벨에서 일관된 고성능 제공

CVS(Cloud Volumes Service)를 게스트 연결 스토리지로 사용합니다

VMware 엔진을 사용하여 Cloud Volumes Service를 구성합니다

Cloud Volumes Service 공유는 VMware 엔진 환경에서 생성된 VM에서 마운트할 수 있습니다. Cloud Volumes Service는 SMB 및 NFS 프로토콜을 지원하므로 Linux 클라이언트에 볼륨을 마운트하고 Windows 클라이언트에 매핑할 수도 있습니다. Cloud Volumes Service 볼륨은 간단한 단계를 통해 설정할 수 있습니다.

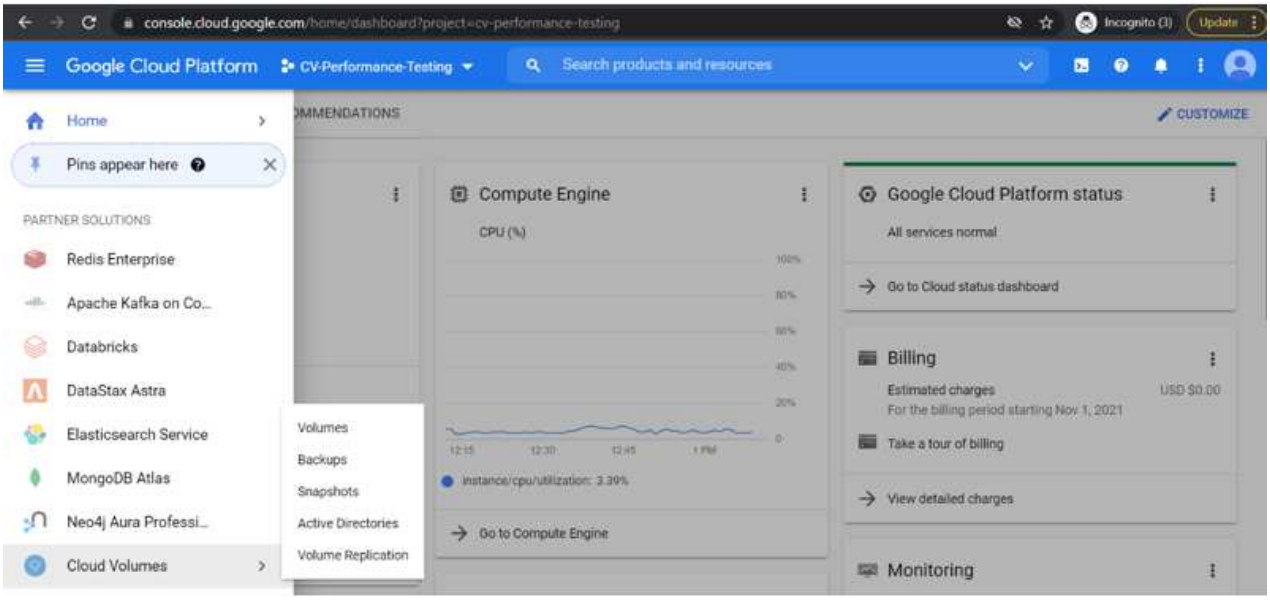
Cloud Volume Service 및 Google Cloud VMware Engine 프라이빗 클라우드는 같은 지역에 있어야 합니다.

Google Cloud Marketplace에서 NetApp Cloud Volumes Service for Google Cloud를 구매, 활성화 및 구성하려면 다음 세부 정보를 따르십시오 "가이드".

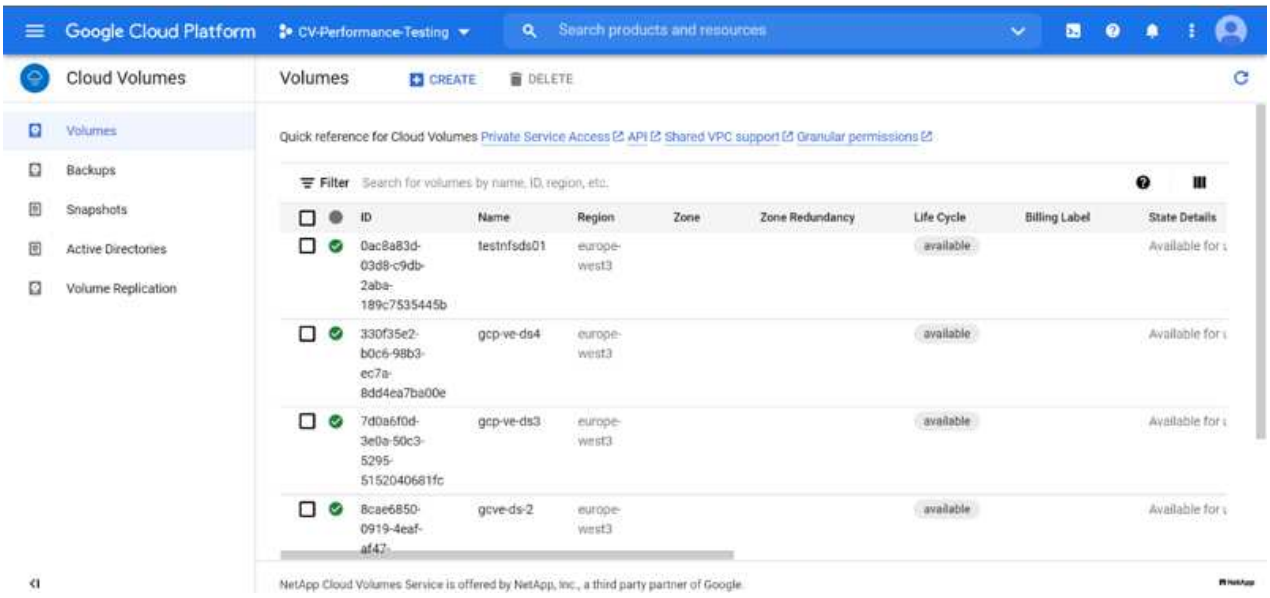
CVS NFS 볼륨을 GCVE 프라이빗 클라우드에 생성합니다

NFS 볼륨을 생성 및 마운트하려면 다음 단계를 수행하십시오.

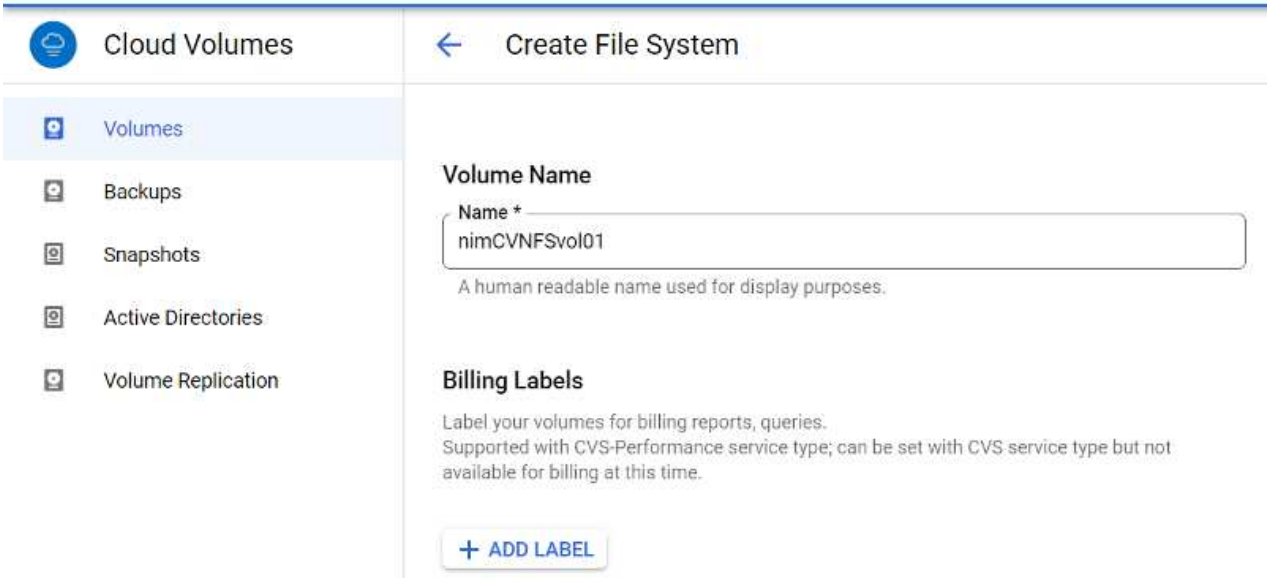
1. Google 클라우드 콘솔 내의 파트너 솔루션에서 Cloud Volumes에 액세스합니다.



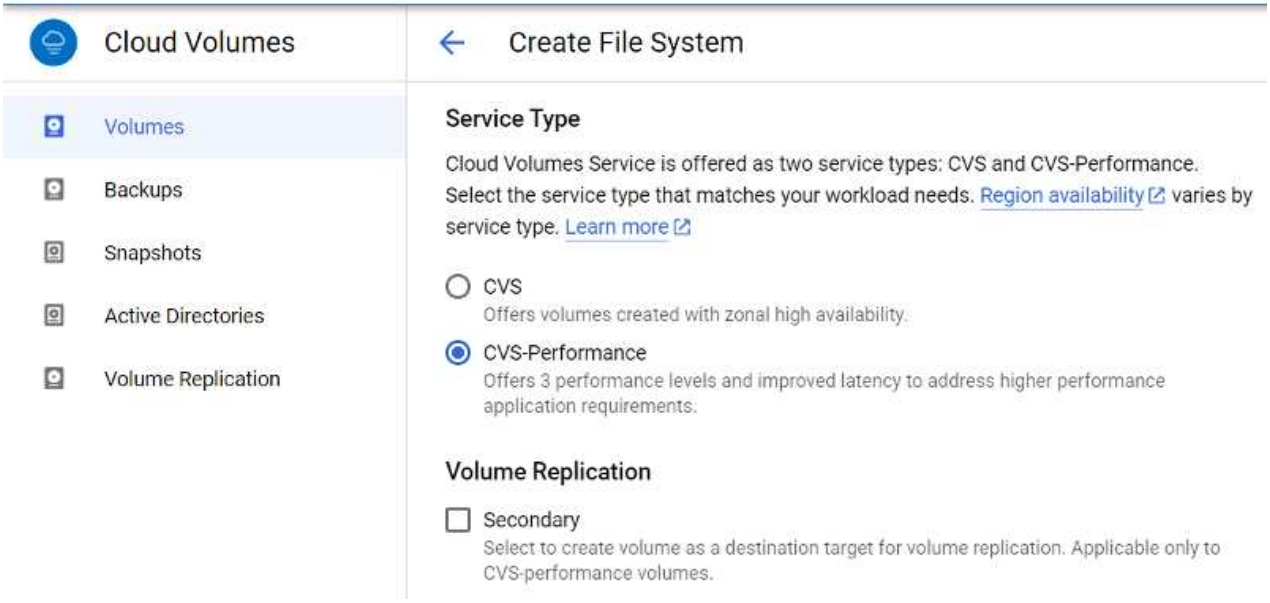
2. Cloud Volumes Console에서 Volumes 페이지로 이동하고 Create를 클릭합니다.



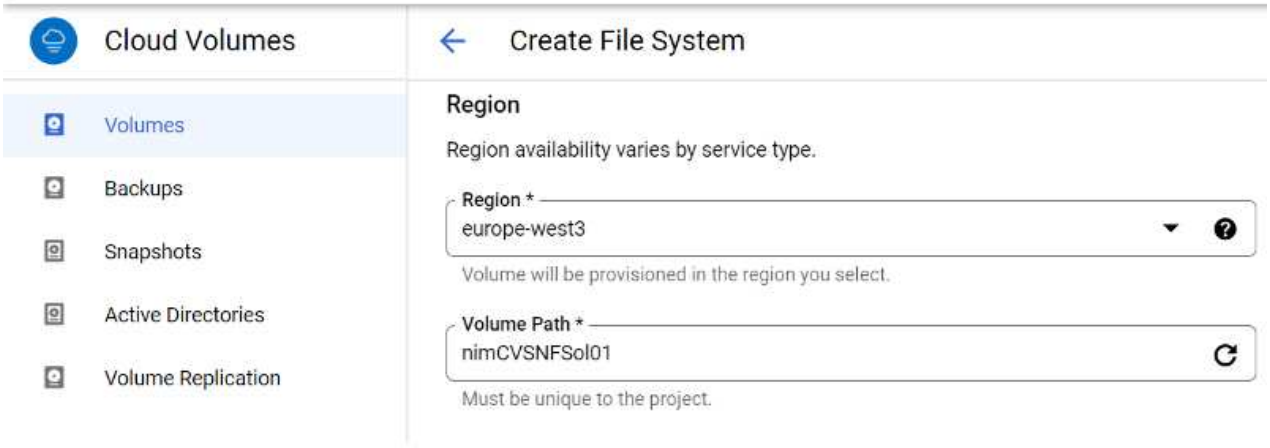
3. 파일 시스템 생성 페이지에서 차지백 메커니즘에 필요한 볼륨 이름 및 청구 레이블을 지정합니다.



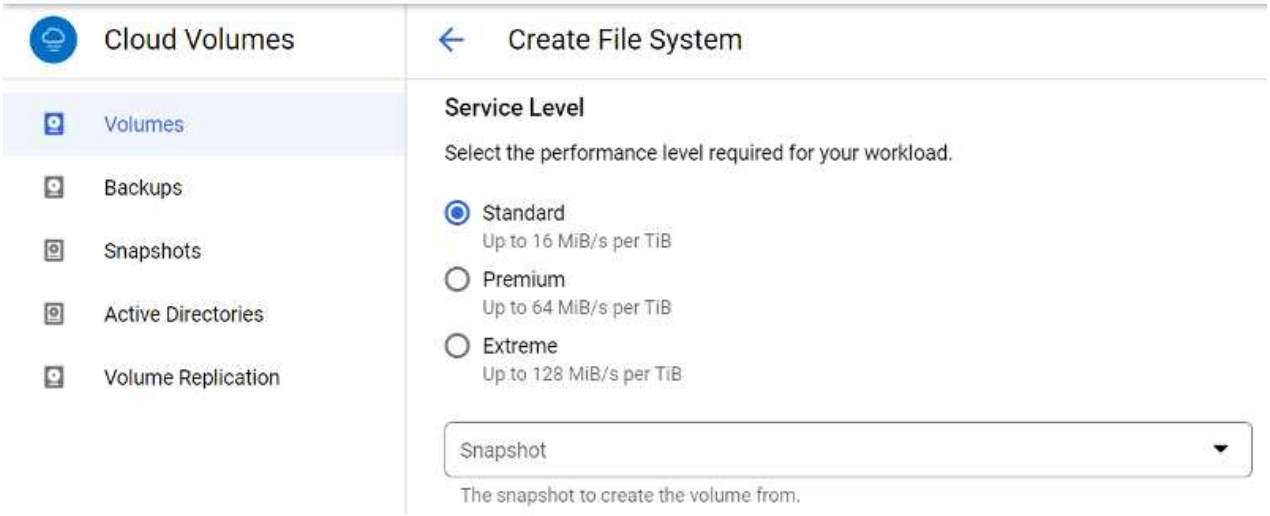
4. 적절한 서비스를 선택합니다. GCVE의 경우 애플리케이션 워크로드 요구 사항에 따라 지연 시간 및 성능 향상을 위해 CVS 성능 및 원하는 서비스 수준을 선택합니다.



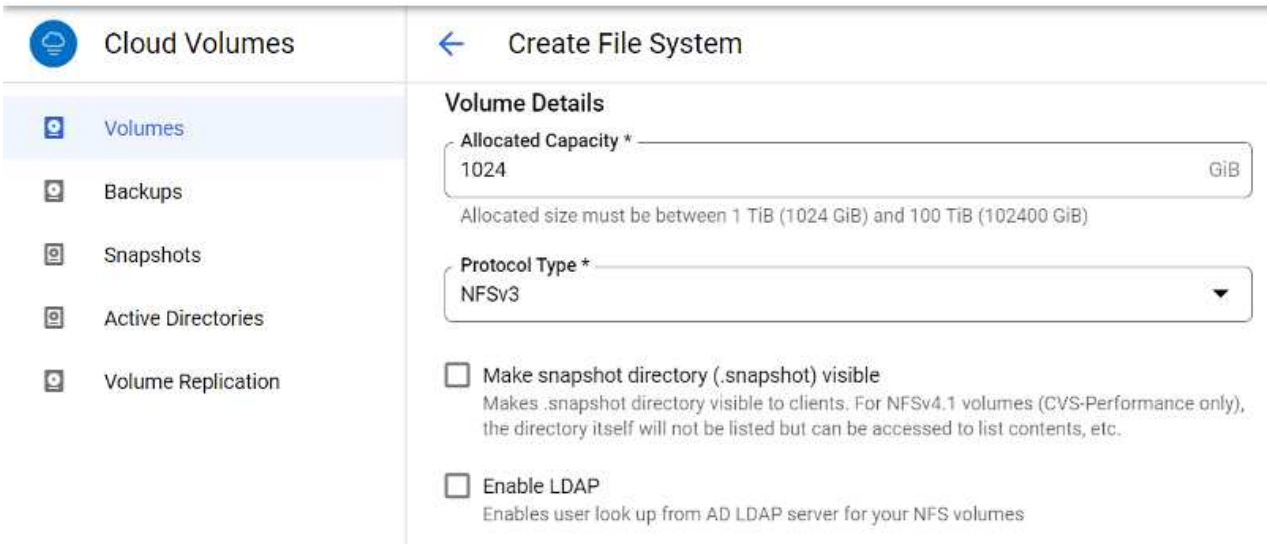
5. 볼륨 및 볼륨 경로에 대해 Google Cloud 영역을 지정합니다. 볼륨 경로는 프로젝트의 모든 클라우드 볼륨에서 고유해야 합니다.



6. 볼륨의 성능 수준을 선택합니다.

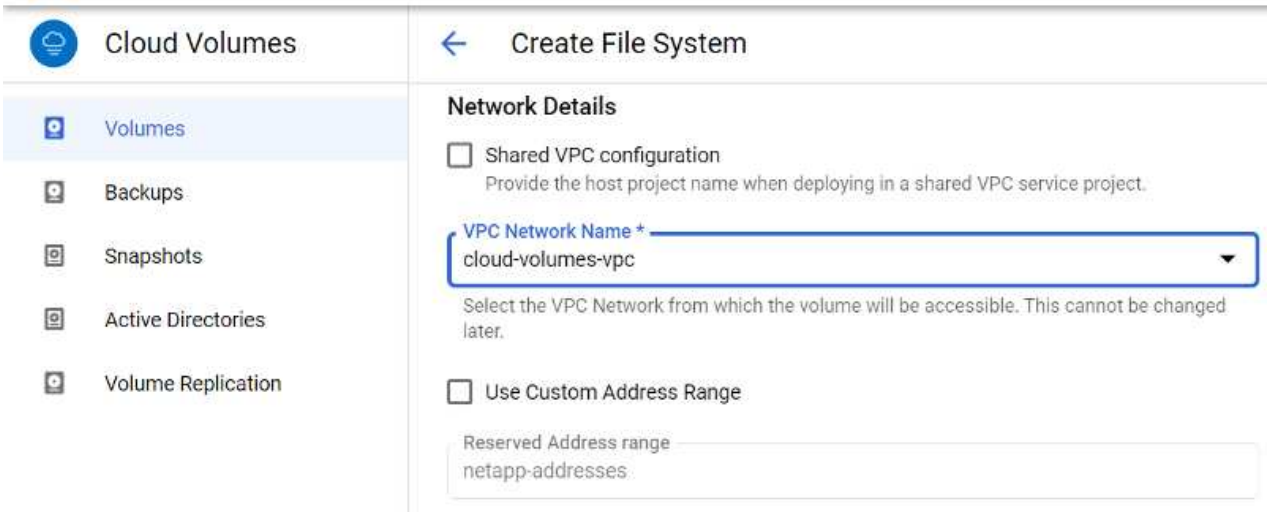


7. 볼륨의 크기와 프로토콜 유형을 지정합니다. 이 테스트에서는 NFSv3을 사용합니다.



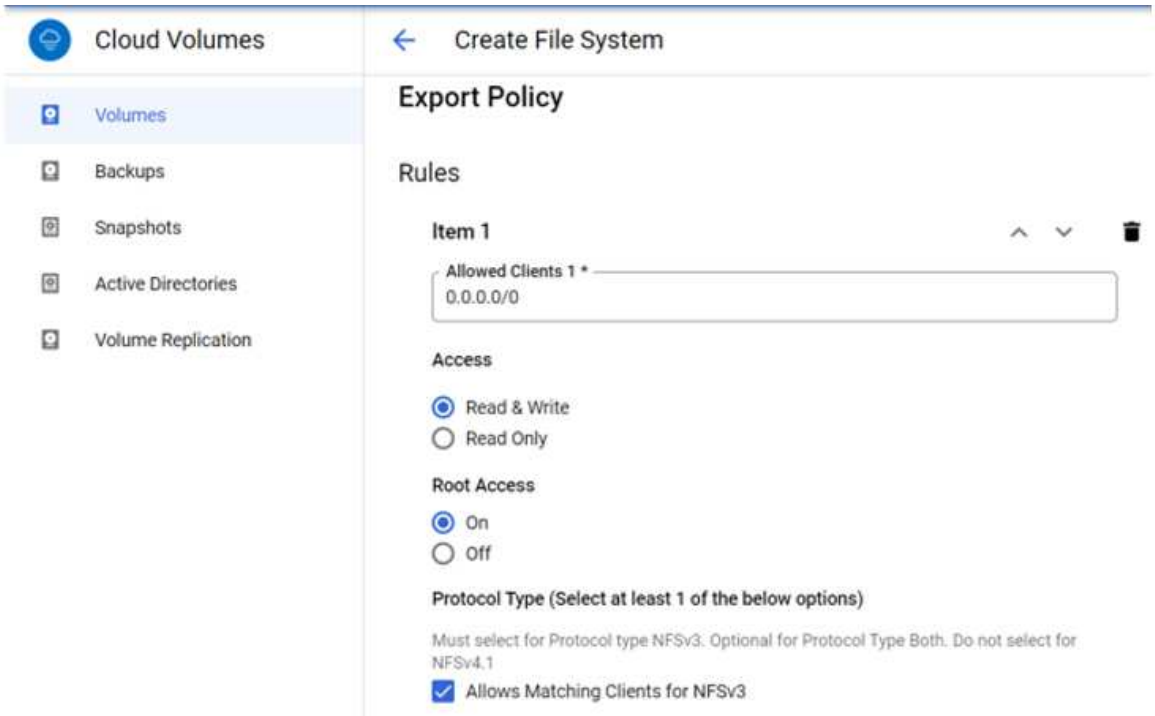
8. 이 단계에서는 볼륨에 액세스할 수 있는 VPC 네트워크를 선택합니다. VPC 피어링을 제자리에 배치했는지 확인합니다.

힌트: VPC 피어링을 수행하지 않은 경우 피어링 명령을 안내하는 팝업 버튼이 표시됩니다. 클라우드 셸 세션을 열고 적절한 명령을 실행하여 VPC를 Cloud Volumes Service 생산자와 동종합니다. 사전에 VPC 피어링을 준비하려는 경우 다음 지침을 참조하십시오.



9. 적절한 규칙을 추가하여 엑스포트 정책 규칙을 관리하고 해당 NFS 버전의 확인란을 선택합니다.

   참고: 내보내기 정책을 추가하지 않으면 NFS 볼륨에 액세스할 수 없습니다.



10. Save(저장) 를 클릭하여 볼륨을 생성합니다.

VMware Engine에서 실행 중인 **VM**에 **NFS** 내보내기를 마운트합니다

NFS 볼륨 마운트를 준비하기 전에 전용 연결의 피어링 상태가 Active(활성)로 표시되는지 확인합니다. 상태가 Active인 경우 mount 명령을 사용합니다.

NFS 볼륨을 마운트하려면 다음을 수행합니다.

1. Cloud Console에서 Cloud Volumes > Volumes로 이동합니다.
2. 볼륨 페이지로 이동합니다
3. NFS 내보내기를 마운트할 NFS 볼륨을 클릭합니다.
4. 오른쪽으로 스크롤하고 자세히 표시 에서 마운트 지침 을 클릭합니다.

VMware VM의 게스트 OS 내에서 마운트 프로세스를 수행하려면 다음 단계를 따르십시오.

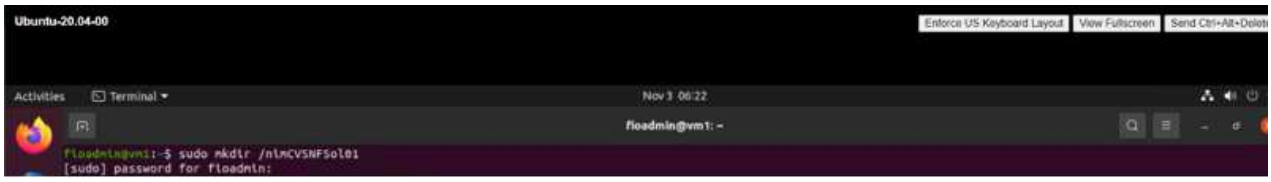
1. SSH 클라이언트 및 SSH를 사용하여 가상 머신에 접속합니다.
2. 인스턴스에 NFS 클라이언트를 설치합니다.
   a. Red Hat Enterprise Linux 또는 SuSE Linux 인스턴스:

```
 sudo yum install -y nfs-utils
.. Ubuntu 또는 Debian 인스턴스에서:
```

```
sudo apt-get install nfs-common
```

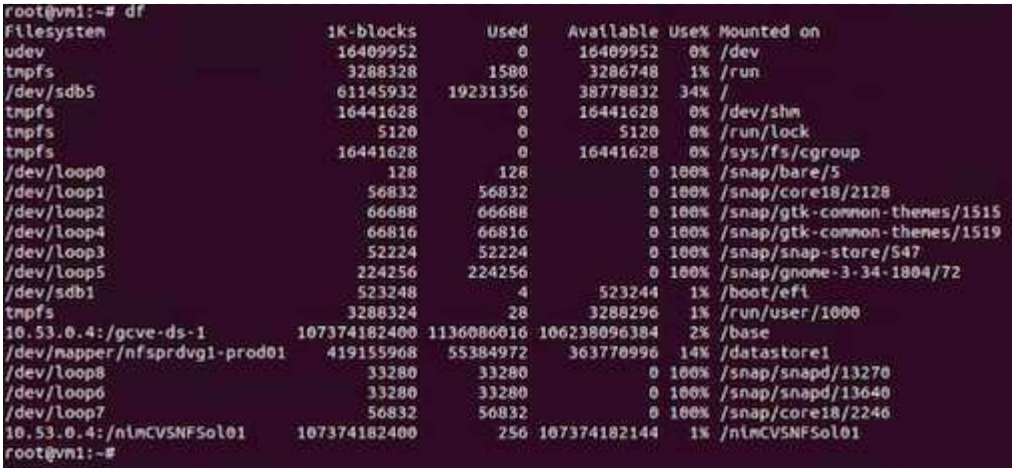
3. 인스턴스에 "/nimCVSNFSol01"과 같은 새 디렉토리를 생성합니다.

```
sudo mkdir /nimCVSNFSol01
```



4. 적절한 명령을 사용하여 볼륨을 마운트합니다. 실습의 명령 예는 다음과 같습니다.

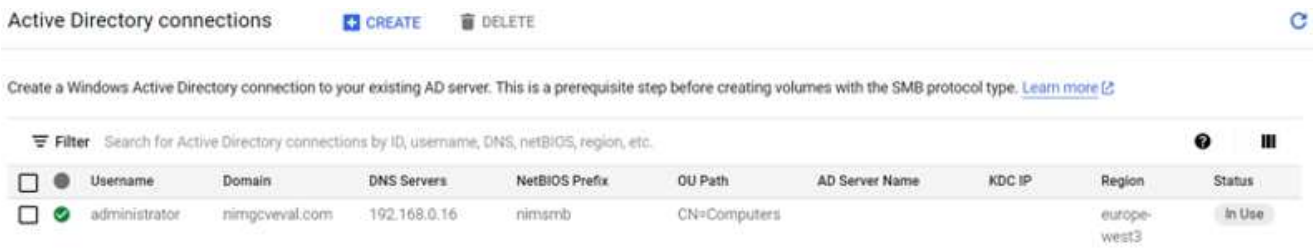
```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```



```
root@vm1:~# df
Filesystem                     1K-blocks        Used    Available Use% Mounted on
udev                            16409952           0     16409952   0% /dev
tmpfs                            3288328        1580      3286748   1% /run
/dev/sdb5                       61145932    19231356     38778832  34% /
tmpfs                           16441628           0     16441628   0% /dev/shm
tmpfs                               5120           0         5120   0% /run/lock
tmpfs                           16441628           0     16441628   0% /sys/fs/cgroup
/dev/loop0                            128         128            0 100% /snap/bare/5
/dev/loop1                          56832       56832            0 100% /snap/core18/2128
/dev/loop2                          66688       66688            0 100% /snap/gtk-common-themes/1515
/dev/loop4                          66816       66816            0 100% /snap/gtk-common-themes/1519
/dev/loop3                          52224       52224            0 100% /snap/snap-store/547
/dev/loop5                         224256      224256            0 100% /snap/gnome-3-34-1804/72
/dev/sdb1                          523248           4       523244   1% /boot/efi
tmpfs                             3288324          28      3288296   1% /run/user/1000
10.53.0.4:/gcve-ds-1          107374182400  1136086016 106238096384   2% /base
/dev/mapper/nfsprdvg1-prod01    419155968    55384972    363770996  14% /datastore1
/dev/loop8                          33280       33280            0 100% /snap/snapd/13270
/dev/loop6                          33280       33280            0 100% /snap/snapd/13640
/dev/loop7                          56832       56832            0 100% /snap/core18/2246
10.53.0.4:/nlmCVSNFSol01      107374182400         256 107374182144   1% /nlmCVSNFSol01
root@vm1:~#
```

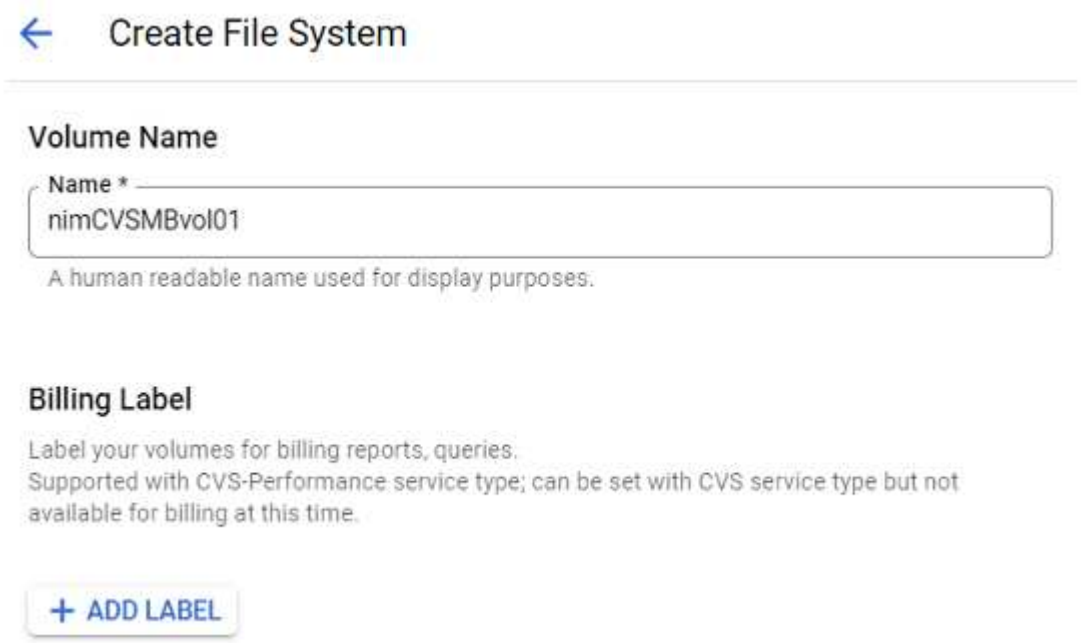
VMware Engine에서 실행 중인 **VM**에 **SMB** 공유 생성 및 마운트

SMB 볼륨의 경우 SMB 볼륨을 생성하기 전에 Active Directory 연결이 구성되어 있는지 확인합니다.

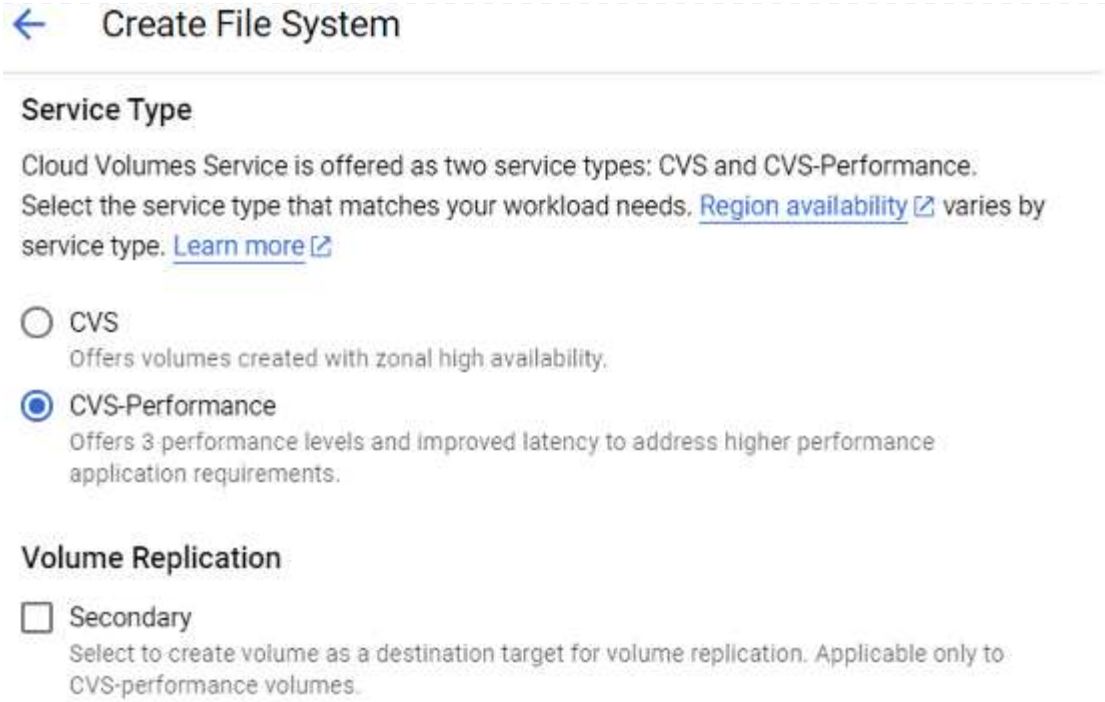


AD 연결이 설정되면 원하는 서비스 수준으로 볼륨을 생성합니다. 단계는 적절한 프로토콜을 선택하는 경우를 제외하고 NFS 볼륨을 생성하는 것과 같습니다.

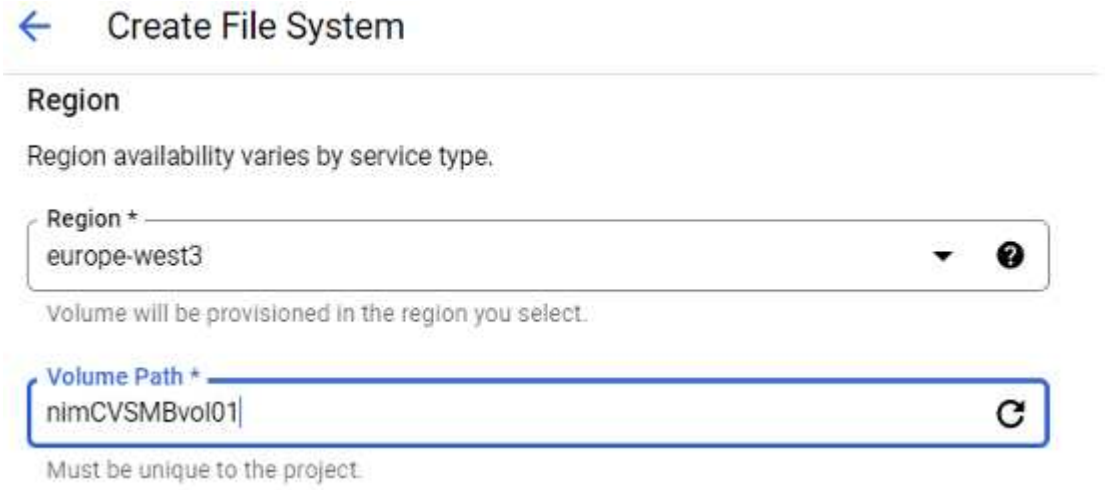
1. Cloud Volumes Console에서 Volumes 페이지로 이동하고 Create를 클릭합니다.
2. 파일 시스템 생성 페이지에서 차지백 메커니즘에 필요한 볼륨 이름 및 청구 레이블을 지정합니다.



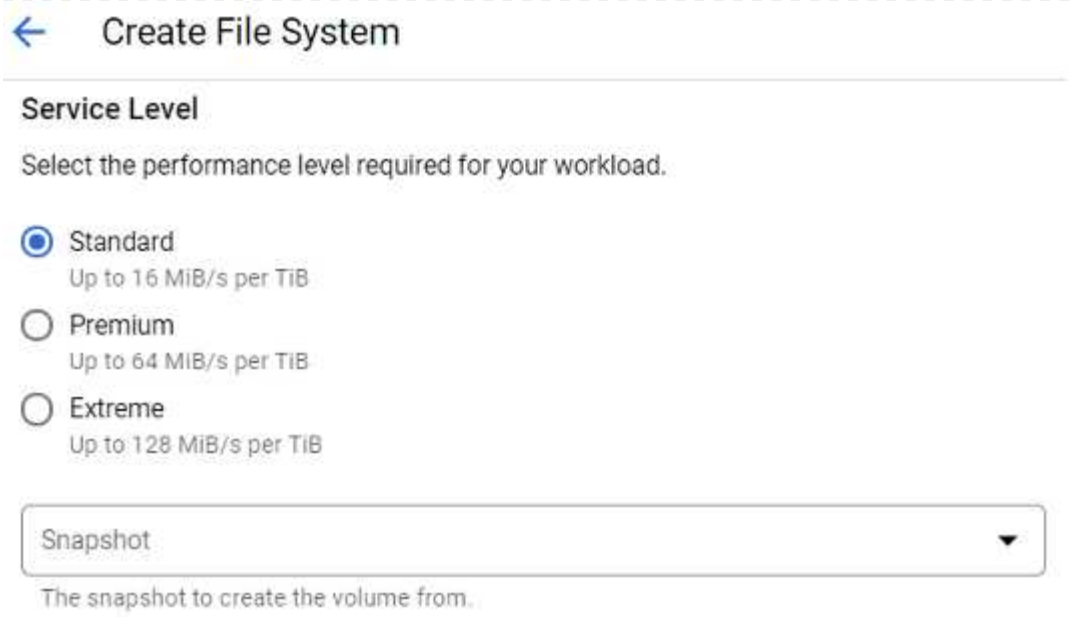
3. 적절한 서비스를 선택합니다. GCVE의 경우 워크로드 요구 사항에 따라 지연 시간을 개선하고 성능을 향상시키하려면 CVS 성능 및 원하는 서비스 수준을 선택합니다.



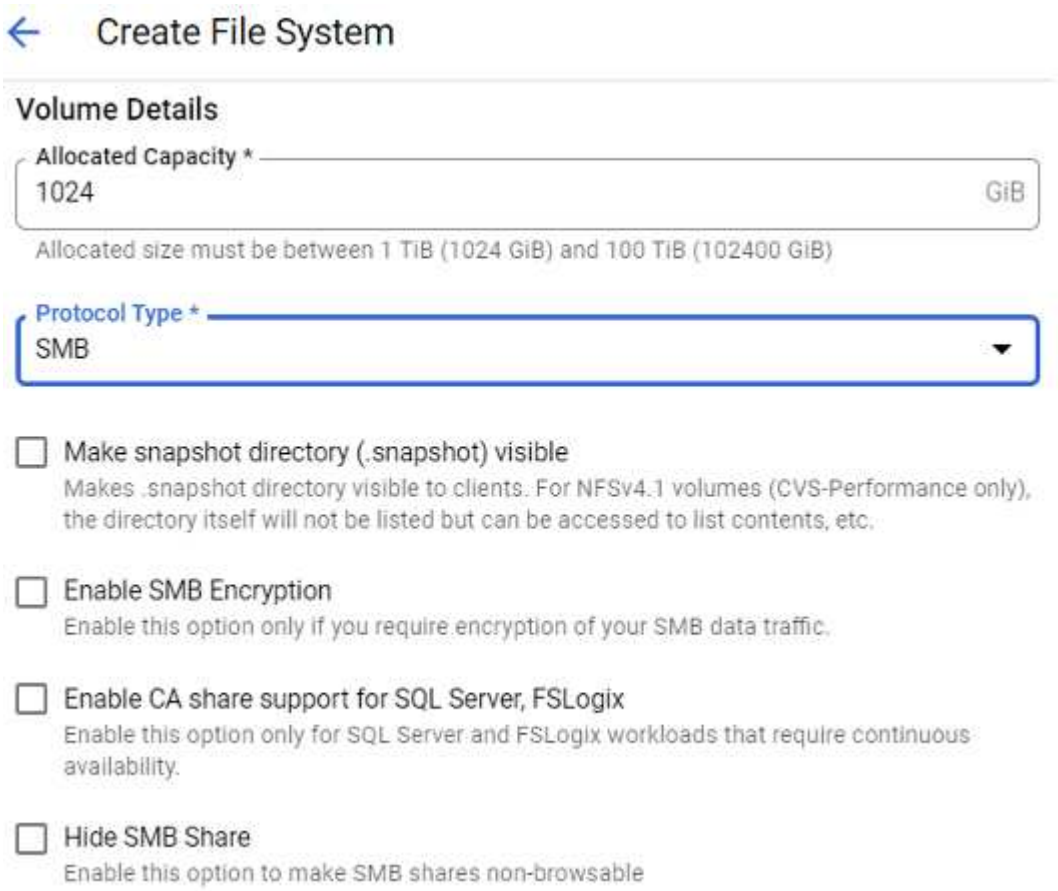
4. 볼륨 및 볼륨 경로에 대해 Google Cloud 영역을 지정합니다. 볼륨 경로는 프로젝트의 모든 클라우드 볼륨에서 고유해야 합니다.



5. 볼륨의 성능 수준을 선택합니다.

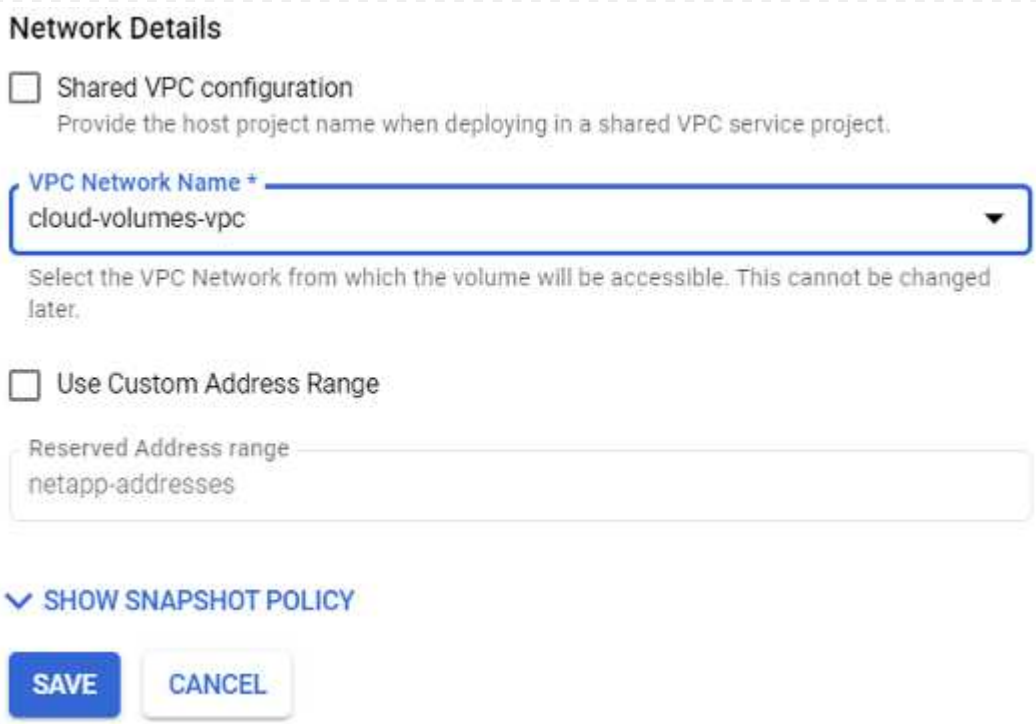


6. 볼륨의 크기와 프로토콜 유형을 지정합니다. 이 테스트에서는 SMB가 사용됩니다.



7. 이 단계에서는 볼륨에 액세스할 수 있는 VPC 네트워크를 선택합니다. VPC 피어링을 제자리에 배치했는지 확인합니다.

   힌트: VPC 피어링을 수행하지 않은 경우 피어링 명령을 안내하는 팝업 버튼이 표시됩니다. 클라우드 셸 세션을 열고 적절한 명령을 실행하여 VPC를 Cloud Volumes Service 생산자와 동종합니다. 미리 VPC 피어링을 준비하려는 경우 이를 참조하십시오 "지침".



8. Save(저장) 를 클릭하여 볼륨을 생성합니다.

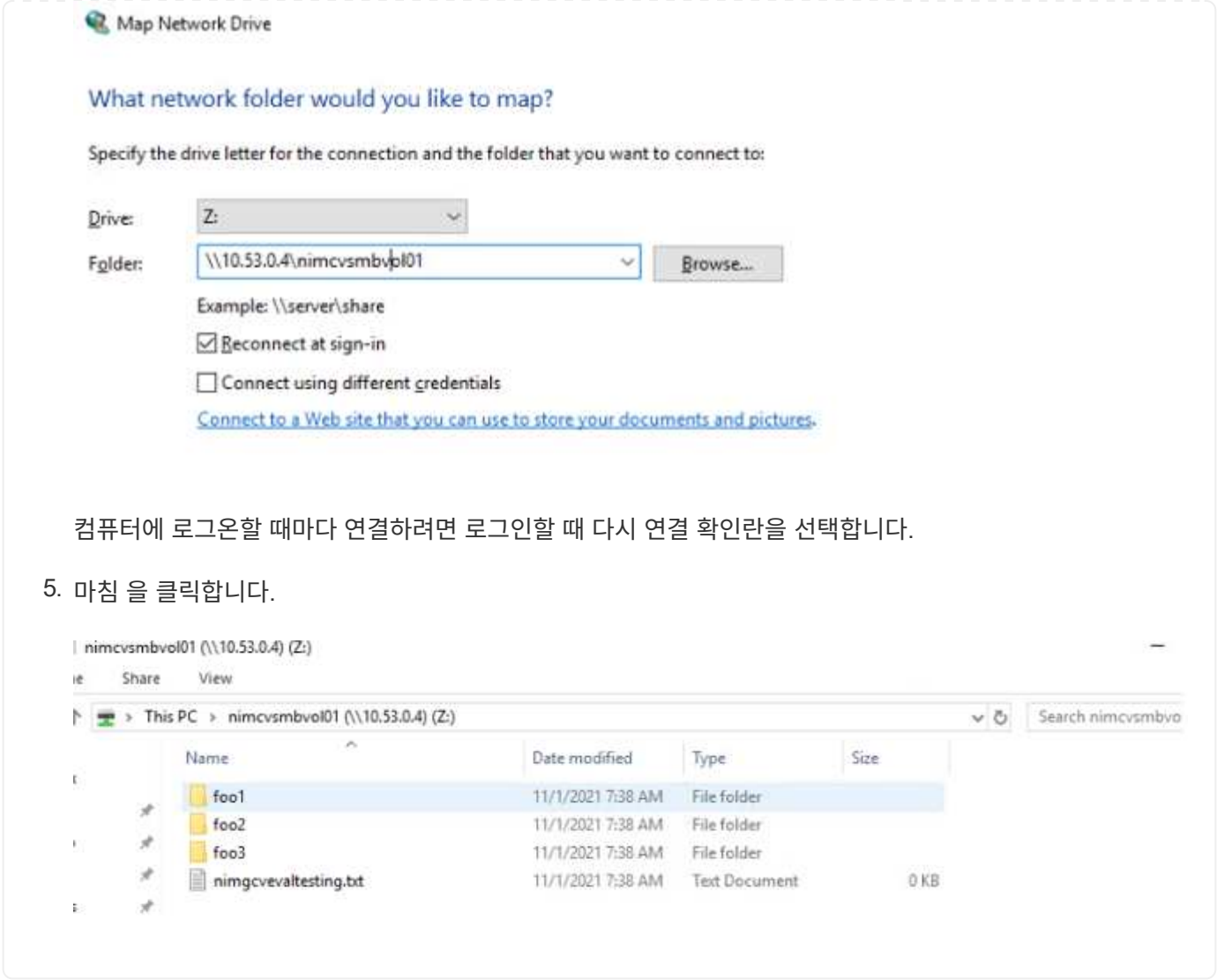
SMB 볼륨을 마운트하려면 다음을 수행합니다.

1. Cloud Console에서 Cloud Volumes > Volumes로 이동합니다.
2. 볼륨 페이지로 이동합니다
3. SMB 공유를 매핑할 SMB 볼륨을 클릭합니다.
4. 오른쪽으로 스크롤하고 자세히 표시 에서 마운트 지침 을 클릭합니다.

VMware VM의 Windows 게스트 OS 내에서 마운트 프로세스를 수행하려면 다음 단계를 수행하십시오.

1. 시작 단추를 클릭한 다음 컴퓨터를 클릭합니다.
2. 네트워크 드라이브 연결 을 클릭합니다.
3. 드라이브 목록에서 사용 가능한 드라이브 문자를 클릭합니다.
4. 폴더 상자에 다음을 입력합니다.

```
\\nimsmb-3830.nimgcveval.com\nimCVSMBvol01
```



컴퓨터에 로그온할 때마다 연결하려면 로그인할 때 다시 연결 확인란을 선택합니다.

5. 마침 을 클릭합니다.

AWS, Azure 및 **GCP**에서 보조 **NFS** 데이터 저장소를 위한 지역 가용성

AWS, Azure 및 Google Cloud Platform(GCP)에서 NFS 데이터 저장소를 추가로 지원하는 글로벌 지역에 대해 자세히 알아보십시오.

AWS 지역 가용성

AWS/VMC에서 보조 NFS 데이터 저장소를 사용할 수 있는 가용성은 Amazon에서 정의합니다. 먼저, VMC와 FSxN을 모두 지정된 지역에서 사용할 수 있는지 확인해야 합니다. 그런 다음 해당 지역에서 FSxN 보조 NFS 데이터 저장소가 지원되는지 여부를 확인해야 합니다.

- VMC의 가용성을 확인합니다 "여기".
- 아마존의 가격 책정 가이드에서는 FSxN(FSx ONTAP)을 사용할 수 있는 위치에 대한 정보를 제공합니다. 해당 정보를 찾을 수 있습니다 "여기".
- VMC에 대한 FSxN 보조 NFS 데이터 저장소의 가용성이 곧 제공될 예정입니다.

정보가 아직 릴리즈되는 동안 다음 차트는 VMC, FSxN 및 FSxN에 대한 현재 지원을 보조 NFS 데이터 저장소로 식별합니다.

미주

* AWS 지역 *	* VMC 가용성 *	* FSx ONTAP 가용성 *	* NFS 데이터 저장소 가용성 *
미국 동부(노던 버지니아)	예	예	예
미국 동부(오하이오)	예	예	예
미국 서부(캘리포니아 북부)	예	아니요	아니요
미국 서부(오리건주)	예	예	예
GovCloud(미국 서부)	예	예	예
캐나다(중부)	예	예	예
남아메리카(상파울루)	예	예	예

마지막 업데이트: 2022년 6월 2일.

유럽

* AWS 지역 *	* VMC 가용성 *	* FSx ONTAP 가용성 *	* NFS 데이터 저장소 가용성 *
유럽(아일랜드)	예	예	예
유럽(런던)	예	예	예
유럽(프랑크푸르트)	예	예	예
유럽(파리)	예	예	예
유럽(밀라노)	예	예	예
유럽(스톡홀름)	예	예	예

마지막 업데이트: 2022년 6월 2일.

아시아 태평양

* AWS 지역 *	* VMC 가용성 *	* FSx ONTAP 가용성 *	* NFS 데이터 저장소 가용성 *
아시아 태평양(시드니)	예	예	예
아시아 태평양(도쿄)	예	예	예
아시아 태평양(오사카)	예	아니요	아니요
아시아 태평양(싱가포르)	예	예	예
아시아 태평양(서울)	예	예	예
아시아 태평양(뭄바이)	예	예	예
아시아 태평양(자카르타)	아니요	아니요	아니요
아시아 태평양(홍콩)	예	예	예

마지막 업데이트: 2022년 9월 28일.

Azure 지역 가용성

Azure/AVS에서 보조 NFS 데이터 저장소의 가용성은 Microsoft에서 정의합니다. 먼저 AVS와 ANF를 특정 지역에서 모두 사용할 수 있는지 확인해야 합니다. 그런 다음 해당 지역에서 ANF 보조 NFS 데이터 저장소가 지원되는지 여부를 확인해야 합니다.

- AVS 및 ANF의 가용성을 확인하십시오 "여기".
- ANF 보조 NFS 데이터 저장소의 가용성을 확인합니다 "여기".

GCP 지역 가용성

GCP가 공개 가용성에 진입할 때 GCP 지역 가용성이 릴리스됩니다.

요약 및 결론**: NetApp** 하이브리드 멀티 클라우드를 **VMware**와 함께 사용해야 하는 이유

주요 하이퍼스케일러를 위한 VMware 솔루션과 NetApp Cloud Volumes는 하이브리드 클라우드를 활용하려는 조직에 최고의 잠재력을 제공합니다. 이 섹션의 나머지 부분에서는 NetApp Cloud Volumes의 통합을 통해 진정한 하이브리드 멀티 클라우드 기능을 실현하는 사용 사례를 소개합니다.

사용 사례 **#1:** 스토리지 최적화

RVtools 출력을 사용하여 사이징 작업을 수행할 때 마력(vCPU/vmem) 스케일이 스토리지와 평행하다는 것이 항상 명백합니다. 스토리지 공간에 필요한 드라이브의 크기가 마력을 훨씬 넘어서는 상황에 처하게 되는 경우가 많습니다.

NetApp Cloud Volumes를 통합하면 간단한 마이그레이션 방식을 통해 vSphere 기반 클라우드 솔루션을 실현할 수 있습니다. 플랫폼 재구축 또는 IP 변경 없이 아키텍처 변경 없이 모든 작업을 수행할 수 있습니다. 또한 이러한 최적화를 통해 vSphere에서 호스트 수를 최소한으로 유지하면서 스토리지 설치 공간을 확장할 수 있으며, 스토리지 계층, 보안 또는 사용 가능한 파일은 변경되지 않습니다. 따라서 구축을 최적화하고 전체 TCO를 35~45% 절감할 수 있습니다. 또한 이러한 통합을 통해 스토리지를 따뜻한 스토리지에서 운영 수준의 성능으로 몇 초 이내에 확장할 수 있습니다.

사용 사례 **2:** 클라우드 마이그레이션

조직에서는 향후 임대 만료, 자본 지출(capex) 지출에서 운영 비용(opex) 지출로 전환해야 하는 재무 지침, 모든 것을 클라우드로 이동하는 하향식 등 다양한 이유로 애플리케이션을 사내 데이터 센터에서 퍼블릭 클라우드로 마이그레이션해야 한다는 압박을 받고 있습니다.

속도가 중요한 경우에는 클라우드의 특정 IaaS 플랫폼에 맞게 애플리케이션을 재구성하고 리팩토링하는 작업이 느리고 비용이 많이 들며 종종 몇 달이 소요되기 때문에 간소화된 마이그레이션 방식만 실현 가능합니다. NetApp Cloud Volumes를 게스트 연결 스토리지를 위한 대역폭 효율적인 SnapMirror 복제(애플리케이션 정합성이 보장된 Snapshot 복사본 및 HCX와 함께 RDM 포함, 클라우드 특정 마이그레이션(예 Azure 마이그레이션) 또는 타사 제품으로 VM 복제), 시간이 많이 소요되는 I/O 필터 메커니즘에 의존하는 것보다 훨씬 더 쉽게 전환할 수 있습니다.

사용 사례 **3:** 데이터 센터 확장

데이터 센터가 특정 시기별 수요 급증 또는 지속적인 유기적 성장으로 인해 용량 제한에 도달할 경우, NetApp Cloud Volumes와 함께 클라우드 호스팅 VMware로 손쉽게 전환할 수 있습니다. NetApp Cloud Volumes를 활용하면 가용성 영역 및 동적 확장 기능에 걸쳐 고가용성을 제공하여 스토리지를 쉽게 생성, 복제 및 확장할 수 있습니다. NetApp Cloud Volumes를 활용하면 확장 클러스터의 필요성을 극복하여 호스트 클러스터 용량을 최소화할 수 있습니다.

사용 사례 **4:** 클라우드로 재해 복구

기존 방식에서는 재해가 발생할 경우 클라우드로 복제된 VM을 복원하기 전에 클라우드의 자체 하이퍼바이저 플랫폼으로 변환해야 합니다. 위기 상황에서 처리할 작업은 아닙니다.

퍼블릭 클라우드 가상화 솔루션과 함께 SnapCenter 및 온프레미스에서 SnapMirror 복제를 사용하여 게스트 연결 스토리지에 NetApp Cloud Volumes를 사용함으로써 재해 복구를 위한 더 나은 접근법을 고안하여, 클라우드 관련 복구 툴과 함께 완전히 일관된 VMware SDDC 인프라에서 VM 복제본을 복구할 수 있습니다(예 Azure Site Recovery) 또는 Veeam과 같은 타사 툴을 사용할 수 있습니다. 또한, 이 접근 방식을 통해 랜섬웨어에서 신속하게 재해 복구 훈련 및 복구를 수행할 수 있습니다. 또한 필요에 따라 호스트를 추가하여 테스트 또는 재해 발생 시 전체 운영 환경으로 확장할 수 있습니다.

사용 사례 **5:** 애플리케이션 현대화

퍼블릭 클라우드에 애플리케이션이 포함된 후에는 강력한 수백 가지 클라우드 서비스를 활용하여 애플리케이션을 현대화하고 확장하려고 할 것입니다. NetApp Cloud Volumes를 사용할 경우 애플리케이션 데이터가 vSAN에 종속되지 않고 Kubernetes를 포함한 광범위한 사용 사례에서 데이터를 이동할 수 있기 때문에 현대화는 쉬운 프로세스입니다.

결론

All-Cloud와 하이브리드 클라우드 중 무엇을 목표로 하든 NetApp Cloud Volumes는 파일 서비스 및 블록 프로토콜과 함께 애플리케이션 워크로드를 구축 및 관리하는 데 탁월한 옵션을 제공하는 한편, 데이터 요구사항을 애플리케이션 계층에 원활하게 구현하여 TCO를 절감합니다.

어떤 사용 사례에서든 즐겨 사용하는 클라우드/하이퍼스케일러와 NetApp Cloud Volumes를 함께 사용하여 사내 및 멀티 클라우드 전체의 클라우드 이점, 일관된 인프라 및 운영을 빠르게 실현하고, 워크로드의 양방향 이동성을 제공하며, 엔터프라이즈급 용량과 성능을 실현할 수 있습니다.

스토리지를 연결하는 데 사용되는 것과 동일한 친숙한 프로세스와 절차입니다. 이는 새로운 이름으로 변경된 데이터의 위치일 뿐입니다. 도구와 프로세스는 그대로 유지되며 NetApp Cloud Volumes는 전체 구축을 최적화하는 데 도움이 됩니다.

VMware 하이브리드 클라우드 사용 사례

VMware를 사용하는 **NetApp** 하이브리드 멀티 클라우드의 사용 사례

하이브리드 클라우드 또는 클라우드 우선 구축을 계획할 때 IT 조직에 중요한 사용 사례에 대한 개요입니다.

보편적인 사용 사례

사용 사례는 다음과 같습니다.

- 재해 복구,
- 데이터 센터 유지 관리 중에 워크로드를 호스팅 * 로컬 데이터 센터에서 프로비저닝되는 것 이상의 추가 리소스가 필요한 빠른 증가,
- VMware 사이트 확장,
- 클라우드로 신속하게 마이그레이션,
- 개발/테스트, 및
- 클라우드 보완 기술을 활용하여 앱 현대화

이 설명서 전체에서 VMware 활용 사례를 사용하여 클라우드 워크로드 참조를 자세히 설명합니다. 이러한 사용 사례는 다음과 같습니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 마이그레이션
- 확장

IT의 여정

대부분의 조직은 혁신과 현대화를 향한 여정을 진행 중입니다. 이 프로세스의 일환으로 기업들은 기존 VMware 투자를 활용하는 동시에 클라우드의 이점을 활용하고 마이그레이션 프로세스를 최대한 원활하게 만드는 방법을 모색하고 있습니다. 이 접근 방식은 데이터가 이미 클라우드에 있기 때문에 현대화에 대한 노력을 매우 쉽게 할 수 있습니다.

이 시나리오에 대한 가장 쉬운 답은 각 하이퍼스케일러의 VMware 오퍼링입니다. NetApp ® Cloud Volumes와 마찬가지로 VMware는 사내 VMware 환경을 클라우드로 이동 또는 확장하는 방법을 제공하므로 클라우드에서 워크로드를 기본적으로 실행하면서 기존 온프레미스 자산, 기술 및 툴을 유지할 수 있습니다. 따라서 서비스 중단이나 IP 변경이 필요하지 않고 IT 팀이 기존 기술과 툴을 사용하여 사내에서 작업하는 방식을 운영할 수 있으므로 위험이 감소합니다. 따라서 클라우드 마이그레이션을 가속화하고 하이브리드 멀티 클라우드 아키텍처로의 전환이 한층 원활해질 수 있습니다.

보충 **NFS** 스토리지 옵션의 중요성 이해

클라우드에 구축된 VMware는 모든 고객에게 고유한 하이브리드 기능을 제공하지만, 제한된 보조 NFS 스토리지 옵션으로 스토리지 집약적인 워크로드를 사용하는 조직에는 유용성이 제한됩니다. 스토리지는 호스트에 직접 연결되므로 스토리지를 확장하는 유일한 방법은 호스트를 추가하는 것입니다. 이렇게 하면 스토리지 집약적인 워크로드의 비용이 35-40% 이상 증가할 수 있습니다. 이러한 워크로드는 추가 마력이 아닌 추가 스토리지만 필요합니다. 하지만 이는 추가 호스트에 대한 비용을 지불하는 것을 의미합니다.

다음 시나리오를 생각해 봅시다.

고객은 CPU와 메모리에 대해 5개의 호스트만 필요로 하지만 스토리지 요구 사항이 많으므로 스토리지 요구 사항을 충족하기 위해 12개의 호스트가 필요합니다. 이 요구사항은 스토리지를 증가하기만 하면 되는 추가 마력을 구매해야 하는 만큼 재무 규모를 넘어주는 결과를 제공합니다.

클라우드 도입 및 마이그레이션을 계획할 때는 항상 최상의 접근 방식을 평가하고 총 투자 비용을 절감하는 가장 쉬운 방법을 찾는 것이 중요합니다. 모든 애플리케이션 마이그레이션의 가장 일반적이고 쉬운 방법은 가상 머신(VM) 또는 데이터 변환이 없는 재호스팅(리프트 및 변속이라고도 함)입니다. NetApp Cloud Volumes를 VMware SDDC(소프트웨어 정의 데이터 센터)와 함께 사용하는 동시에 vSAN을 보완하는 것은 쉬운 전환 옵션을 제공합니다.

Amazon VMC(VMware Managed Cloud)를 위한 **NetApp** 솔루션

NetApp이 AWS에 제공하는 솔루션에 대해 자세히 알아보십시오.

VMware는 클라우드 워크로드를 다음 세 가지 범주 중 하나로 정의합니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 마이그레이션
- 확장

다음 섹션에서 사용 가능한 솔루션을 찾아봅니다.

보호

- "AWS에서 VMC를 사용한 재해 복구(게스트 연결)"
- "Veeam 백업 및 복구. ONTAP용 FSx로 VMC에서 복원"
- "ONTAP 및 VMC용 FSx를 통한 재해 복구(DRO"
- "Veeam Replication 및 FSx for ONTAP를 사용하여 AWS 기반 VMware Cloud로 재해 복구"

마이그레이션

- "VMware HCX를 사용하여 워크로드를 FSxN 데이터 저장소로 마이그레이션합니다"

확장

곧 출시 예정!!

Azure VMware 솔루션용 **NetApp** 솔루션**(AVS)**

NetApp이 Azure에 제공하는 솔루션에 대해 자세히 알아보십시오.

VMware는 클라우드 워크로드를 다음 세 가지 범주 중 하나로 정의합니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 마이그레이션
- 확장

다음 섹션에서 사용 가능한 솔루션을 찾아봅니다.

보호

- "ANF 및 Jetstream을 사용한 재해 복구(보조 NFS 데이터 저장소)"
- "ANF 및 CVO(게스트 연결 스토리지)를 사용한 재해 복구"
- "ANF 및 AVS를 통한 재해 복구(DRO"
- "Azure VMware Solution으로 재해 복구를 위해 Veeam Replication 및 Azure NetApp Files 데이터 저장소를 사용합니다"

마이그레이션

- "VMware HCX를 사용하여 워크로드를 Azure NetApp Files 데이터 저장소로 마이그레이션합니다"

확장

곧 출시 예정!!

Google Cloud VMware Engine용 **NetApp** 솔루션**(GCVE)**

NetApp이 GCP에 제공하는 솔루션에 대해 자세히 알아보십시오.

VMware는 클라우드 워크로드를 다음 세 가지 범주 중 하나로 정의합니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 마이그레이션
- 확장

다음 섹션에서 사용 가능한 솔루션을 찾아봅니다.

보호

- "SnapCenter, Cloud Volumes ONTAP, Veeam 복제를 통한 애플리케이션 재해 복구"
- "NetApp SnapCenter를 사용한 애플리케이션 정합성 보장 재해 복구 및 NetApp CVS에 Veeam 복제 GCVE"

마이그레이션

- "VMware HCX를 사용하여 NetApp Cloud Volume Service NFS 데이터 저장소로 워크로드 마이그레이션"
- "Veeam을 사용하여 NetApp Cloud Volume Service NFS 데이터 저장소로 VM 복제"

확장

곧 출시 예정!!

AWS VMC를 위한 NetApp 솔루션

NetApp이 AWS VMware 클라우드(VMC)에 제공하는 기능에 대해 자세히 알아보십시오. NetApp은 게스트 연결 스토리지 장치로, 보충 NFS 데이터 저장소에서 마이그레이션 워크플로우에 전환하여 클라우드, 백업/복원 및 재해 복구를 확대/급증할 수 있습니다.

다음 옵션 중 하나를 선택하여 원하는 콘텐츠의 섹션으로 이동합니다.

- "AWS에서 VMC 구성"
- "VMC용 NetApp 스토리지 옵션"
- "NetApp/VMware 클라우드 솔루션"

AWS에서 VMC 구성

온프레미스에서와 마찬가지로 클라우드 기반 가상화 환경을 계획하는 것은 VM 및 마이그레이션을 생성할 수 있는 성공적인 프로덕션 준비 환경에 매우 중요합니다.

이 섹션에서는 AWS SDDC에서 VMware Cloud를 설정 및 관리하고, NetApp 스토리지를 연결하는 데 사용할 수 있는 옵션과 함께 사용하는 방법을 설명합니다.

게스트 내 스토리지는 Cloud Volumes ONTAP을 AWS VMC에 연결하는 유일한 지원 방법입니다.

설치 프로세스는 다음 단계로 나눌 수 있습니다.

- VMware Cloud for AWS 구축 및 구성
- VMware Cloud를 FSx ONTAP에 연결합니다

자세한 내용을 확인하십시오 "VMC에 대한 구성 단계".

VMC용 NetApp 스토리지 옵션

AWS VMC에서 NetApp 스토리지를 guess connected 또는 보완 NFS 데이터 저장소로 여러 가지 방법으로 활용할 수 있습니다.

를 방문하십시오 "지원되는 NetApp 스토리지 옵션" 를 참조하십시오.

AWS는 다음과 같은 구성에서 NetApp 스토리지를 지원합니다.

- FSX ONTAP를 게스트 연결 스토리지로 사용합니다
- CVO(Cloud Volumes ONTAP)를 게스트 연결 스토리지로 사용합니다
- FSX ONTAP는 보조 NFS 데이터 저장소입니다

자세한 내용을 확인하십시오 "VMC에 대한 게스트 연결 스토리지 옵션". 자세한 내용을 확인하십시오 "VMC에 대한 보조 NFS 데이터 저장소 옵션".

솔루션 사용 사례

NetApp 및 VMware 클라우드 솔루션을 사용하면 많은 사용 사례를 AWS VMC에 쉽게 구축할 수 있습니다. 활용 사례는 VMware에서 정의한 각 클라우드 영역에 대해 정의됩니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 확장
- 마이그레이션

"AWS VMC용 NetApp 솔루션을 찾아보십시오"

AWS/VMC에서 워크로드 보호

TR-4931: Amazon Web Services 및 Guest Connect에서 VMware Cloud를 사용한 재해 복구

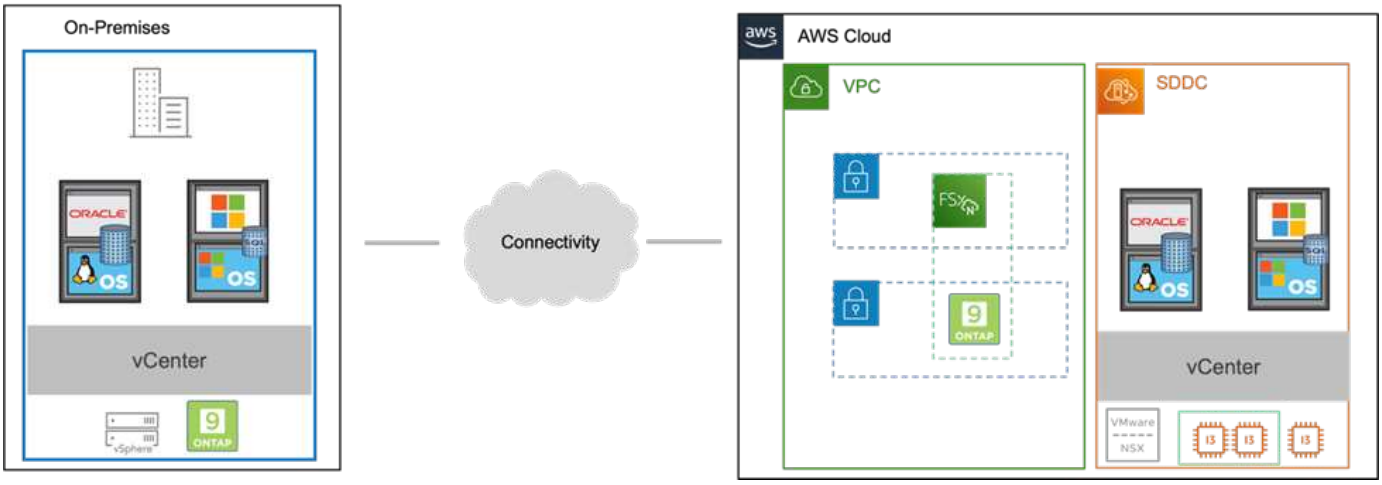
저자: Chris Reno, Josh Powell, Suesh Thoppay - NetApp 솔루션 엔지니어링

개요

조직에서는 중대한 운영 중단이 발생할 경우 비즈니스 크리티컬 애플리케이션을 신속하게 복구할 수 있도록 검증된 DR(재해 복구) 환경과 계획을 반드시 수립해야 합니다. 이 솔루션은 사내 및 AWS 기반의 VMware Cloud 모두에서 VMware 및 NetApp 기술을 중심으로 DR 사용 사례를 시연하는 데 초점을 맞춥니다.

NetApp은 오랫동안 VMware와 통합해왔습니다. 수만 명의 고객이 가상화 환경의 스토리지 파트너로 NetApp을 선택했다는 것이 증명되었습니다. 이러한 통합은 클라우드의 게스트 연결 옵션 및 최근 NFS 데이터 저장소와의 통합에서도 계속됩니다. 이 솔루션은 일반적으로 게스트 연결 스토리지라고 하는 사용 사례에 중점을 둡니다.

게스트 연결 스토리지에서 게스트 VMDK는 VMware 프로비저닝된 데이터 저장소에 구축되고 애플리케이션 데이터는 iSCSI 또는 NFS에 보관되며 VM에 직접 매핑됩니다. 다음 그림과 같이 Oracle 및 MS SQL 애플리케이션을 사용하여 DR 시나리오를 보여 줍니다.



가정, 전제 조건 및 구성 요소 개요

이 솔루션을 구축하기 전에 구성 요소 개요, 솔루션을 구축하는 데 필요한 전제 조건 및 이 솔루션을 문서화하는 데 필요한 가정을 검토하십시오.

"DR 솔루션 요구 사항, 사전 요청 및 계획"

SnapCenter를 사용하여 **DR** 수행

이 솔루션에서 SnapCenter는 SQL Server 및 Oracle 애플리케이션 데이터에 대해 애플리케이션 정합성이 보장되는 스냅샷을 제공합니다. 이 구성은 SnapMirror 기술과 함께 사내 AFF와 FSx ONTAP 클러스터 간에 고속 데이터 복제를 제공합니다. 또한 Veeam Backup & Replication은 가상 머신에 백업 및 복원 기능을 제공합니다.

이 섹션에서는 백업 및 복원을 위한 SnapCenter, SnapMirror 및 Veeam의 구성에 대해 살펴봅니다.

다음 섹션에서는 보조 사이트에서 페일오버를 완료하는 데 필요한 구성 및 단계에 대해 설명합니다.

SnapMirror 관계 및 보존 일정을 구성합니다

SnapCenter는 장기간 아카이브 및 보존을 위해 운영 스토리지 시스템(운영 > 미러) 및 보조 스토리지 시스템(운영 > 소산) 내의 SnapMirror 관계를 업데이트할 수 있습니다. 이렇게 하려면 SnapMirror를 사용하여 대상 볼륨과 소스 볼륨 간의 데이터 복제 관계를 설정하고 초기화해야 합니다.

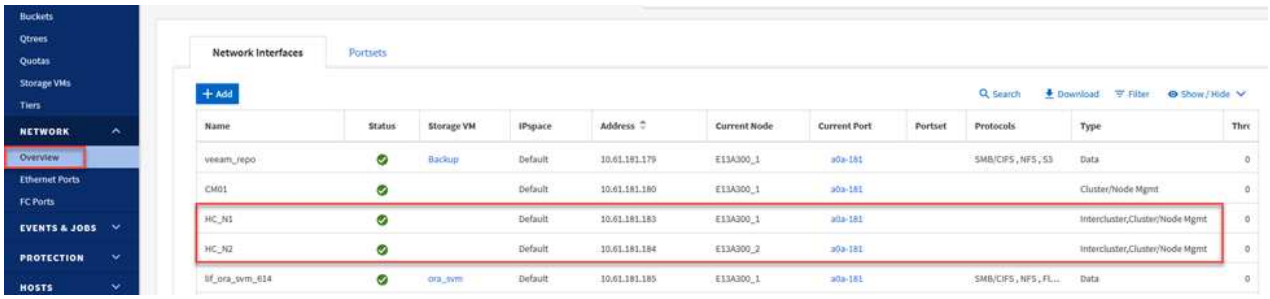
소스 및 타겟 ONTAP 시스템은 Amazon VPC 피어링, 전송 게이트웨이, AWS Direct Connect 또는 AWS VPN을 사용하여 피어링된 네트워크에 있어야 합니다.

온프레미스 ONTAP 시스템과 FSx ONTAP 간에 SnapMirror 관계를 설정하려면 다음 단계가 필요합니다.

을 참조하십시오 "ONTAP용 FSX – ONTAP 사용 설명서" FSx를 사용하여 SnapMirror 관계를 만드는 방법에 대한 자세한 내용은 를 참조하십시오.

사내에 상주하는 소스 ONTAP 시스템의 경우 System Manager 또는 CLI에서 클러스터 간 LIF 정보를 검색할 수 있습니다.

1. ONTAP System Manager에서 네트워크 개요 페이지로 이동하여 FSx가 설치된 AWS VPC와 통신하도록 구성된 Type:Intercluster의 IP 주소를 검색합니다.



2. FSx의 Intercluster IP 주소를 검색하려면 CLI에 로그인하여 다음 명령을 실행합니다.

```
FSx-Dest::> network interface show -role intercluster
```

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
FsxId0ae40e08acc0dea67
            inter_1      up/up    172.30.15.42/25    FsxId0ae40e08acc0dea67-01
                                                                   e0e     true
            inter_2      up/up    172.30.14.28/26    FsxId0ae40e08acc0dea67-02
                                                                   e0e     true
2 entries were displayed.
```

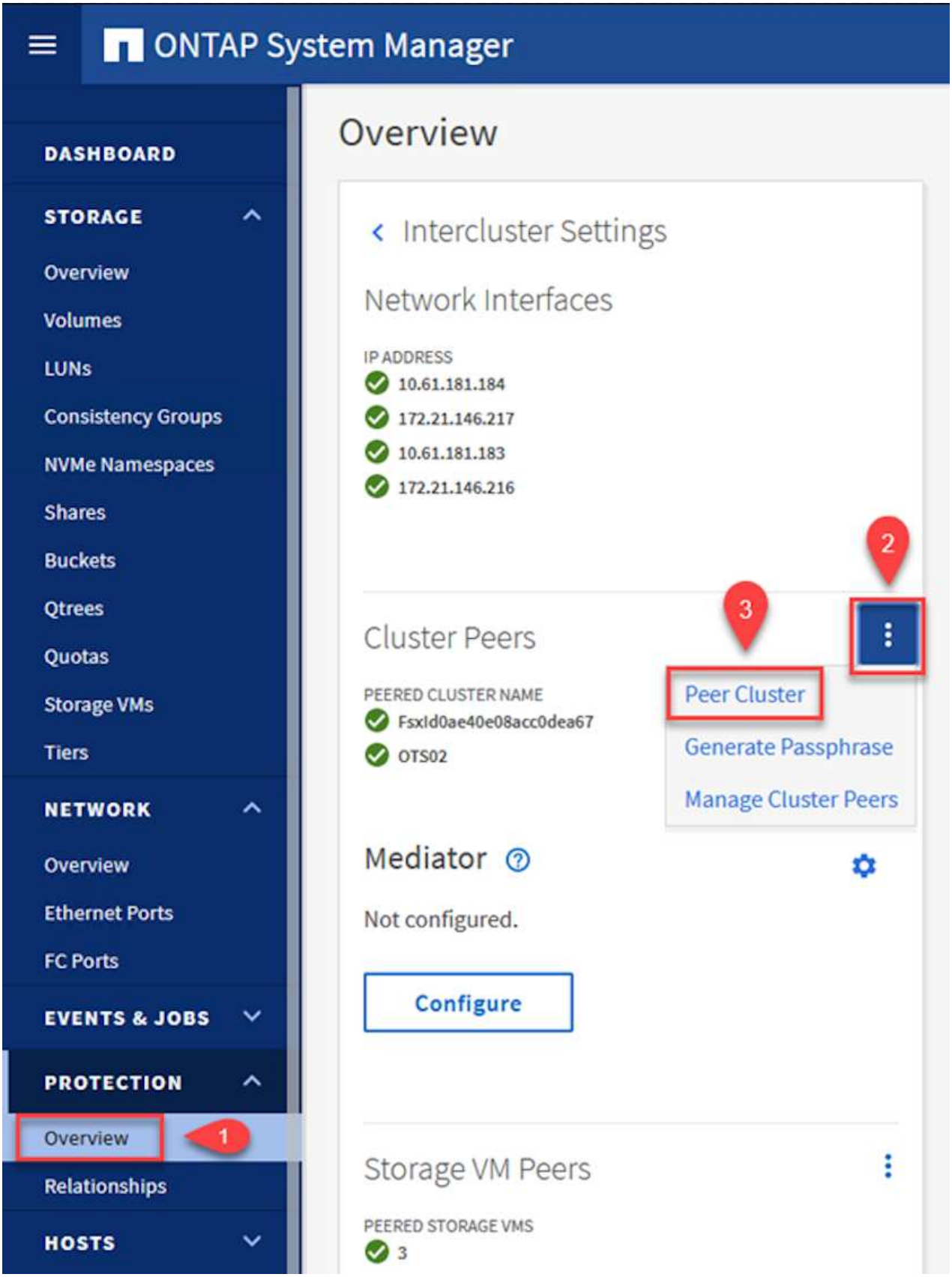
ONTAP와 **FSx** 간에 클러스터 피어링을 설정합니다

ONTAP 클러스터 간에 클러스터 피어링을 설정하려면 시작 ONTAP 클러스터에 입력된 고유한 암호가 다른 피어 클러스터에서 확인되어야 합니다.

1. 'cluster peer create' 명령을 사용하여 대상 FSx 클러스터에서 피어링을 설정합니다. 메시지가 표시되면 소스 클러스터에서 나중에 사용되는 고유한 암호를 입력하여 생성 프로세스를 마칩니다.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

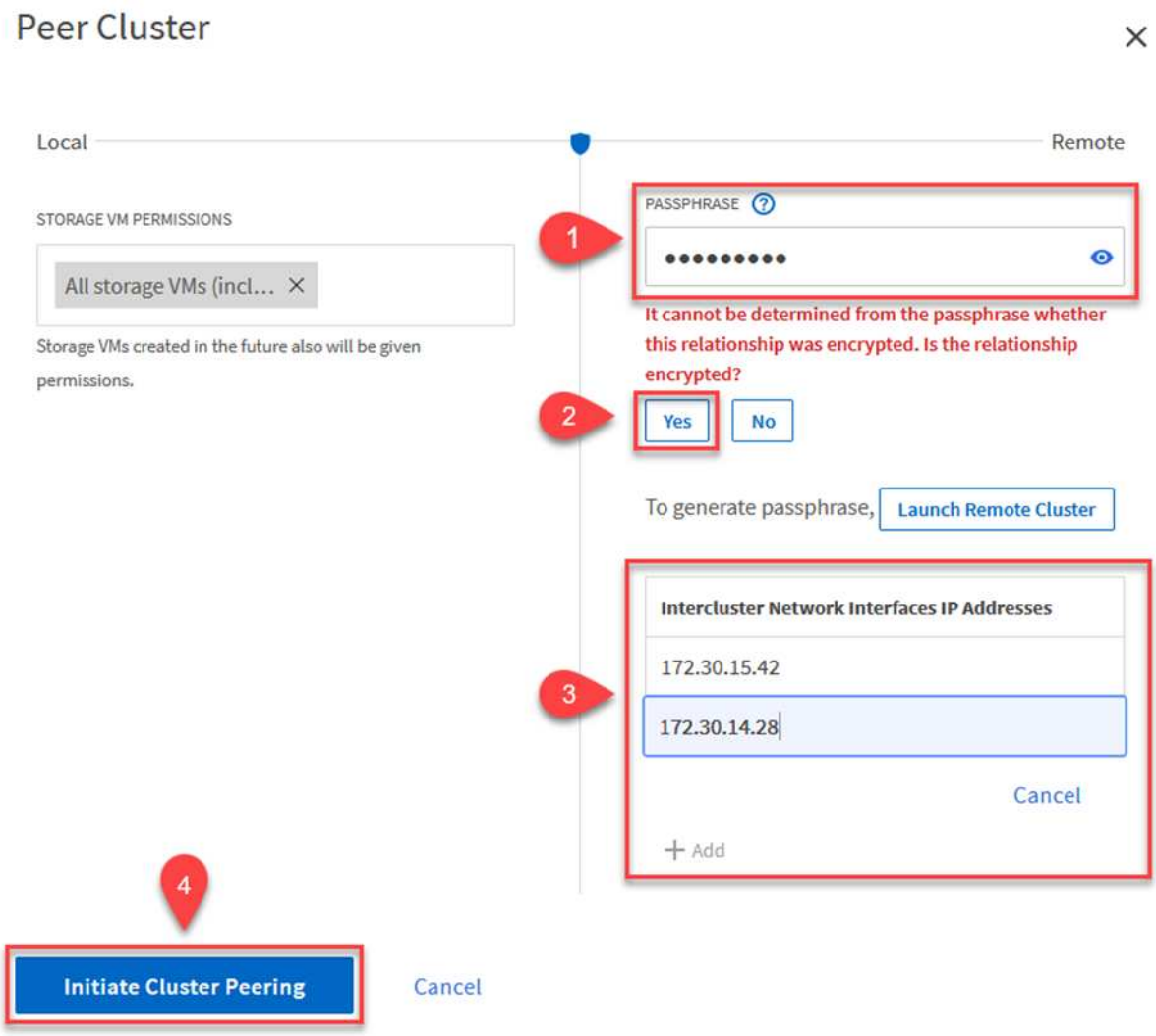
2. 소스 클러스터에서 ONTAP System Manager 또는 CLI를 사용하여 클러스터 피어 관계를 설정할 수 있습니다. ONTAP 시스템 관리자에서 보호 > 개요 로 이동하고 피어 클러스터 를 선택합니다.



3. 피어 클러스터 대화 상자에서 필요한 정보를 입력합니다.
   a. 대상 FSx 클러스터에서 피어 클러스터 관계를 설정하는 데 사용된 암호를 입력합니다.
   b. 암호화된 관계를 설정하려면 Yes를 선택합니다.

c. 대상 FSx 클러스터의 인터클러스터 LIF IP 주소를 입력합니다.

d. 클러스터 피어링 시작 을 클릭하여 프로세스를 마칩니다.



4. 다음 명령을 사용하여 FSx 클러스터에서 클러스터 피어 관계의 상태를 확인합니다.

```
FSx-Dest::> cluster peer show
```

```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability   Authentication
------------------------- --------------------- -------------- --------------
E13A300                   1-80-000011           Available      ok
```

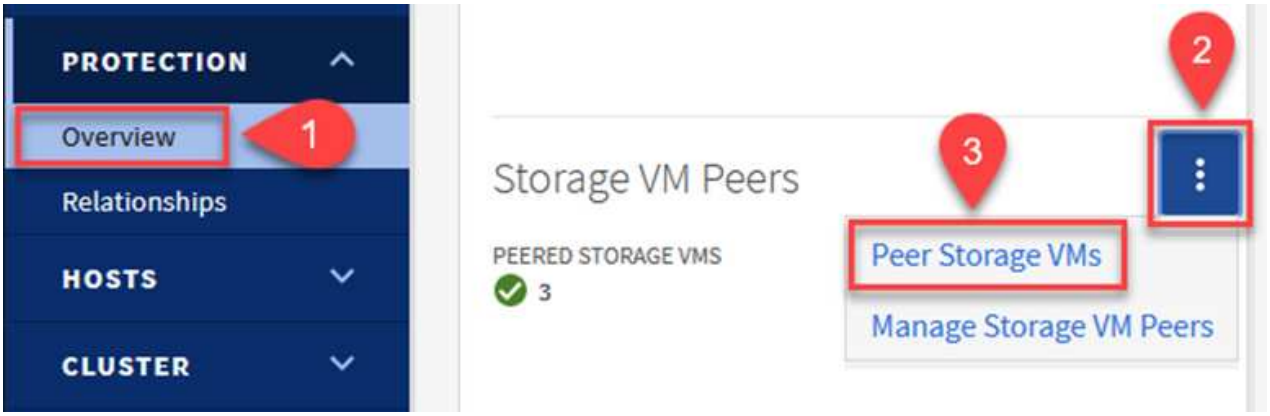
SVM 피어링 관계를 설정합니다

다음 단계는 SnapMirror 관계에 있는 볼륨을 포함하는 소스 스토리지 가상 시스템과 타겟 스토리지 가상 시스템 간에 SVM 관계를 설정하는 것입니다.

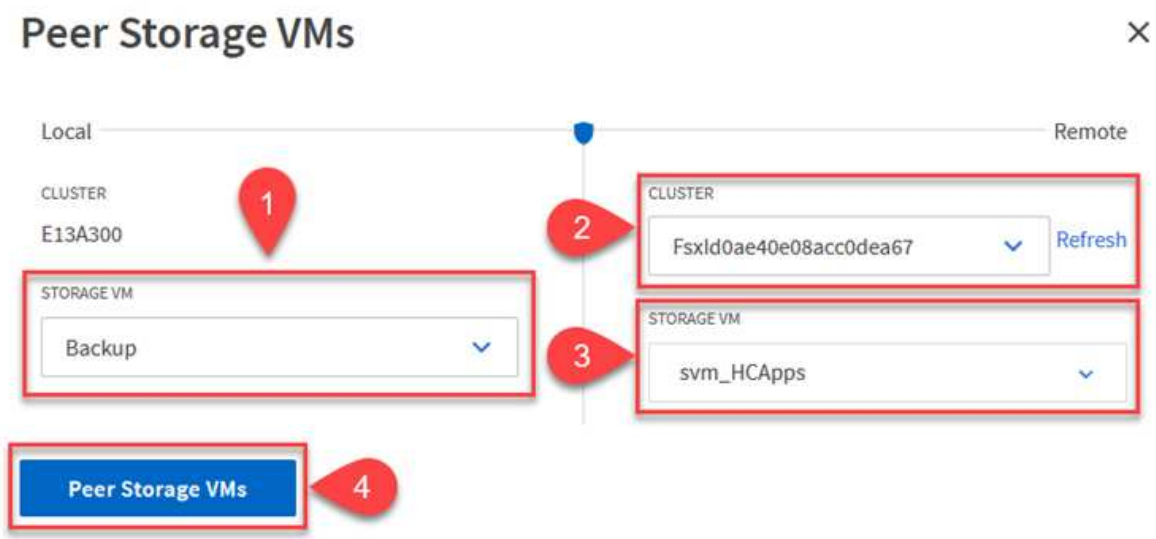
1. 소스 FSx 클러스터에서 CLI에서 다음 명령을 사용하여 SVM 피어 관계를 생성합니다.

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. 소스 ONTAP 클러스터에서 ONTAP System Manager 또는 CLI와 피어링 관계를 수락합니다.
3. ONTAP 시스템 관리자에서 보호 > 개요 로 이동하고 스토리지 VM 피어 아래에서 피어 스토리지 VM 을 선택합니다.



4. 피어 스토리지 VM 대화 상자에서 필수 필드를 입력합니다.
   - 소스 스토리지 VM입니다
   - 타겟 클러스터
   - 대상 스토리지 VM입니다



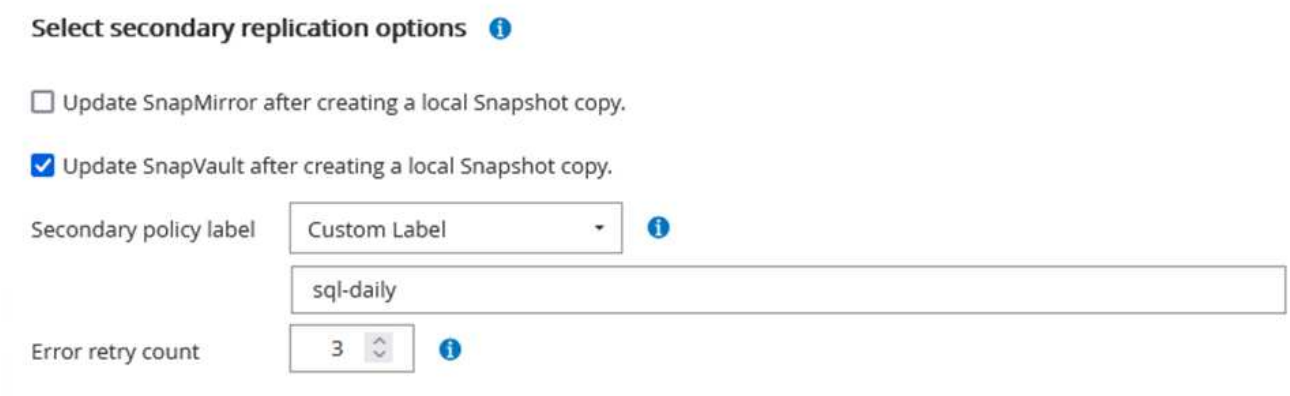
5. 피어 스토리지 VM 을 클릭하여 SVM 피어링 프로세스를 완료합니다.

SnapCenter는 운영 스토리지 시스템에서 스냅샷 복사본으로 존재하는 백업의 보존 일정을 관리합니다. SnapCenter에서 정책을 생성할 때 설정됩니다. SnapCenter는 보조 스토리지 시스템에 보존되는 백업에 대한 보존 정책을 관리하지 않습니다. 이러한 정책은 보조 FSx 클러스터에서 생성되고 소스 볼륨과 SnapMirror 관계에 있는 대상 볼륨에 연결된 SnapMirror 정책을 통해 별도로 관리됩니다.

SnapCenter 정책을 생성할 때 SnapCenter 백업을 수행할 때 생성되는 각 스냅샷의 SnapMirror 레이블에 추가되는 2차 정책 레이블을 지정할 수 있습니다.

ⓘ 보조 스토리지에서 이러한 레이블은 스냅샷 보존을 적용하기 위해 대상 볼륨과 관련된 정책 규칙과 일치합니다.

다음 예제는 SQL Server 데이터베이스 및 로그 볼륨의 일일 백업에 사용되는 정책의 일부로 생성된 모든 스냅샷에 존재하는 SnapMirror 레이블을 보여줍니다.



SQL Server 데이터베이스에 대한 SnapCenter 정책을 만드는 방법에 대한 자세한 내용은 을 참조하십시오 "SnapCenter 설명서".

우선 유지할 스냅샷 복사본 수를 결정하는 규칙을 사용하여 SnapMirror 정책을 생성해야 합니다.

1. FSx 클러스터에서 SnapMirror 정책을 생성합니다.

```
FSx-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. SnapCenter 정책에 지정된 2차 정책 레이블과 일치하는 SnapMirror 레이블을 사용하여 정책에 규칙을 추가합니다.

```
FSx-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

다음 스크립트는 정책에 추가할 수 있는 규칙의 예를 제공합니다.

```
FSx-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy
Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

각 SnapMirror 레이블과 유지할 스냅샷 수(보존 기간)에 대한 추가 규칙을 생성합니다.

대상 볼륨을 생성합니다

소스 볼륨에서 스냅샷 복사본을 받을 FSx에 대상 볼륨을 생성하려면 FSx ONTAP에서 다음 명령을 실행합니다.

```
FSx-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

소스 볼륨과 타겟 볼륨 간의 **SnapMirror** 관계를 생성합니다

소스 볼륨과 타겟 볼륨 간에 SnapMirror 관계를 생성하려면 FSx ONTAP에서 다음 명령을 실행합니다.

```
FSx-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

SnapMirror 관계 초기화

SnapMirror 관계를 초기화합니다. 이 프로세스에서는 소스 볼륨에서 생성된 새 스냅샷을 시작하여 타겟 볼륨에 복사합니다.

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

온-프레미스에서 **Windows SnapCenter** 서버를 배포하고 구성합니다.

Windows SnapCenter Server를 사내에 배포합니다

이 솔루션은 NetApp SnapCenter를 사용하여 SQL Server 및 Oracle 데이터베이스의 애플리케이션 정합성이 보장되는 백업을 수행합니다. Veeam Backup & Replication을 사용하여 가상 머신의 VMDK를 백업하면 사내 및 클라우드 기반 데이터 센터를 위한 포괄적인 재해 복구 솔루션을 제공할 수 있습니다.

SnapCenter 소프트웨어는 NetApp Support 사이트에서 제공되며 도메인 또는 작업 그룹에 있는 Microsoft Windows 시스템에 설치할 수 있습니다. 자세한 계획 가이드 및 설치 지침은 에서 확인할 수 있습니다 "NetApp 문서 센터".

SnapCenter 소프트웨어는 에서 얻을 수 있습니다 "이 링크".

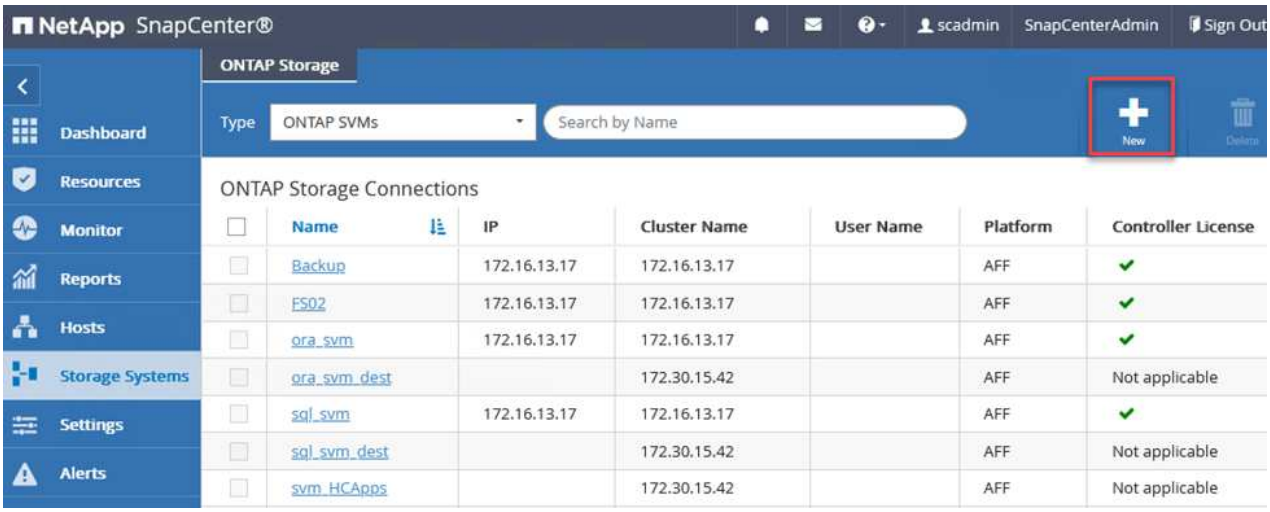
설치가 완료되면 *https://Virtual_Cluster_IP_or_FQDN:8146* 를 사용하여 웹 브라우저에서 SnapCenter 콘솔에 액세스할 수 있습니다.

콘솔에 로그인한 후 백업 SQL Server 및 Oracle 데이터베이스에 대해 SnapCenter를 구성해야 합니다.

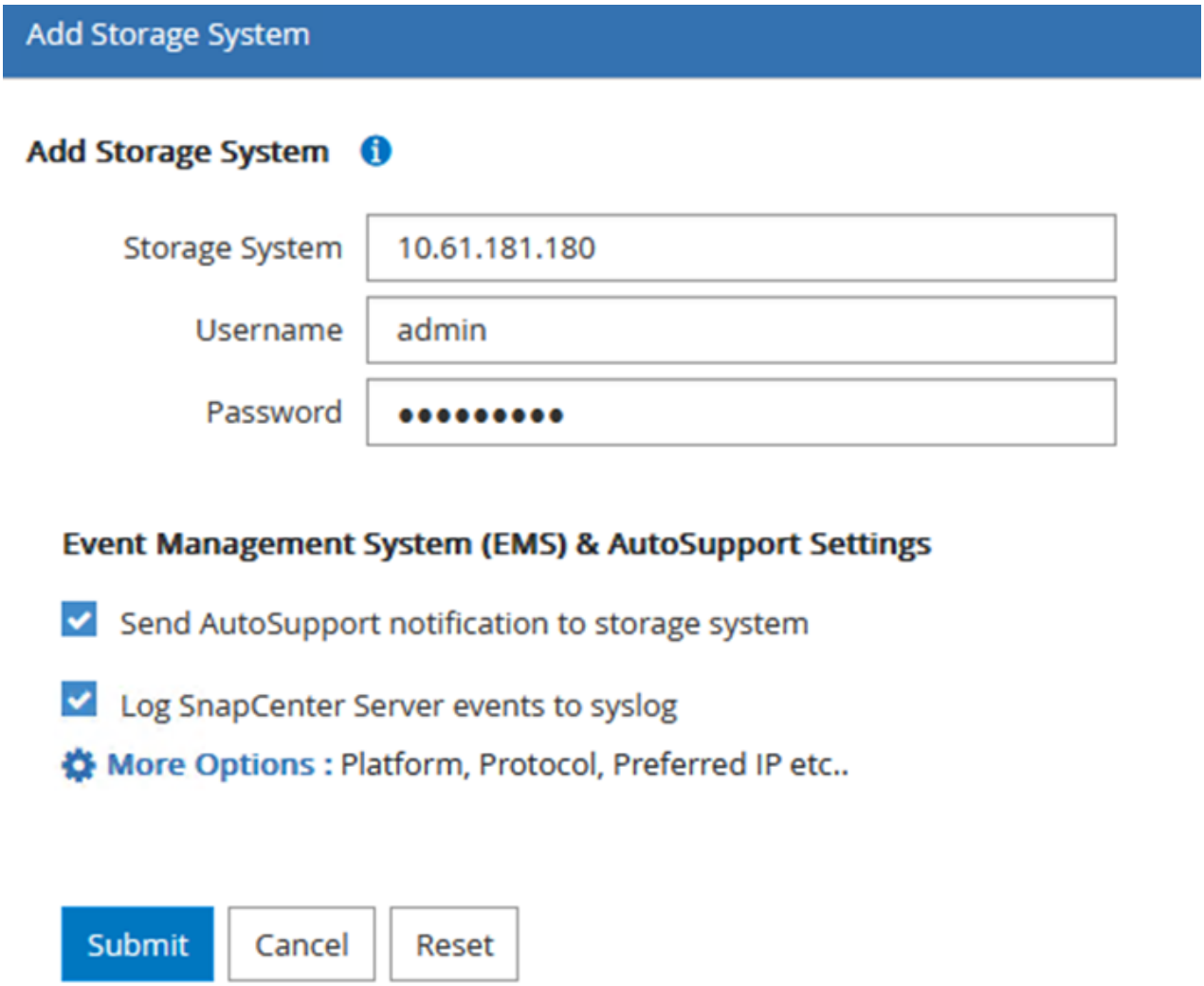
SnapCenter에 스토리지 컨트롤러를 추가합니다

SnapCenter에 스토리지 컨트롤러를 추가하려면 다음 단계를 수행하십시오.

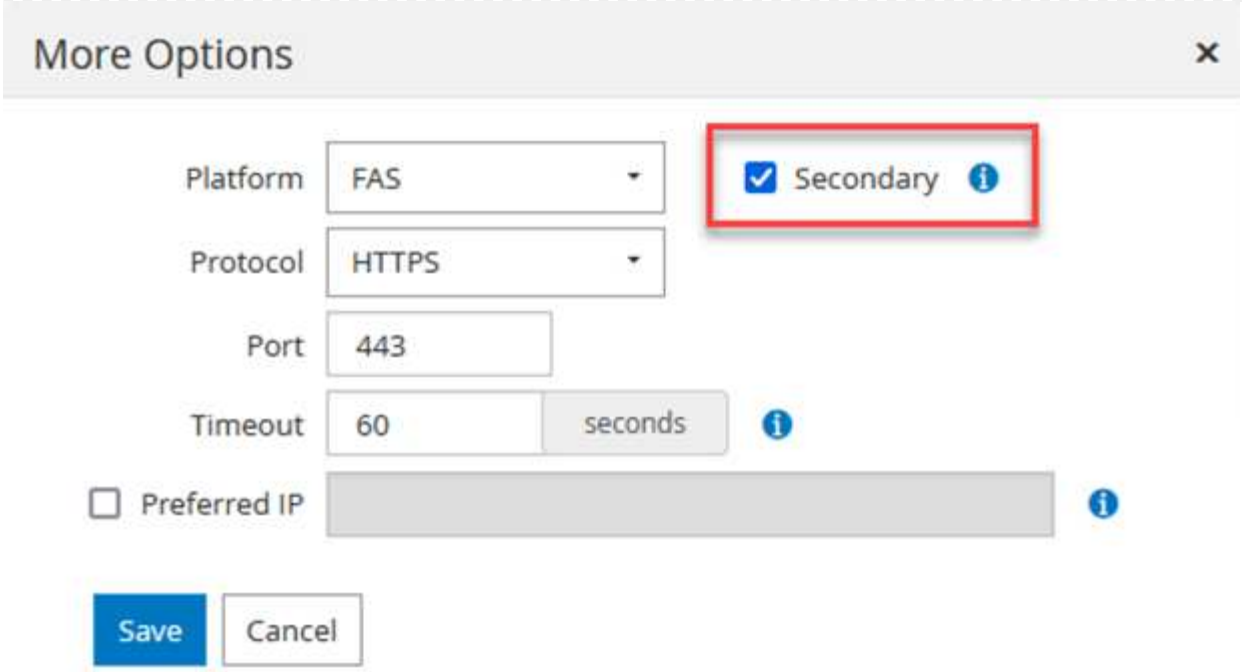
1. 왼쪽 메뉴에서 스토리지 시스템 을 선택한 다음 새로 만들기 를 클릭하여 스토리지 컨트롤러를 SnapCenter에 추가하는 프로세스를 시작합니다.



2. 스토리지 시스템 추가 대화 상자에서 로컬 온-프레미스 ONTAP 클러스터의 관리 IP 주소와 사용자 이름 및 암호를 추가합니다. 그런 다음 제출 을 클릭하여 스토리지 시스템 검색을 시작합니다.



3. 이 과정을 반복하여 FSx ONTAP 시스템을 SnapCenter에 추가합니다. 이 경우 Add Storage System 창의 아래쪽에 있는 More Options 를 선택하고 Secondary 의 확인란을 클릭하여 FSx 시스템을 SnapMirror 복사본 또는 기본 백업 스냅샷으로 업데이트된 보조 스토리지 시스템으로 지정합니다.

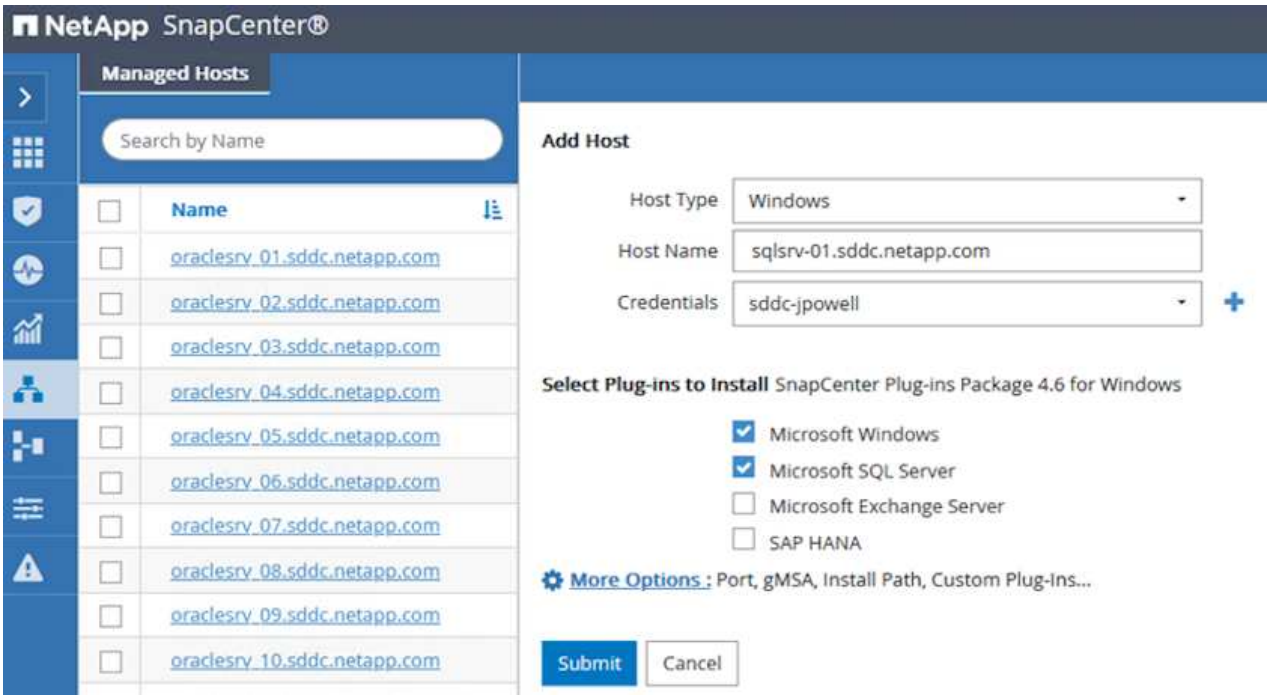


SnapCenter에 스토리지 시스템을 추가하는 방법에 대한 자세한 내용은 에서 설명서를 참조하십시오 "이 링크".

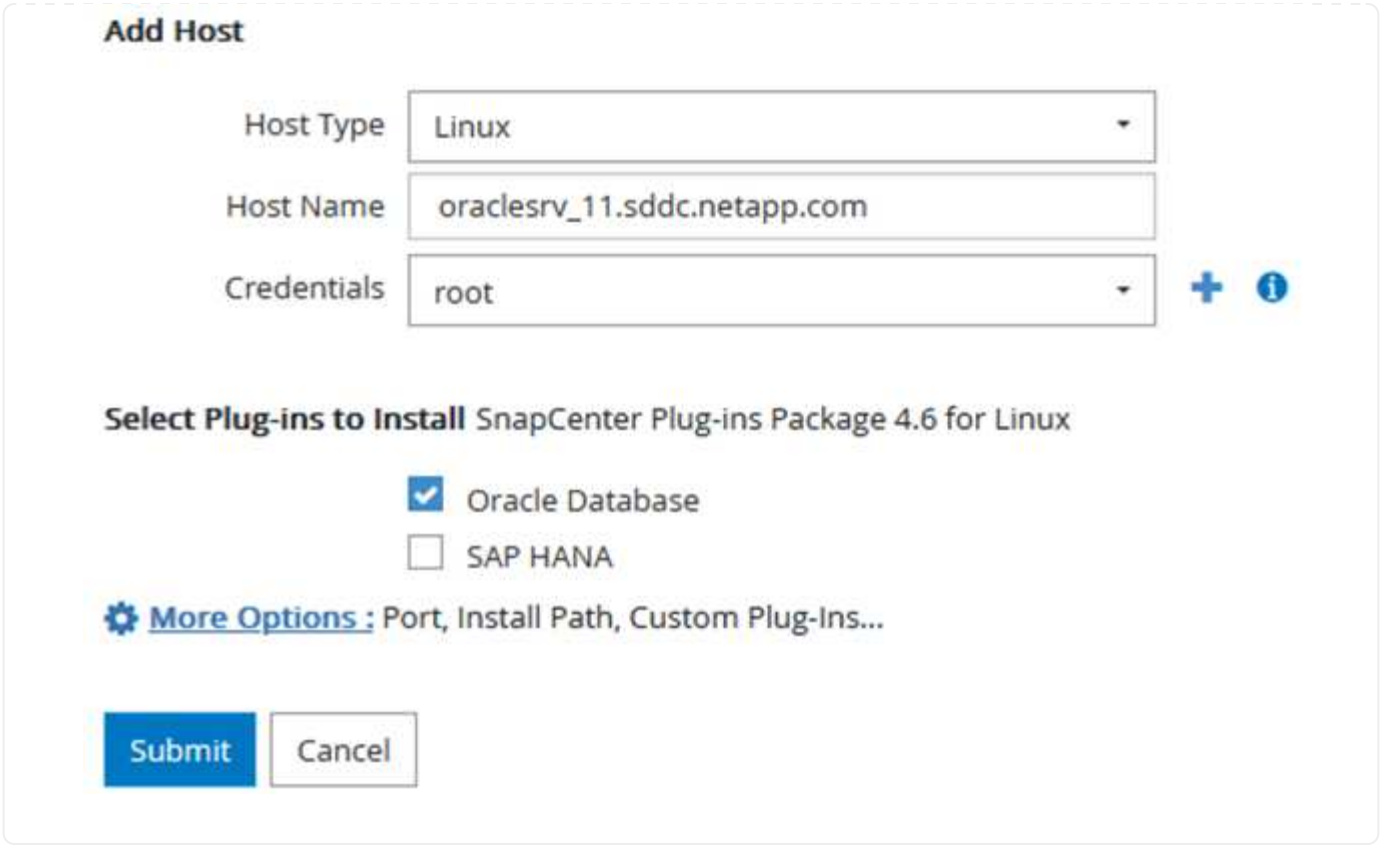
SnapCenter에 호스트를 추가합니다

다음 단계는 SnapCenter에 호스트 애플리케이션 서버를 추가하는 것입니다. 이 프로세스는 SQL Server와 Oracle에서 모두 비슷합니다.

1. 왼쪽 메뉴에서 호스트 를 선택한 다음 추가 를 클릭하여 스토리지 컨트롤러를 SnapCenter에 추가하는 프로세스를 시작합니다.
2. 호스트 추가 창에서 호스트 유형, 호스트 이름 및 호스트 시스템 자격 증명을 추가합니다. 플러그인 유형을 선택합니다. SQL Server의 경우 Microsoft Windows 및 Microsoft SQL Server 플러그인을 선택합니다.



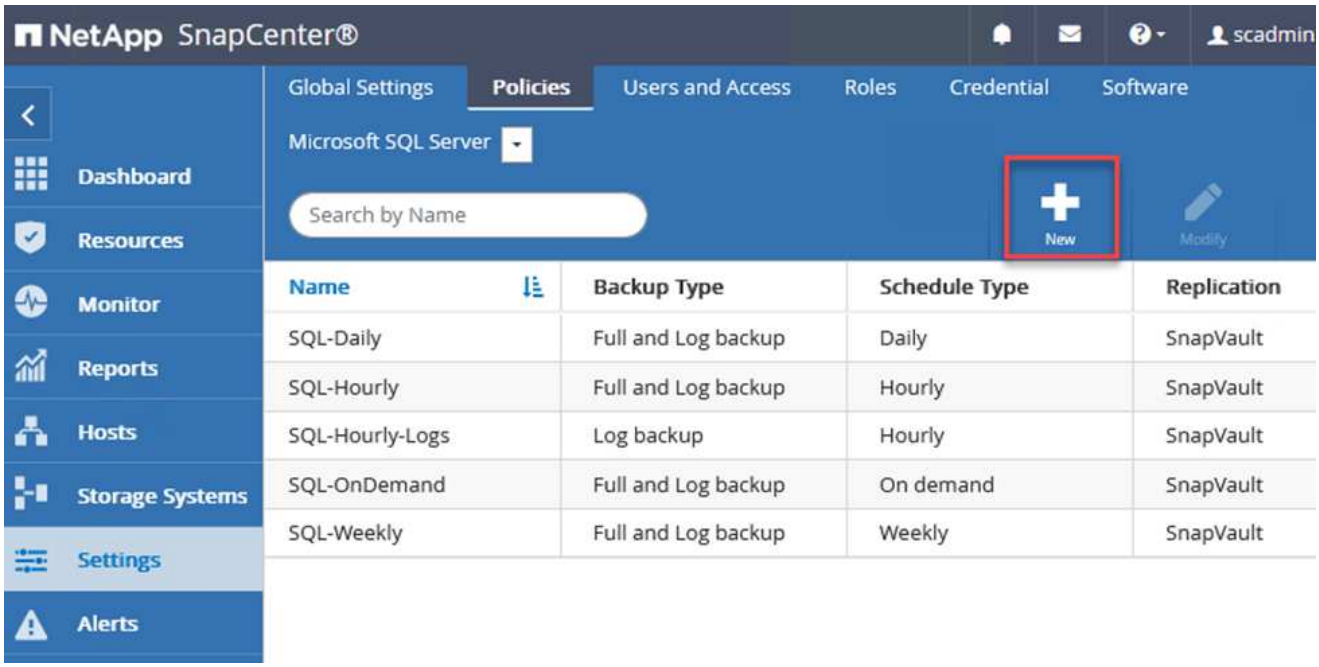
3. Oracle의 경우 호스트 추가 대화 상자에서 필수 필드를 입력하고 Oracle Database 플러그인의 확인란을 선택합니다. 그런 다음 제출 을 클릭하여 검색 프로세스를 시작하고 호스트를 SnapCenter에 추가합니다.


Add Host
Host Type
Linux
Host Name
oraclesrv_11.sddc.netapp.com
Credentials
root
Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux
Oracle Database
SAP HANA
More Options : Port, Install Path, Custom Plug-Ins...
Submit
Cancel

SnapCenter 정책을 생성합니다

정책은 백업 작업에 대해 따라야 할 특정 규칙을 설정합니다. 여기에는 백업 일정, 복제 유형 및 SnapCenter에서 트랜잭션 로그 백업 및 잘라내기를 처리하는 방식이 포함되며 이에 국한되지 않습니다.

SnapCenter 웹 클라이언트의 설정 섹션에서 정책에 액세스할 수 있습니다.

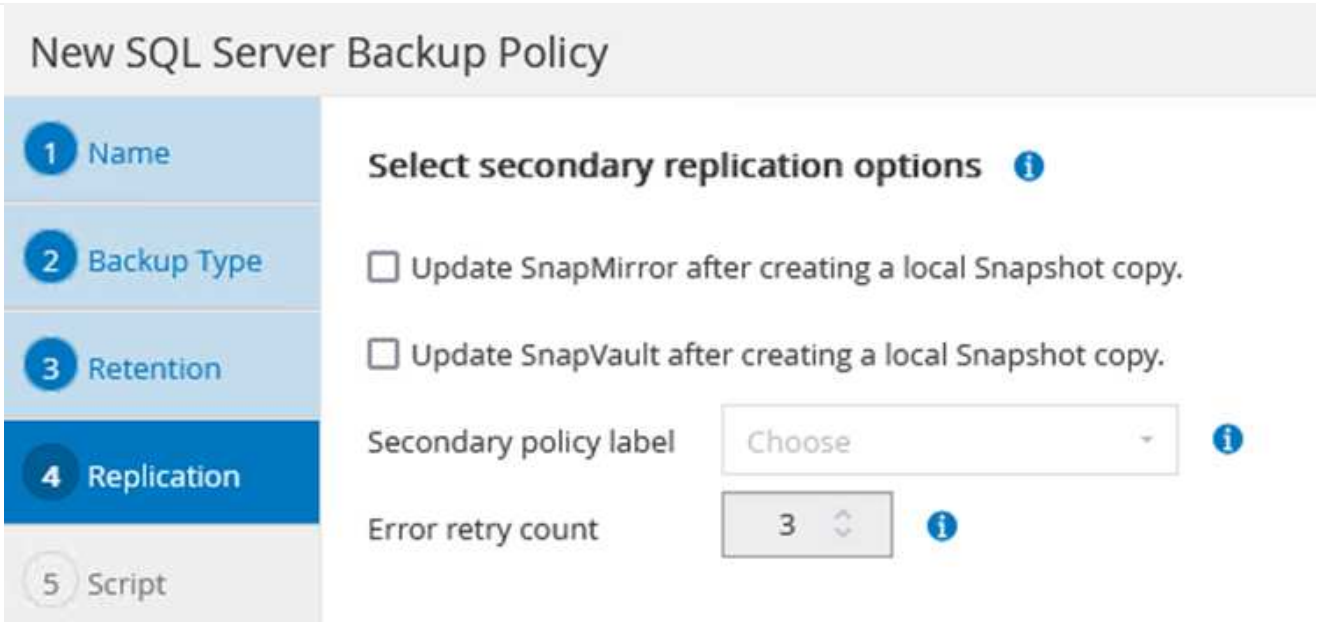


SQL Server 백업에 대한 정책을 생성하는 방법에 대한 자세한 내용은 를 참조하십시오 "SnapCenter 설명서".

Oracle 백업에 대한 정책을 생성하는 방법에 대한 자세한 내용은 를 참조하십시오 "SnapCenter 설명서".

- 참고: *
- 정책 생성 마법사를 진행하는 동안 복제 섹션을 특별히 기록해 둡니다. 이 섹션에서는 백업 프로세스 중에 사용할 보조 SnapMirror 복사본의 유형을 설명합니다.
- “로컬 스냅샷 복사본을 생성한 후 SnapMirror 업데이트” 설정은 동일한 클러스터에 상주하는 두 스토리지 가상 시스템 사이에 SnapMirror 관계가 존재하는 경우 SnapMirror 관계를 업데이트하는 것을 의미합니다.
- “로컬 스냅샷 복사본을 만든 후 SnapVault 업데이트” 설정은 두 개의 개별 클러스터와 온-프레미스 ONTAP 시스템과 Cloud Volumes ONTAP 또는 FSxN 사이에 존재하는 SnapMirror 관계를 업데이트하는 데 사용됩니다.

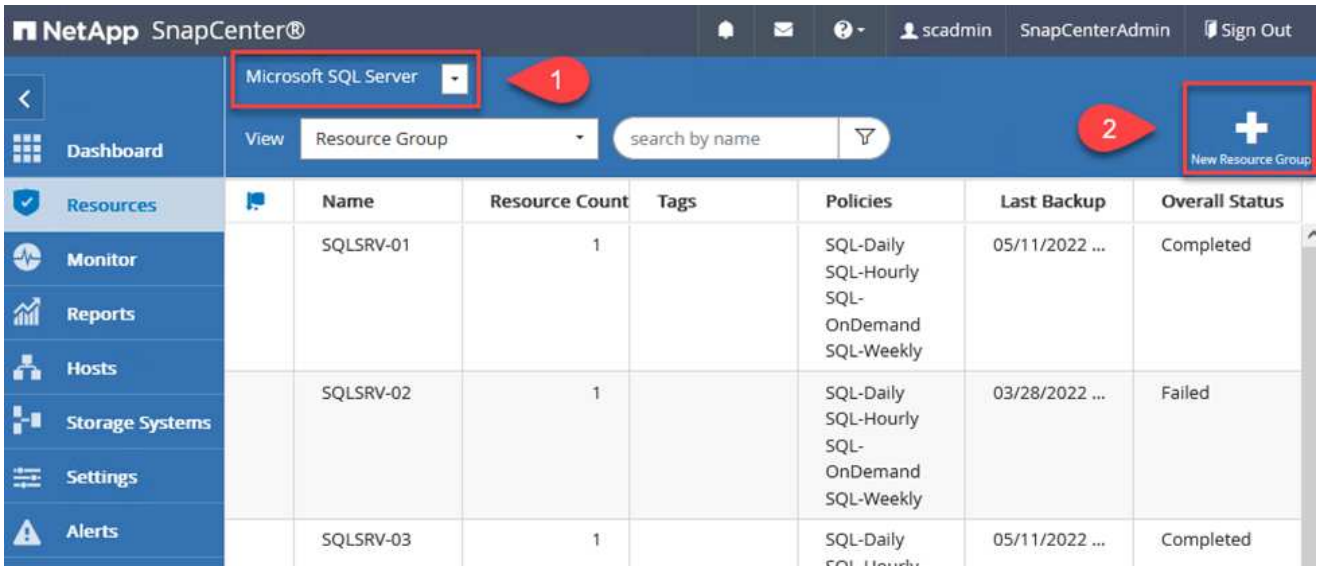
다음 이미지는 이전 옵션과 백업 정책 마법사에서 이러한 옵션이 표시되는 방식을 보여 줍니다.



SnapCenter 리소스 그룹을 생성합니다

리소스 그룹을 사용하면 백업에 포함할 데이터베이스 리소스와 해당 리소스에 대해 수행한 정책을 선택할 수 있습니다.

1. 왼쪽 메뉴의 리소스 섹션으로 이동합니다.
2. 창 위쪽에서 작업할 리소스 유형(이 경우 Microsoft SQL Server)을 선택한 다음 새 리소스 그룹을 클릭합니다.



SnapCenter 설명서는 SQL Server 및 Oracle 데이터베이스 모두에 대한 리소스 그룹을 생성하는 단계별 세부 정보를 제공합니다.

SQL 리소스 백업의 경우 에 따릅니다 "이 링크".

Oracle 리소스 백업에 대해서는 을 참조하십시오 "이 링크".

Veeam Backup Server를 구축 및 구성합니다

Veeam 백업 및 복제 소프트웨어는 Veeam 스케일 아웃 백업 저장소(SOBR)를 사용하여 애플리케이션 가상 머신을 백업하고 백업 복사본을 Amazon S3 버킷에 아카이빙하는 데 사용됩니다. Veeam을 이 솔루션의 Windows 서버에 구축했습니다. Veeam 구축에 대한 자세한 지침은 를 참조하십시오 "Veeam Help Center 기술 문서".

Veeam 스케일아웃 백업 저장소를 구성합니다

소프트웨어를 배포하고 라이센스를 받은 후에는 백업 작업을 위한 타겟 스토리지로 SOBR(스케일 아웃 백업 저장소)을 생성할 수 있습니다. 재해 복구를 위해 VM 데이터를 오프 사이트로 백업하는 데에도 S3 버킷을 포함해야 합니다.

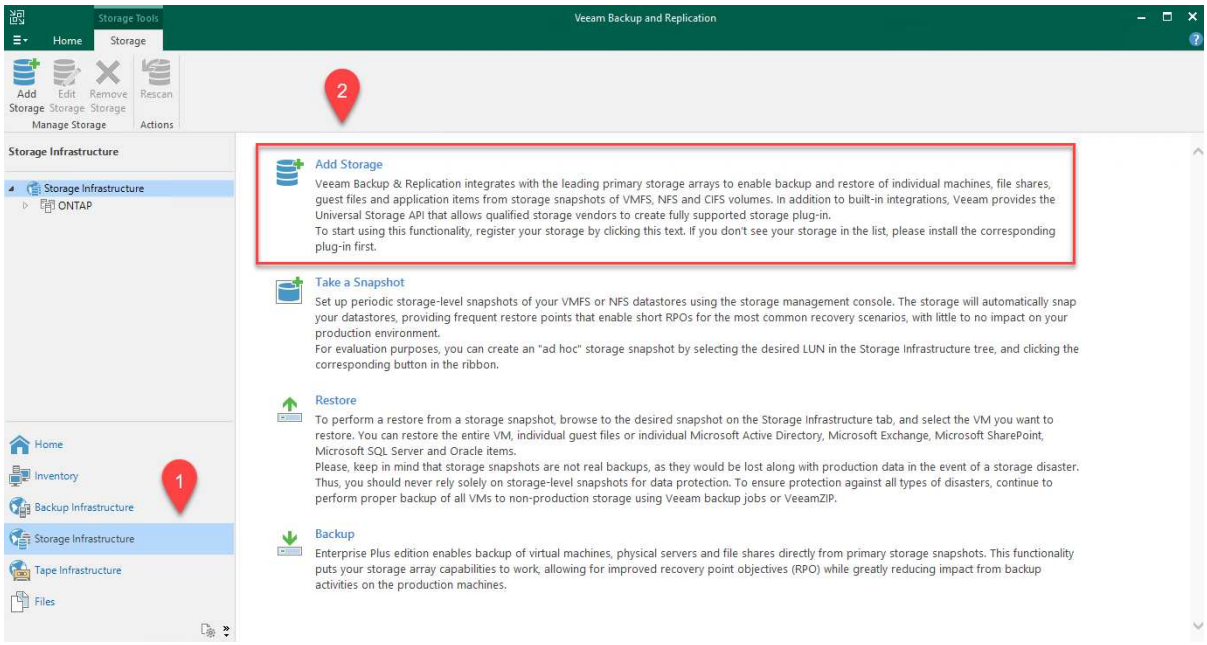
시작하기 전에 다음 필수 구성 요소를 참조하십시오.

1. 백업을 위한 타겟 스토리지로 사내 ONTAP 시스템에 SMB 파일 공유를 생성합니다.
2. SOBR에 포함할 Amazon S3 버킷을 생성합니다. 오프사이트 백업을 위한 저장소입니다.

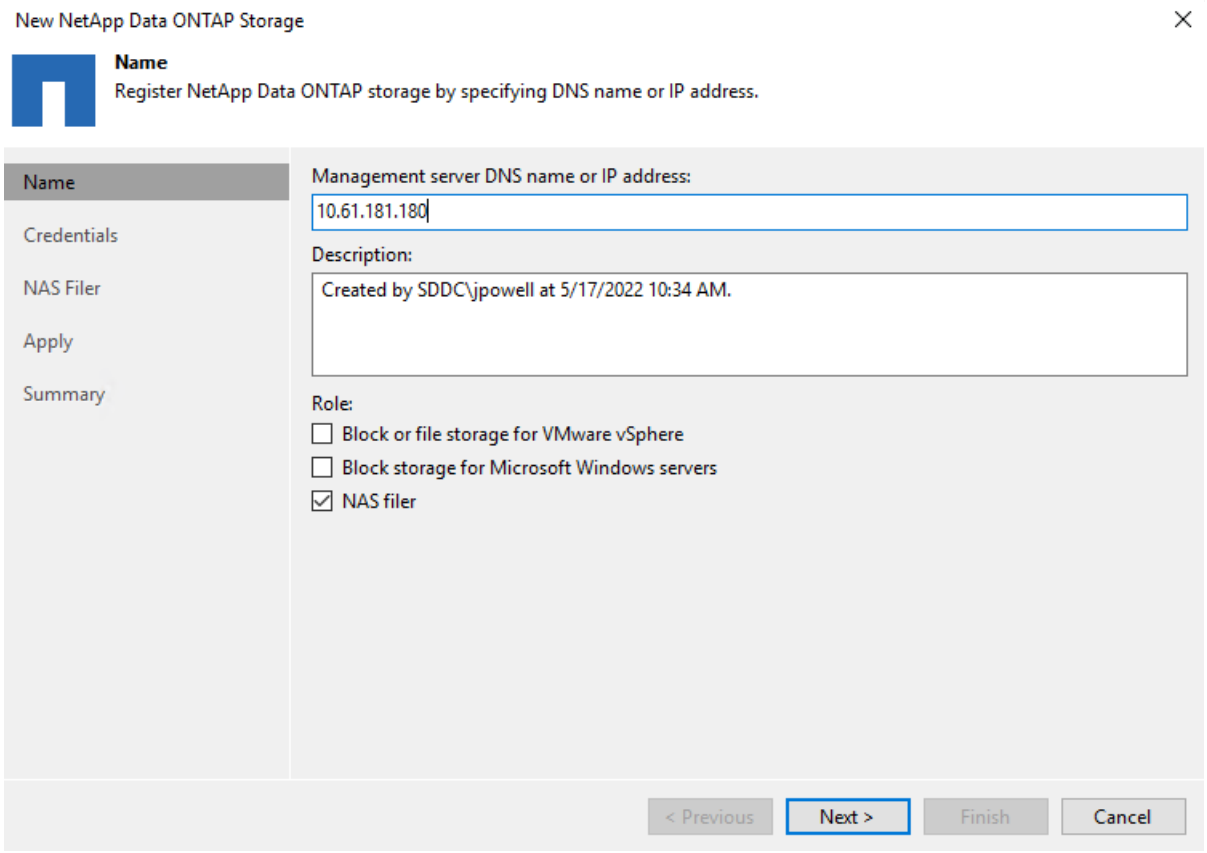
Veeam에 ONTAP 스토리지를 추가합니다

먼저, Veeam에서 ONTAP 스토리지 클러스터와 관련 SMB/NFS 파일 시스템을 스토리지 인프라로 추가합니다.

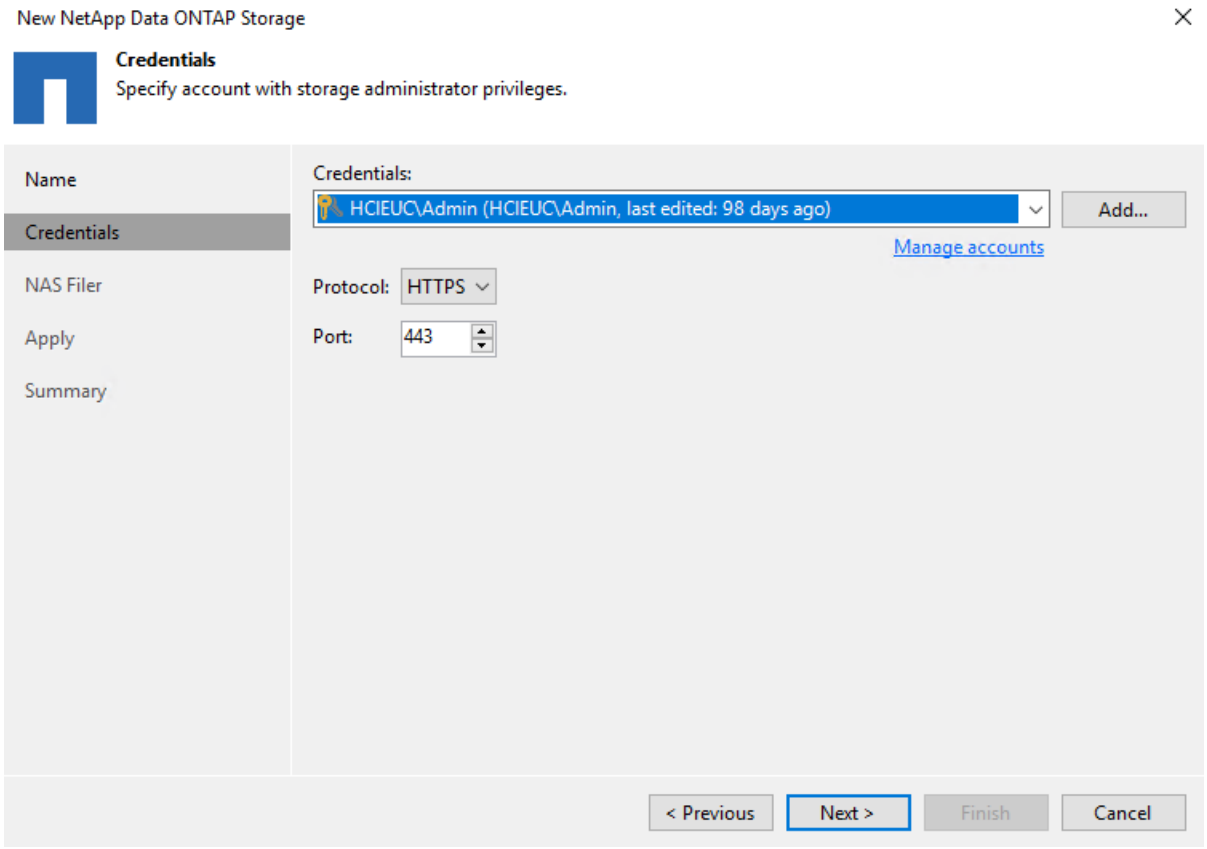
1. Veeam 콘솔을 열고 로그인합니다. Storage Infrastructure로 이동한 다음 Add Storage를 선택합니다.



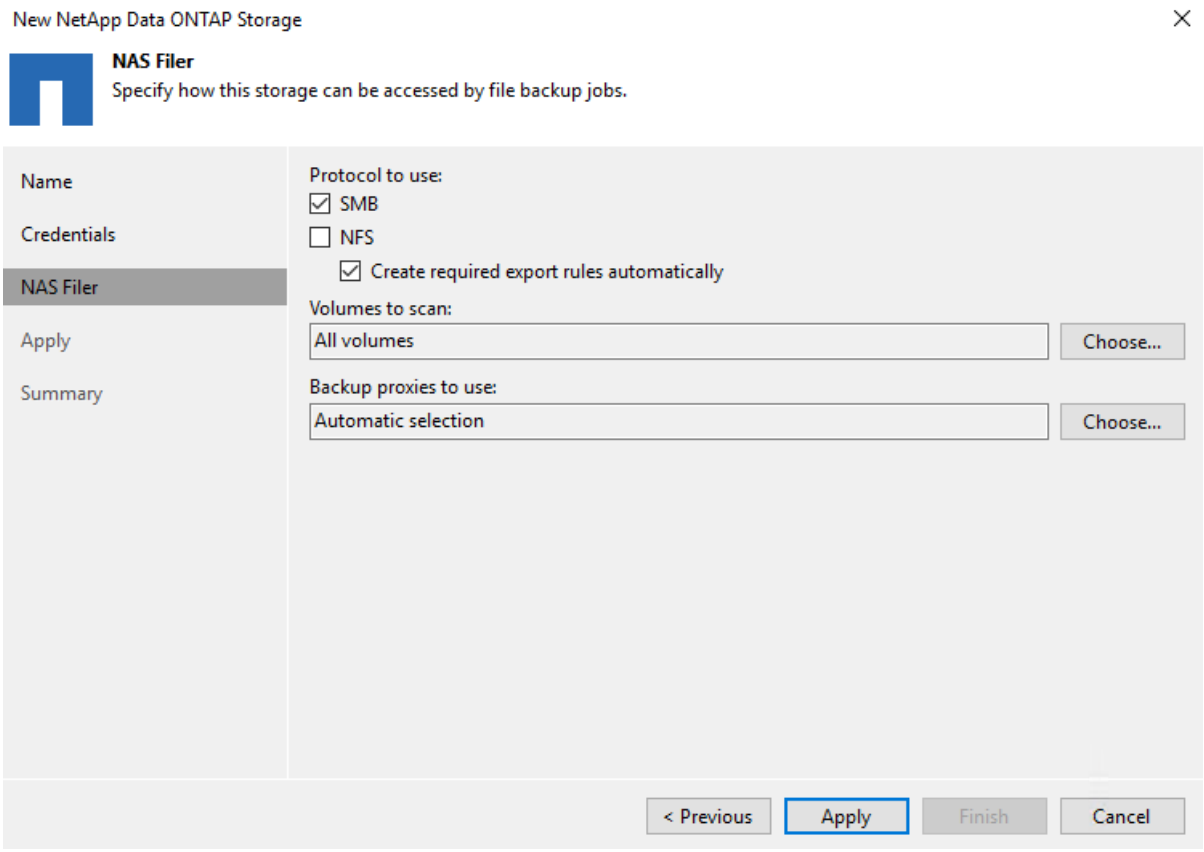
2. 스토리지 추가 마법사에서 NetApp을 스토리지 공급업체로 선택한 다음 Data ONTAP를 선택합니다.
3. 관리 IP 주소를 입력하고 NAS Filer 상자를 선택합니다. 다음 을 클릭합니다.



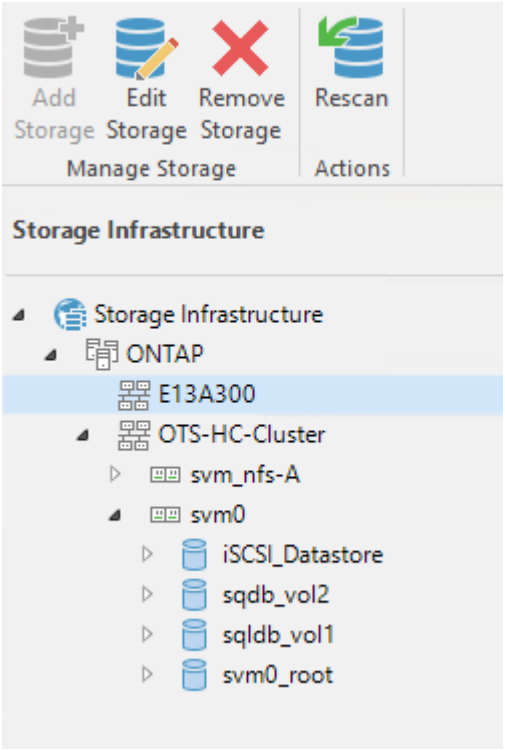
4. 자격 증명을 추가하여 ONTAP 클러스터에 액세스합니다.



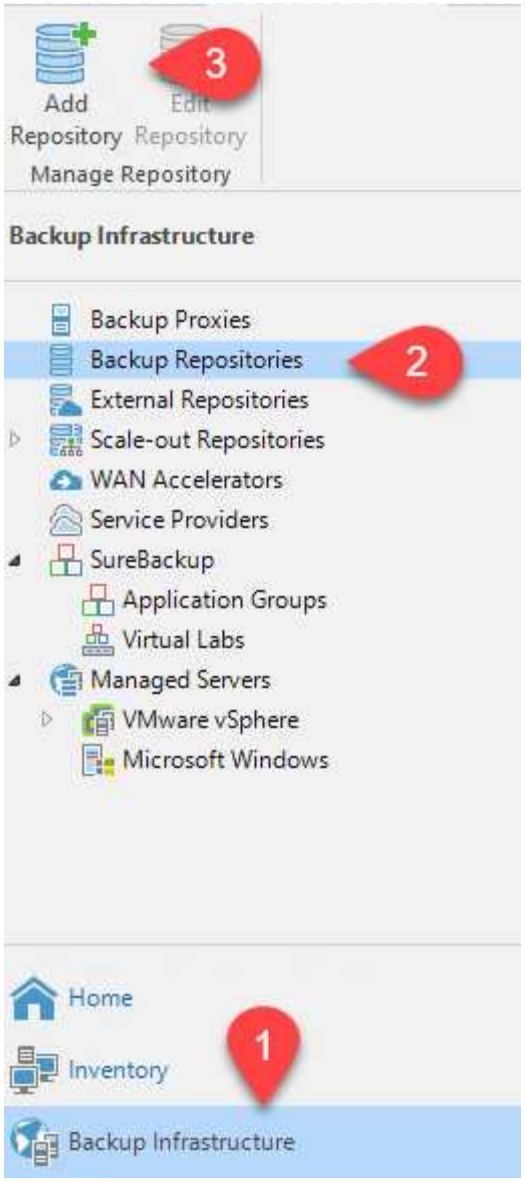
5. NAS Filer 페이지에서 검사할 프로토콜을 선택하고 Next 를 선택합니다.



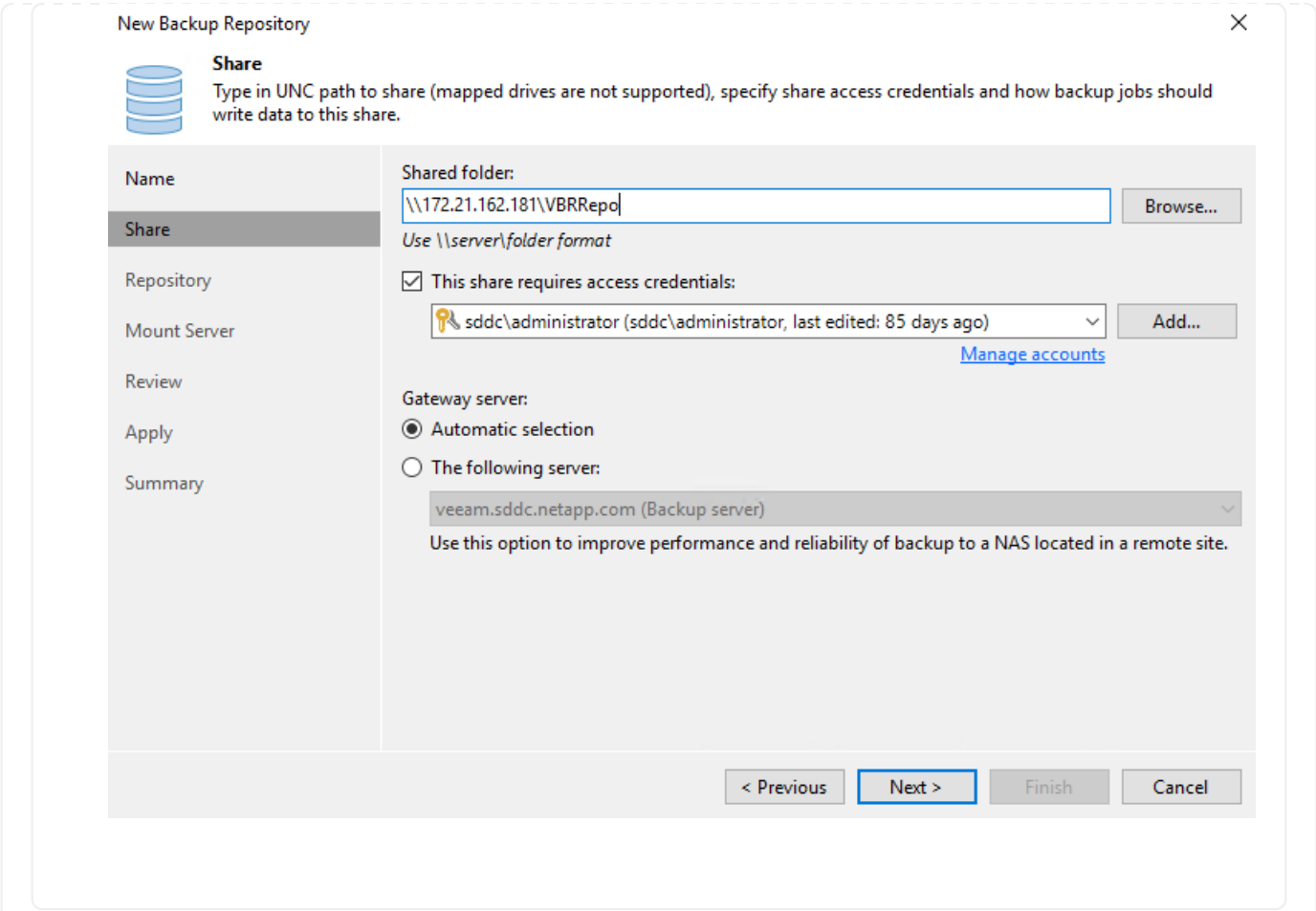
6. 마법사의 적용 및 요약 페이지를 완료하고 마침 을 클릭하여 스토리지 검색 프로세스를 시작합니다. 검사가 완료되면 ONTAP 클러스터가 NAS 파일러와 함께 사용 가능한 리소스로 추가됩니다.



7. 새로 검색된 NAS 공유를 사용하여 백업 리포지토리를 생성합니다. Backup Infrastructure에서 Backup Repositories를 선택하고 Add Repository 메뉴 항목을 클릭합니다.



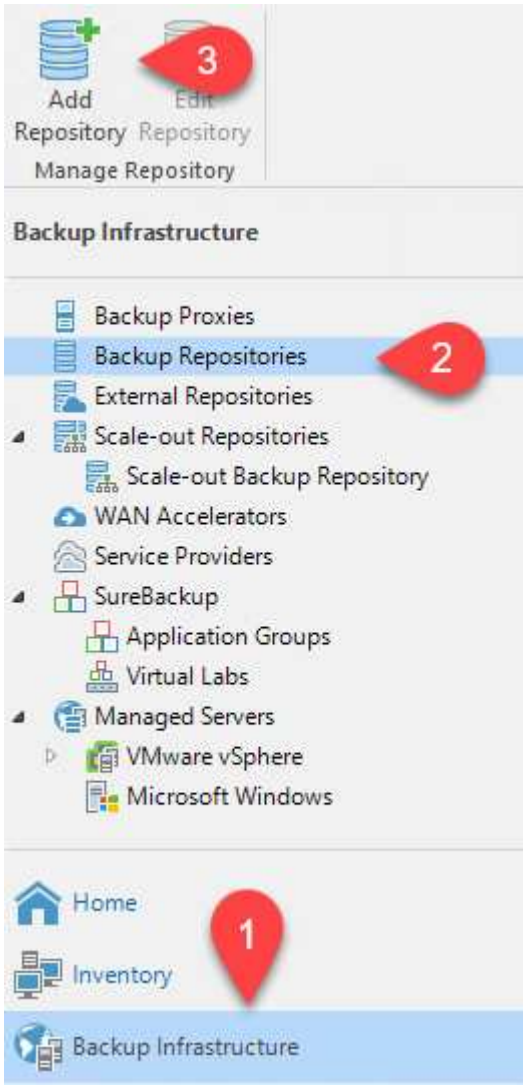
8. 새 백업 저장소 마법사의 모든 단계를 수행하여 리포지토리를 생성합니다. Veeam Backup Repositories 생성에 대한 자세한 내용은 를 참조하십시오 "Veeam 문서를 참조하십시오".


New Backup Repository
Share
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.
Name
Share
Repository
Mount Server
Review
Apply
Summary
Shared folder:
\\172.21.162.181\VBRRepo
Browse...
Use \\server\folder format
This share requires access credentials:
sddc\administrator (sddc\administrator, last edited: 85 days ago)
Add...
Manage accounts
Gateway server:
Automatic selection
The following server:
veeam.sddc.netapp.com (Backup server)
Use this option to improve performance and reliability of backup to a NAS located in a remote site.
< Previous
Next >
Finish
Cancel

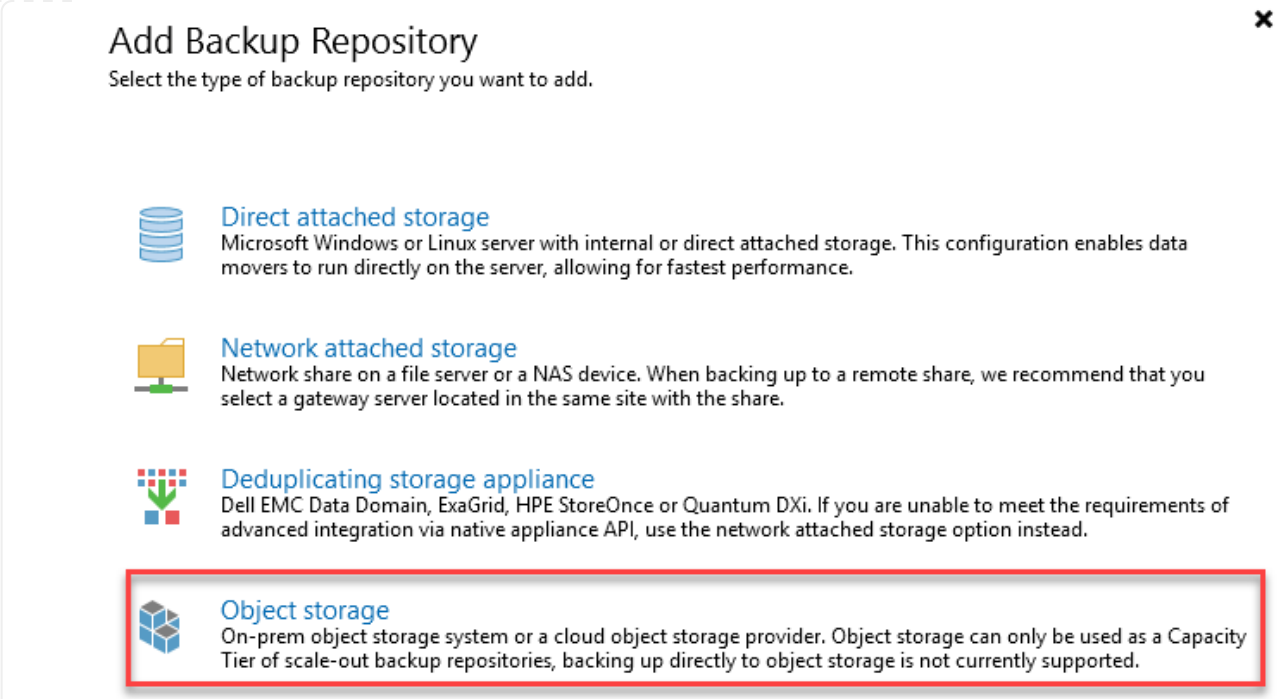
Amazon S3 버킷을 백업 저장소로 추가합니다

다음 단계는 Amazon S3 스토리지를 백업 저장소로 추가하는 것입니다.

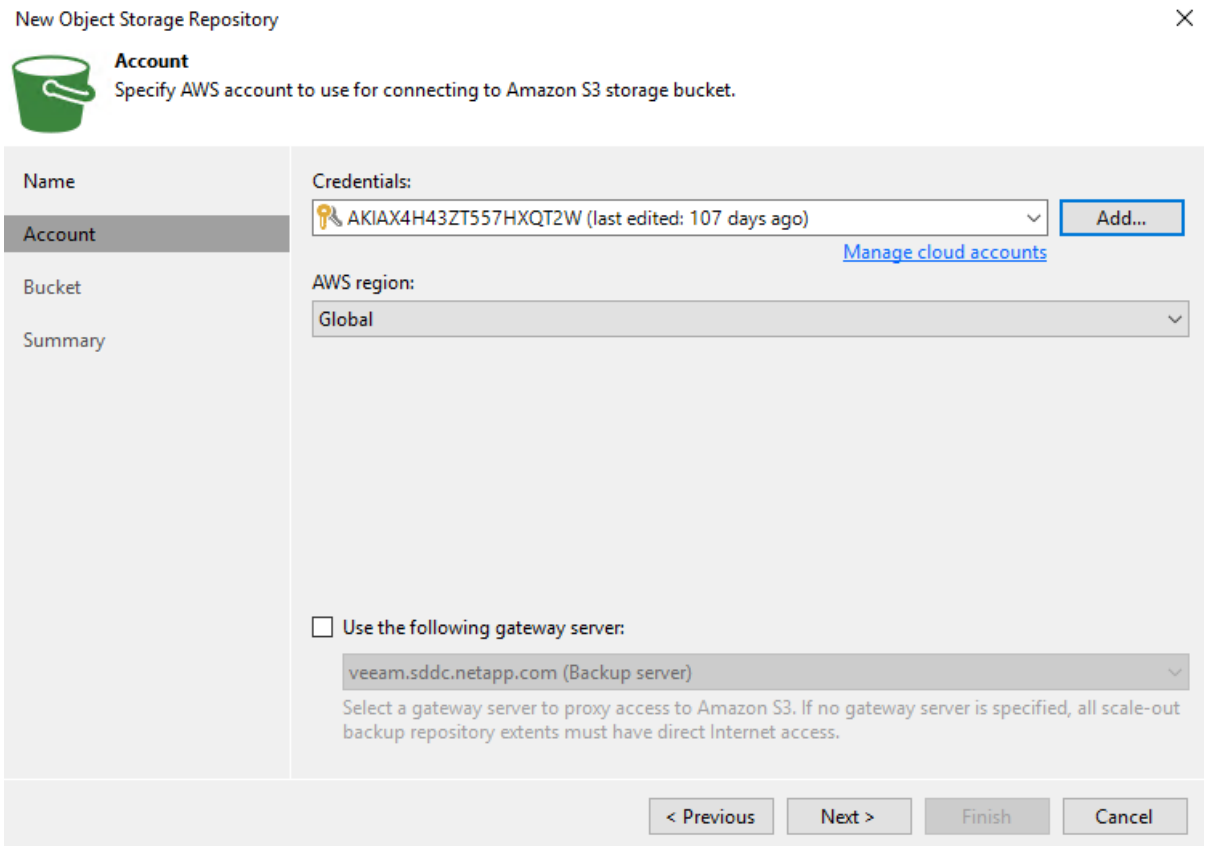
1. Backup Infrastructure > Backup Repositories 로 이동합니다. 리포지토리 추가 를 클릭합니다.



2. 백업 저장소 추가 마법사에서 오브젝트 스토리지 를 선택한 다음 Amazon S3를 선택합니다. 그러면 New Object Storage Repository 마법사가 시작됩니다.



3. 오브젝트 스토리지 저장소의 이름을 입력하고 Next를 클릭합니다.
4. 다음 섹션에서 자격 증명을 입력합니다. AWS 액세스 키와 비밀 키가 필요합니다.

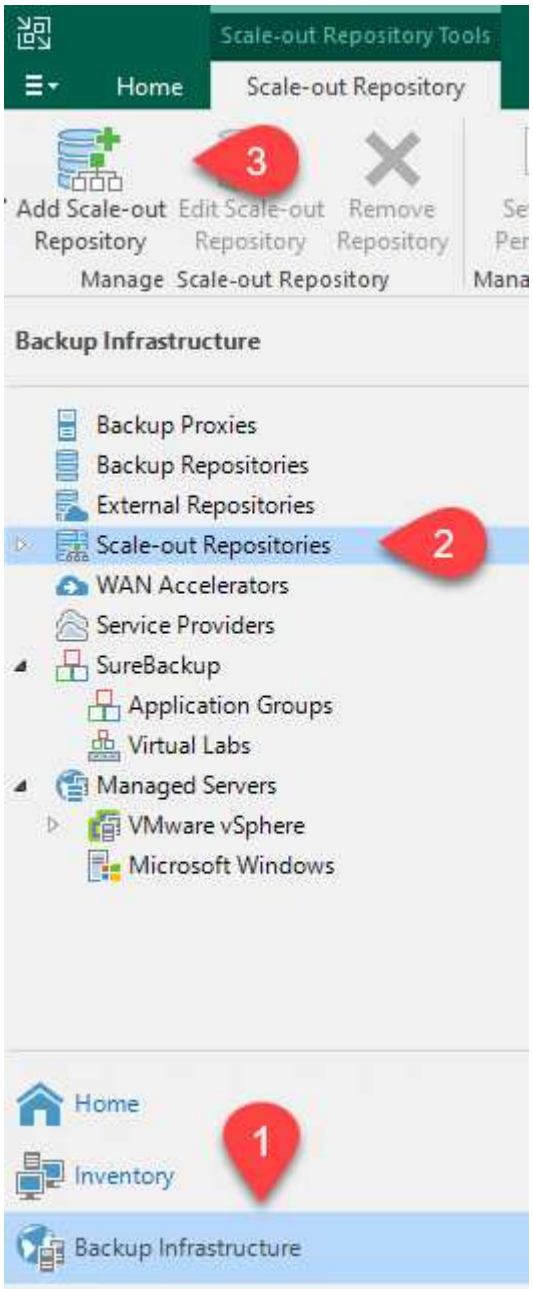


5. Amazon 구성이 로드되면 데이터 센터, 버킷 및 폴더를 선택하고 적용 을 클릭합니다. 마지막으로 마침을 클릭하여 마법사를 닫습니다.

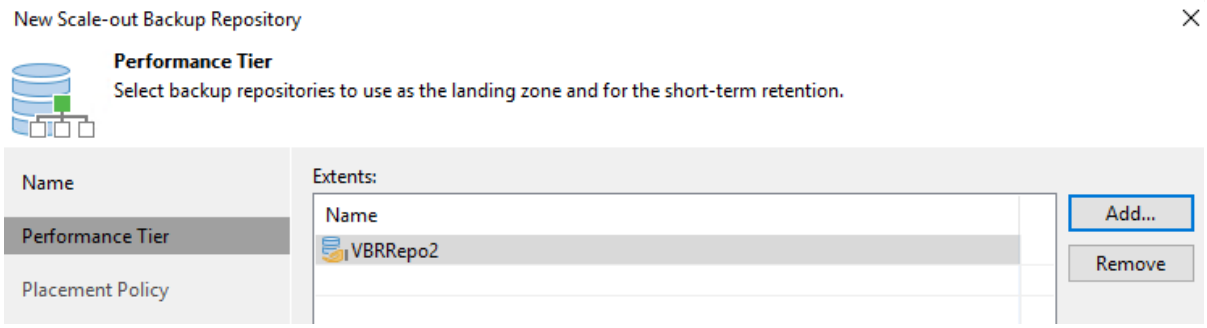
스케일아웃 백업 저장소를 생성합니다

이제 Veeam에 스토리지 저장소를 추가했으므로 재해 복구를 위해 SOBR을 생성하여 백업 복사본을 외부 Amazon S3 오브젝트 스토리지에 자동으로 계층화할 수 있습니다.

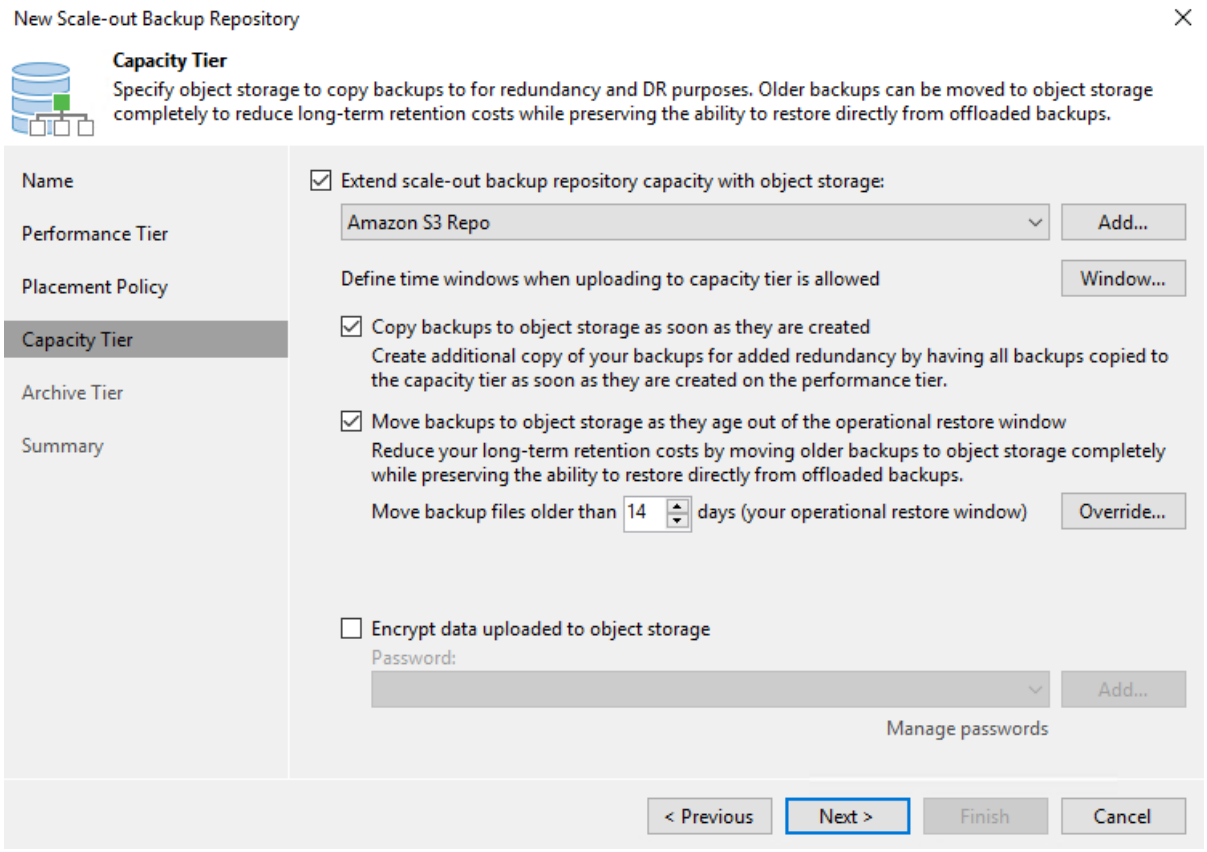
1. 백업 인프라 에서 스케일 아웃 리포지토리 를 선택한 다음 스케일 아웃 리포지토리 추가 메뉴 항목을 클릭합니다.



2. 새 스케일 아웃 백업 리포지토리에서 SOBR의 이름을 제공하고 다음을 클릭합니다.
3. 성능 계층의 경우 로컬 ONTAP 클러스터에 상주하는 SMB 공유가 포함된 백업 저장소를 선택합니다.



4. 배치 정책의 경우 데이터 인접성 또는 요구 사항에 따른 성능 을 선택합니다. 다음을 선택합니다.
5. 용량 계층의 경우 Amazon S3 오브젝트 스토리지로 SOBR을 확장합니다. 재해 복구를 위해, 2차 백업을 적시에 제공할 수 있도록 백업이 생성되는 즉시 Copy Backups to Object Storage 를 선택합니다.



6. 마지막으로 적용 및 마침 을 선택하여 SOBR 생성을 마칩니다.

스케일아웃 백업 저장소 작업을 생성합니다

Veeam을 구성하는 마지막 단계는 새로 생성한 SOBR을 백업 대상으로 사용하여 백업 작업을 생성하는 것입니다. 백업 작업 생성은 스토리지 관리자의 일반적인 일부이며 여기서는 자세한 단계를 다루지 않습니다. Veeam에서 백업 작업 생성에 대한 자세한 내용은 를 참조하십시오 "Veeam Help Center 기술 문서".

BlueXP 백업 및 복구 툴 및 구성

애플리케이션 VM 및 데이터베이스 볼륨을 AWS에서 실행되는 VMware Cloud Volume 서비스로 페일오버하려면 SnapCenter Server와 Veeam Backup and Replication Server의 실행 중인 인스턴스를 설치 및 구성해야 합니다. 페일오버가 완료된 후 사내 데이터 센터에 대한 페일백이 계획 및 실행될 때까지 정상적인 백업 작업을 재개하도록 이러한 툴을 구성해야 합니다.

보조 Windows SnapCenter 서버를 배포합니다

SnapCenter 서버는 VMware 클라우드 SDDC에 구축하거나 VMware 클라우드 환경에 대한 네트워크 연결을 통해 VPC에 상주하는 EC2 인스턴스에 설치됩니다.

SnapCenter 소프트웨어는 NetApp Support 사이트에서 제공되며 도메인 또는 작업 그룹에 있는 Microsoft Windows 시스템에 설치할 수 있습니다. 자세한 계획 가이드 및 설치 지침은 에서 확인할 수 있습니다 "NetApp 문서화 센터".

SnapCenter 소프트웨어는 에서 찾을 수 있습니다 "이 링크".

보조 Windows SnapCenter 서버를 구성합니다

FSx ONTAP에 미러링된 애플리케이션 데이터를 복구하려면 먼저 온-프레미스 SnapCenter 데이터베이스의 전체 복원을 수행해야 합니다. 이 프로세스가 완료되면 VM과의 통신이 다시 설정되고 FSx ONTAP를 기본 스토리지로 사용하여 응용 프로그램 백업을 다시 시작할 수 있습니다.

이를 위해서는 SnapCenter 서버에서 다음 항목을 완료해야 합니다.

1. 원래 온-프레미스 SnapCenter 서버와 동일하게 컴퓨터 이름을 구성합니다.
2. VMware 클라우드 및 FSx ONTAP 인스턴스와 통신하도록 네트워킹을 구성합니다.
3. SnapCenter 데이터베이스를 복원하는 절차를 완료합니다.
4. SnapCenter가 재해 복구 모드에 있는지 확인하여 이제 FSx가 백업용 기본 스토리지인지 확인합니다.
5. 복구된 가상 머신과 통신이 다시 설정되었는지 확인합니다.

2차 Veeam Backup & amp; Replication Server를 구축합니다

Veeam Backup & Replication 서버를 AWS의 VMware Cloud 또는 EC2 인스턴스에 설치할 수 있습니다. 자세한 구현 지침은 를 참조하십시오 "Veeam Help Center 기술 문서".

Secondary Veeam Backup & amp; Replication Server를 구성합니다

Amazon S3 스토리지에 백업된 가상 머신의 복구를 수행하려면 Veeam Server를 Windows 서버에 설치하고 원래 백업 저장소가 포함된 VMware Cloud, FSx ONTAP 및 S3 버킷과 통신하도록 구성해야 합니다. 또한 VM이 복구된 후 새 백업을 수행하려면 FSx ONTAP에 새 백업 리포지토리가 구성되어 있어야 합니다.

이 프로세스를 수행하려면 다음 항목을 완료해야 합니다.

1. 네트워킹을 구성하여 원래 백업 저장소가 포함된 VMware Cloud, FSx ONTAP 및 S3 버킷과 통신합니다.
2. FSx ONTAP에서 SMB 공유를 새 백업 리포지토리로 구성합니다.
3. 사내에서 스케일아웃 백업 저장소의 일부로 사용된 원래 S3 버킷을 마운트합니다.
4. VM을 복구한 후 SQL 및 Oracle VM을 보호하기 위한 새로운 백업 작업을 설정합니다.

Veeam을 사용하여 VM을 복원하는 방법에 대한 자세한 내용은 섹션을 참조하십시오 "Veeam Full Restore로 애플리케이션 VM을 복구합니다".

재해 복구를 위한 **SnapCenter** 데이터베이스 백업

SnapCenter를 사용하면 재해 발생 시 SnapCenter 서버를 복구하기 위해 기본 MySQL 데이터베이스와 구성 데이터를 백업 및 복구할 수 있습니다. 이 솔루션을 위해 VPC에 상주하는 AWS EC2 인스턴스에서 SnapCenter 데이터베이스 및 구성을 복구했습니다. 이 단계에 대한 자세한 내용은 을 참조하십시오 "이 링크".

SnapCenter 백업 사전 요구 사항

SnapCenter 백업에 필요한 사전 요구 사항은 다음과 같습니다.

- 백업된 데이터베이스 및 구성 파일을 찾기 위해 사내 ONTAP 시스템에서 생성된 볼륨 및 SMB 공유입니다.
- 사내 ONTAP 시스템과 AWS 계정의 FSx 또는 CVO 간 SnapMirror 관계 이 관계는 백업된 SnapCenter 데이터베이스 및 구성 파일이 포함된 스냅샷을 전송하는 데 사용됩니다.
- EC2 인스턴스 또는 VMware Cloud SDDC의 VM에 클라우드 계정에 설치된 Windows Server
- VMware 클라우드의 Windows EC2 인스턴스 또는 VM에 설치된 SnapCenter

SnapCenter 백업 및 복원 프로세스 요약

- 백업 db 및 config 파일을 호스팅하기 위해 사내 ONTAP 시스템에 볼륨을 생성합니다.
- 온프레미스와 FSx/CVO 간에 SnapMirror 관계를 설정합니다.
- SMB 공유를 마운트합니다.
- API 작업을 수행하기 위한 Swagger 인증 토큰을 검색합니다.
- DB 복구 프로세스를 시작합니다.
- xcopy 유틸리티를 사용하여 db 및 config 파일 로컬 디렉토리를 SMB 공유에 복사합니다.
- FSx에서 ONTAP 볼륨의 클론을 생성합니다(사내에서 SnapMirror를 통해 복사됨).
- FSx에서 EC2/VMware Cloud로 SMB 공유를 마운트합니다.
- SMB 공유에서 로컬 디렉토리로 복구 디렉토리를 복사합니다.
- Swagger에서 SQL Server 복원 프로세스를 실행합니다.

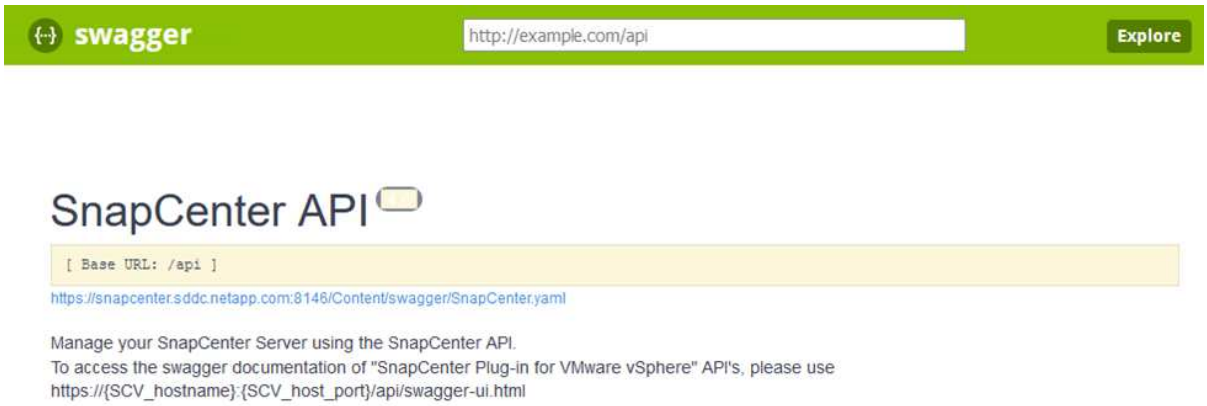
SnapCenter 데이터베이스 및 구성을 백업합니다

SnapCenter는 REST API 명령을 실행하기 위한 웹 클라이언트 인터페이스를 제공합니다. Swagger를 통해 REST API에 액세스하는 방법에 대한 자세한 내용은 에서 SnapCenter 설명서를 참조하십시오 "이 링크".

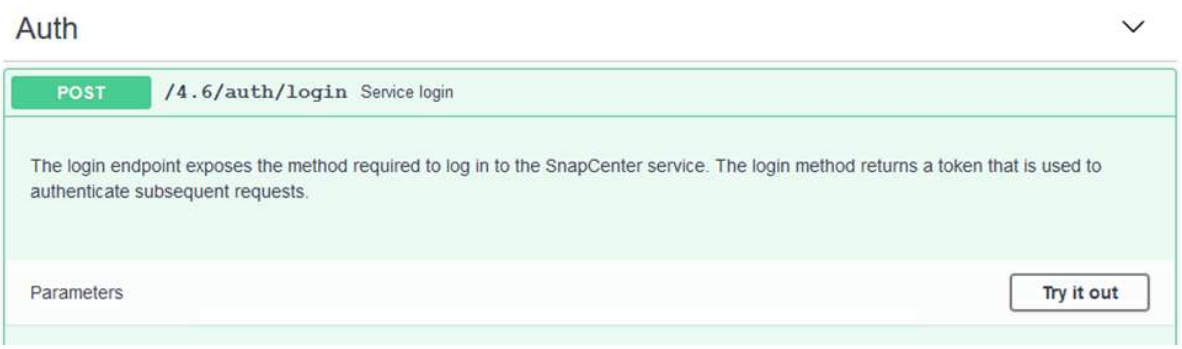
Swagger에 로그인하고 인증 토큰을 얻습니다

Swagger 페이지로 이동한 후 인증 토큰을 검색하여 데이터베이스 복원 프로세스를 시작해야 합니다.

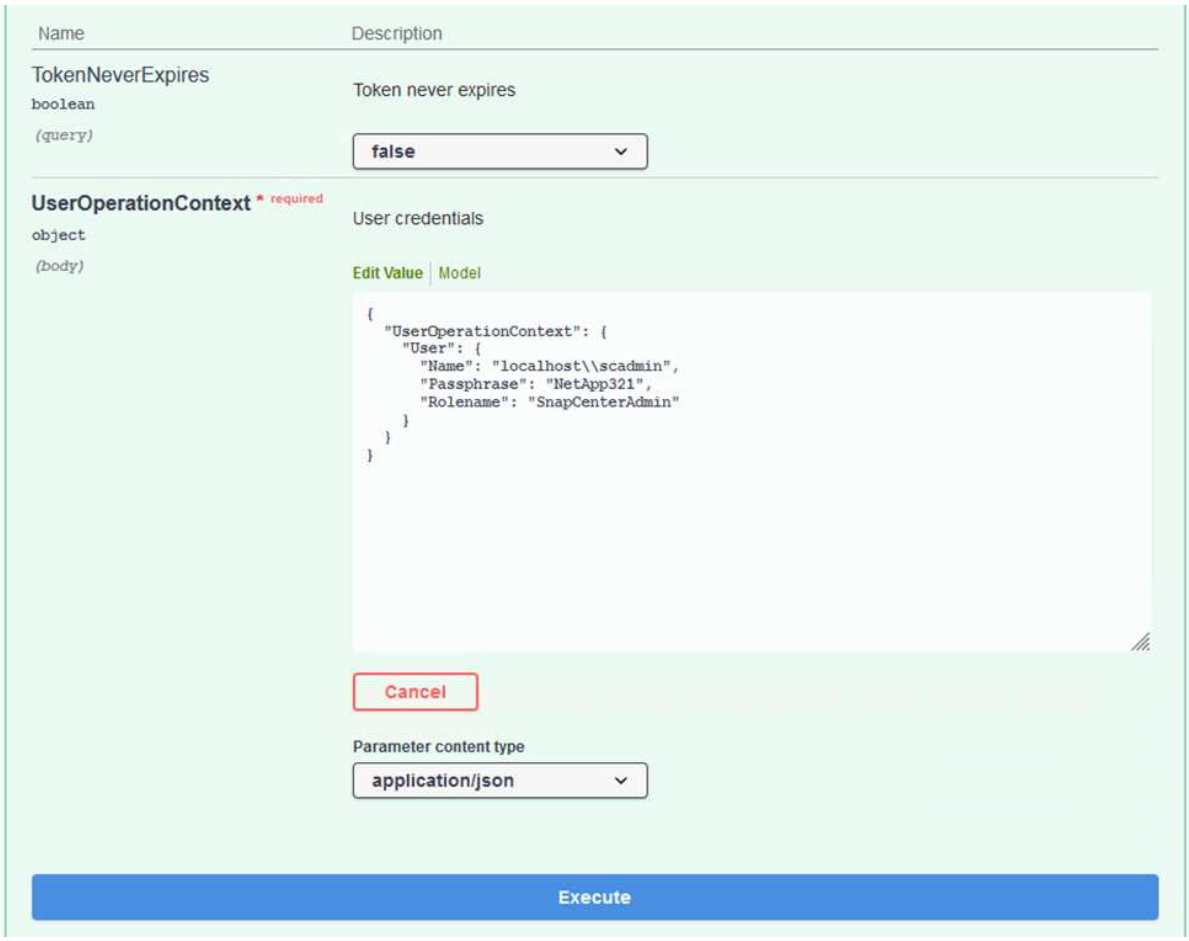
1. https://<SnapCenter 서버 IP >:8146/swagger/_에서 SnapCenter Swagger API 웹 페이지에 액세스합니다.



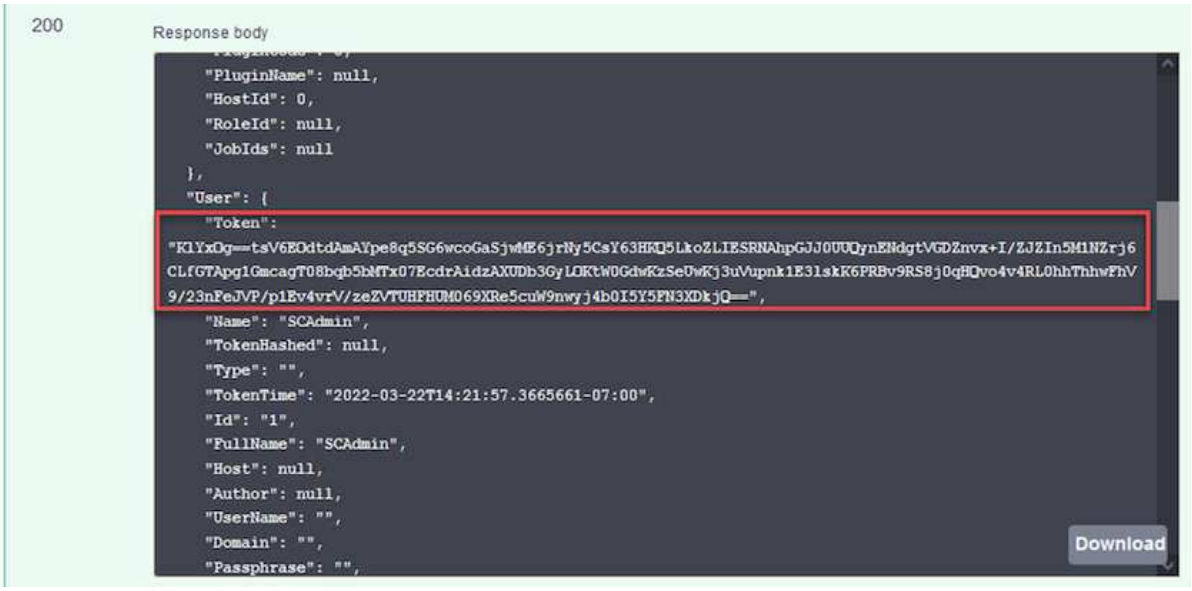
2. 인증 섹션을 확장하고 시험 사용 을 클릭합니다.



3. UserOperationContext 영역에서 SnapCenter 자격 증명 및 역할을 입력하고 실행 을 클릭합니다.



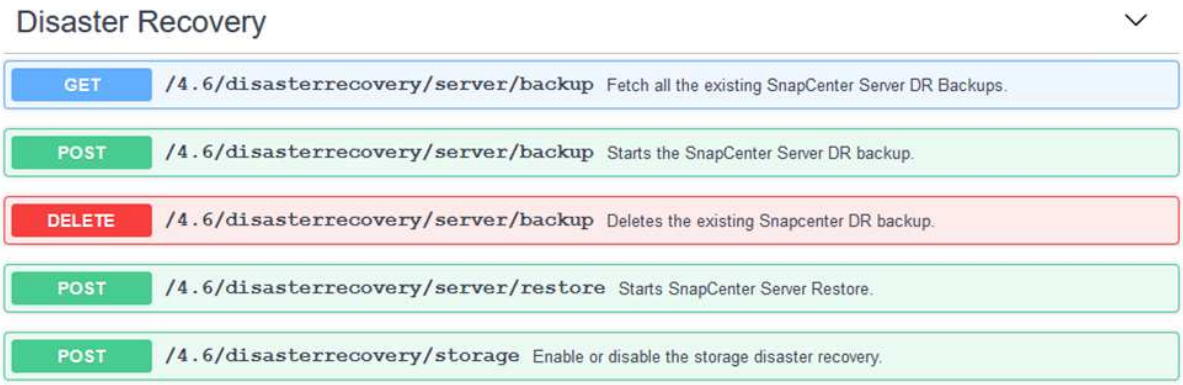
4. 아래의 응답 본문에서 토큰을 볼 수 있습니다. 백업 프로세스를 실행할 때 인증을 위해 토큰 텍스트를 복사합니다.



SnapCenter 데이터베이스 백업을 수행합니다

그런 다음 Swagger 페이지의 Disaster Recovery 영역으로 이동하여 SnapCenter 백업 프로세스를 시작합니다.

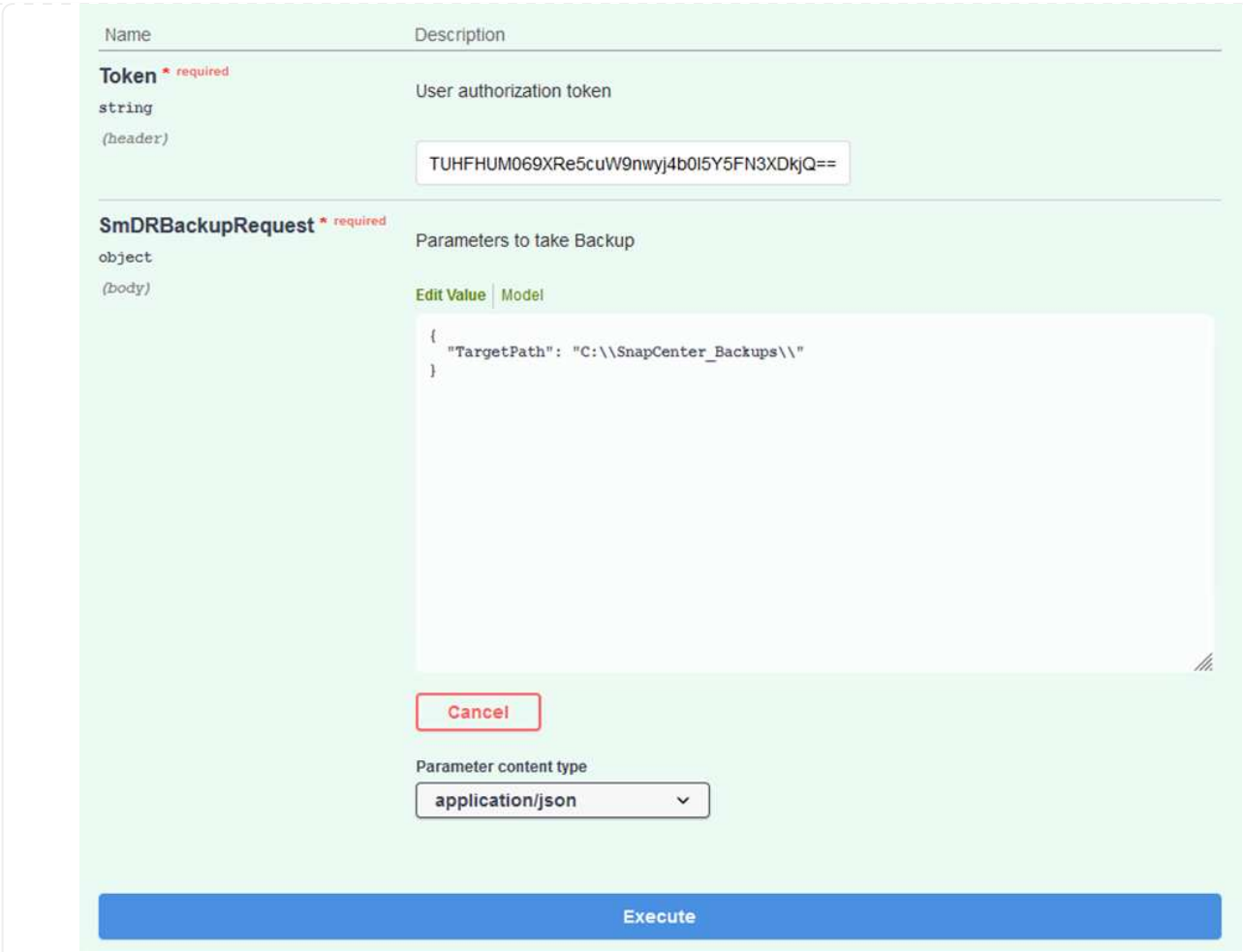
1. 재해 복구 영역을 클릭하여 확장합니다.



2. '/4.6/disasterrecovery/server/backup' 섹션을 확장하고 try it을 클릭합니다.

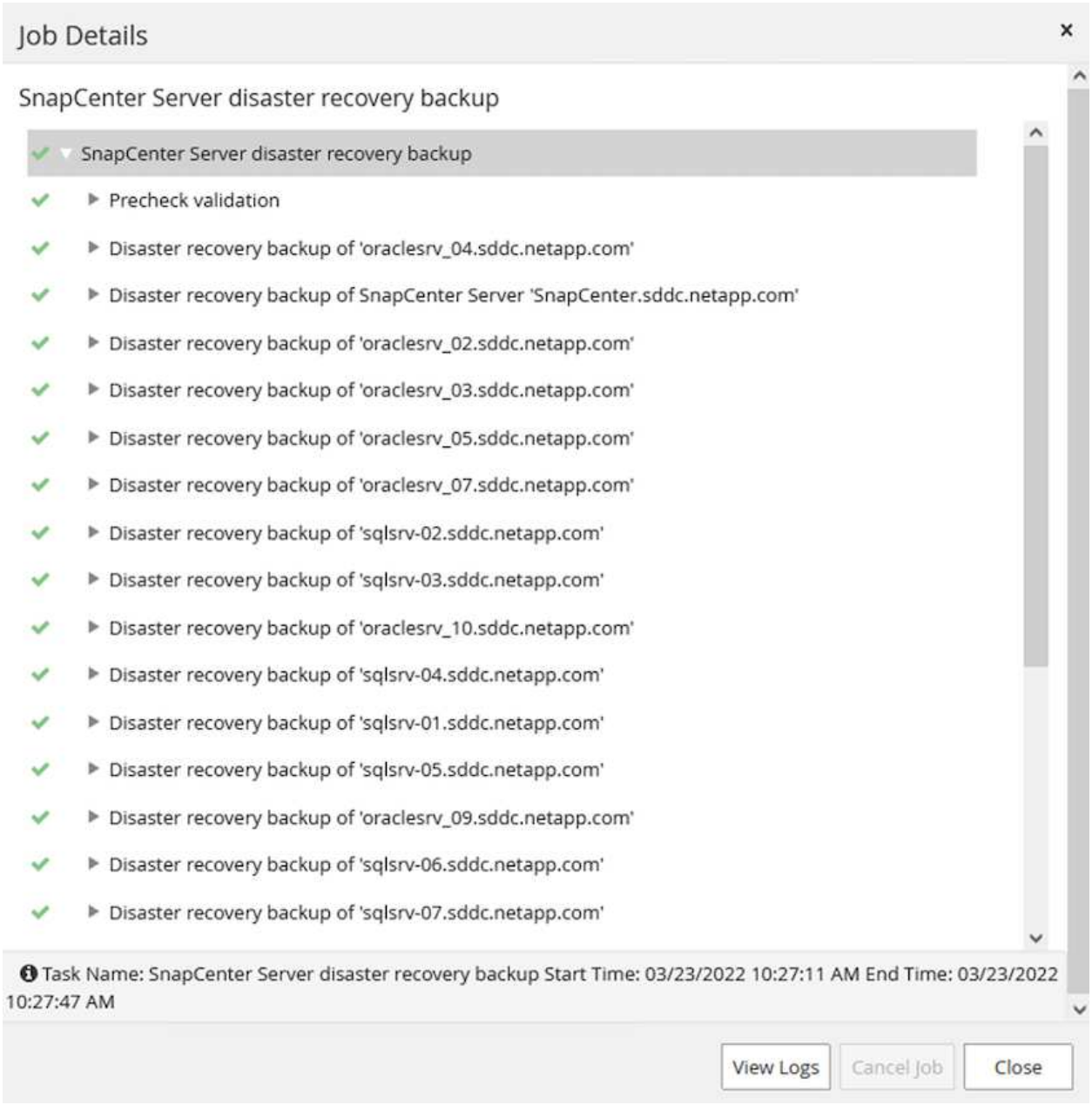
3. SmDRBackupRequest 섹션에서 올바른 로컬 대상 경로를 추가하고 Execute 를 선택하여 SnapCenter 데이터베이스 및 구성의 백업을 시작합니다.

> 백업 프로세스에서는 NFS 또는 CIFS 파일 공유에 직접 백업할 수 없습니다.


Name
Description
Token * required
string
(header)
User authorization token
TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==
SmDRBackupRequest * required
object
(body)
Parameters to take Backup
Edit Value
Model
{
"TargetPath": "C:\\SnapCenter_Backups\\"
}
Cancel
Parameter content type
application/json
Execute

SnapCenter에서 백업 작업을 모니터링합니다

데이터베이스 복원 프로세스를 시작할 때 SnapCenter에 로그인하여 로그 파일을 검토합니다. 모니터 섹션에서 SnapCenter 서버 재해 복구 백업의 세부 정보를 볼 수 있습니다.



XCOPY 유틸리티를 사용하여 **SMB** 공유에 데이터베이스 백업 파일을 복사합니다

그런 다음 SnapCenter 서버의 로컬 드라이브에서 데이터를 SnapMirror로 복제하는 데 사용되는 CIFS 공유로 AWS의 FSx 인스턴스에 있는 보조 위치로 백업을 이동해야 합니다. 파일 권한을 유지하는 특정 옵션과 함께 xcopy를 사용합니다.

관리자 권한으로 명령 프롬프트를 엽니다. 명령 프롬프트에서 다음 명령을 입력합니다.

```
xcopy  <Source_Path>  \\<Destination_Server_IP>\<Folder_Path> /O /X
/E /H /K
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O
/X /E /H /K
```

페일오버

운영 사이트에서 재해가 발생합니다

운영 사내 데이터 센터에서 재해가 발생할 경우 당사의 시나리오에서는 AWS의 VMware Cloud를 사용하여 Amazon Web Services 인프라에 있는 2차 사이트로 페일오버합니다. 가상 시스템과 사내 ONTAP 클러스터에 더 이상 액세스할 수 없다고 가정합니다. 또한, SnapCenter 및 Veeam 가상 머신을 더 이상 액세스할 수 없으며 2차 사이트에서 다시 구축해야 합니다.

이 섹션에서는 클라우드 환경으로의 인프라 페일오버에 대해 다루며 다음 주제를 다룹니다.

- SnapCenter 데이터베이스 복원 새 SnapCenter 서버가 설정된 후, 보조 FSx 스토리지가 기본 스토리지 장치가 될 수 있도록 MySQL 데이터베이스 및 구성 파일을 복원하고 데이터베이스를 재해 복구 모드로 전환합니다.
- Veeam Backup & Replication을 사용하여 애플리케이션 가상 머신을 복구합니다. VM 백업이 포함된 S3 스토리지를 연결하고 백업을 가져온 다음 AWS의 VMware Cloud로 복원합니다.
- SnapCenter를 사용하여 SQL Server 응용 프로그램 데이터를 복원합니다.
- SnapCenter를 사용하여 Oracle 애플리케이션 데이터를 복구합니다.

SnapCenter 데이터베이스 복원 프로세스

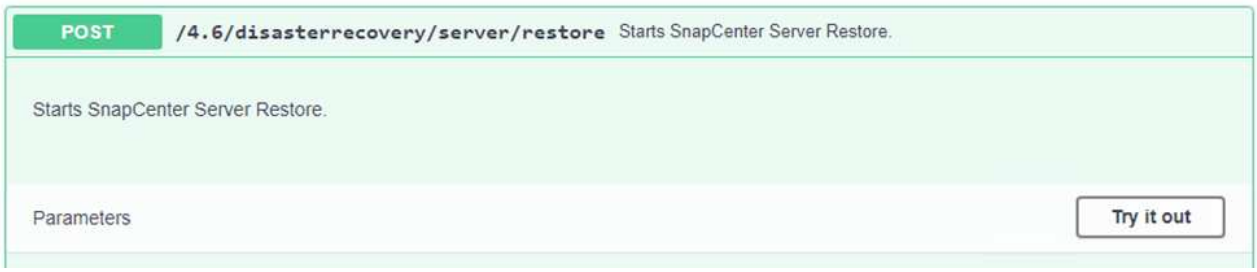
SnapCenter는 MySQL 데이터베이스 및 구성 파일의 백업 및 복원을 허용하여 재해 복구 시나리오를 지원합니다. 이를 통해 관리자는 사내 데이터 센터에서 SnapCenter 데이터베이스의 정기적인 백업을 유지하고 나중에 해당 데이터베이스를 보조 SnapCenter 데이터베이스로 복원할 수 있습니다.

원격 SnapCenter 서버에서 SnapCenter 백업 파일에 액세스하려면 다음 단계를 수행하십시오.

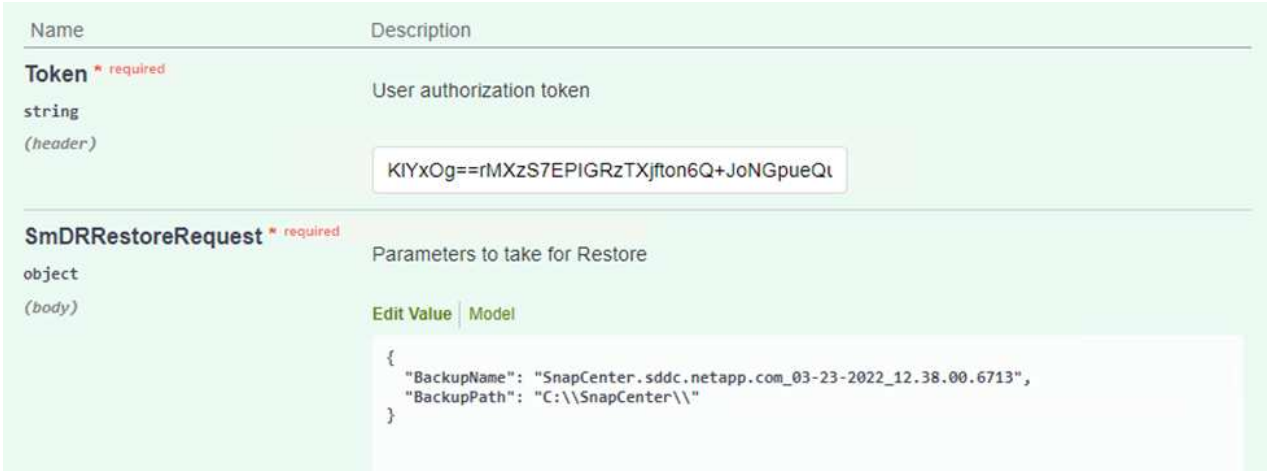
1. FSx 클러스터에서 SnapMirror 관계를 중단하여 볼륨을 읽기/쓰기로 만듭니다.
2. 필요한 경우 CIFS 서버를 생성하고 복제된 볼륨의 연결 경로를 가리키는 CIFS 공유를 생성합니다.
3. xcopy를 사용하여 보조 SnapCenter 시스템의 로컬 디렉토리에 백업 파일을 복사합니다.
4. SnapCenter v4.6을 설치합니다.
5. SnapCenter 서버의 FQDN이 원래 서버와 동일한지 확인합니다. 이 작업은 DB 복원이 성공하려면 필요합니다.

복원 프로세스를 시작하려면 다음 단계를 수행하십시오.

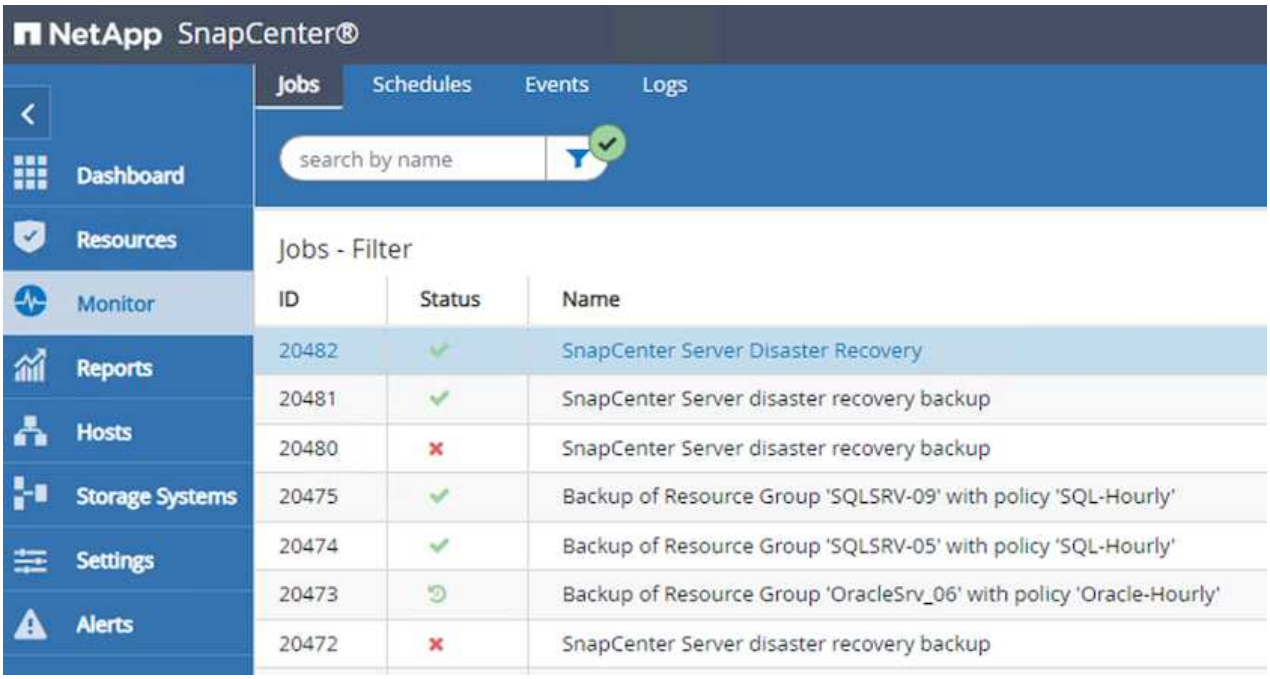
1. 보조 SnapCenter 서버의 Swagger API 웹 페이지로 이동하고 이전 지침에 따라 인증 토큰을 얻습니다.
2. Swagger 페이지의 Disaster Recovery 섹션으로 이동하여 "/4.6/disasterrecovery/server/restore"를 선택하고 Try It Out을 클릭합니다.

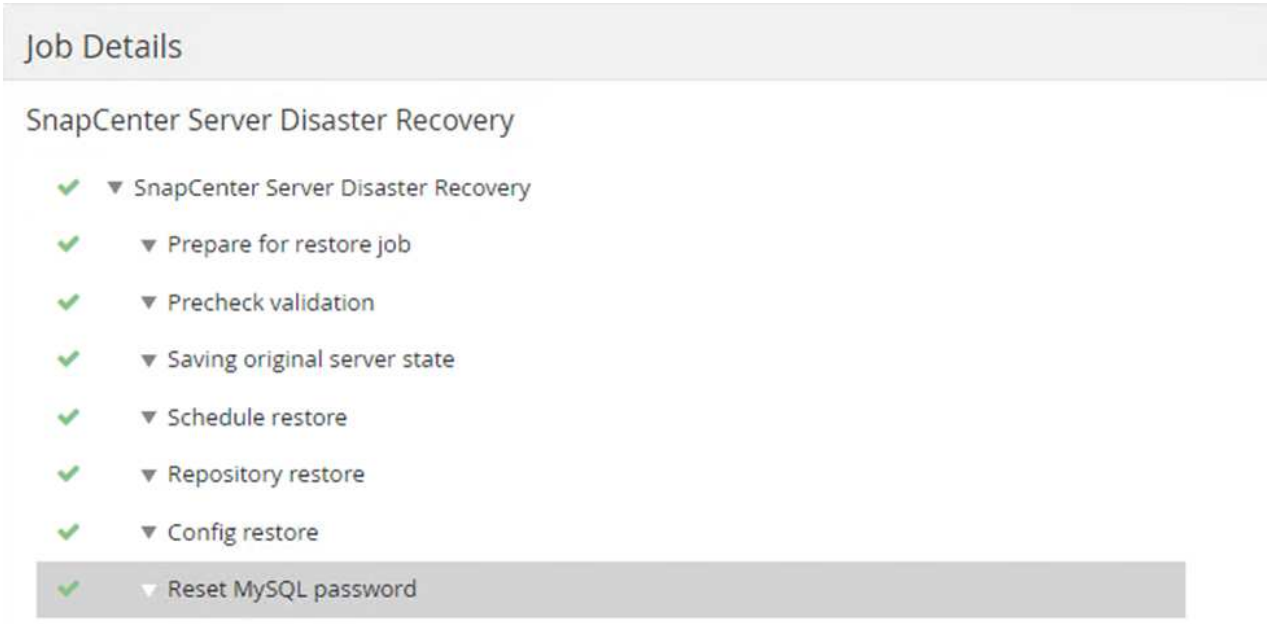


3. 인증 토큰을 붙여 넣고 SmDRResterRequest 섹션에서 백업 이름과 보조 SnapCenter 서버의 로컬 디렉터리를 붙여 넣습니다.



4. 실행 버튼을 선택하여 복원 프로세스를 시작합니다.
5. SnapCenter에서 모니터 섹션으로 이동하여 복구 작업의 진행률을 확인합니다.





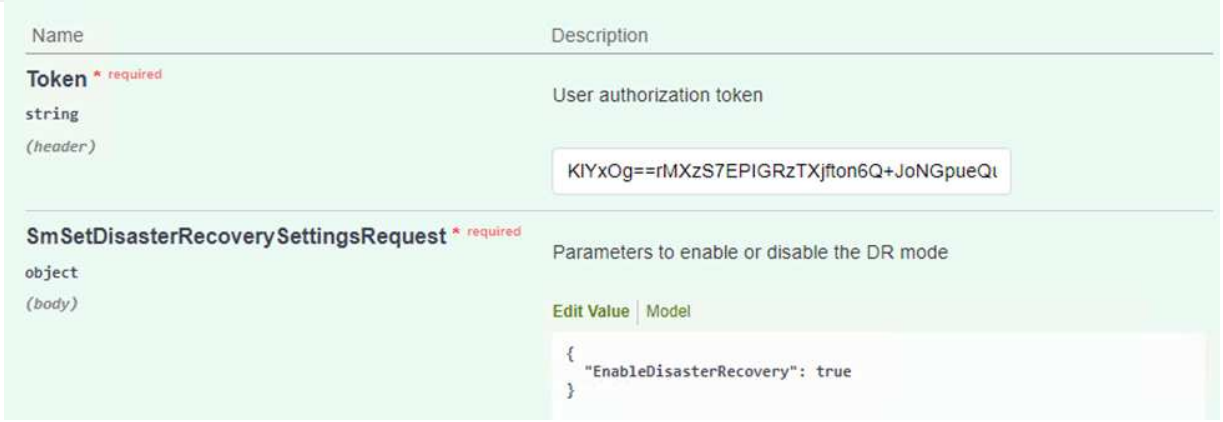
6. 보조 스토리지에서 SQL Server 복원을 사용하려면 SnapCenter 데이터베이스를 재해 복구 모드로 전환해야 합니다. 이 작업은 별도의 작업으로 수행되며 Swagger API 웹 페이지에서 시작됩니다.

   a. Disaster Recovery(재해 복구) 섹션으로 이동하여 '/4.6/Disasterrecovery/storage(4.6/Disasterrecovery/storage)'를 클릭합니다.

   b. 사용자 인증 토큰을 붙여 넣습니다.

   c. SmSetDisasterRecoverySettingsRequest 섹션에서 EnableDisasterRecover 를 true 로 변경합니다.

   d. 실행 을 클릭하여 SQL Server에 대한 재해 복구 모드를 활성화합니다.



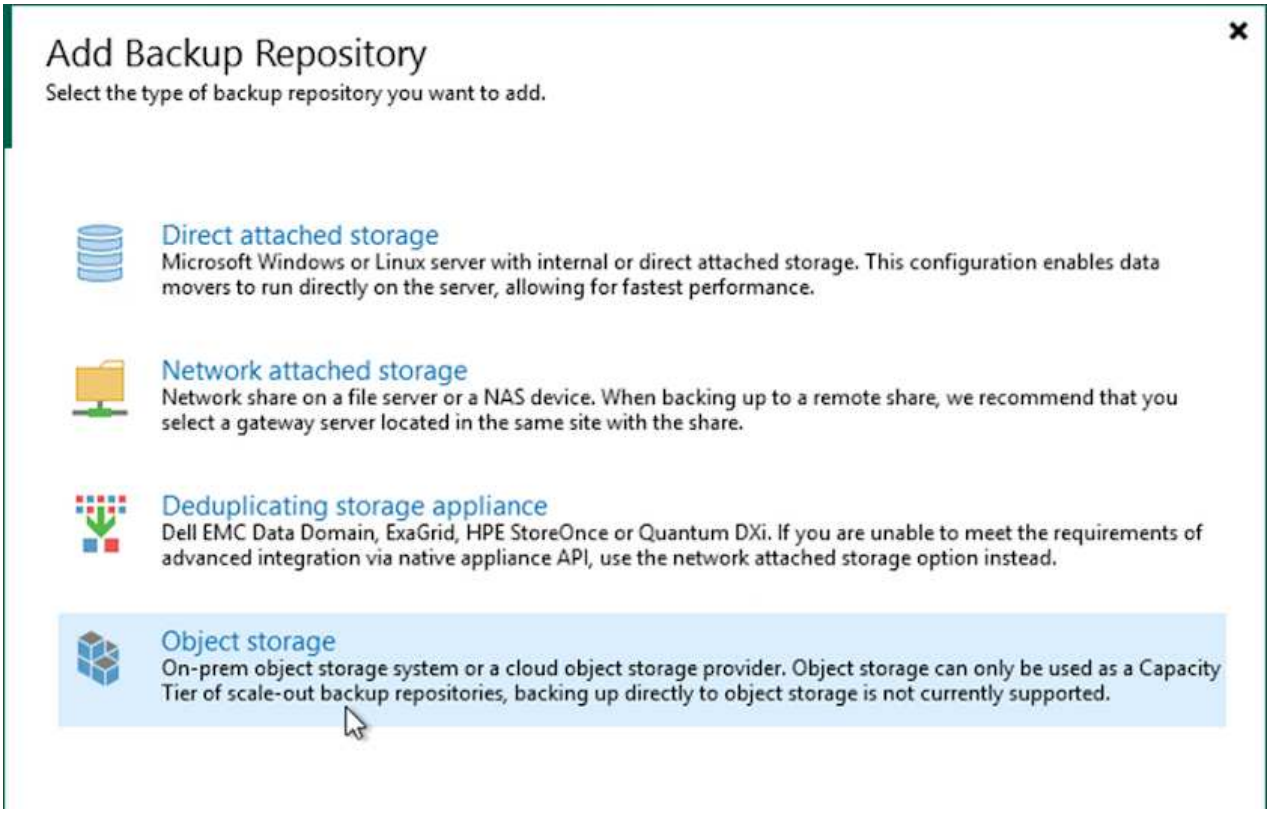
추가 절차에 대한 설명을 참조하십시오.

Veeam 전체 복원으로 애플리케이션 **VM**을 복원합니다

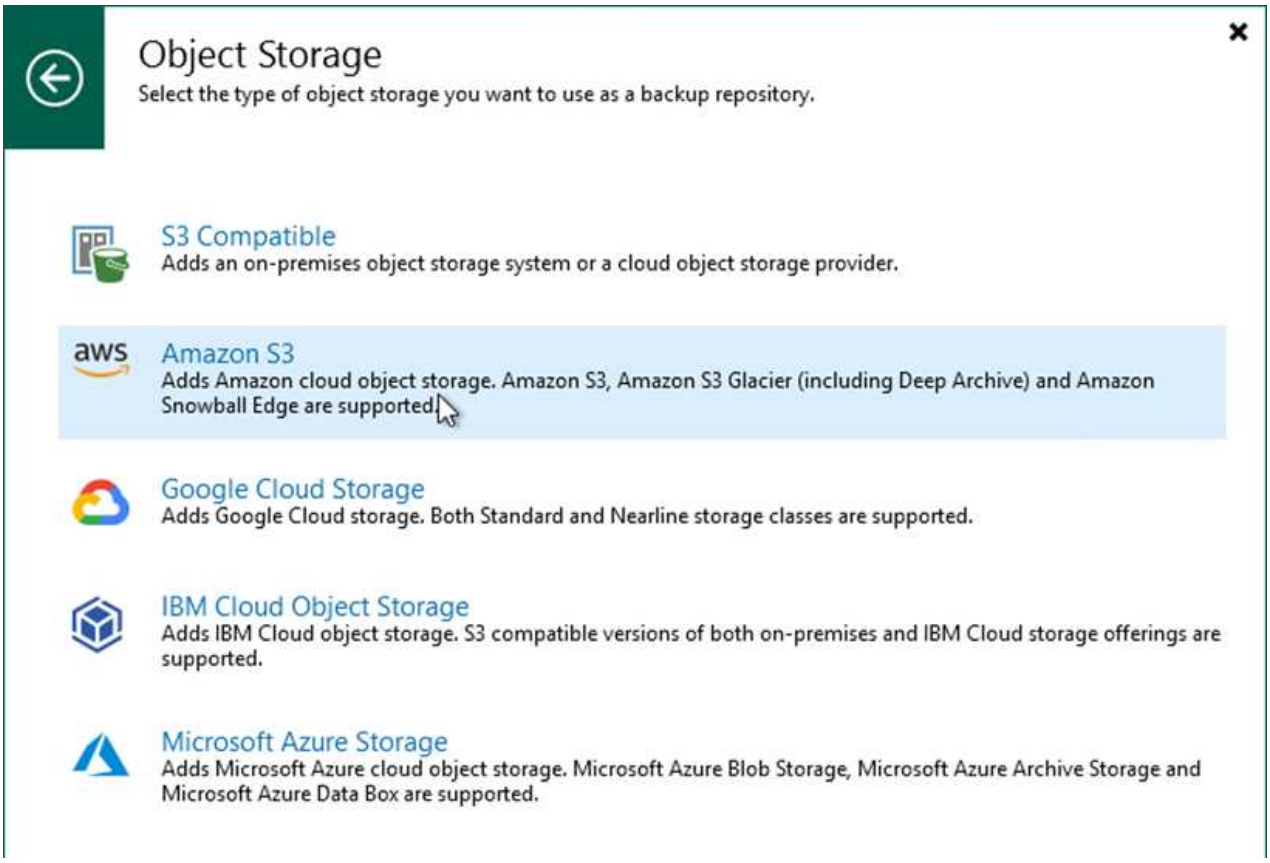
2차 Veeam 서버에서 S3 스토리지의 백업을 가져오고 SQL Server 및 Oracle VM을 VMware Cloud 클러스터로 복원합니다.

사내 스케일아웃 백업 리포지토리에 속하는 S3 오브젝트에서 백업을 가져오려면 다음 단계를 완료합니다.

1. 백업 리포지토리 로 이동하고 상단 메뉴에서 리포지토리 추가 를 클릭하여 백업 리포지토리 추가 마법사를 시작합니다. 마법사의 첫 번째 페이지에서 백업 저장소 유형으로 오브젝트 스토리지 를 선택합니다.

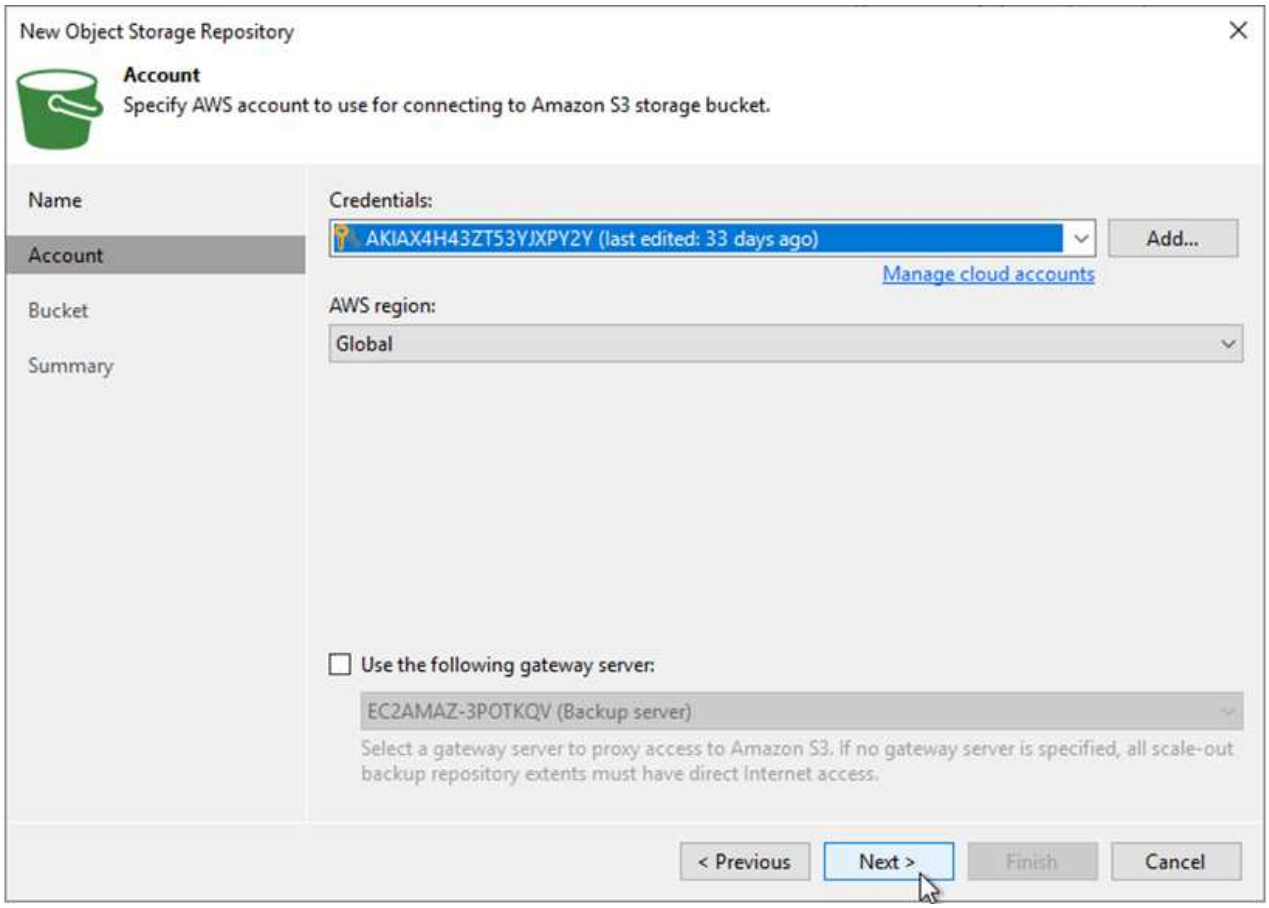


2. 오브젝트 스토리지 유형으로 Amazon S3를 선택합니다.

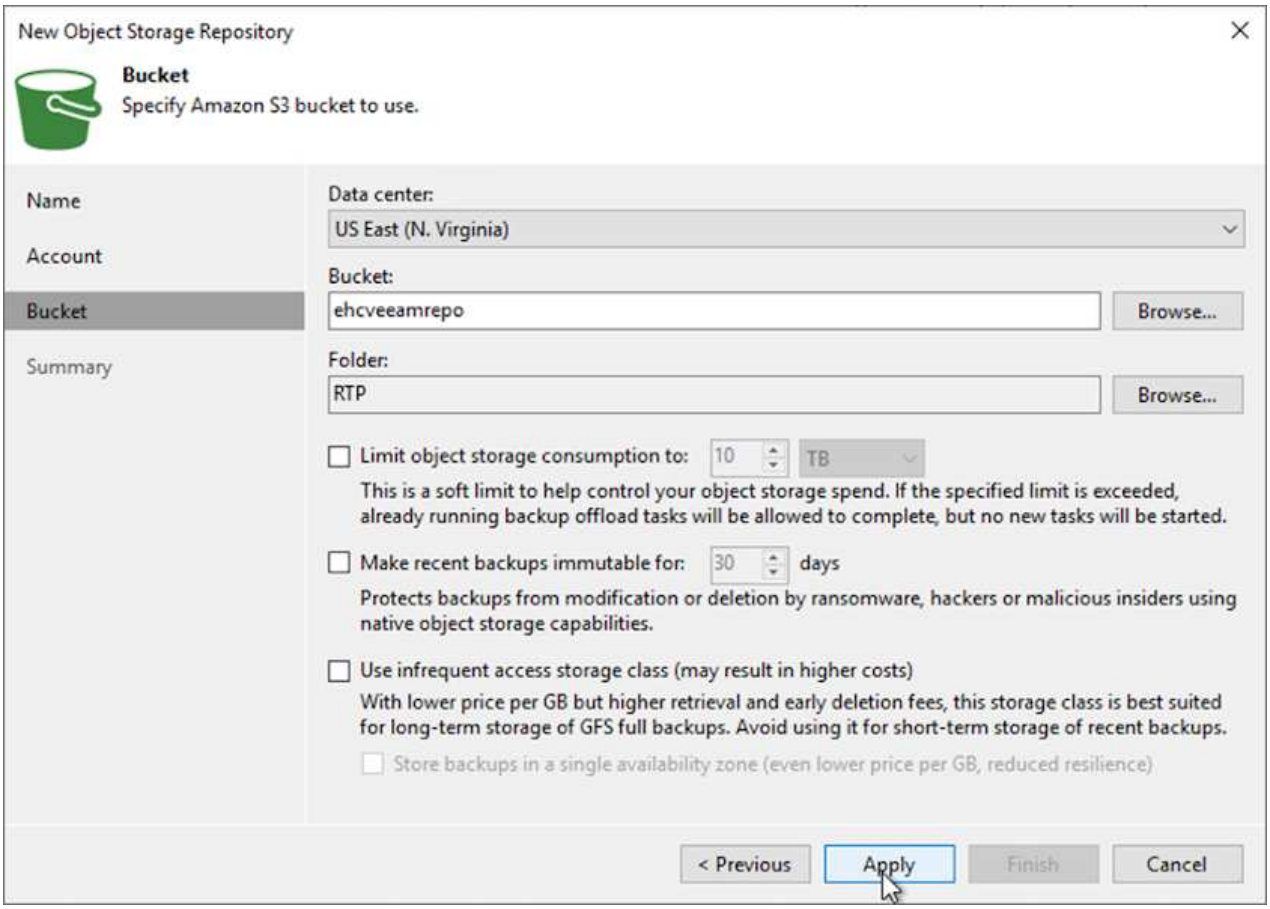


3. Amazon Cloud Storage Services 목록에서 Amazon S3를 선택합니다.

4. 드롭다운 목록에서 미리 입력한 자격 증명을 선택하거나 클라우드 스토리지 리소스에 액세스하기 위한 새 자격 증명을 추가합니다. 다음을 클릭하여 계속합니다.



5. 버킷 페이지에서 데이터 센터, 버킷, 폴더 및 원하는 옵션을 입력합니다. 적용 을 클릭합니다.

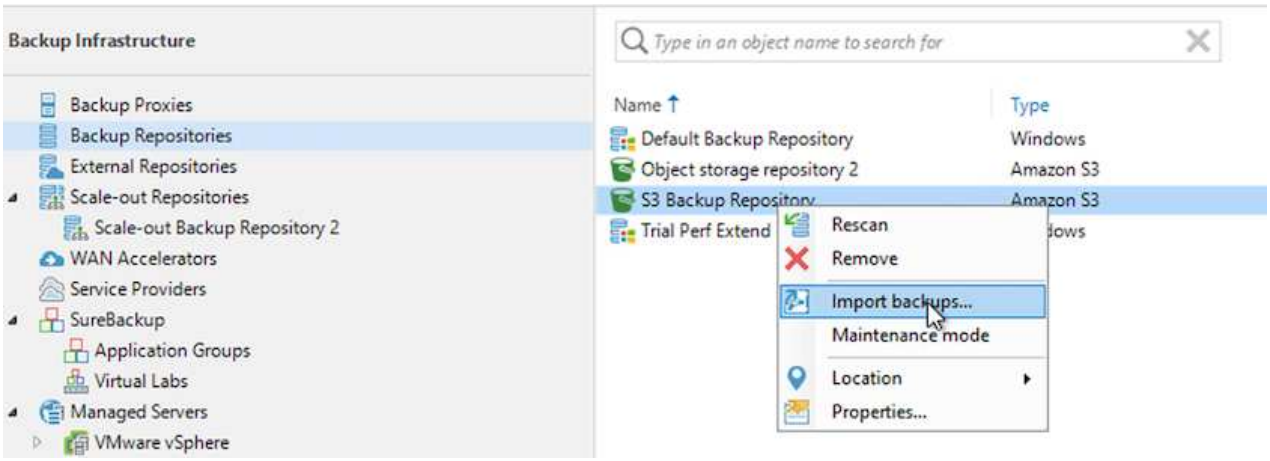


6. 마지막으로 마침 을 선택하여 프로세스를 완료하고 리포지토리를 추가합니다.

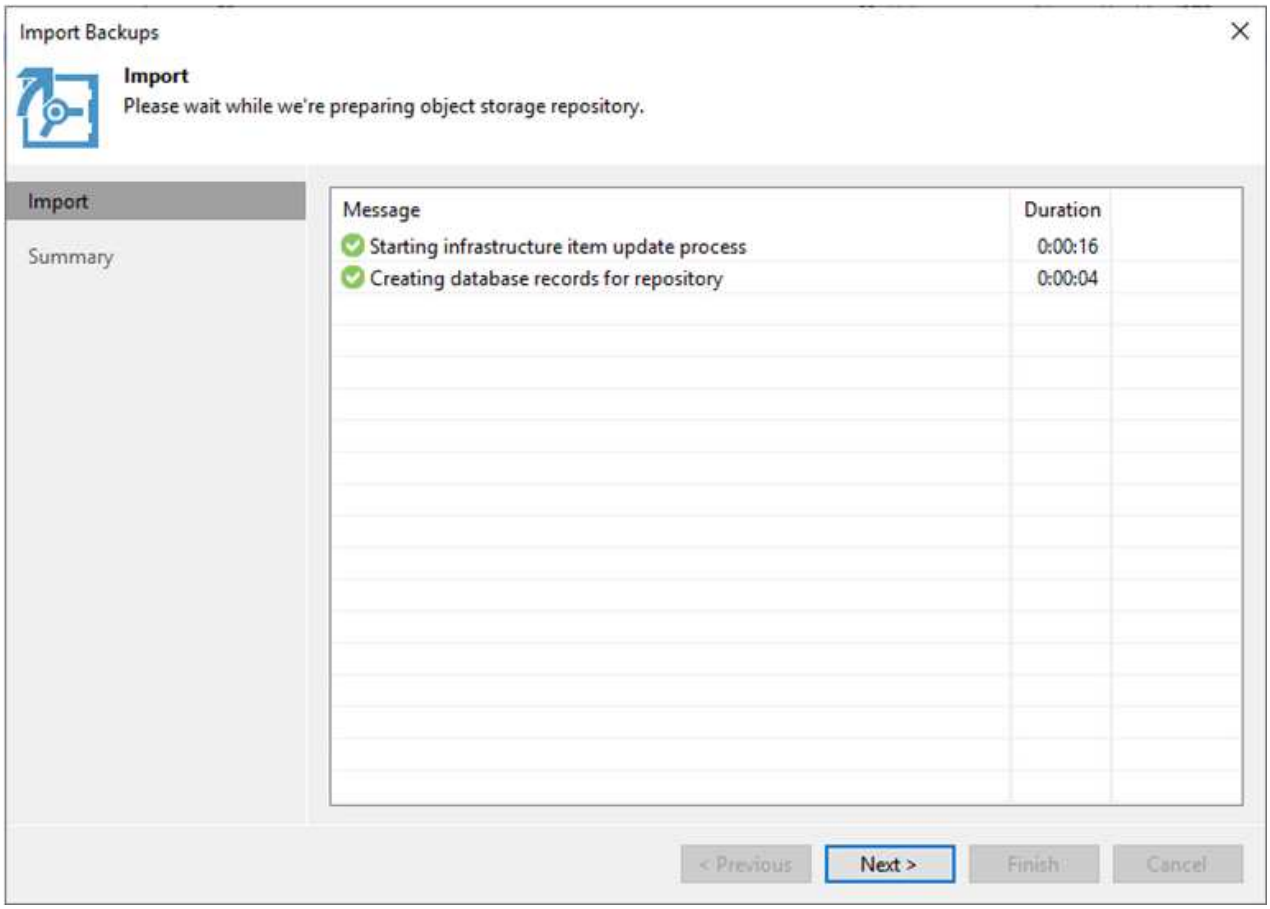
S3 오브젝트 스토리지에서 백업을 가져옵니다

이전 섹션에 추가된 S3 리포지토리에서 백업을 가져오려면 다음 단계를 완료합니다.

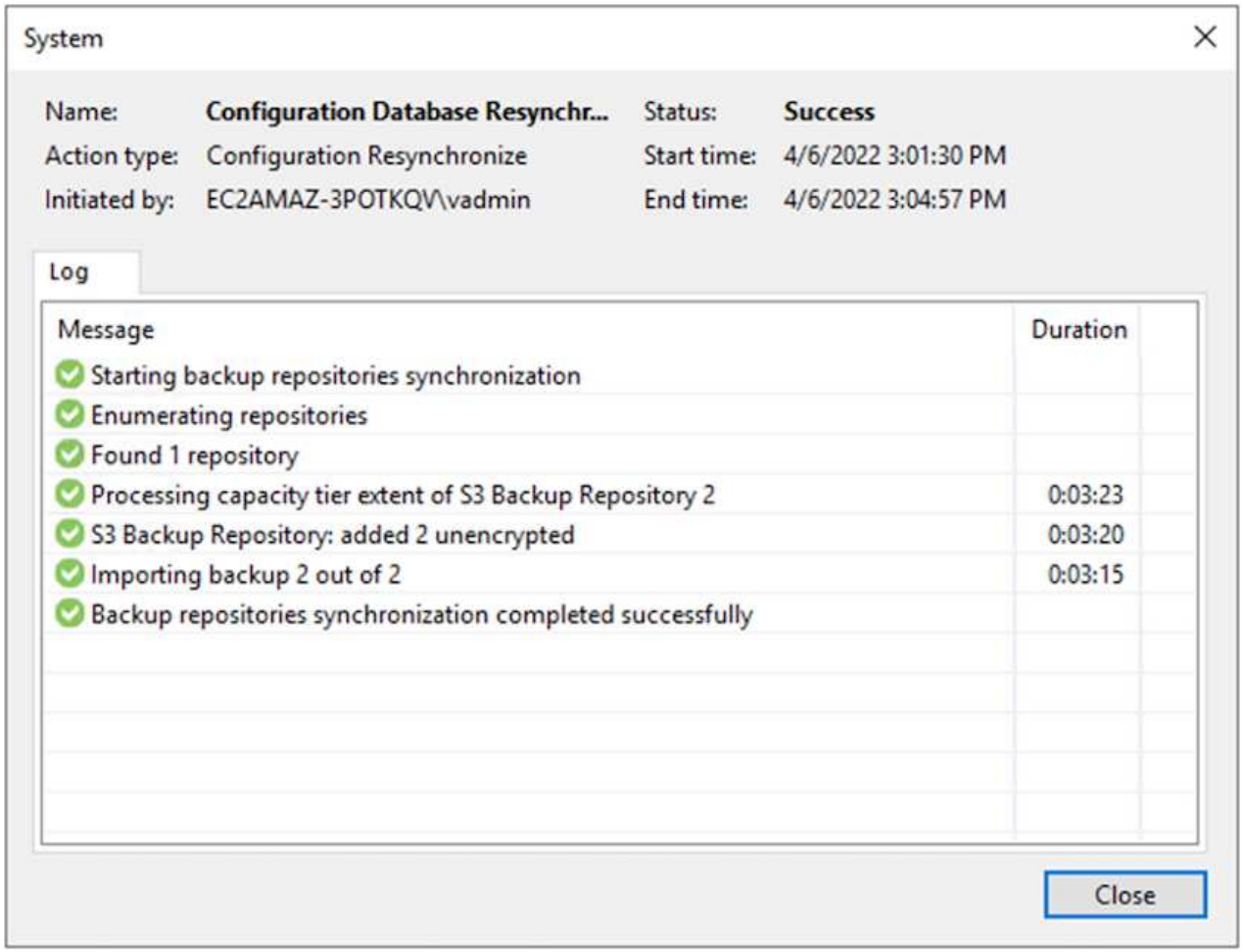
1. S3 백업 리포지토리에서 백업 가져오기 를 선택하여 백업 가져오기 마법사를 시작합니다.



2. 가져오기에 대한 데이터베이스 레코드가 생성된 후 요약 화면에서 다음 을 선택한 다음 마침 을 선택하여 가져오기 프로세스를 시작합니다.

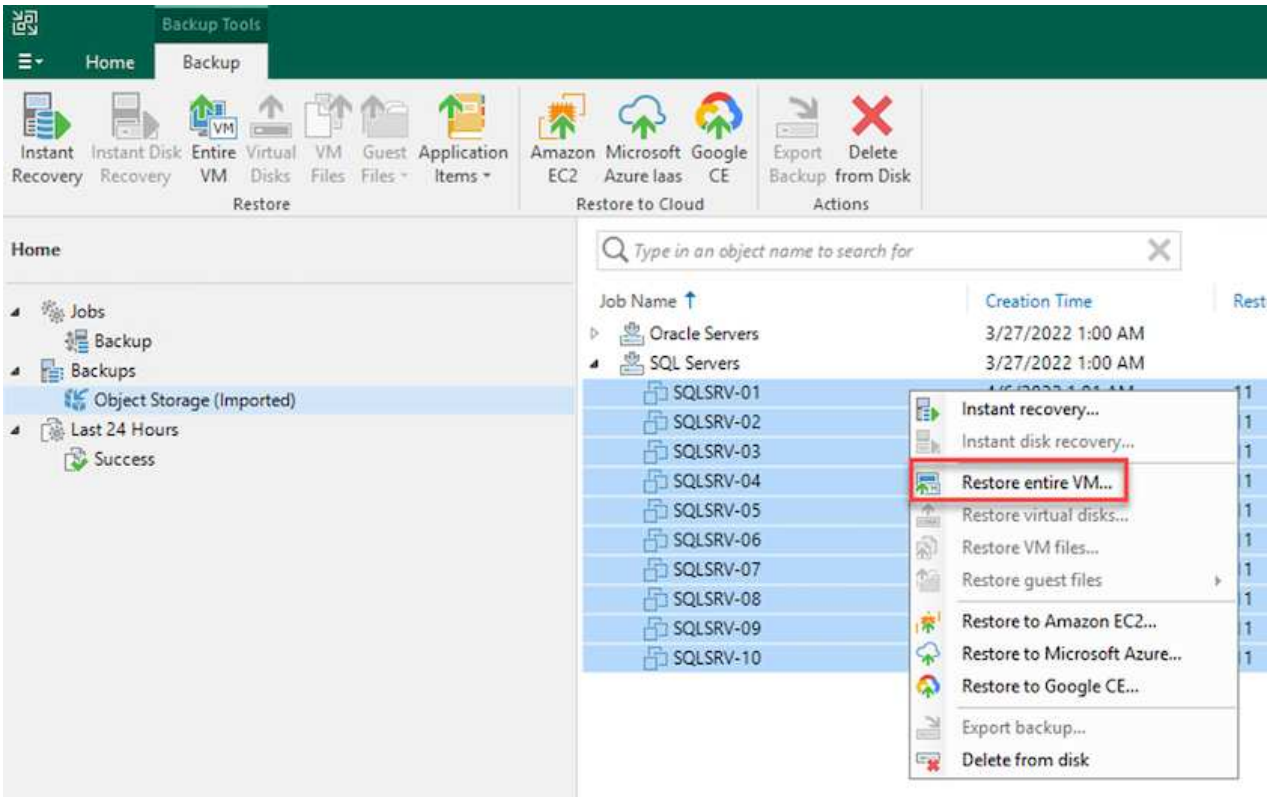


3. 가져오기가 완료되면 VM을 VMware Cloud 클러스터로 복구할 수 있습니다.

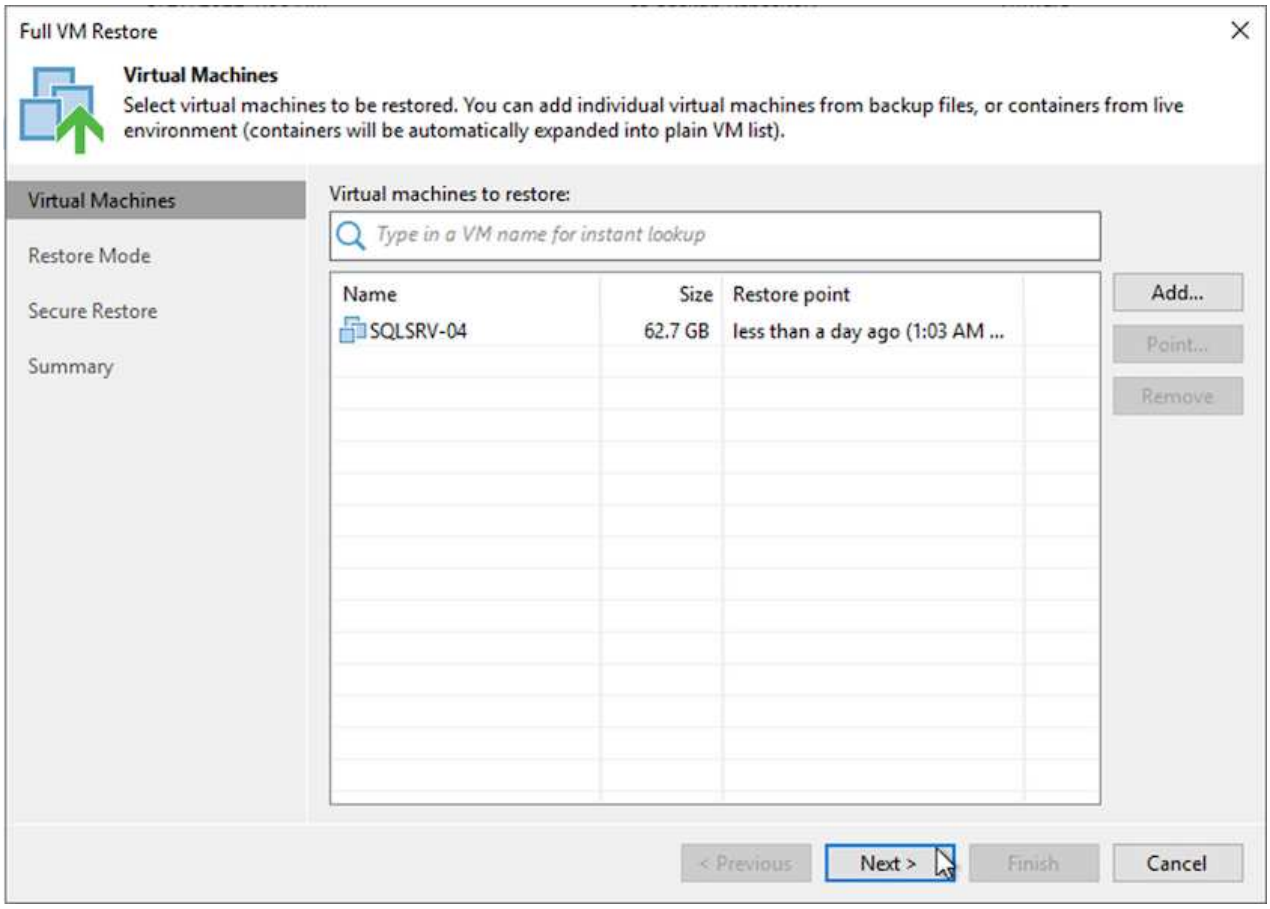

System
Name: Configuration Database Resynchr...
Status: Success
Action type: Configuration Resynchronize
Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\vadmin
End time: 4/6/2022 3:04:57 PM
Log
Message
Duration
Starting backup repositories synchronization
Enumerating repositories
Found 1 repository
Processing capacity tier extent of S3 Backup Repository 2
0:03:23
S3 Backup Repository: added 2 unencrypted
0:03:20
Importing backup 2 out of 2
0:03:15
Backup repositories synchronization completed successfully
Close

SQL 및 Oracle 가상 머신을 AWS 워크로드 도메인/클러스터의 VMware Cloud로 복구하려면 다음 단계를 수행하십시오.

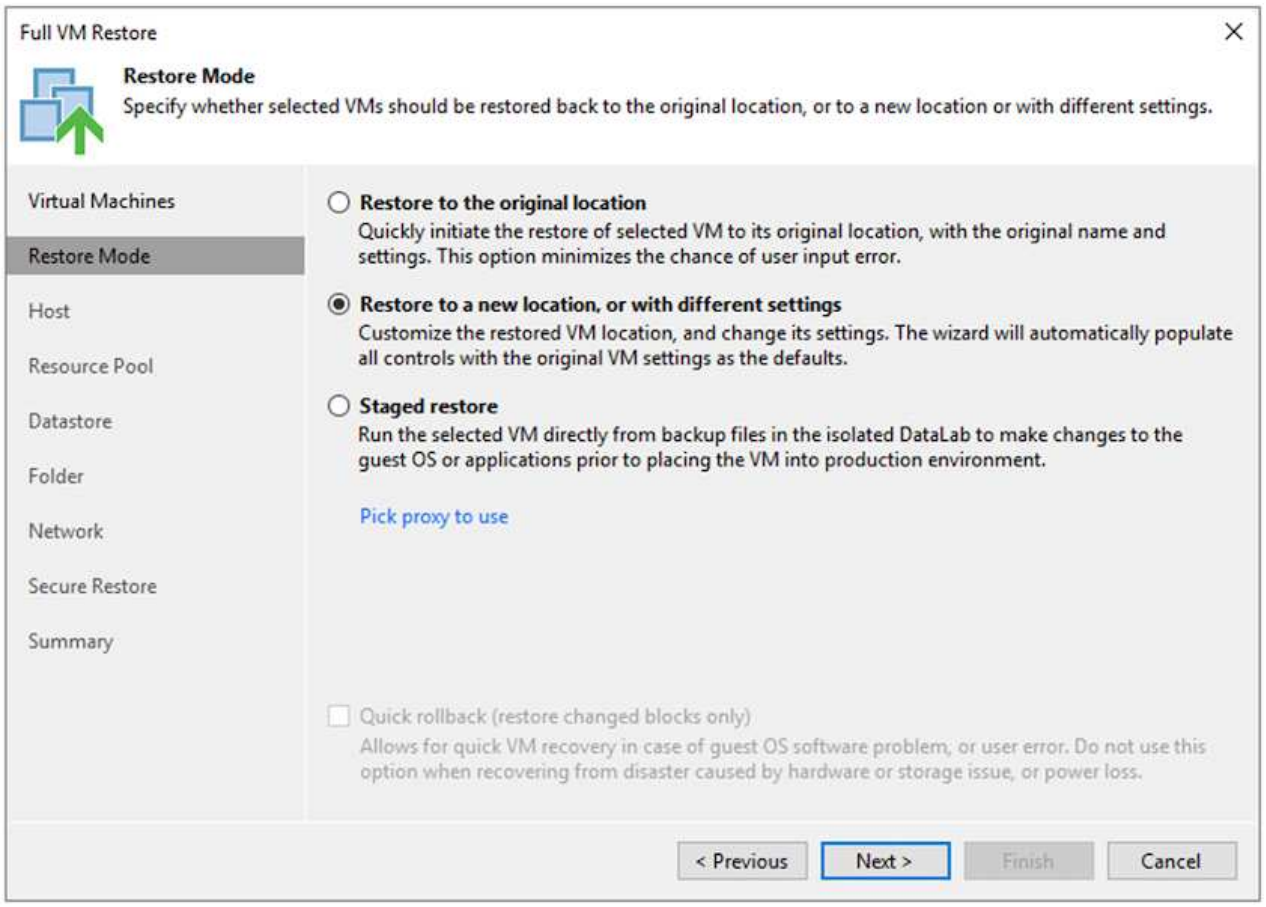
1. Veeam Home 페이지에서 가져온 백업이 포함된 객체 스토리지를 선택하고 복구할 VM을 선택한 다음 마우스 오른쪽 버튼을 클릭하고 Restore Entire VM을 선택합니다.



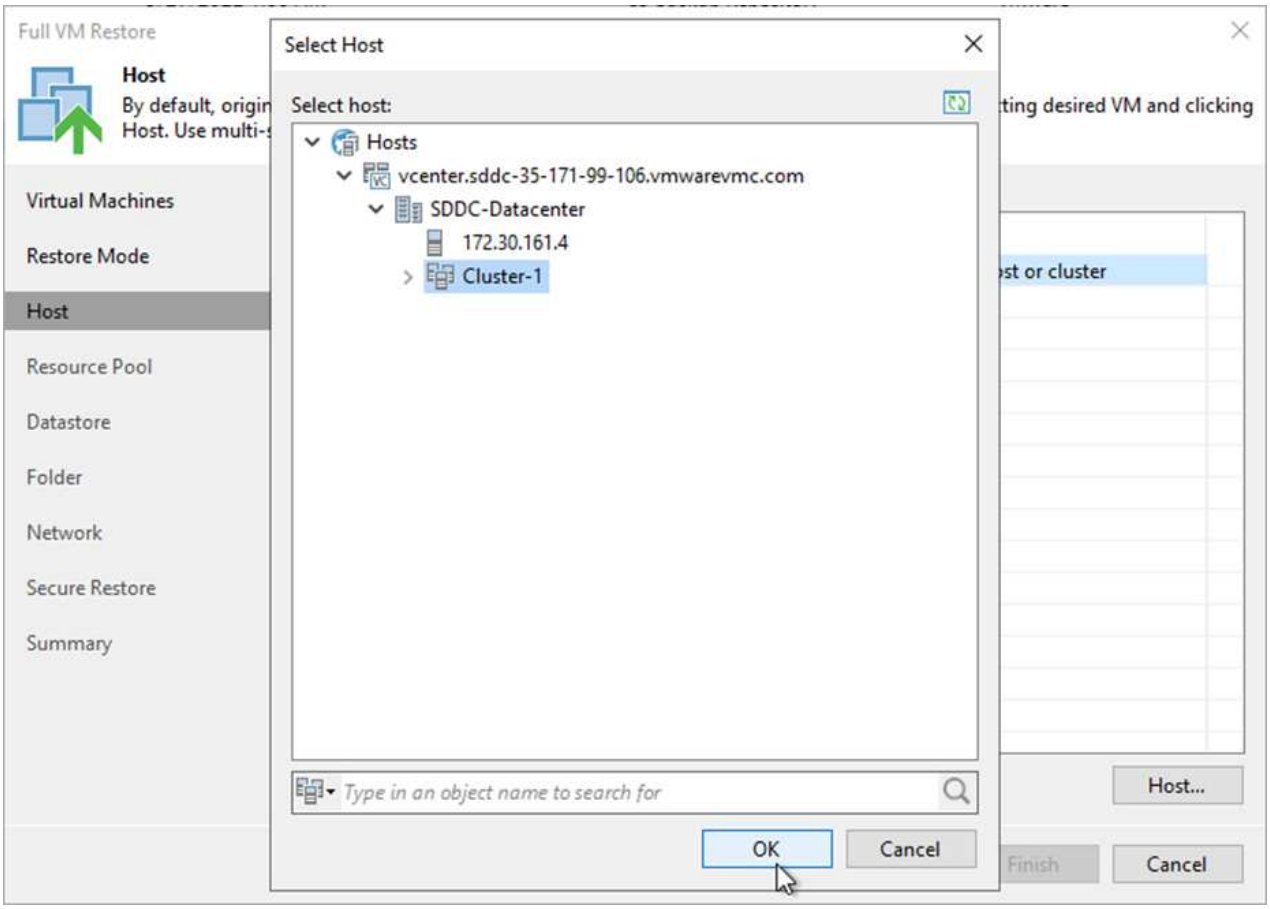
2. 전체 VM 복원 마법사의 첫 페이지에서 원하는 경우 백업할 VM을 수정하고 다음을 선택합니다.



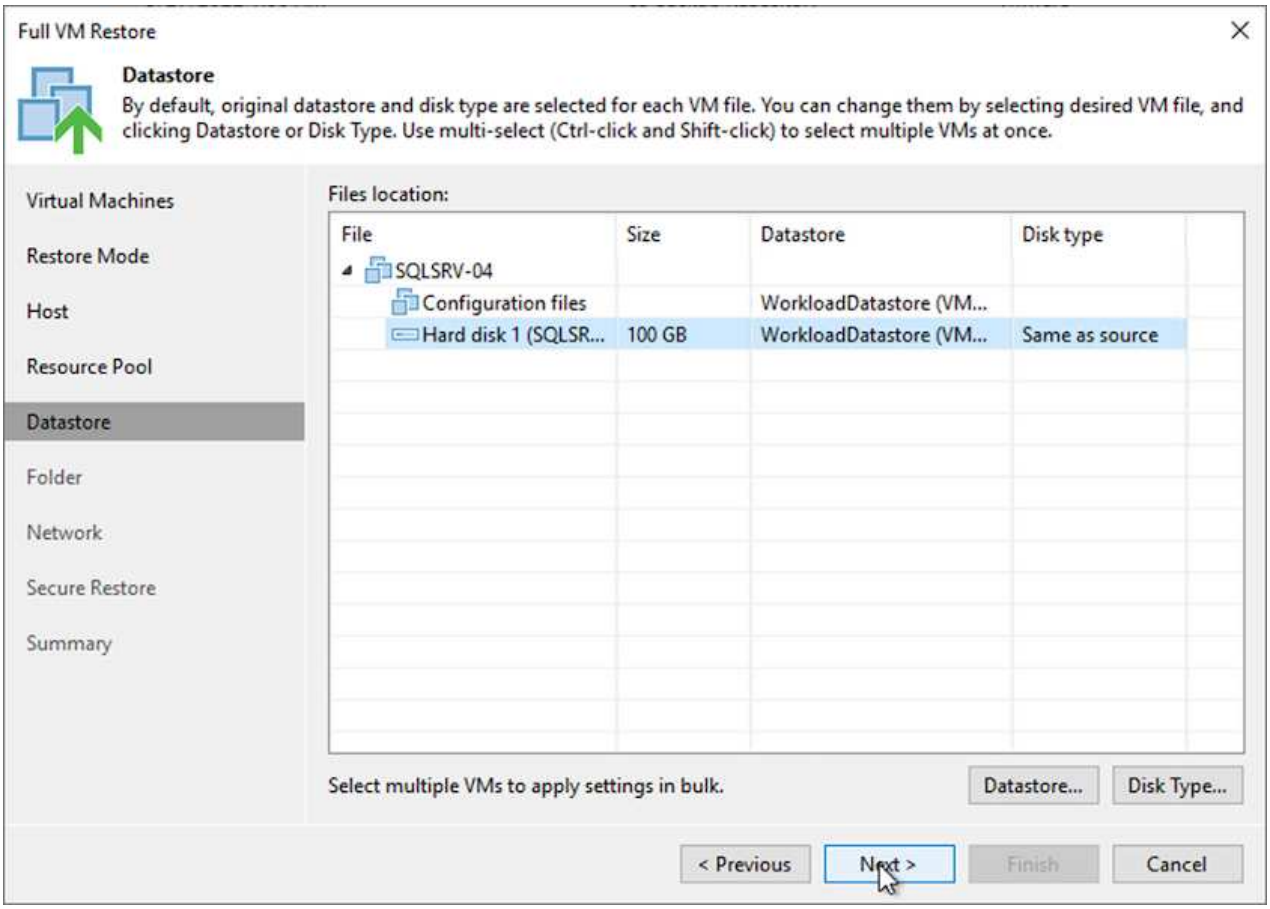
3. 복원 모드 페이지에서 새 위치로 복원 또는 다른 설정으로 복원 을 선택합니다.



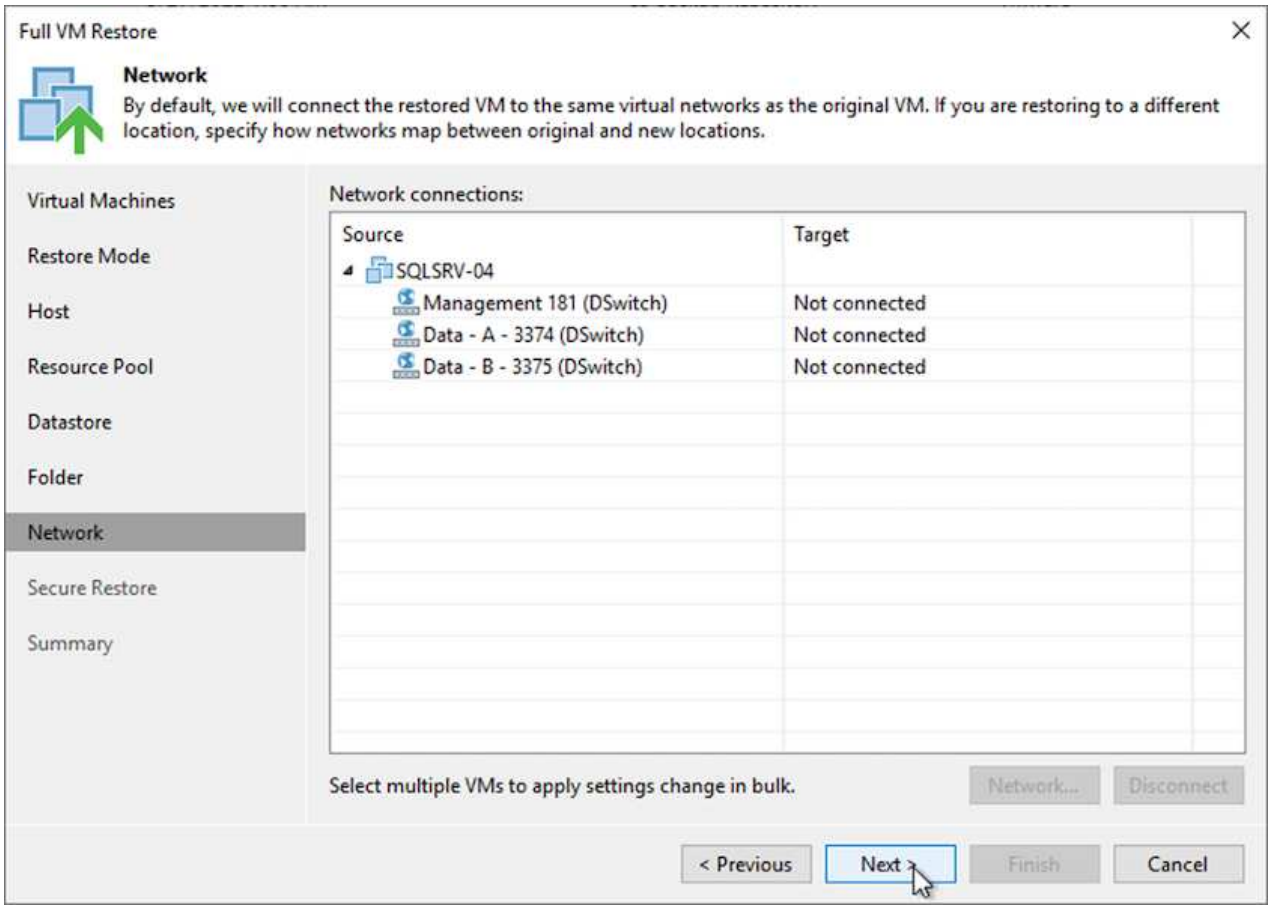
4. 호스트 페이지에서 VM을 복구할 타겟 ESXi 호스트 또는 클러스터를 선택합니다.

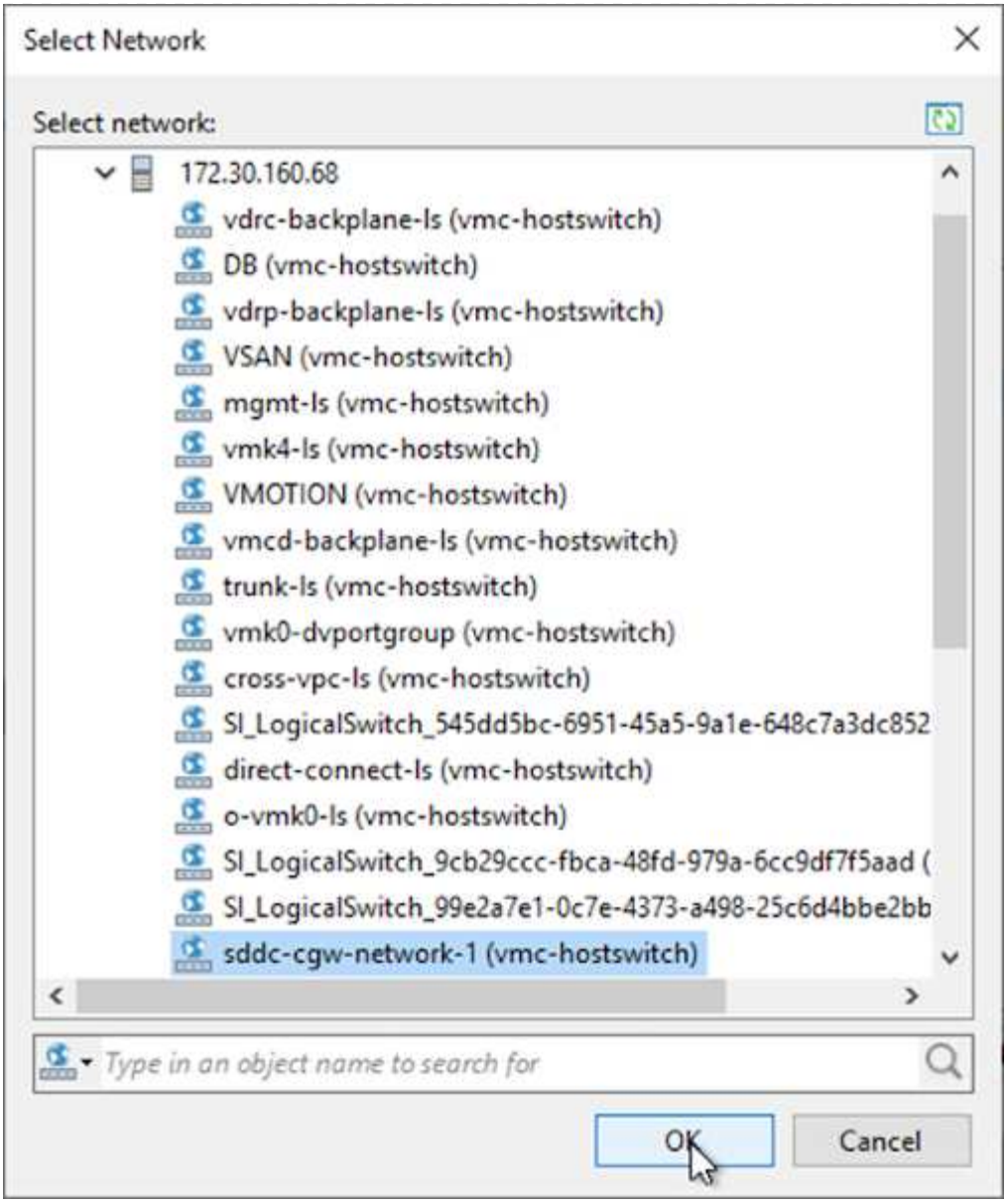


5. Datastores 페이지에서 구성 파일과 하드 디스크 모두에 대한 타겟 데이터 저장소 위치를 선택합니다.



6. 네트워크 페이지에서 VM의 원래 네트워크를 새 대상 위치의 네트워크에 매핑합니다.


Full VM Restore
Network
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.
Virtual Machines
Restore Mode
Host
Resource Pool
Datastore
Folder
Network
Secure Restore
Summary
Network connections:
Source
Target
SQLSRV-04
Management 181 (DSwitch)
Not connected
Data - A - 3374 (DSwitch)
Not connected
Data - B - 3375 (DSwitch)
Not connected
Select multiple VMs to apply settings change in bulk.
Network...
Disconnect
< Previous
Next >
Finish
Cancel



7. 복원된 VM에서 맬웨어를 검사할지 여부를 선택하고 요약 페이지를 검토한 다음 마침 을 클릭하여 복원을 시작합니다.

SQL Server 응용 프로그램 데이터를 복원합니다

다음 프로세스에서는 사내 사이트가 작동 불능 상태가 되는 재해가 발생할 경우 AWS의 VMware Cloud Services에서 SQL Server를 복구하는 방법에 대한 지침을 제공합니다.

복구 단계를 계속 진행하려면 다음 필수 구성 요소가 완료된 것으로 가정합니다.

1. Veeam Full Restore를 사용하여 Windows Server VM을 VMware Cloud SDDC로 복구했습니다.
2. 보조 SnapCenter 서버가 설정되었고 섹션에 설명된 단계를 사용하여 SnapCenter 데이터베이스 복원 및 구성이 완료되었습니다 "SnapCenter 백업 및 복원 프로세스 요약"

VM: SQL Server VM에 대한 사후 복원 구성

VM 복원이 완료된 후 SnapCenter 내에서 호스트 VM을 재검색할 수 있도록 네트워킹 및 기타 항목을 구성해야 합니다.

1. 관리 및 iSCSI 또는 NFS에 새 IP 주소를 할당합니다.
2. Windows 도메인에 호스트를 연결합니다.
3. DNS 또는 SnapCenter 서버의 호스트 파일에 호스트 이름을 추가합니다.

SnapCenter 플러그인이 현재 도메인과 다른 도메인 자격 증명을 사용하여 배포된 경우 SQL Server VM의 Windows용 플러그인 서비스에 대한 로그온 계정을 변경해야 합니다. 로그온 계정을 변경한 후 SnapCenter SMCore, Windows용 플러그인 및 SQL Server 서비스용 플러그인을 다시 시작합니다.

SnapCenter에서 복원된 VM을 자동으로 다시 검색하려면 FQDN이 SnapCenter 온-프레미스에 원래 추가된 VM과 동일해야 합니다.

SQL Server 복구를 위한 **FSx** 스토리지를 구성합니다

SQL Server VM의 재해 복구 복원 프로세스를 수행하려면 FSx 클러스터에서 기존 SnapMirror 관계를 중단하고 볼륨에 대한 액세스를 부여해야 합니다. 이렇게 하려면 다음 단계를 완료하십시오.

1. SQL Server 데이터베이스 및 로그 볼륨에 대한 기존 SnapMirror 관계를 해제하려면 FSx CLI에서 다음 명령을 실행합니다.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. SQL Server Windows VM의 iSCSI IQN이 포함된 이니시에이터 그룹을 생성하여 LUN에 대한 액세스 권한 부여:

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName
-protocol iSCSI -ostype windows -initiator IQN
```

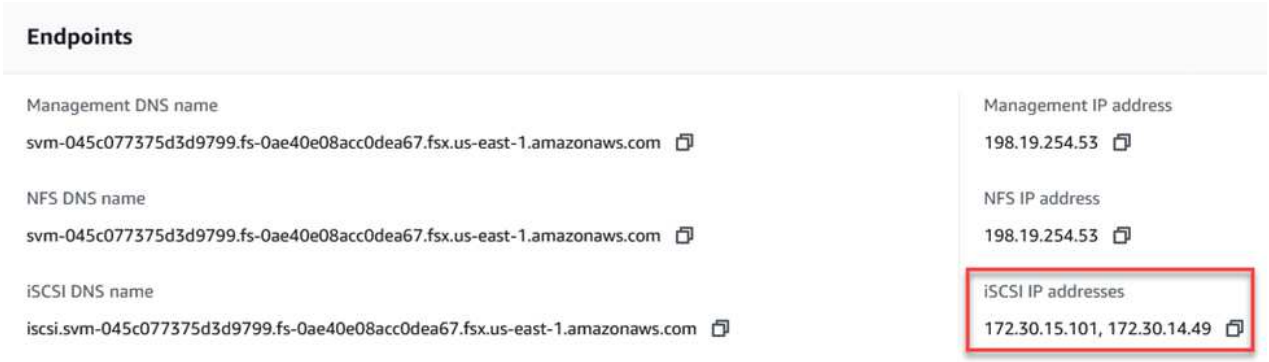
3. 마지막으로 LUN을 방금 생성한 이니시에이터 그룹에 매핑합니다.

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

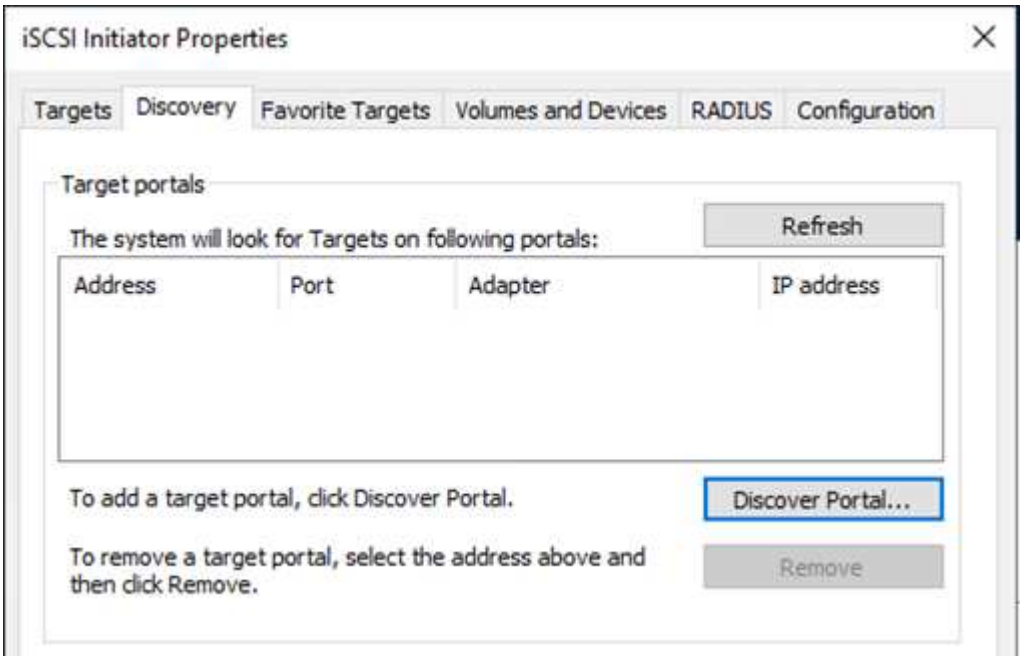
4. 경로 이름을 찾으려면 'lun show' 명령을 실행합니다.

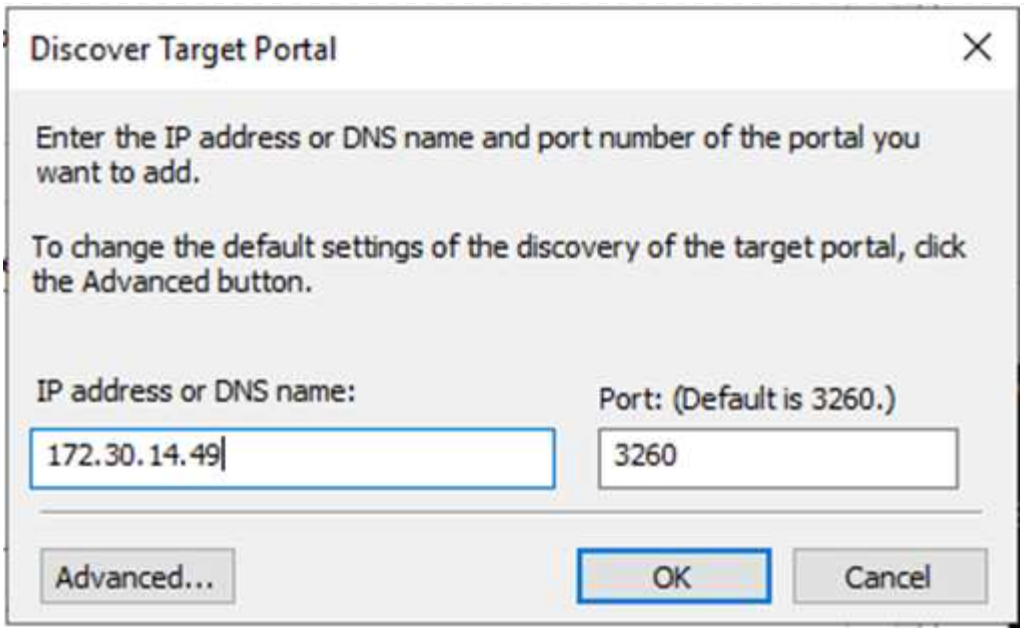
iSCSI 액세스를 위해 **Windows VM**을 설정하고 파일 시스템을 검색합니다

1. SQL Server VM에서 iSCSI 네트워크 어댑터를 설정하여 FSx 인스턴스의 iSCSI 타겟 인터페이스에 대한 연결로 설정된 VMware 포트 그룹에서 통신합니다.
2. iSCSI 초기자 등록 정보 유틸리티를 열고 검색, 즐겨찾기 대상 및 대상 탭에서 이전 연결 설정을 지웁니다.
3. FSx 인스턴스/클러스터에서 iSCSI 논리 인터페이스에 액세스하기 위한 IP 주소를 찾습니다. AWS 콘솔의 Amazon FSx > ONTAP > Storage Virtual Machines에서 찾을 수 있습니다.

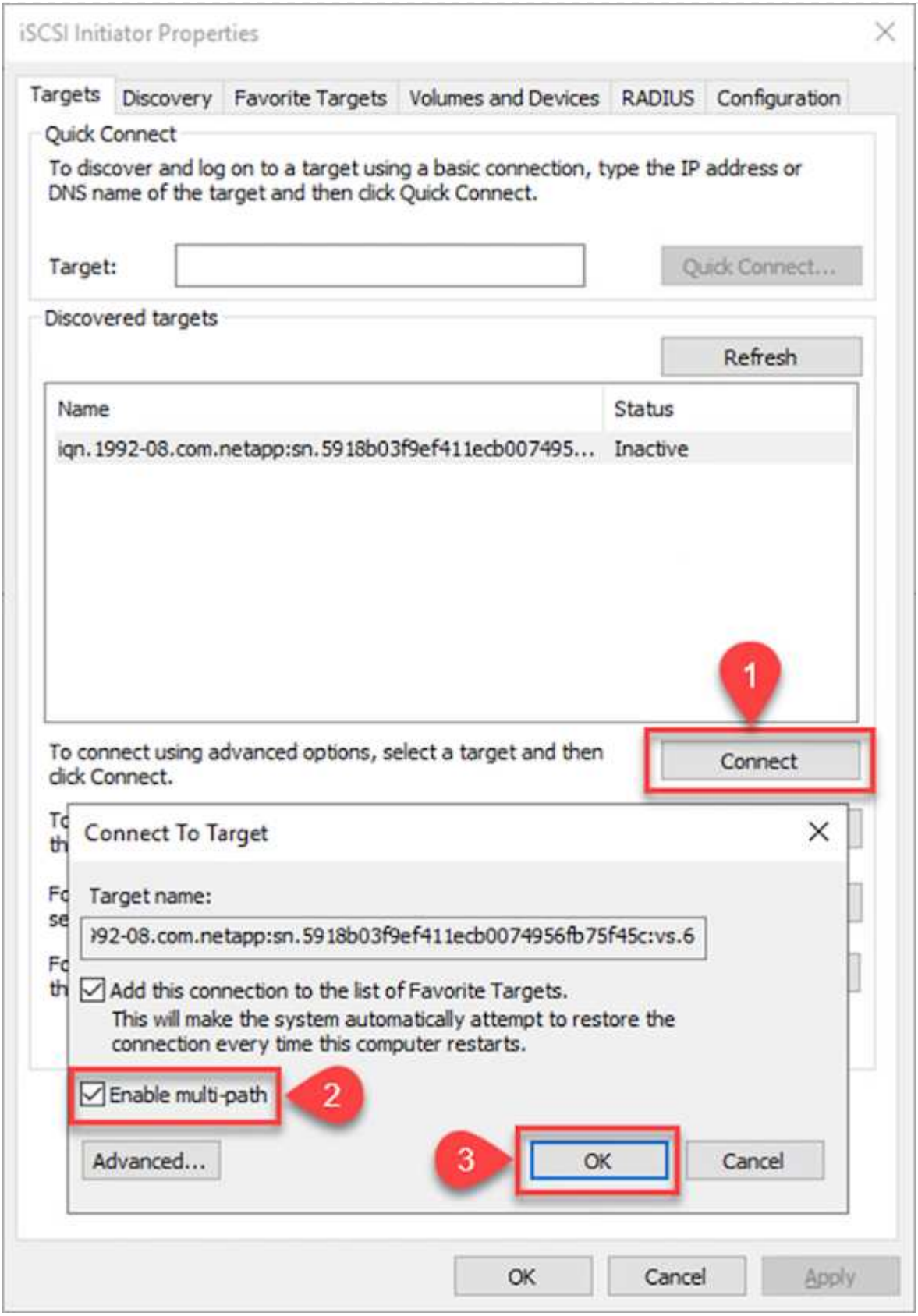


4. 검색 탭에서 포털 검색 을 클릭하고 FSx iSCSI 대상의 IP 주소를 입력합니다.

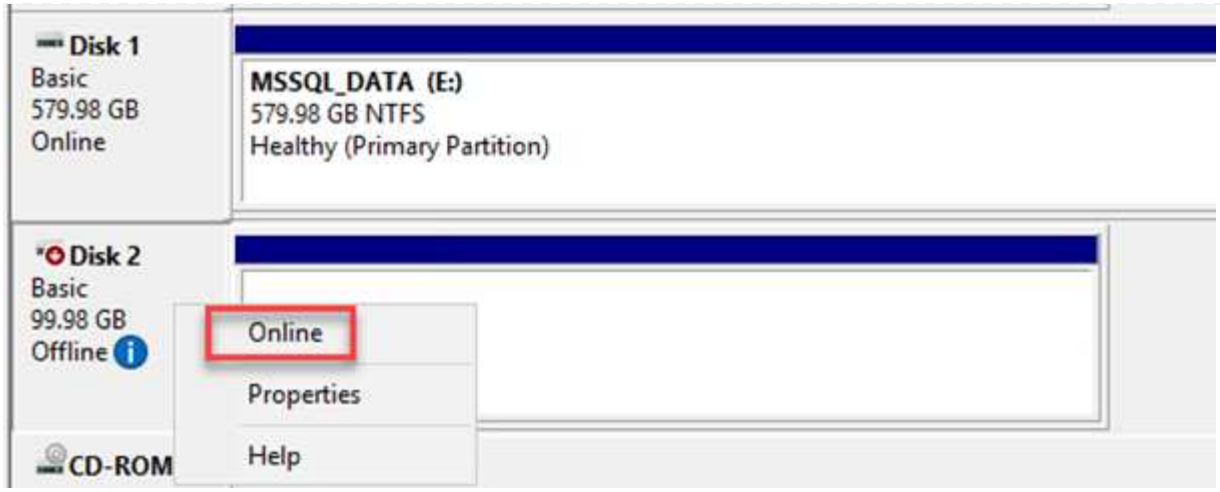




5. 대상 탭에서 연결을 클릭하고 구성에 적합한 경우 다중 경로 사용을 선택한 다음 확인을 클릭하여 대상에 연결합니다.

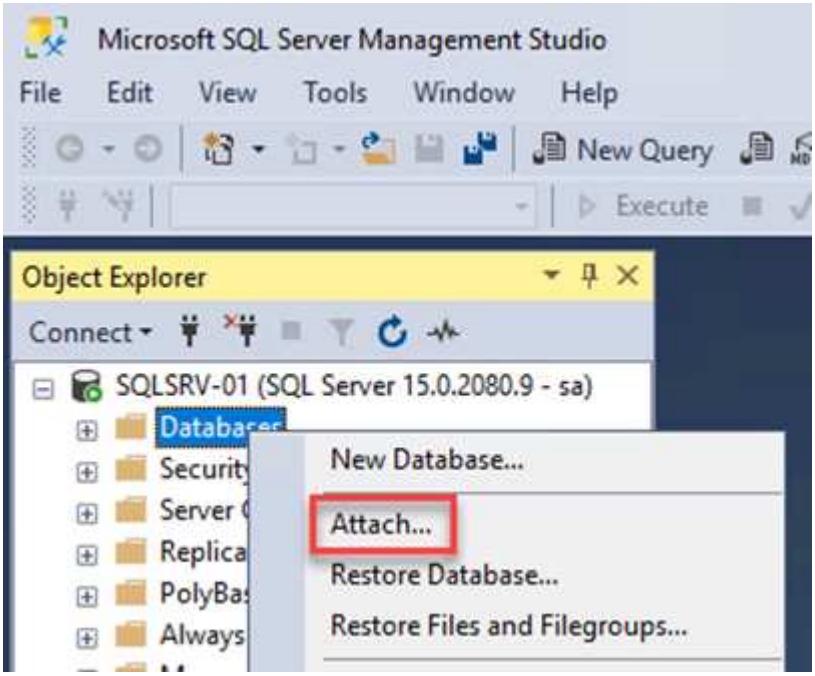


6. 컴퓨터 관리 유틸리티를 열고 디스크를 온라인 상태로 전환합니다. 이전에 사용했던 것과 동일한 드라이브 문자가 유지되는지 확인합니다.

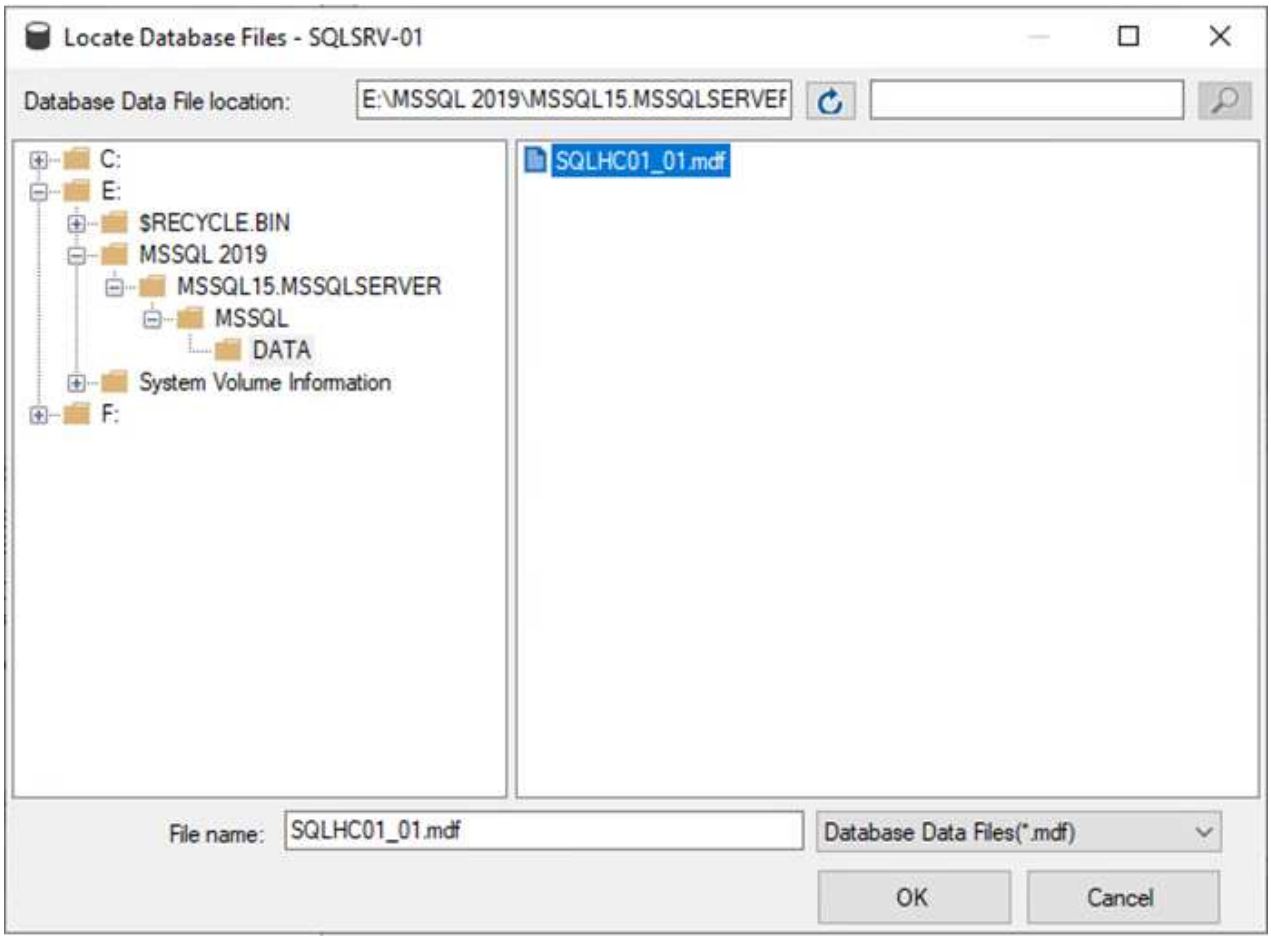

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

SQL Server 데이터베이스를 연결합니다

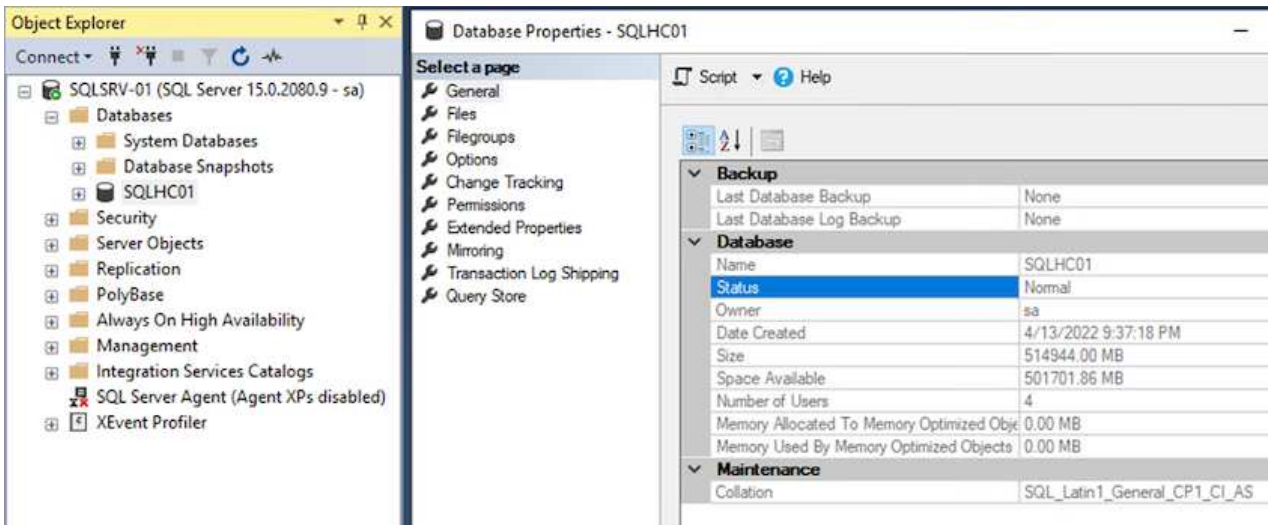
1. SQL Server VM에서 Microsoft SQL Server Management Studio를 열고 연결 을 선택하여 데이터베이스에 연결하는 프로세스를 시작합니다.



2. 추가 를 클릭하고 SQL Server 기본 데이터베이스 파일이 들어 있는 폴더로 이동한 다음 해당 파일을 선택하고 확인 을 클릭합니다.



3. 트랜잭션 로그가 별도의 드라이브에 있는 경우 트랜잭션 로그가 포함된 폴더를 선택합니다.
4. 완료되면 확인 을 클릭하여 데이터베이스를 연결합니다.

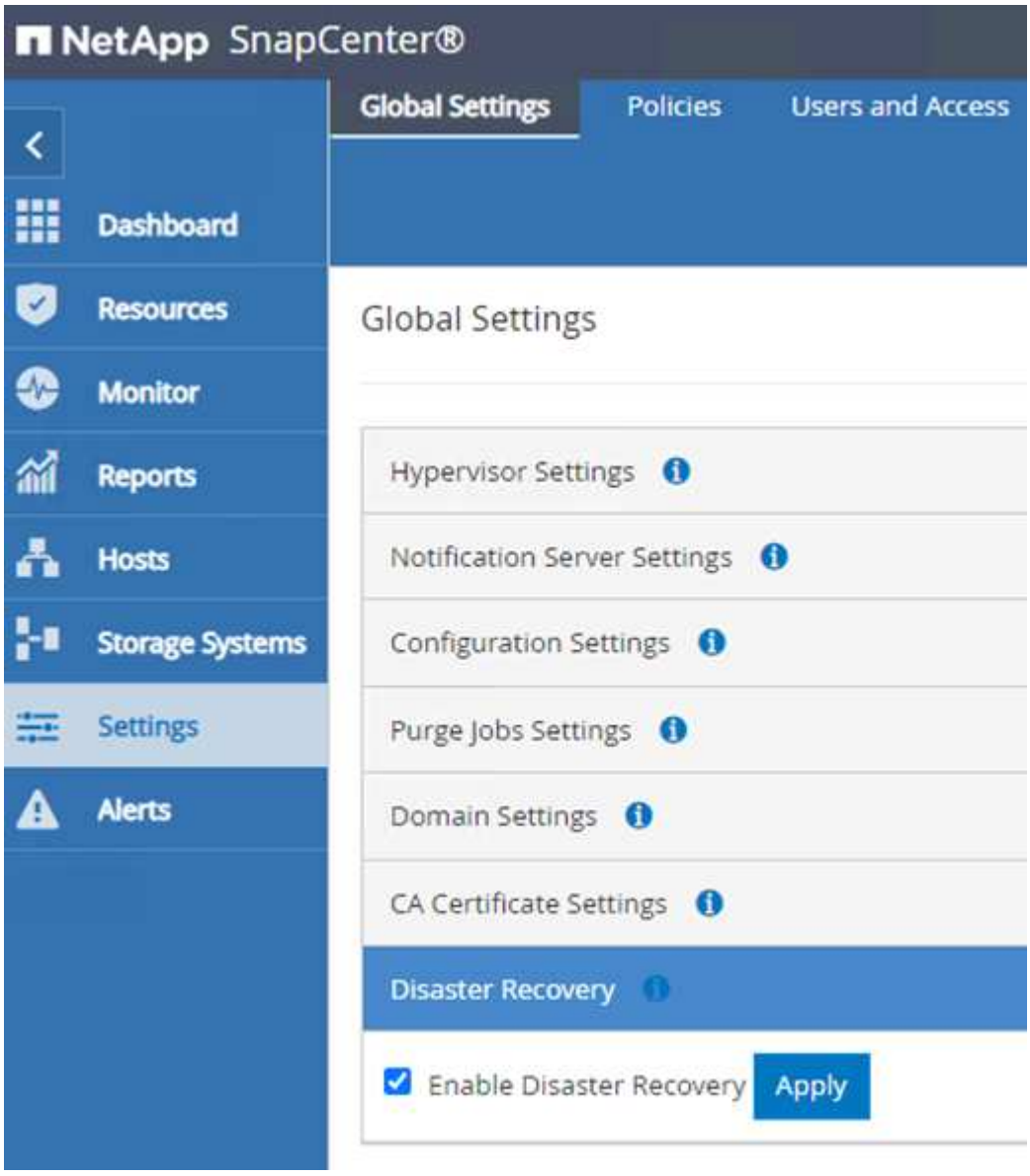


SQL Server 플러그인과 **SnapCenter** 통신을 확인합니다

SnapCenter 데이터베이스가 이전 상태로 복원되면 SQL Server 호스트가 자동으로 다시 검색됩니다. 이 작업이 올바르게 작동하려면 다음 필수 조건을 염두에 두십시오.

- SnapCenter를 재해 복구 모드로 전환해야 합니다. 이 작업은 Swagger API 또는 재해 복구의 글로벌 설정을 통해 수행할 수 있습니다.
- SQL Server의 FQDN은 온-프레미스 데이터 센터에서 실행 중인 인스턴스와 동일해야 합니다.
- 원래 SnapMirror 관계가 끊어야 합니다.
- 데이터베이스가 포함된 LUN은 SQL Server 인스턴스 및 연결된 데이터베이스에 마운트되어야 합니다.

SnapCenter가 재해 복구 모드에 있는지 확인하려면 SnapCenter 웹 클라이언트 내에서 설정 으로 이동합니다. 글로벌 설정 탭으로 이동한 다음 재해 복구 를 클릭합니다. 재해 복구 활성화 확인란이 활성화되어 있는지 확인합니다.



Oracle 애플리케이션 데이터를 복구합니다

다음 프로세스에서는 사내 사이트가 작동 불가능한 재해 발생 시 AWS의 VMware Cloud Services에서 Oracle 애플리케이션 데이터를 복구하는 방법에 대한 지침을 제공합니다.

복구 단계를 계속하려면 다음 필수 구성 요소를 완료하십시오.

1. Veeam Full Restore를 사용하여 Oracle Linux 서버 VM을 VMware Cloud SDDC로 복구했습니다.
2. 보조 SnapCenter 서버가 설정되었으며 이 섹션에 설명된 단계를 사용하여 SnapCenter 데이터베이스 및 구성 파일이 복원되었습니다 "SnapCenter 백업 및 복원 프로세스 요약"

Oracle 복원을 위해 FSx 구성 - SnapMirror 관계를 끊습니다

FSxN 인스턴스에서 호스팅되는 보조 스토리지 볼륨을 Oracle 서버에서 액세스할 수 있도록 하려면 먼저 기존 SnapMirror 관계를 해제해야 합니다.

1. FSx CLI에 로그인한 후 다음 명령을 실행하여 올바른 이름으로 필터링된 볼륨을 확인합니다.

```
FSx-Dest::> volume show -volume VolumeName*
```

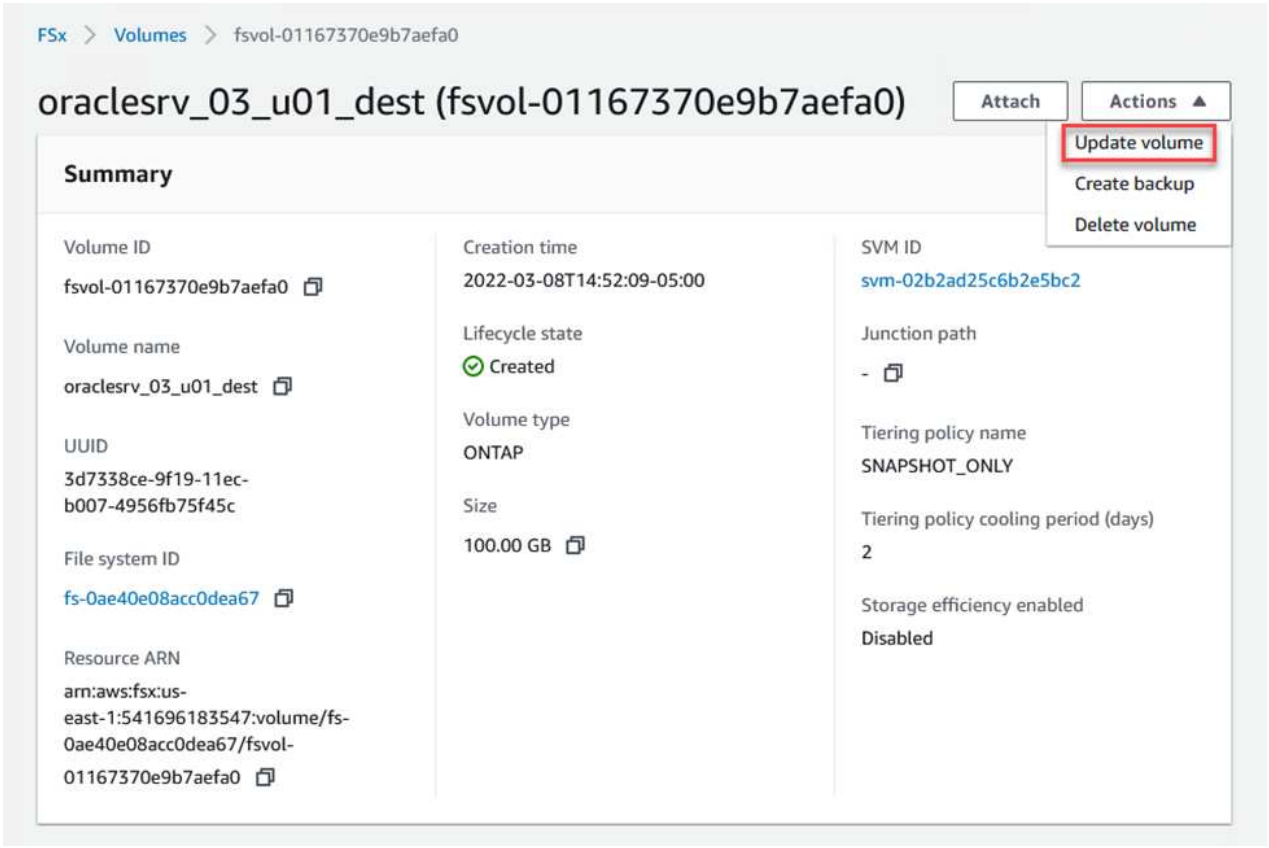
```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        online     DP        100GB    93.12GB    6%
ora_svm_dest
          oraclesrv_03_u02_dest
                       aggr1        online     DP        200GB    34.98GB   82%
ora_svm_dest
          oraclesrv_03_u03_dest
                       aggr1        online     DP        150GB    33.37GB   77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::>
```

2. 다음 명령을 실행하여 기존 SnapMirror 관계를 중단하십시오.

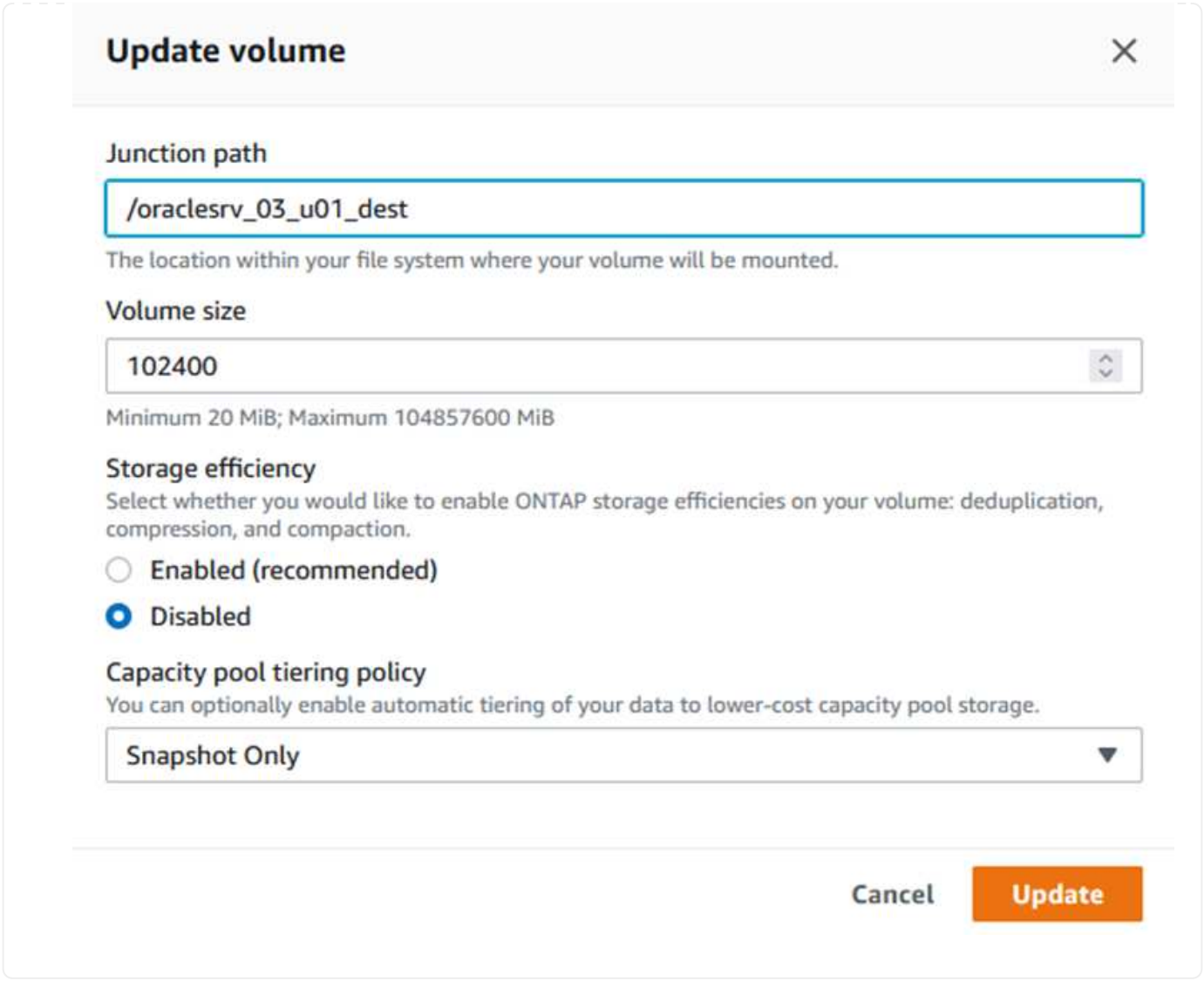
```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. Amazon FSx 웹 클라이언트에서 junction-path를 업데이트합니다.



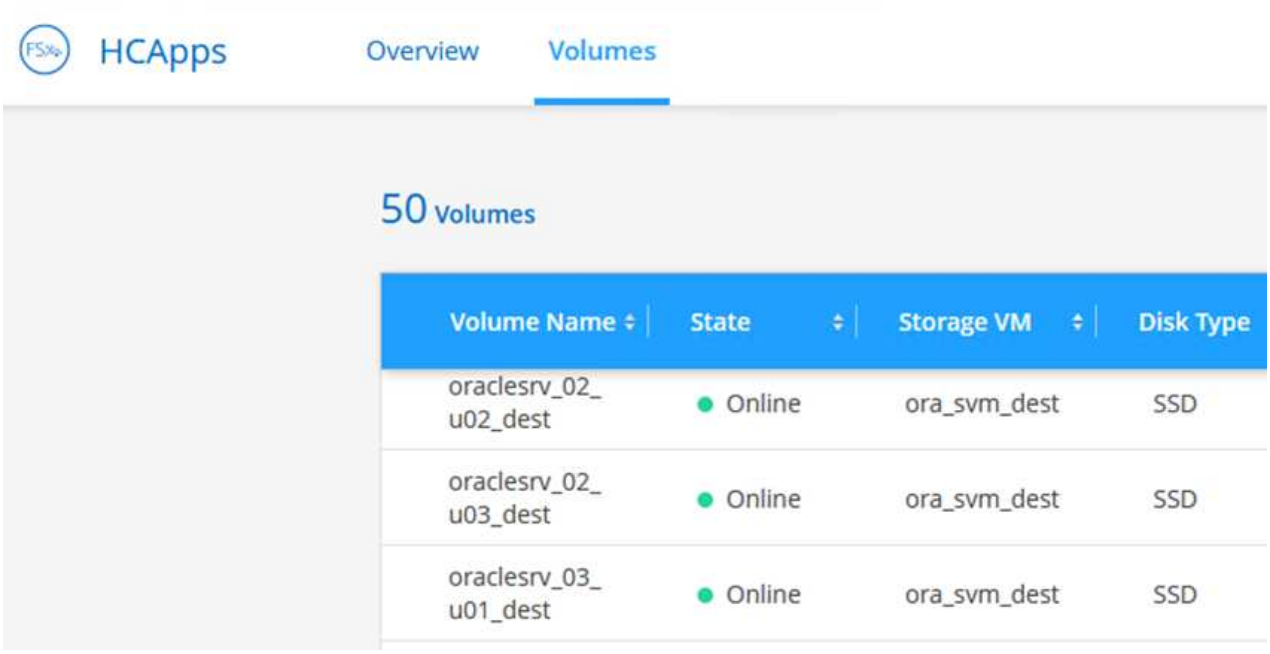
4. 접합 경로 이름을 추가하고 업데이트 를 클릭합니다. Oracle 서버에서 NFS 볼륨을 마운트할 때 이 연결 경로를 지정합니다.


Update volume
Junction path
/oraclesrv_03_u01_dest
The location within your file system where your volume will be mounted.
Volume size
102400
Minimum 20 MiB; Maximum 104857600 MiB
Storage efficiency
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.
Enabled (recommended)
Disabled
Capacity pool tiering policy
You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.
Snapshot Only
Cancel
Update

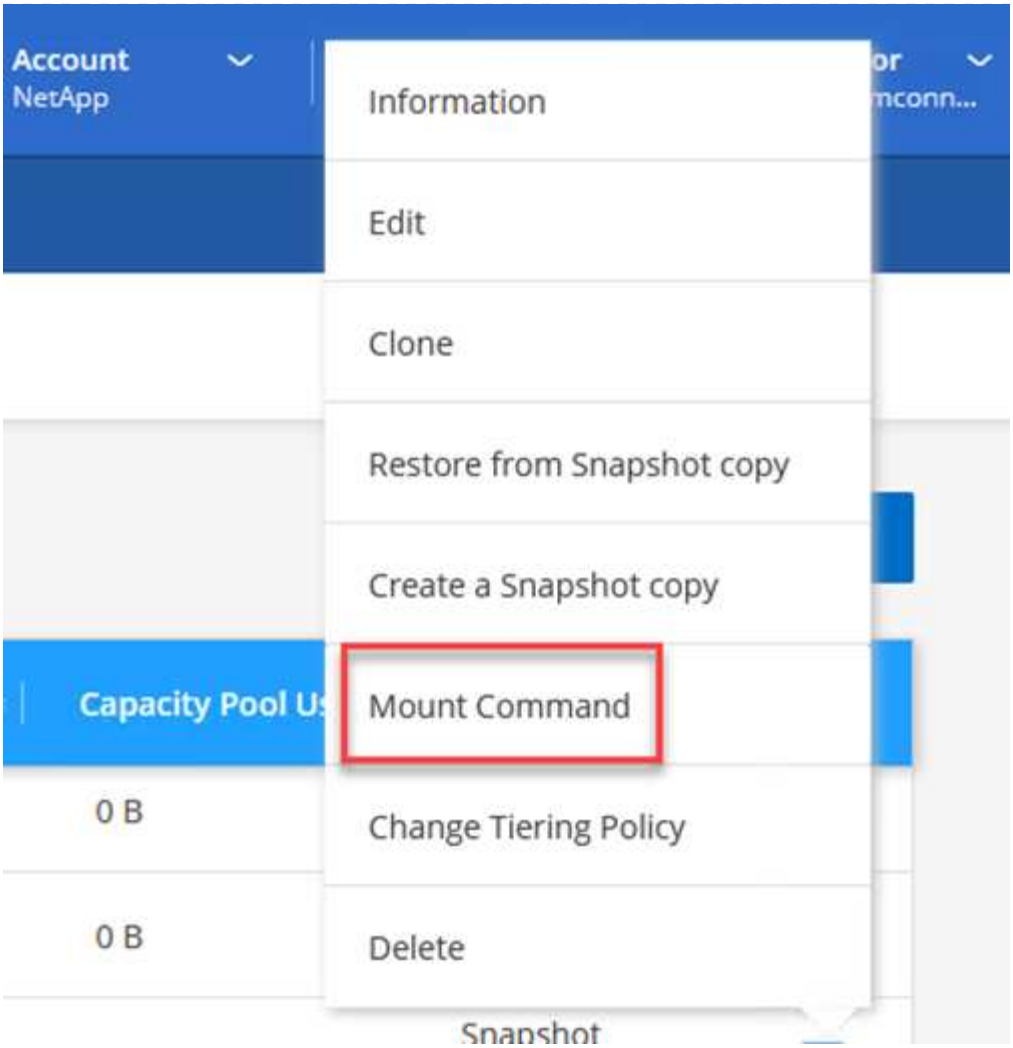
Oracle Server에서 **NFS** 볼륨을 마운트합니다

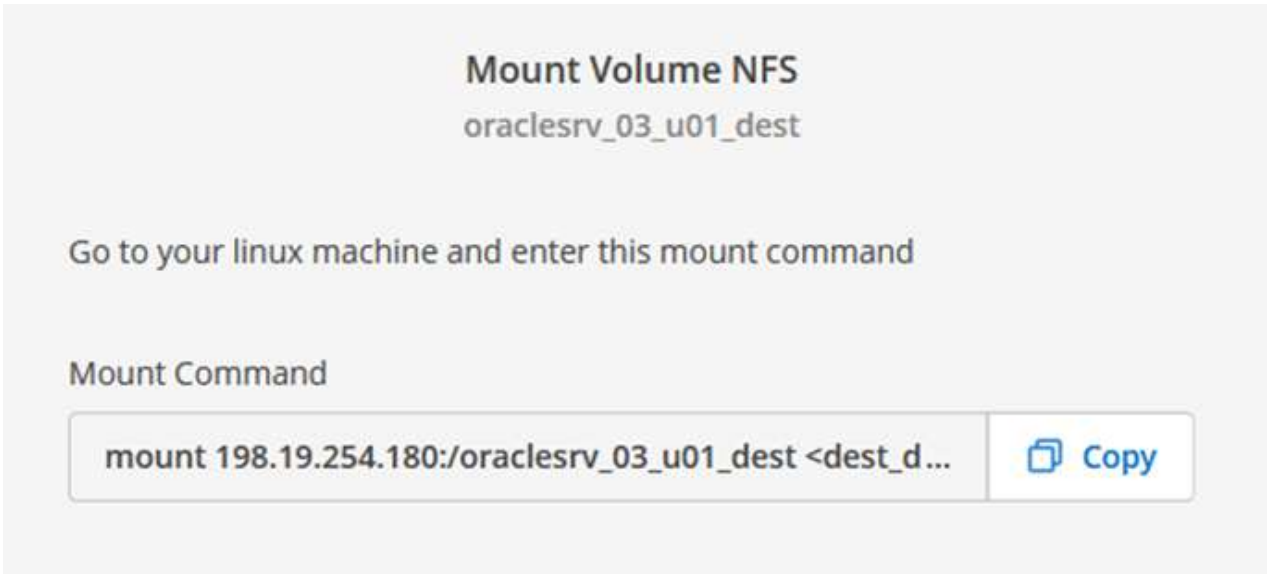
Cloud Manager에서 Oracle 데이터베이스 파일 및 로그가 포함된 NFS 볼륨을 마운트하기 위한 올바른 NFS LIF IP 주소를 사용하여 마운트 명령을 얻을 수 있습니다.

1. Cloud Manager에서 FSx 클러스터의 볼륨 목록에 액세스합니다.



2. 작업 메뉴에서 마운트 명령을 선택하여 Oracle Linux 서버에서 사용할 마운트 명령을 보고 복사합니다.





3. Oracle Linux Server에 NFS 파일 시스템을 마운트합니다. NFS 공유를 마운트하는 디렉토리가 Oracle Linux 호스트에 이미 있습니다.
4. Oracle Linux 서버에서 mount 명령을 사용하여 NFS 볼륨을 마운트합니다.

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

Oracle 데이터베이스와 연결된 각 볼륨에 대해 이 단계를 반복합니다.

재부팅 시 NFS 마운트를 영구적으로 만들려면 '/etc/fstab' 파일을 편집하여 마운트 명령을 포함합니다.

5. Oracle 서버를 재부팅합니다. Oracle 데이터베이스는 정상적으로 시작되어 사용할 수 있어야 합니다.

장애 복구

이 솔루션에 설명된 페일오버 프로세스가 성공적으로 완료되면 SnapCenter 및 Veeam이 AWS에서 백업 기능을 재개합니다. 이제 ONTAP용 FSx는 원래 사내 데이터 센터와 SnapMirror 관계가 없는 기본 스토리지로 지정됩니다. 정상적인 기능을 사내에서 다시 시작한 후 이 설명서에 나와 있는 것과 동일한 프로세스를 사용하여 데이터를 사내 ONTAP 스토리지 시스템에 다시 미러링할 수 있습니다.

또한 이 설명서에 나와 있는 것처럼 SnapCenter를 구성하여 ONTAP용 FSx에서 온프레미스에 있는 ONTAP 스토리지 시스템으로 애플리케이션 데이터 볼륨을 미러링할 수 있습니다. 마찬가지로, Veeam을 구성하여 스케일아웃 백업 저장소를 사용하여 Amazon S3에 백업 복사본을 복제함으로써 사내 데이터 센터에 상주하는 Veeam 백업 서버에 액세스할 수 있습니다.

페일백은 이 문서의 범위를 벗어나지만 장애 복구는 여기에 설명된 세부 프로세스와 거의 차이가 없습니다.

결론

이 문서에 제공된 사용 사례는 NetApp과 VMware의 통합을 강조하는 검증된 재해 복구 기술에 초점을 맞춥니다. NetApp ONTAP 스토리지 시스템은 검증된 데이터 미러링 기술을 제공하므로 조직이 주요 클라우드 공급자와 함께 상주하면서 사내 및 ONTAP 기술을 아우르는 재해 복구 솔루션을 설계할 수 있습니다.

AWS 기반 ONTAP용 FSX는 SnapCenter 및 SyncMirror와 원활하게 통합되어 애플리케이션 데이터를 클라우드로 복제할 수 있는 솔루션 중 하나입니다. Veeam 백업 및 복제는 NetApp ONTAP 스토리지 시스템과 긴밀하게 통합되며 vSphere 기본 스토리지에 대한 페일오버를 제공할 수 있는 또 다른 잘 알려진 기술입니다.

이 솔루션은 SQL Server 및 Oracle 애플리케이션 데이터를 호스팅하는 ONTAP 시스템의 게스트 연결 스토리지를 사용하는 재해 복구 솔루션을 제공합니다. SnapCenter with SnapMirror를 사용하면 ONTAP 시스템에서 애플리케이션 볼륨을 보호하고 클라우드에 있는 FSx 또는 CVO로 복제할 수 있는 관리가 쉬운 솔루션을 제공할 수 있습니다. SnapCenter는 모든 애플리케이션 데이터를 AWS의 VMware 클라우드로 페일오버하는 DR 지원 솔루션입니다.

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹 사이트를 검토하십시오.

- 솔루션 설명서 링크

  "VMware 솔루션을 사용하는 NetApp 하이브리드 멀티 클라우드"

  "NetApp 솔루션"

저자: Josh Powell - NetApp 솔루션 엔지니어링

개요

Veeam Backup & Replication은 VMware Cloud의 데이터를 보호하는 효과적이고 안정적인 솔루션입니다. 이 솔루션은 Veeam 백업 및 복제를 사용하여 VMware 클라우드의 ONTAP NFS 데이터 저장소용 FSx에 상주하는 애플리케이션 VM을 백업 및 복원하기 위한 적절한 설정 및 구성을 보여 줍니다.

VMware Cloud(AWS의 경우)는 NFS 데이터 저장소를 보조 스토리지로 사용할 수 있도록 지원하며, FSx for NetApp ONTAP는 SDDC 클러스터의 ESXi 호스트 수에 관계없이 확장할 수 있는 클라우드 애플리케이션에 대량의 데이터를 저장해야 하는 고객을 위한 안전한 솔루션입니다. 이 통합 AWS 스토리지 서비스는 기존의 모든 NetApp ONTAP 기능을 갖춘 고효율 스토리지를 제공합니다.

사용 사례

이 솔루션은 다음과 같은 사용 사례를 해결합니다.

- NetApp ONTAP용 FSx를 백업 저장소로 사용하여 VMC에서 호스팅되는 Windows 및 Linux 가상 머신의 백업 및 복원
- NetApp ONTAP용 FSx를 백업 저장소로 사용하여 Microsoft SQL Server 애플리케이션 데이터를 백업 및 복원합니다.
- NetApp ONTAP용 FSx를 백업 저장소로 사용하여 Oracle 애플리케이션 데이터를 백업 및 복원합니다.

ONTAP용 **Amazon FSx**를 사용하는 **NFS** 데이터 저장소입니다

이 솔루션의 모든 가상 머신은 ONTAP 보조 NFS 데이터 저장소용 FSx에 상주합니다. ONTAP용 FSx를 보조 NFS 데이터 저장소로 사용하면 여러 가지 이점을 얻을 수 있습니다. 예를 들어, 다음을 수행할 수 있습니다.

- 복잡한 설정 및 관리 없이도 확장 가능하고 가용성이 높은 파일 시스템을 클라우드에서 생성할 수 있습니다.
- 기존 VMware 환경과 통합되므로 친숙한 툴 및 프로세스를 사용하여 클라우드 리소스를 관리할 수 있습니다.
- 스냅샷 및 복제와 같이 ONTAP에서 제공하는 고급 데이터 관리 기능을 활용하여 데이터를 보호하고 가용성을 보장합니다.

솔루션 구축 개요

이 목록에는 Veeam 백업 및 복제를 구성하고, ONTAP용 FSx를 백업 저장소로 사용하여 백업 및 복원 작업을 실행하고, SQL Server 및 Oracle VM 및 데이터베이스의 복원을 수행하는 데 필요한 높은 수준의 단계가 나와 있습니다.

1. Veeam 백업 및 복제를 위한 iSCSI 백업 저장소로 사용할 ONTAP 파일 시스템용 FSx를 생성합니다.
2. Veeam 프록시를 구축하여 백업 워크로드를 분산하고 ONTAP용 FSx에서 호스팅되는 iSCSI 백업 저장소를 마운트합니다.
3. SQL Server, Oracle, Linux 및 Windows 가상 머신을 백업하도록 Veeam 백업 작업을 구성합니다.
4. SQL Server 가상 머신 및 개별 데이터베이스를 복구합니다.
5. Oracle 가상 머신 및 개별 데이터베이스를 복원합니다.

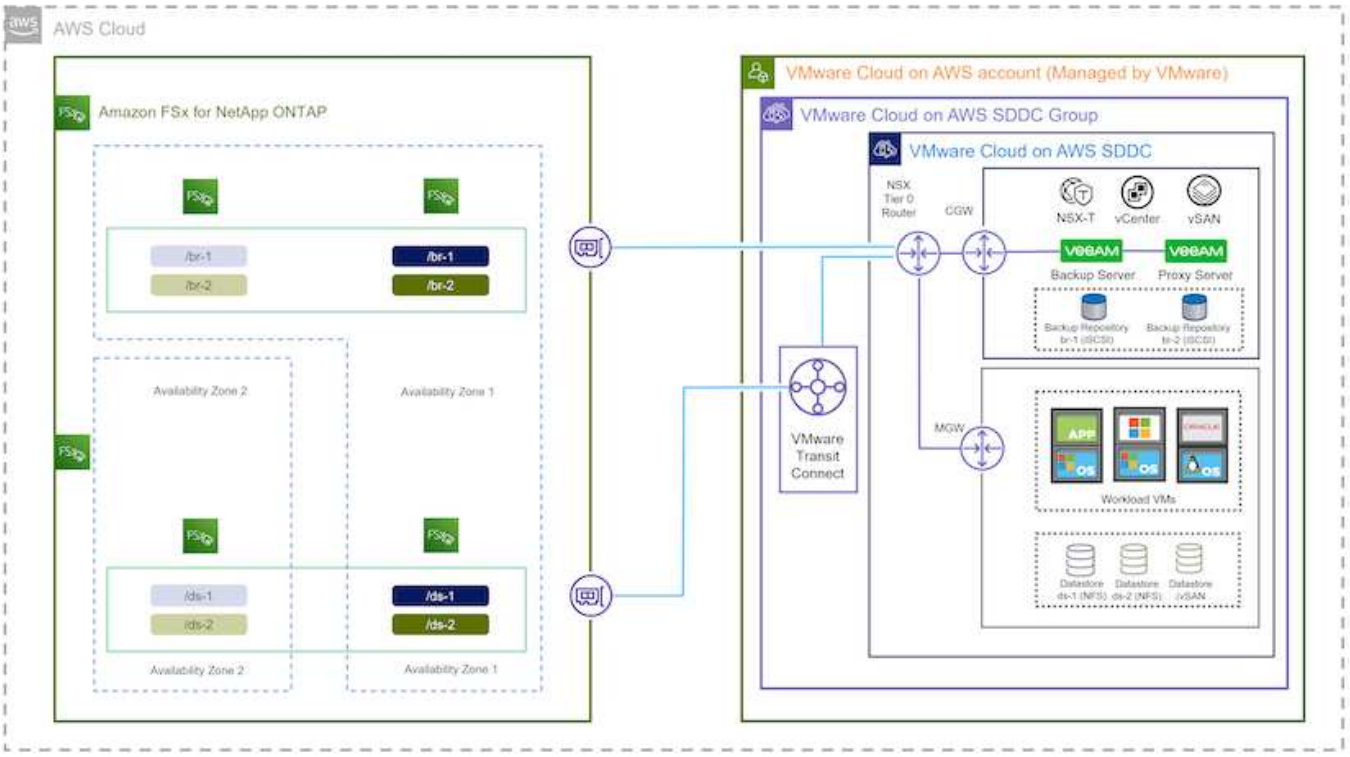
필수 구성 요소

이 솔루션의 목적은 VMware Cloud에서 실행되고 NetApp ONTAP용 FSx에서 호스팅하는 NFS 데이터 저장소에 있는 가상 머신의 데이터 보호를 시연하는 것입니다. 이 솔루션에서는 다음 구성 요소가 구성되어 사용할 준비가 되어 있다고 가정합니다.

1. VMware 클라우드에 연결된 NFS 데이터 저장소가 하나 이상 있는 ONTAP 파일 시스템용 FSX
2. Veeam Backup & Replication 소프트웨어가 설치된 Microsoft Windows Server VM
    - Veeam Backup & Replication 서버에서 IP 주소 또는 정규화된 도메인 이름을 사용하여 vCenter 서버를 검색했습니다.
3. 솔루션을 구축하는 동안 Veeam Backup Proxy 구성 요소와 함께 Microsoft Windows Server VM이 설치됩니다.
4. ONTAP NFS 데이터 저장소용 FSx에 상주하는 VMDK 및 애플리케이션 데이터가 있는 Microsoft SQL Server VM 이 솔루션에서는 두 개의 별도 VMDK에 두 개의 SQL 데이터베이스를 구축했습니다.
    - 참고: 최상의 데이터베이스 및 트랜잭션 로그 파일은 성능 및 안정성을 향상시키기 위해 별도의 드라이브에 배치됩니다. 이는 트랜잭션 로그가 순차적으로 작성되는 반면 데이터베이스 파일은 무작위로 작성되기 때문에 발생합니다.
5. ONTAP NFS 데이터 저장소용 FSx에 상주하는 VMDK 및 애플리케이션 데이터가 있는 Oracle 데이터베이스 VM
6. ONTAP NFS 데이터 저장소용 FSx에 상주하는 VMDK가 있는 Linux 및 Windows 파일 서버 VM
7. Veeam을 사용하려면 백업 환경의 서버와 구성 요소 간 통신에 특정 TCP 포트가 필요합니다. Veeam 백업 인프라 구성 요소에서 필요한 방화벽 규칙이 자동으로 생성됩니다. 네트워크 포트 요구 사항의 전체 목록은 의 포트 섹션을 참조하십시오 "Veeam Backup and Replication User Guide for VMware vSphere를 참조하십시오".

고급 아키텍처

이 솔루션의 테스트/검증은 최종 배포 환경과 일치하거나 일치하지 않을 수 있는 랩에서 수행되었습니다. 자세한 내용은 다음 섹션을 참조하십시오.



하드웨어/소프트웨어 구성 요소

이 솔루션의 목적은 VMware Cloud에서 실행되고 NetApp ONTAP용 FSx에서 호스팅하는 NFS 데이터 저장소에 있는 가상 머신의 데이터 보호를 시연하는 것입니다. 이 솔루션에서는 다음 구성 요소가 이미 구성되어 있고 사용할 준비가 되어 있다고 가정합니다.

- Microsoft Windows VM은 ONTAP NFS 데이터 저장소용 FSx에 있습니다
- Linux(CentOS) VM은 ONTAP NFS 데이터 저장소용 FSx에 있습니다
- Microsoft SQL Server VM은 ONTAP NFS 데이터 저장소용 FSx에 있습니다
  - 두 개의 데이터베이스가 별도의 VMDK에서 호스팅됩니다
- ONTAP NFS 데이터 저장소용 FSx에 있는 Oracle VM

솔루션 구축

이 솔루션에서는 Veeam Backup and Replication 소프트웨어를 사용하여 AWS 기반 VMware Cloud SDDC에서 SQL Server, Oracle, Windows 및 Linux 파일 서버 가상 시스템의 백업 및 복구를 수행하는 솔루션을 구축 및 검증하는 방법에 대한 자세한 지침을 제공합니다. 이 솔루션의 가상 머신은 FSx for ONTAP에서 호스팅하는 보조 NFS 데이터 저장소에 상주합니다. 또한 Veeam 백업 저장소에 사용할 iSCSI 볼륨을 호스팅하기 위해 ONTAP 파일 시스템용 별도의 FSx가 사용됩니다.

ONTAP 파일 시스템 생성을 위한 FSx, 백업 저장소로 사용할 iSCSI 볼륨 마운트, 백업 작업 생성 및 실행, VM 및 데이터베이스 복원 수행 등을 살펴보겠습니다.

NetApp ONTAP용 FSx에 대한 자세한 내용은 를 참조하십시오 "ONTAP용 FSX 사용 설명서".

Veeam Backup and Replication에 대한 자세한 내용은 을 참조하십시오 "Veeam Help Center 기술 문서" 사이트.

AWS에서 Veeam Backup and Replication을 VMware Cloud로 사용할 때의 고려 사항 및 제한 사항은 을 참조하십시오 "AWS 기반 VMware 클라우드 및 Dell EMC 지원 기반 VMware 클라우드 고려 사항 및 제한 사항".

Veeam 프록시 서버를 구축하십시오

Veeam 프록시 서버는 Veeam Backup & Replication 소프트웨어의 구성 요소로, 소스와 백업 또는 복제 타겟 간의 매개 역할을 합니다. 프록시 서버는 데이터를 로컬로 처리하여 백업 작업 중에 데이터 전송을 최적화하고 가속화할 수 있도록 지원하며, 서로 다른 전송 모드를 사용하여 VMware vStorage APIs for Data Protection 또는 직접 스토리지 액세스를 통해 데이터에 액세스할 수 있습니다.

Veeam 프록시 서버 설계를 선택할 때는 필요한 동시 작업 수와 전송 모드 또는 스토리지 액세스 유형을 고려해야 합니다.

프록시 서버의 수와 시스템 요구 사항에 대한 사이징은 를 참조하십시오 "Veeam VMware vSphere 모범 사례 가이드".

Veeam Data Mover는 Veeam Proxy Server의 구성 요소이며 소스에서 VM 데이터를 가져오고 타겟으로 전송하기 위한 수단으로 전송 모드를 사용합니다. 전송 모드는 백업 작업을 구성하는 동안 지정됩니다. 직접 스토리지 액세스를 사용하여 NFS 데이터 저장소에서 데이터 백업의 효율성을 높일 수 있습니다.

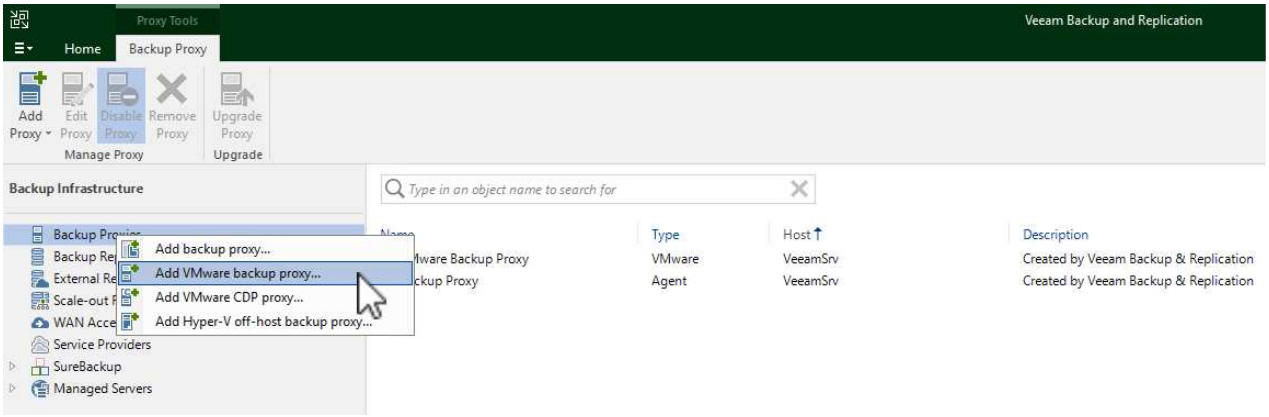
운송 모드에 대한 자세한 내용은 를 참조하십시오 "Veeam Backup and Replication User Guide for VMware vSphere를 참조하십시오".

다음 단계에서는 VMware Cloud SDDC의 Windows VM에 Veeam Proxy Server를 구축하는 방법을 살펴봅니다.

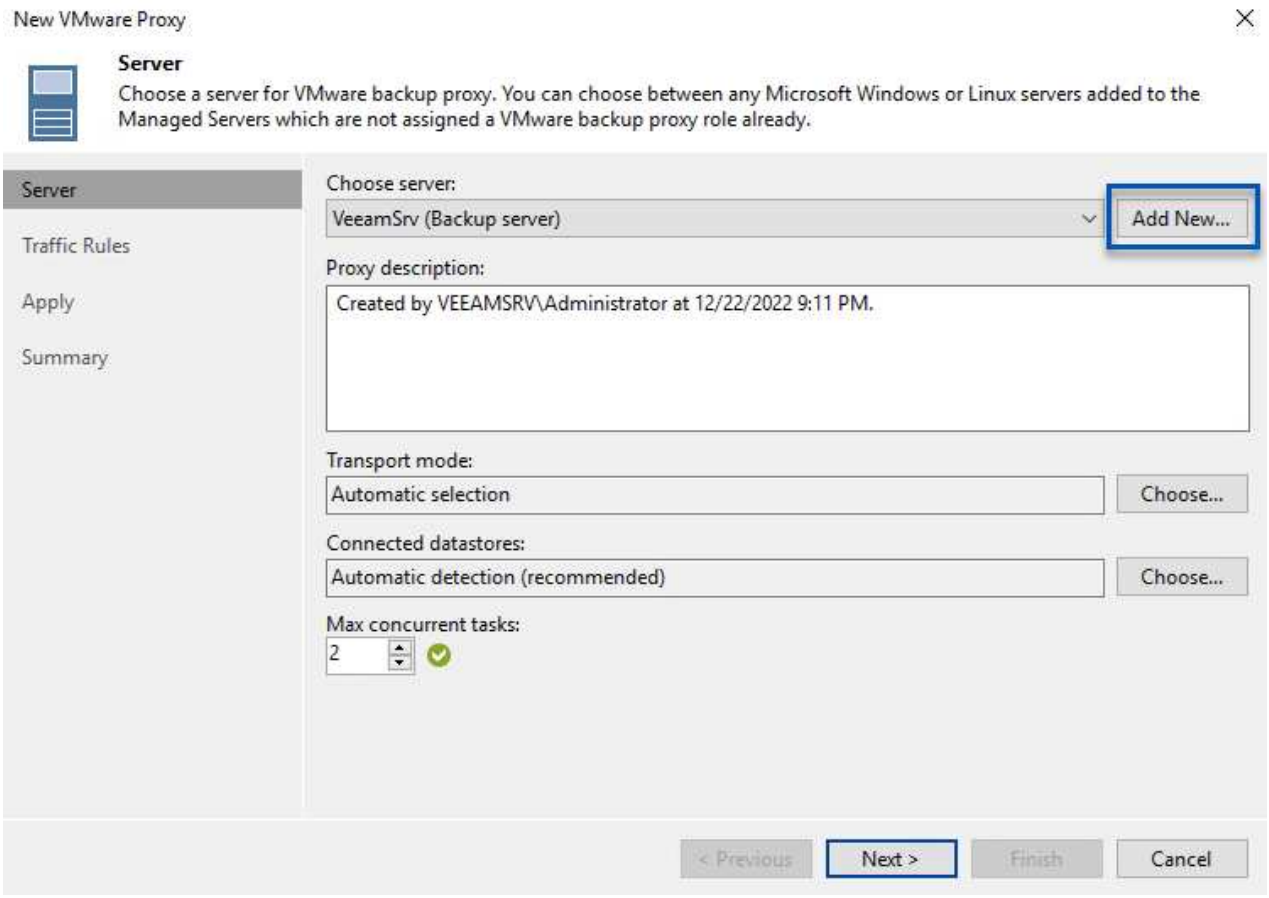
Veeam Proxy를 구축하여 백업 워크로드를 분산합니다

이 단계에서는 Veeam 프록시를 기존 Windows VM에 구축합니다. 따라서 운영 Veeam Backup Server와 Veeam Proxy 간에 백업 작업을 분산할 수 있습니다.

1. Veeam Backup and Replication 서버에서 관리 콘솔을 열고 왼쪽 하단 메뉴에서 * Backup Infrastructure * 를 선택합니다.
2. Backup Proxies * 를 마우스 오른쪽 버튼으로 클릭하고 * Add VMware backup proxy… * 를 클릭하여 마법사를 엽니다.

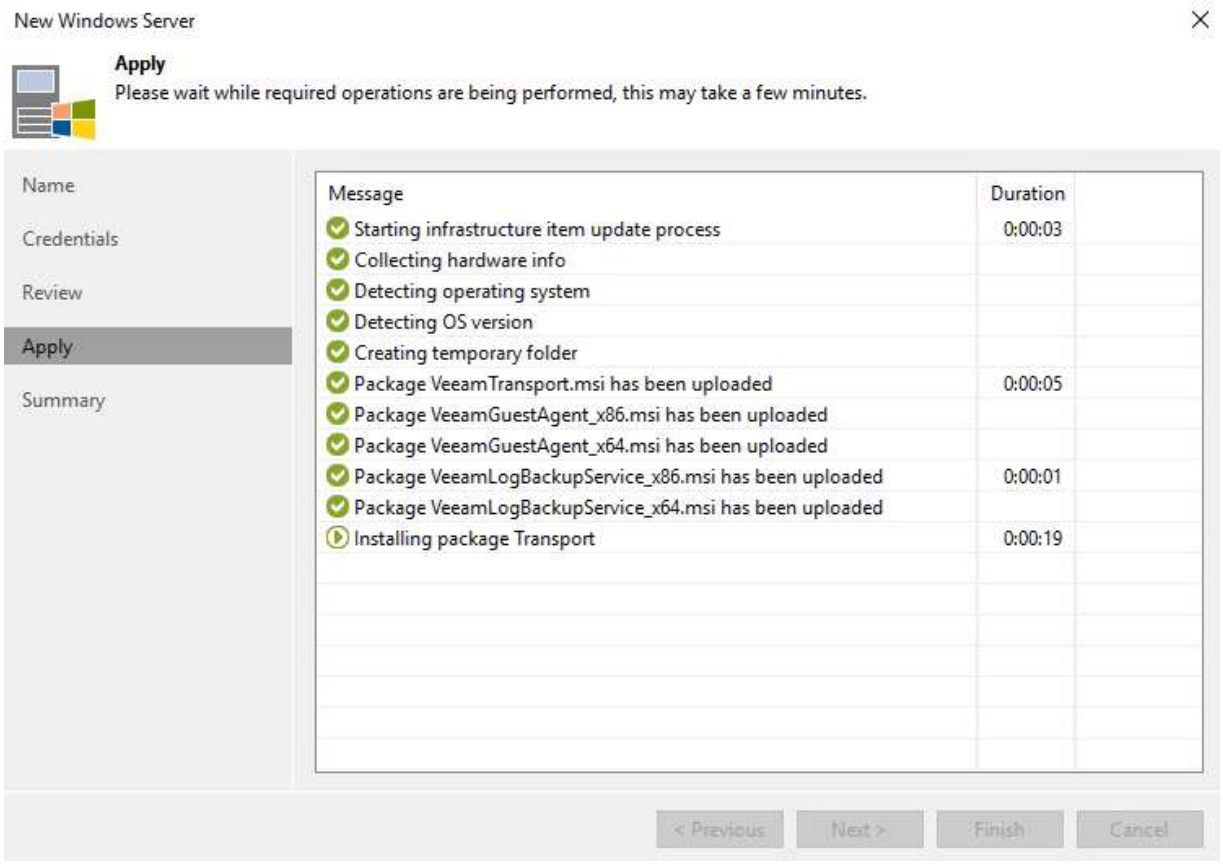


3. VMware 프록시 추가 * 마법사에서 * 새로 추가… * 버튼을 클릭하여 새 프록시 서버를 추가합니다.

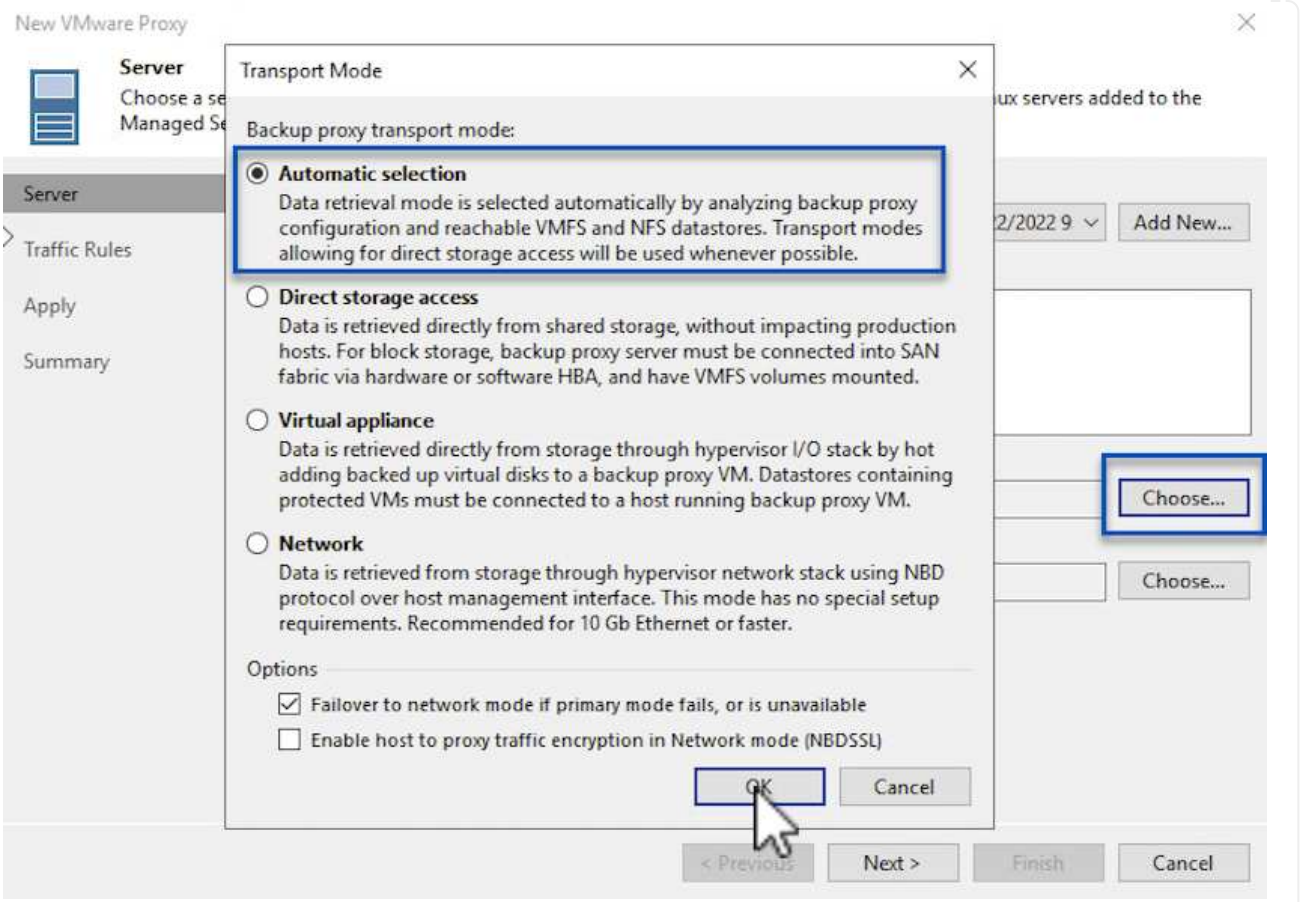


4. Microsoft Windows를 추가하려면 을 선택하고 프롬프트에 따라 서버를 추가합니다.

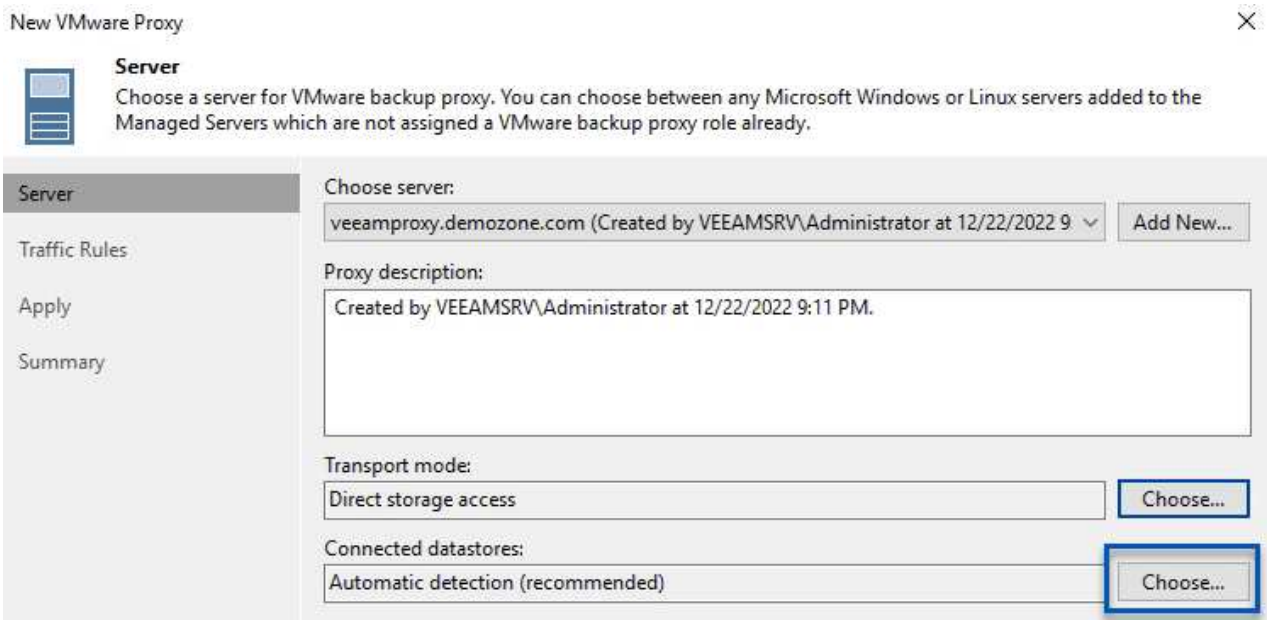
- DNS 이름 또는 IP 주소를 입력합니다
- 새 시스템의 자격 증명에 사용할 계정을 선택하거나 새 자격 증명을 추가합니다
- 설치할 구성 요소를 검토한 다음 * 적용 * 을 클릭하여 배포를 시작합니다

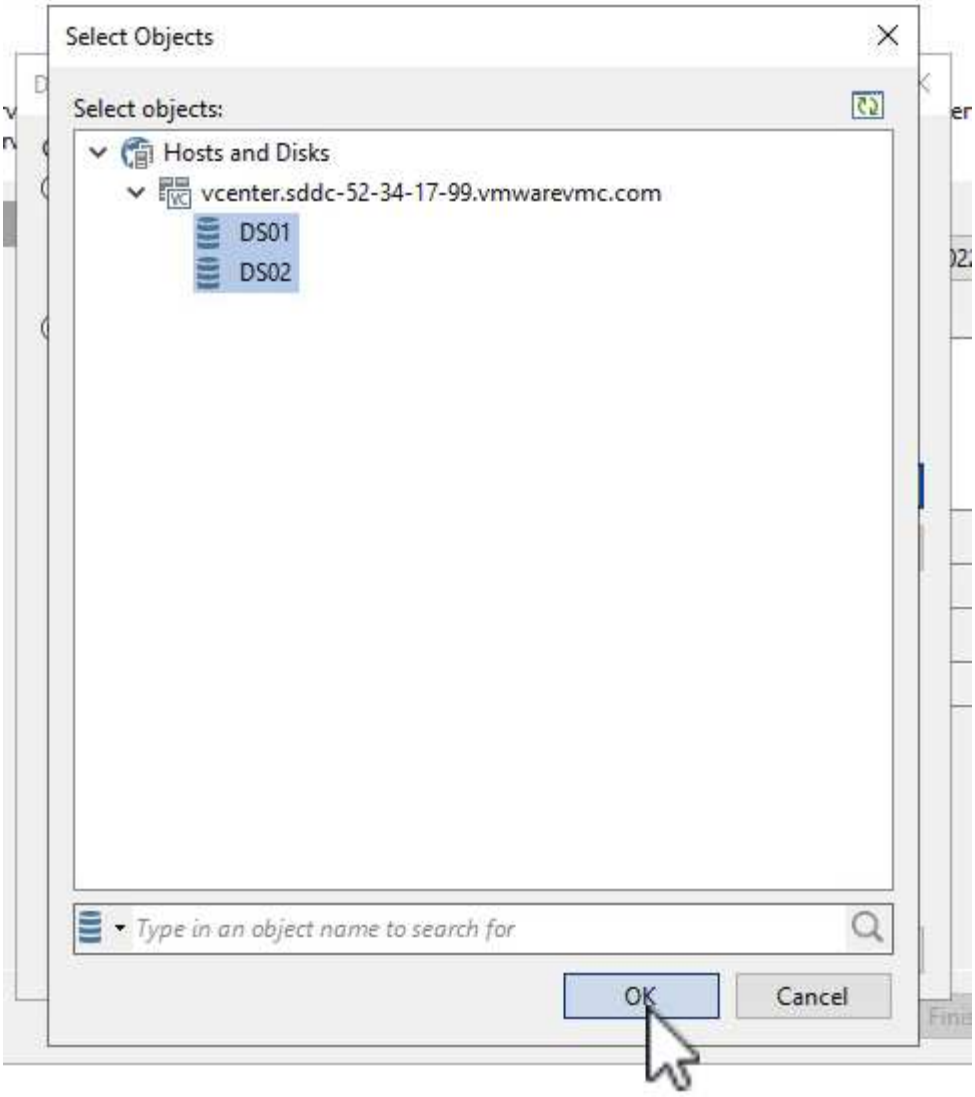


5. 새 VMware 프록시 * 마법사로 돌아가서 전송 모드를 선택합니다. 여기서는 * 자동 선택 * 을 선택했습니다.

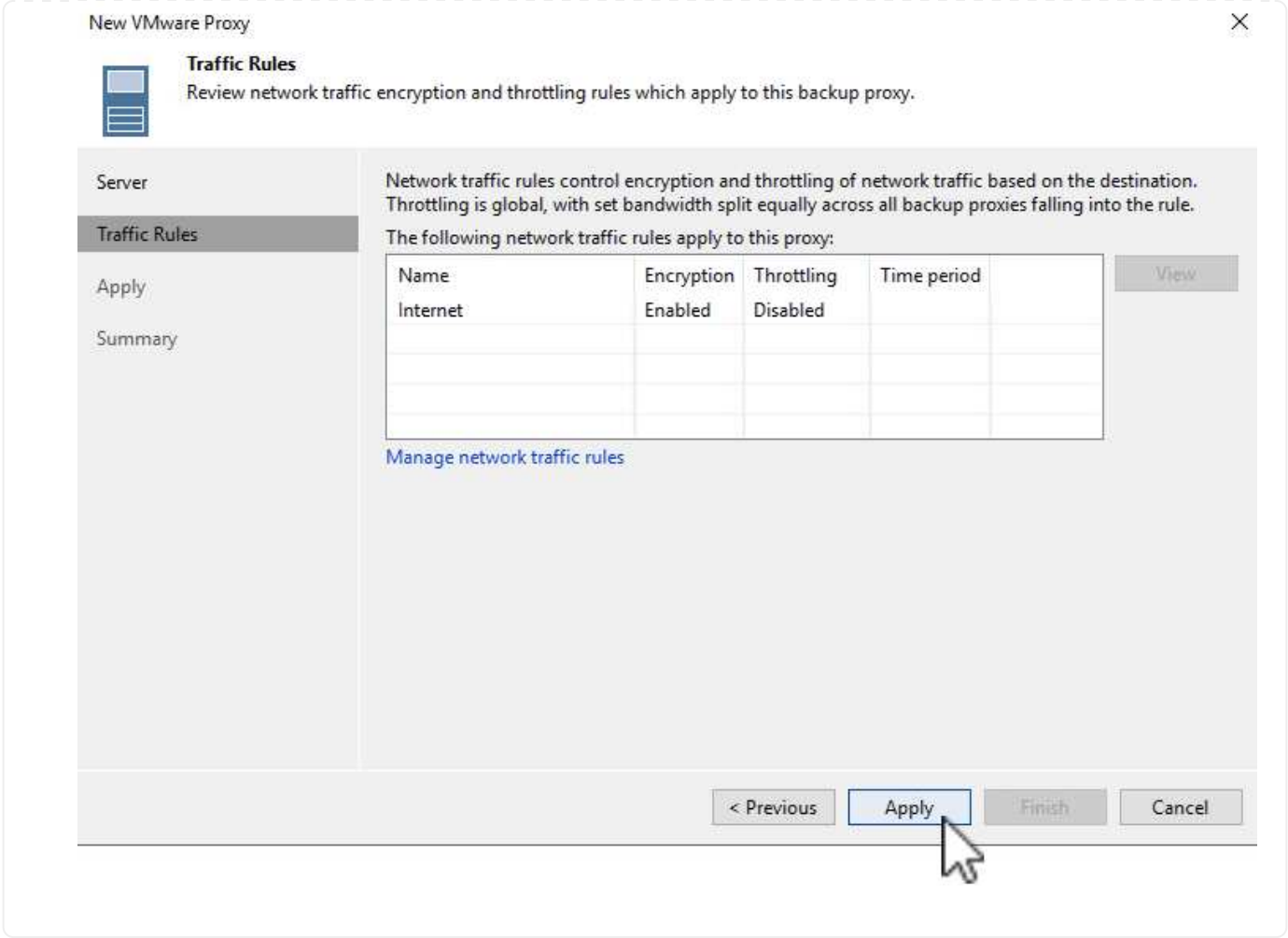


6. VMware 프록시에서 직접 액세스할 수 있는 연결된 데이터 저장소를 선택합니다.





7. 원하는 암호화 또는 임계치 조절과 같은 특정 네트워크 트래픽 규칙을 구성하고 적용합니다. 완료되면 * Apply * 버튼을 클릭하여 구축을 완료합니다.



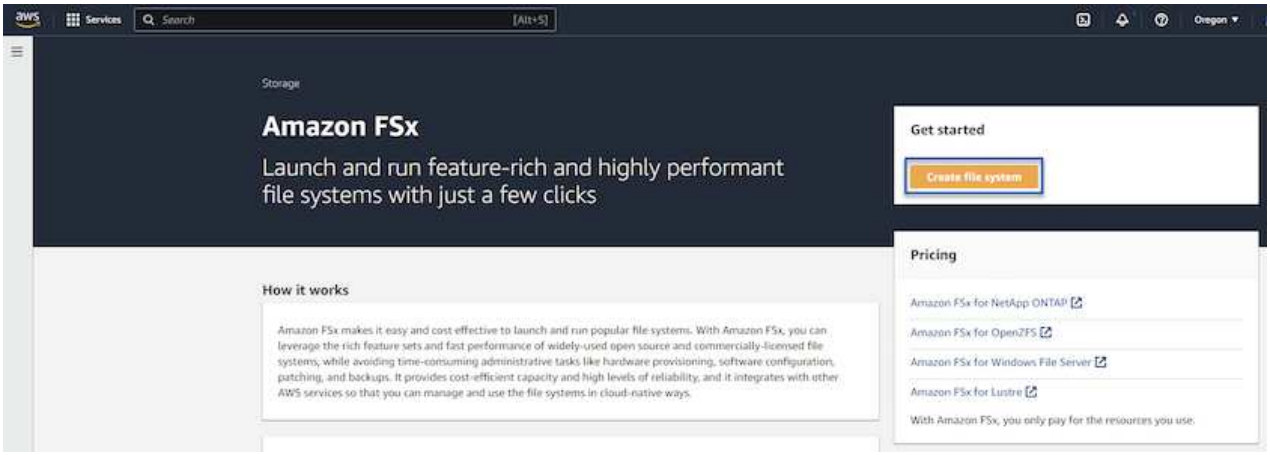
스토리지 및 백업 리포지토리를 구성합니다

Primary Veeam Backup 서버와 Veeam Proxy 서버는 직접 연결된 스토리지의 형태로 백업 저장소에 액세스할 수 있습니다. 이 섹션에서는 ONTAP 파일 시스템용 FSx 생성, Veeam 서버에 iSCSI LUN 마운트 및 백업 저장소 생성에 대해 설명합니다.

ONTAP 파일 시스템용 FSx를 생성합니다

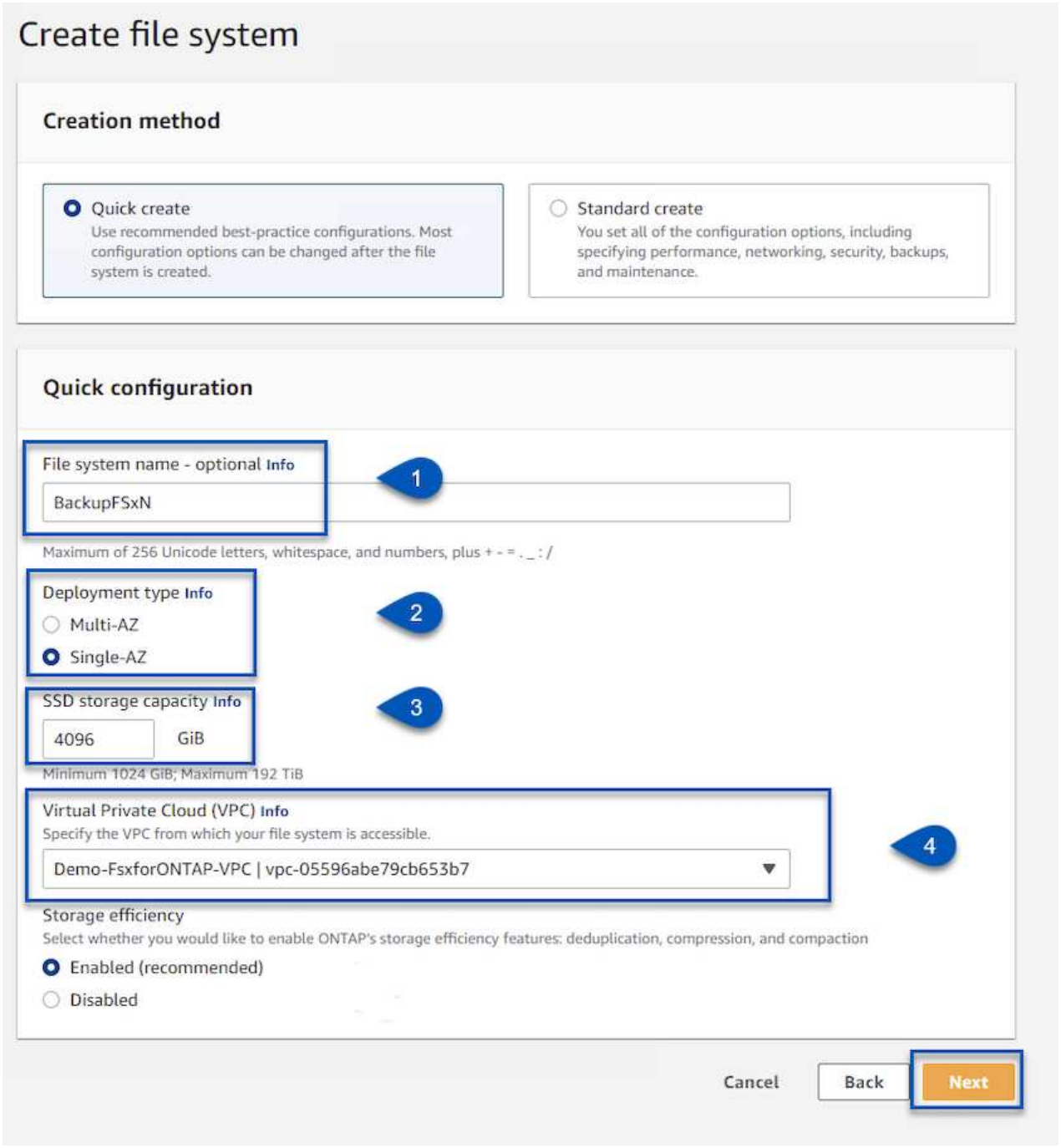
Veeam 백업 리포지토리를 위한 iSCSI 볼륨을 호스팅하는 데 사용할 ONTAP 파일 시스템용 FSx를 생성합니다.

1. AWS 콘솔에서 FSx로 이동한 다음 * 파일 시스템 생성 * 으로 이동합니다



2. 계속하려면 * Amazon FSx for NetApp ONTAP * 를 선택하고 * Next * 를 선택합니다.

3. ONTAP 클러스터용 FSx가 상주할 파일 시스템 이름, 구축 유형, SSD 스토리지 용량 및 VPC를 입력합니다. VMware Cloud에서 가상 머신 네트워크와 통신하도록 VPC를 구성해야 합니다. 다음 * 을 클릭합니다.



4. 배포 단계를 검토하고 * 파일 시스템 생성 * 을 클릭하여 파일 시스템 생성 프로세스를 시작합니다.

iSCSI LUN을 구성 및 마운트합니다

FSx for ONTAP에서 iSCSI LUN을 생성 및 구성하고 Veeam 백업 및 프록시 서버에 마운트합니다. 나중에 이러한 LUN을 사용하여 Veeam 백업 저장소를 생성할 수 있습니다.

ONTAP용 FSx에서 iSCSI LUN을 생성하는 과정은 여러 단계로 이루어집니다. 볼륨을 생성하는 첫 번째 단계는 Amazon FSx 콘솔 또는 NetApp ONTAP CLI에서 수행할 수 있습니다.

ONTAP용 FSx 사용에 대한 자세한 내용은 를 참조하십시오 "ONTAP용 FSX 사용 설명서".

1. NetApp ONTAP CLI에서 다음 명령을 사용하여 초기 볼륨을 생성합니다.

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name
-aggregate aggregate_name -size vol_size -type RW
```

2. 이전 단계에서 생성한 볼륨을 사용하여 LUN 생성:

```
FSx-Backup::> lun create -vserver svm_name -path
/vol/vol_name/lun_name -size size -ostype windows -space-allocation
enabled
```

3. Veeam 백업 및 프록시 서버의 iSCSI IQN이 포함된 이니시에이터 그룹을 생성하여 LUN에 대한 액세스 권한을 부여합니다.

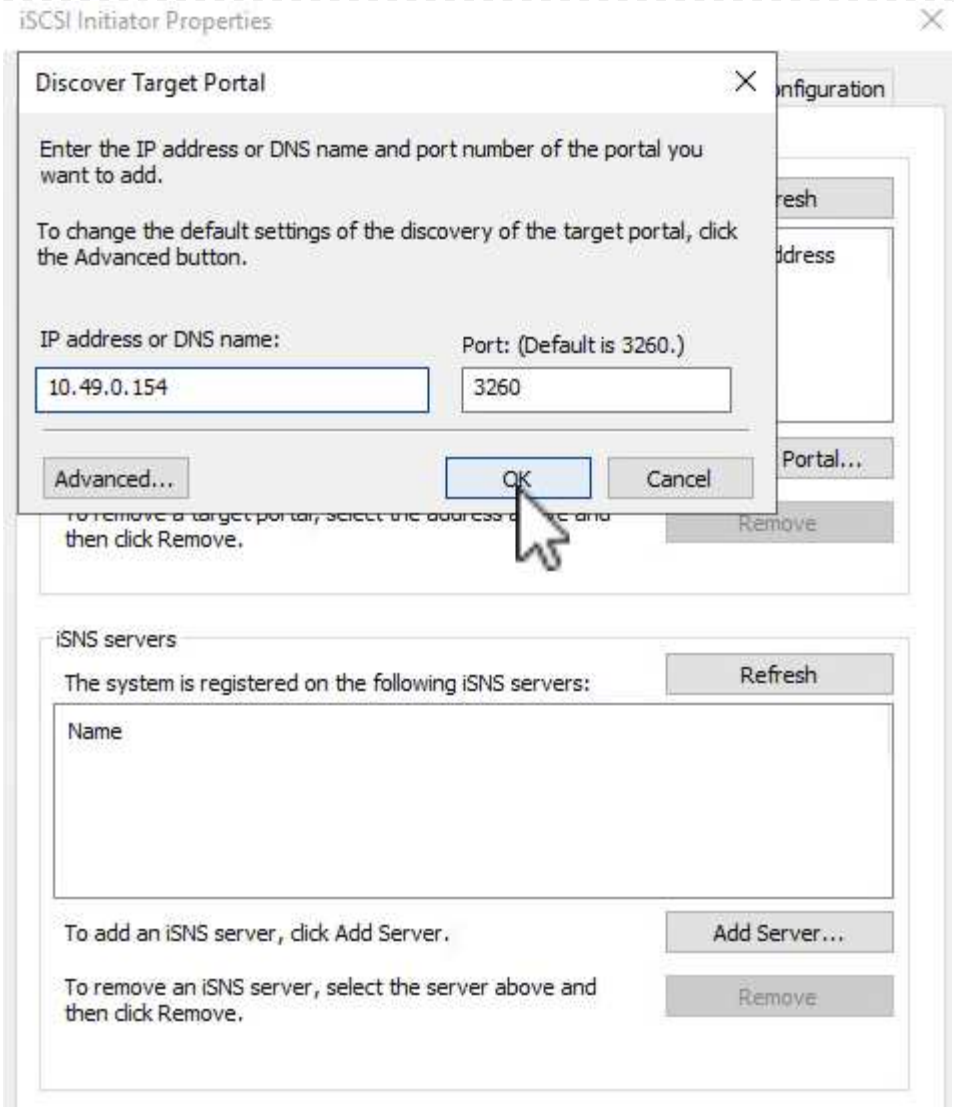
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

위의 단계를 완료하려면 먼저 Windows 서버의 iSCSI 이니시에이터 속성에서 IQN을 검색해야 합니다.

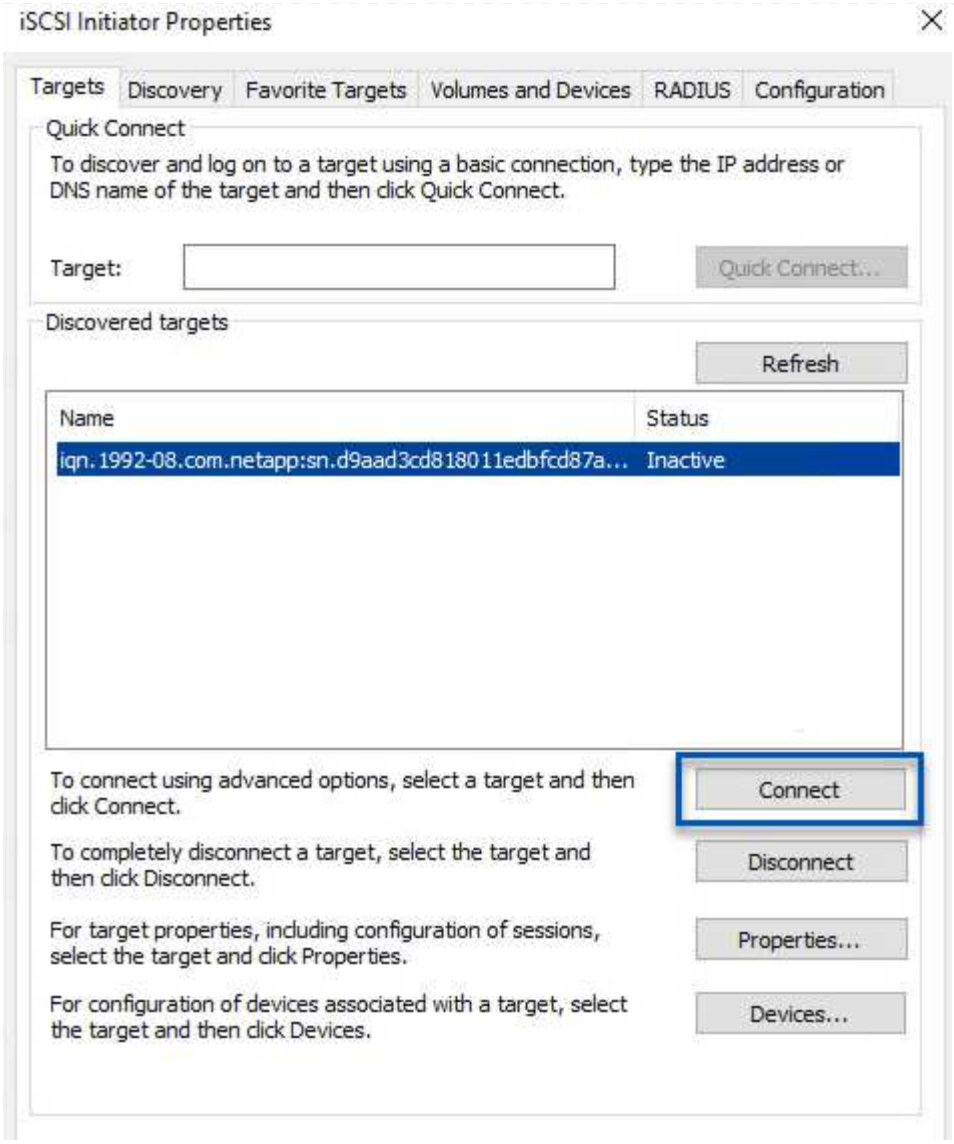
4. 마지막으로 LUN을 방금 생성한 이니시에이터 그룹에 매핑합니다.

```
FSx-Backup::> lun mapping create -vserver svm_name -path
/vol/vol_name/lun_name igroup igroup_name
```

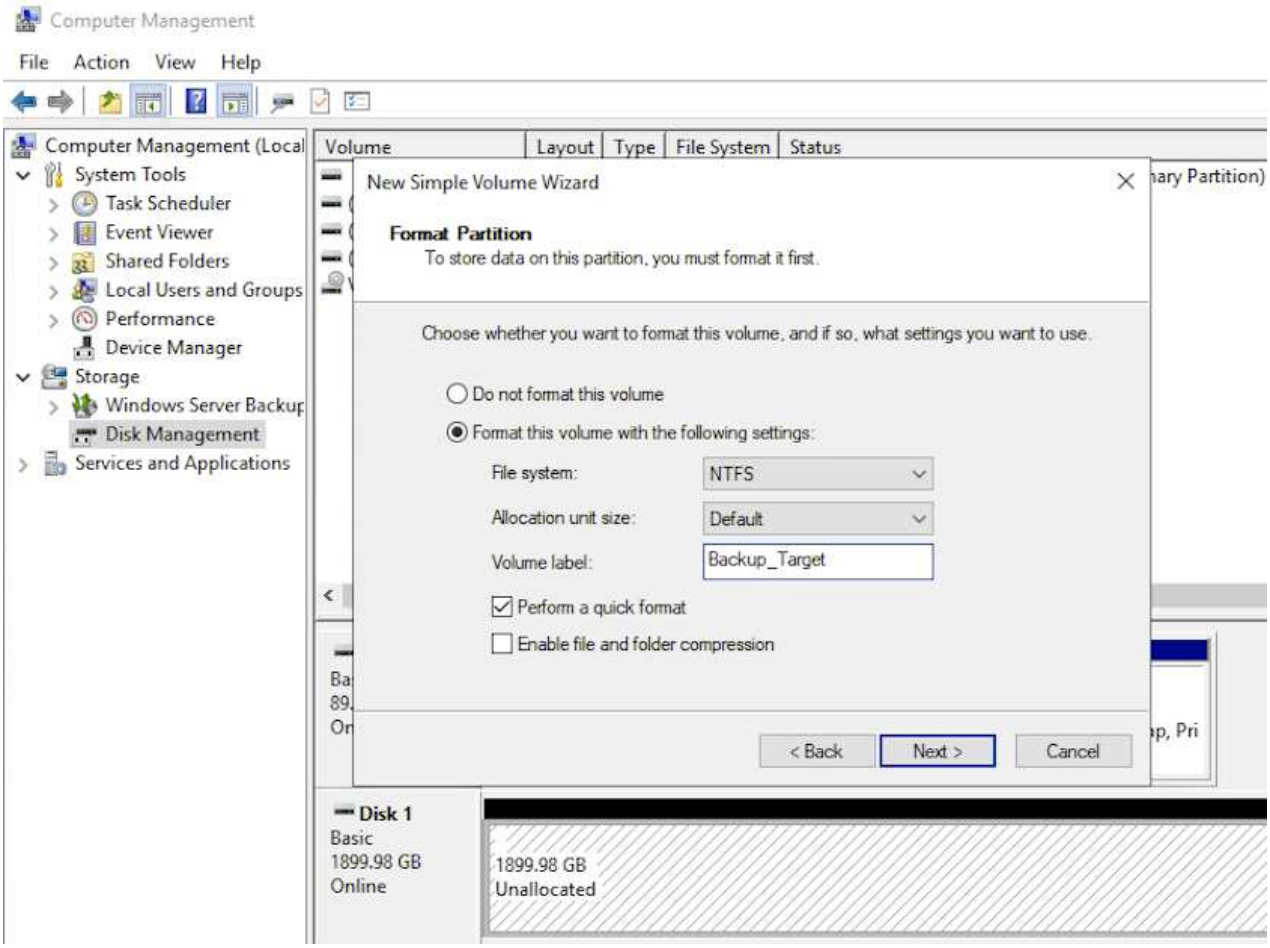
5. iSCSI LUN을 마운트하려면 Veeam Backup & Replication Server에 로그인하고 iSCSI Initiator Properties를 엽니다. 검색 * 탭으로 이동하여 iSCSI 대상 IP 주소를 입력합니다.



6. Targets * 탭에서 비활성 LUN을 강조 표시하고 * Connect * 를 클릭합니다. 다중 경로 사용 * 상자를 선택하고 * 확인 * 을 클릭하여 LUN에 연결합니다.



7. 디스크 관리 유틸리티에서 새 LUN을 초기화하고 원하는 이름 및 드라이브 문자로 볼륨을 생성합니다. 다중 경로 사용 * 상자를 선택하고 * 확인 * 을 클릭하여 LUN에 연결합니다.

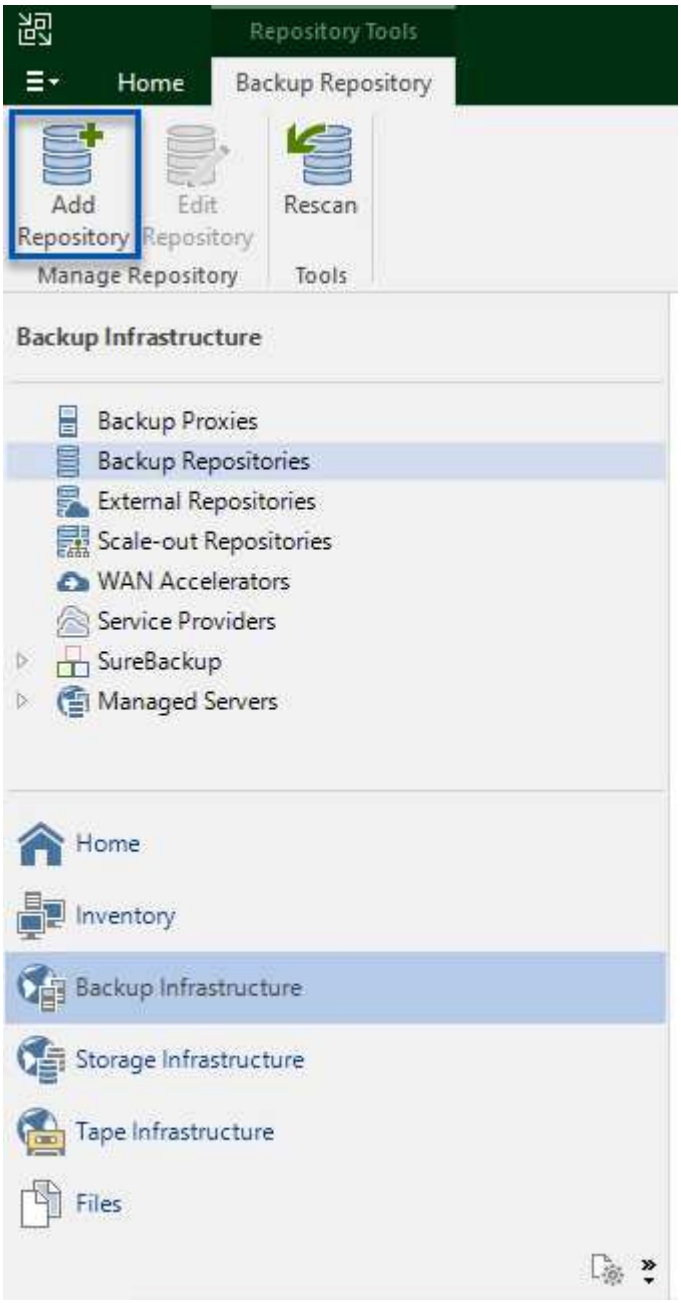


8. 이 단계를 반복하여 Veeam 프록시 서버에 iSCSI 볼륨을 마운트합니다.

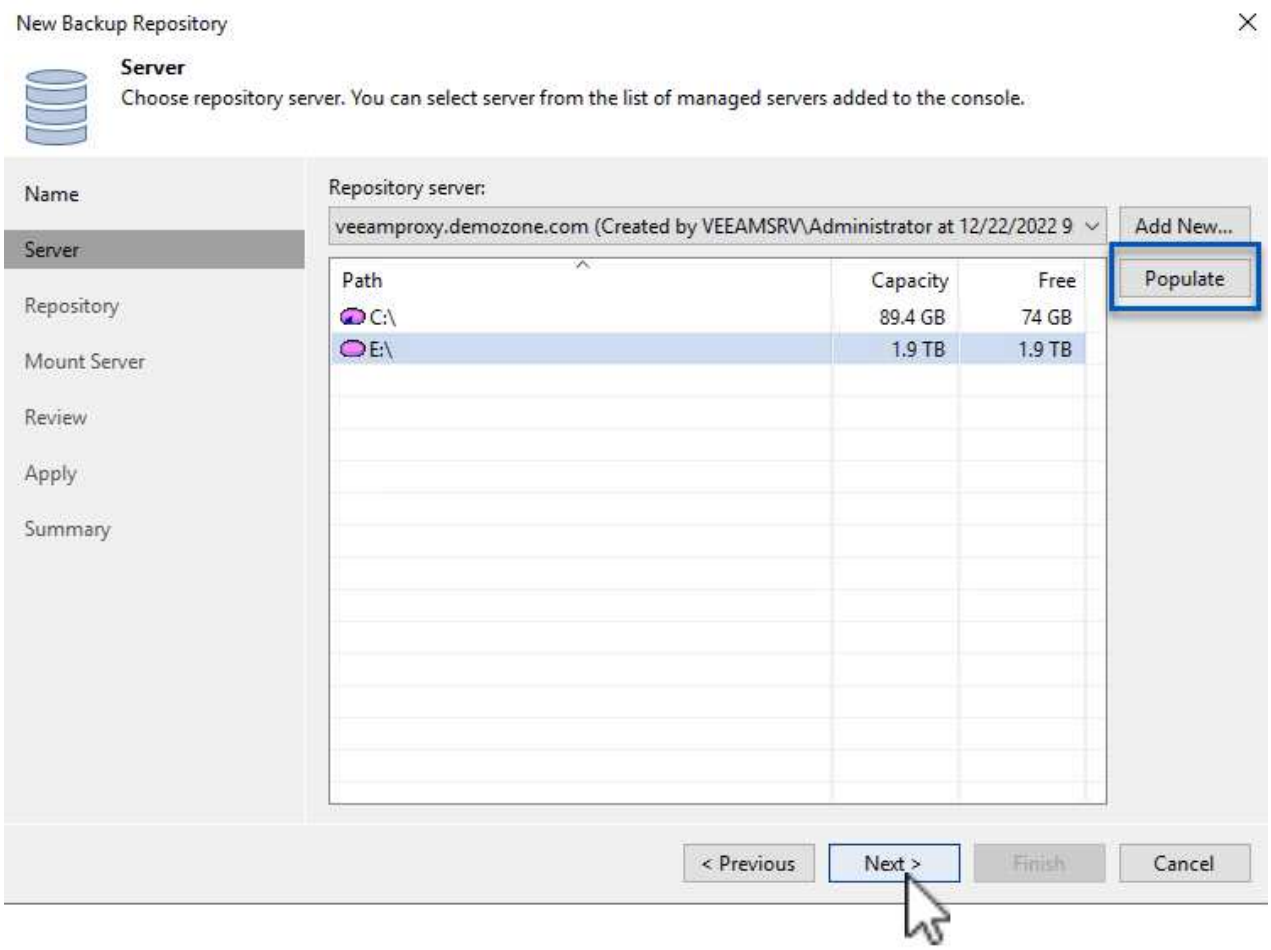
Veeam 백업 리포지토리를 생성합니다

Veeam Backup and Replication 콘솔에서 Veeam Backup 및 Veeam Proxy 서버의 백업 저장소를 생성합니다. 이러한 저장소는 가상 머신 백업의 백업 타겟으로 사용됩니다.

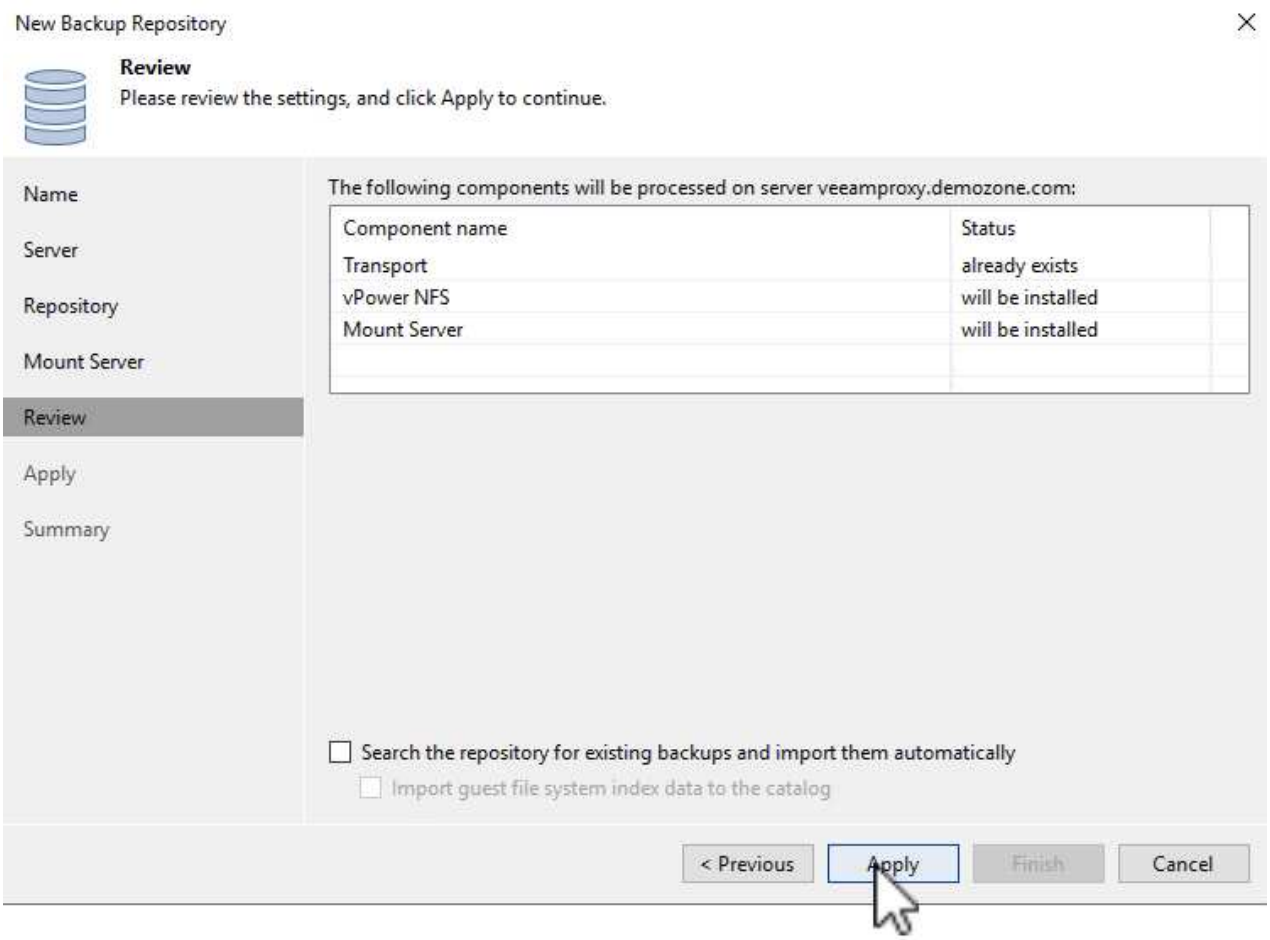
1. Veeam Backup and Replication 콘솔의 왼쪽 아래에서 * Backup Infrastructure * 를 클릭한 다음 * Add Repository * 를 선택합니다



2. New Backup Repository(새 백업 리포지토리) 마법사에서 리포지토리 이름을 입력한 다음 드롭다운 목록에서 서버를 선택하고 * 채우기 * 버튼을 클릭하여 사용할 NTFS 볼륨을 선택합니다.



3. 다음 페이지에서 고급 복구를 수행할 때 백업을 마운트하는 데 사용할 마운트 서버를 선택합니다. 기본적으로 이 서버는 저장소 저장소가 연결된 동일한 서버입니다.
4. 선택 항목을 검토하고 * Apply * 를 클릭하여 백업 리포지토리 생성을 시작합니다.



5. 추가 프록시 서버에 대해 이 단계를 반복합니다.

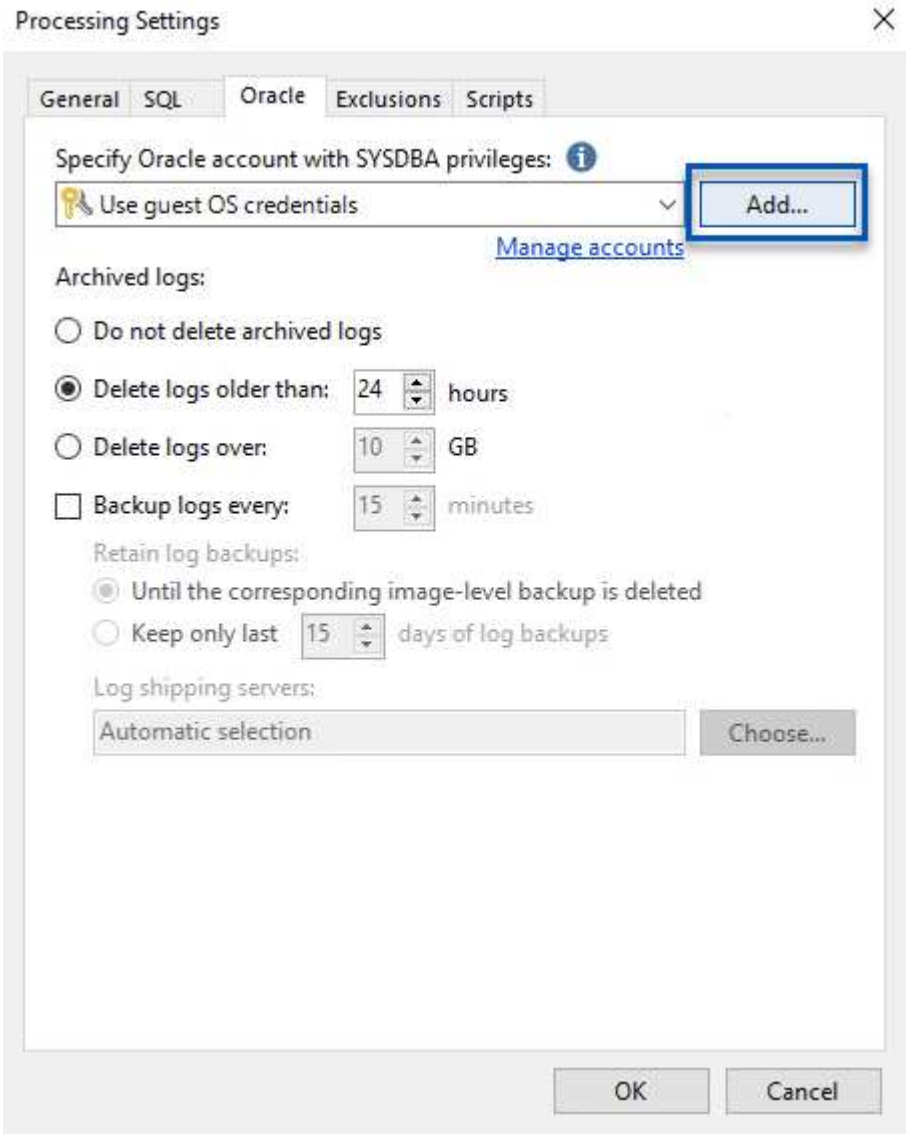
Veeam 백업 작업을 구성합니다

이전 섹션의 백업 리포지토리를 사용하여 백업 작업을 생성해야 합니다. 백업 작업 생성은 스토리지 관리자의 일반적인 일부이며 여기서는 모든 단계를 다루지 않습니다. Veeam에서 백업 작업 생성에 대한 자세한 내용은 를 참조하십시오 "Veeam Help Center 기술 문서".

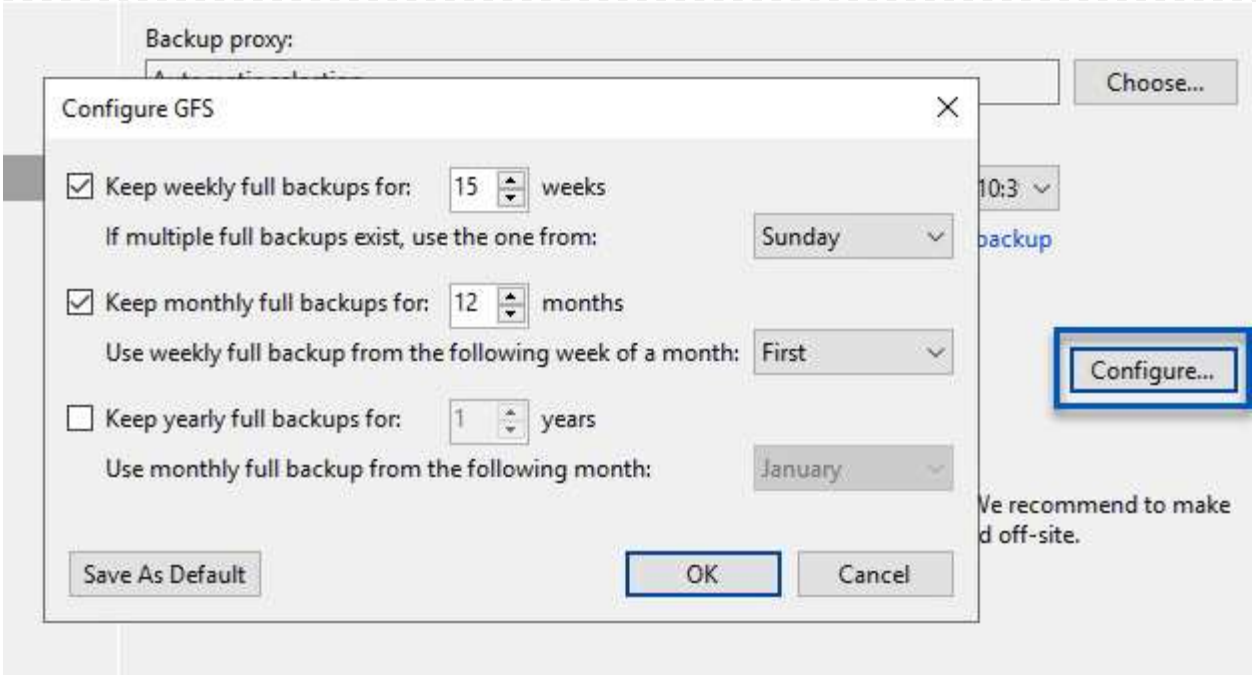
이 솔루션에서는 다음에 대해 별도의 백업 작업이 생성되었습니다.

- Microsoft Windows SQL Server를 참조하십시오
- Oracle 데이터베이스 서버
- Windows 파일 서버
- Linux 파일 서버

1. 애플리케이션 인식 처리를 통해 일관된 백업을 생성하고 트랜잭션 로그 처리를 수행할 수 있습니다.
2. 애플리케이션 인식 처리를 활성화한 후 게스트 OS 자격 증명과 다를 수 있으므로 애플리케이션에 관리자 권한이 있는 올바른 자격 증명을 추가합니다.



3. 백업의 보존 정책을 관리하려면 * 보관용으로 특정 전체 백업을 더 오래 보존 * 을 선택하고 * 구성… * 버튼을 클릭하여 정책을 구성합니다.



Veeam 전체 복원으로 애플리케이션 **VM**을 복원합니다

Veeam을 사용하여 전체 복원을 수행하는 것은 애플리케이션 복원을 수행하는 첫 번째 단계입니다. VM의 전체 복원 전원이 켜져 있고 모든 서비스가 정상적으로 실행 중임을 확인했습니다.

서버 복원은 스토리지 관리자의 정상적인 일부이며 여기서는 모든 단계를 다루지 않습니다. Veeam에서 전체 복원을 수행하는 방법에 대한 자세한 내용은 를 참조하십시오 "Veeam Help Center 기술 문서".

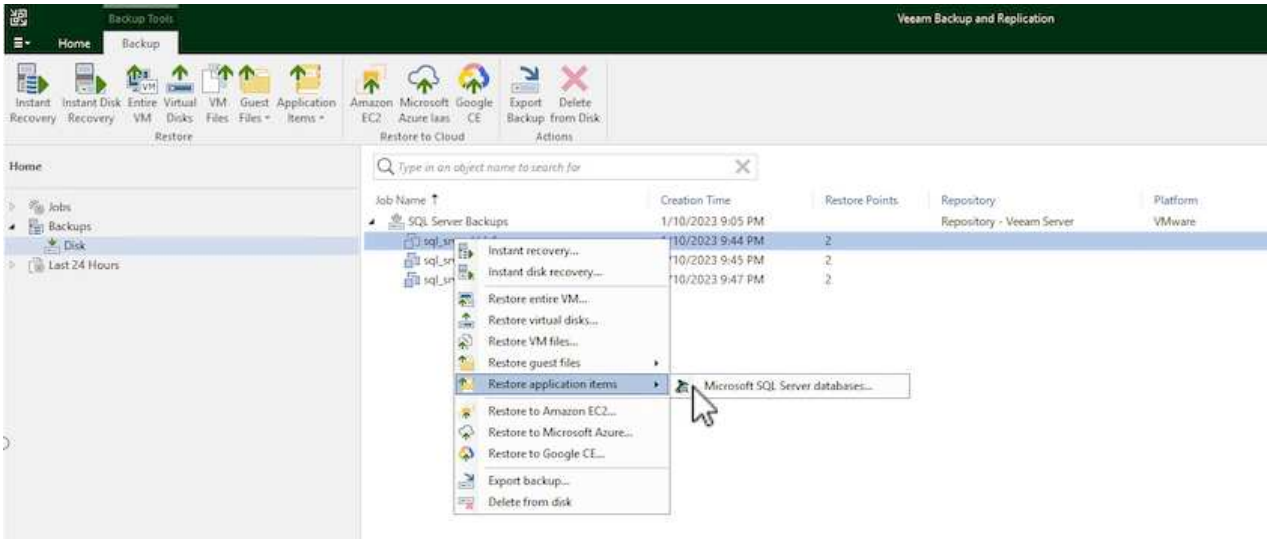
SQL Server 데이터베이스를 복구합니다

Veeam Backup & Replication은 SQL Server 데이터베이스를 복구하는 데 필요한 몇 가지 옵션을 제공합니다. 이 검증을 위해 Veeam Explorer for SQL Server with Instant Recovery를 사용하여 SQL Server 데이터베이스의 복원을 수행했습니다. SQL Server 인스턴트 복구는 전체 데이터베이스 복원을 기다리지 않고 SQL Server 데이터베이스를 신속하게 복원할 수 있는 기능입니다. 이러한 신속한 복구 프로세스는 다운타임을 최소화하고 비즈니스 연속성을 보장합니다. 작동 방식은 다음과 같습니다.

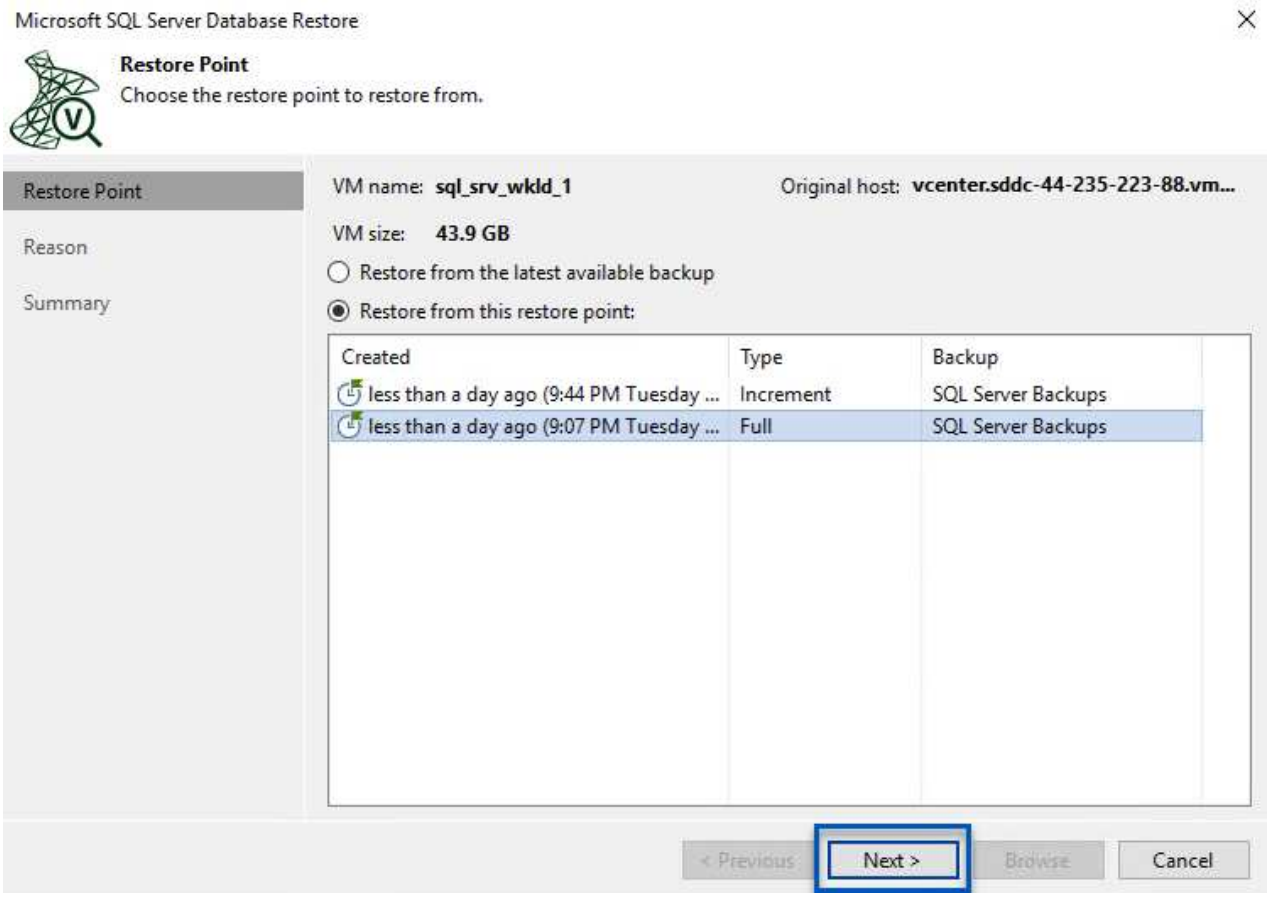
- Veeam Explorer * 는 복구할 SQL Server 데이터베이스가 포함된 백업 * 을 마운트합니다.
- 소프트웨어 * 는 마운트된 파일에서 직접 데이터베이스 * 를 게시하여 대상 SQL Server 인스턴스의 임시 데이터베이스로 액세스할 수 있도록 합니다.
- 임시 데이터베이스를 사용하는 동안 Veeam Explorer * 가 사용자 쿼리 * 를 이 데이터베이스로 리디렉션하여 사용자가 데이터에 계속 액세스하고 사용할 수 있도록 합니다.
- 배경에서 Veeam * 은 전체 데이터베이스 복원 * 을 수행하여 임시 데이터베이스에서 원래 데이터베이스 위치로 데이터를 전송합니다.
- 전체 데이터베이스 복원이 완료되면 Veeam Explorer * 가 사용자 쿼리를 원래 * 데이터베이스로 다시 전환하고 임시 데이터베이스를 제거합니다.

Veeam Explorer 인스턴트 복구를 사용하여 **SQL Server** 데이터베이스를 복원합니다

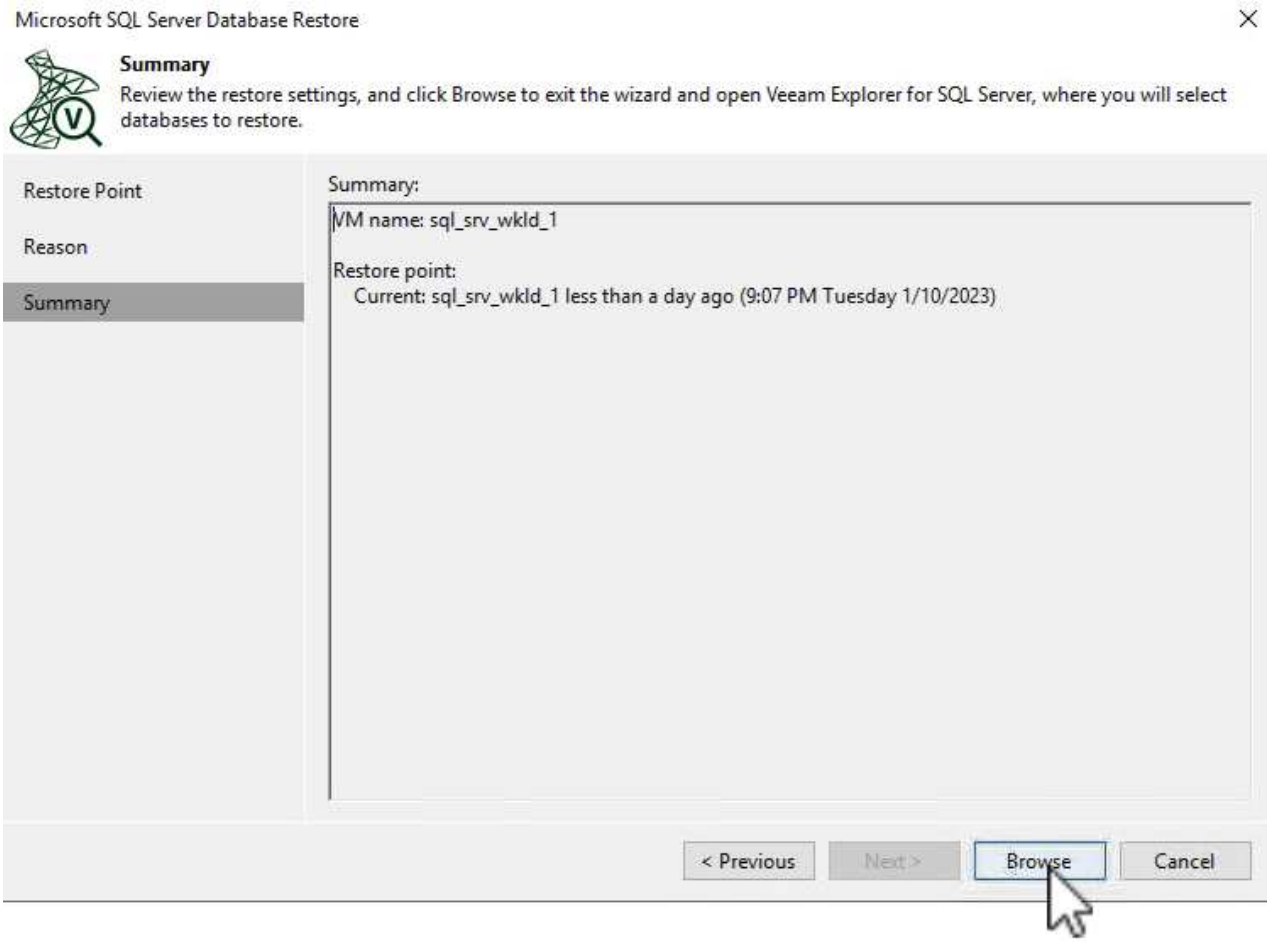
1. Veeam Backup and Replication 콘솔에서 SQL Server 백업 목록으로 이동하여 서버를 마우스 오른쪽 버튼으로 클릭하고 * Restore application items * 를 선택한 다음 * Microsoft SQL Server database… * 를 선택합니다.



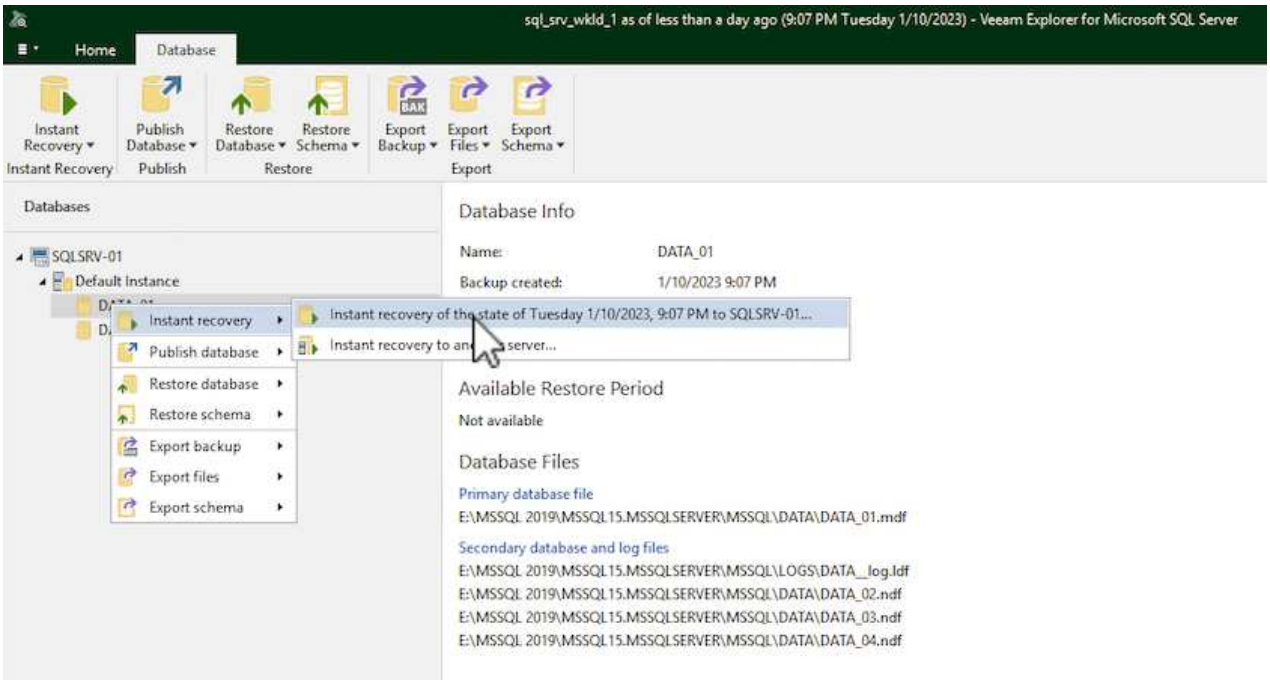
2. Microsoft SQL Server 데이터베이스 복원 마법사의 목록에서 복원 지점을 선택하고 * 다음 * 을 클릭합니다.



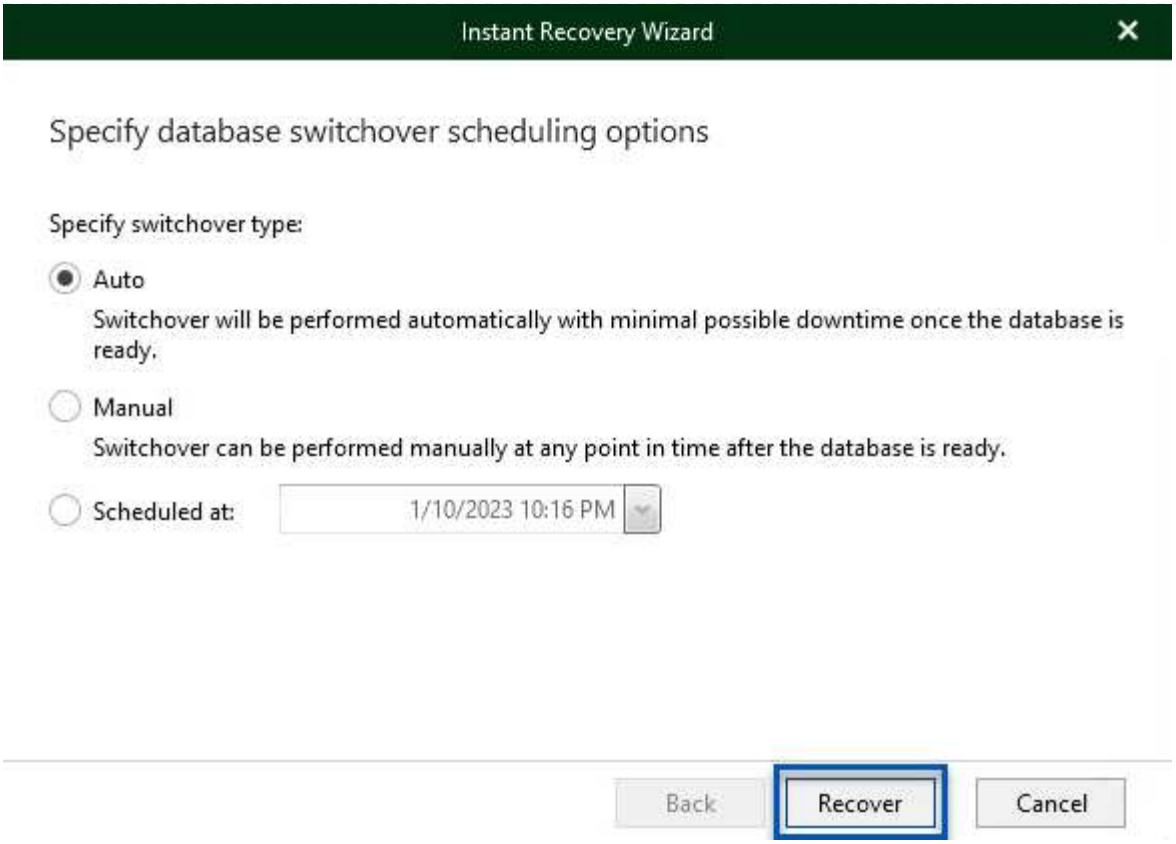
3. 원하는 경우 * Restore Reason * 을 입력한 다음 Summary 페이지에서 * Browse * 버튼을 클릭하여 Veeam Explorer for Microsoft SQL Server를 시작합니다.



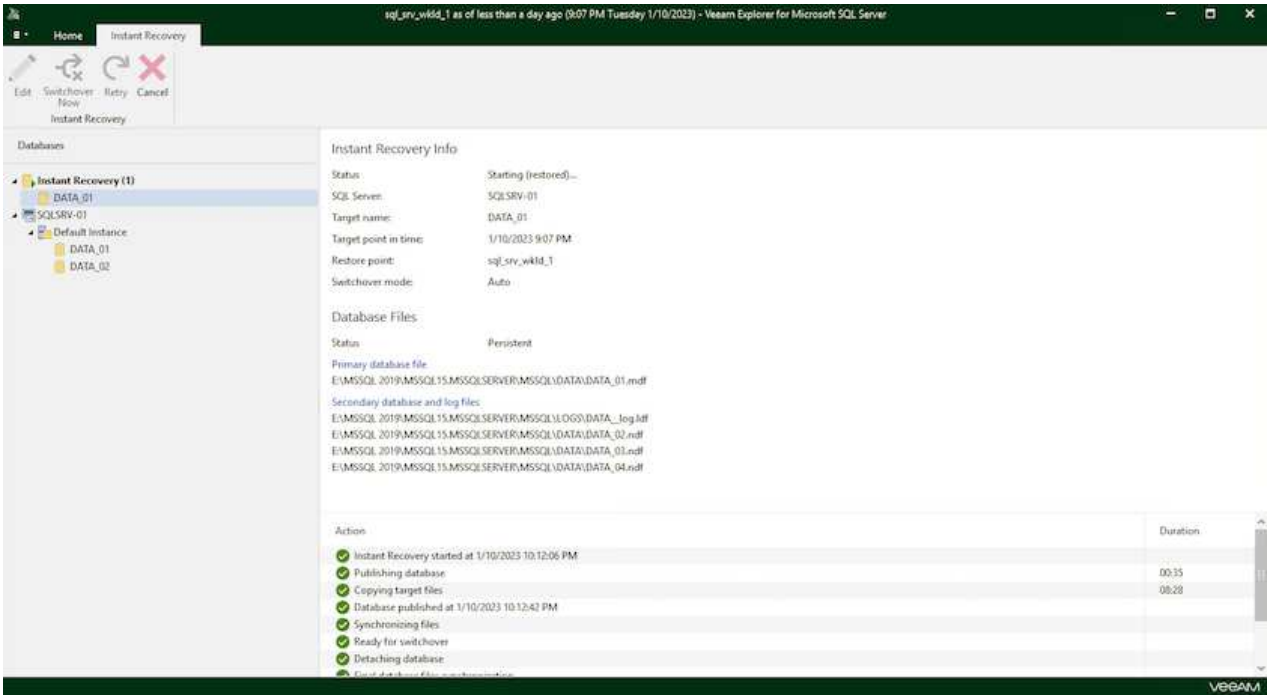
4. Veeam Explorer에서 데이터베이스 인스턴스 목록을 확장하고 * Instant recovery * 를 마우스 오른쪽 버튼으로 클릭한 다음 복구할 특정 복원 지점을 선택합니다.



5. 인스턴트 복구 마법사에서 전환 유형을 지정합니다. 이 작업은 최소한의 가동 중지 시간, 수동 또는 지정된 시간에 자동으로 수행할 수 있습니다. 그런 다음 * 복구 * 버튼을 클릭하여 복원 프로세스를 시작합니다.



6. 복구 프로세스는 Veeam Explorer에서 모니터링할 수 있습니다.



Veeam Explorer로 SQL Server 복원 작업을 수행하는 방법에 대한 자세한 내용은 의 Microsoft SQL Server 섹션을 참조하십시오 "Veeam Explorers 사용자 가이드".

Veeam Explorer로 **Oracle** 데이터베이스를 복구합니다

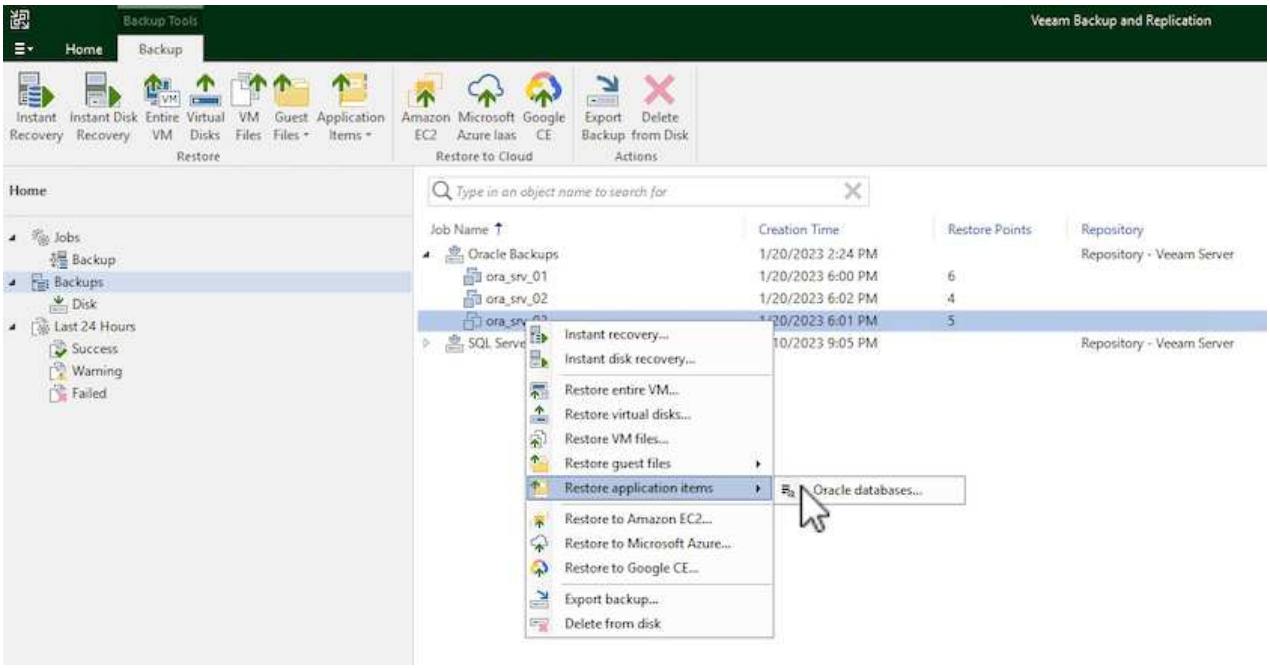
Oracle 데이터베이스용 Veeam Explorer를 사용하면 표준 Oracle 데이터베이스 복원 또는 즉각적인 복구를 통해 무중단 복원을 수행할 수 있습니다. 또한 빠른 액세스, Data Guard 데이터베이스 복구 및 RMAN 백업으로부터의 복구를 위해 데이터베이스를 게시하는 기능도 지원합니다.

Veeam Explorer로 Oracle 데이터베이스 복원 작업을 수행하는 방법에 대한 자세한 내용은 의 Oracle 섹션을 참조하십시오 "Veeam Explorers 사용자 가이드".

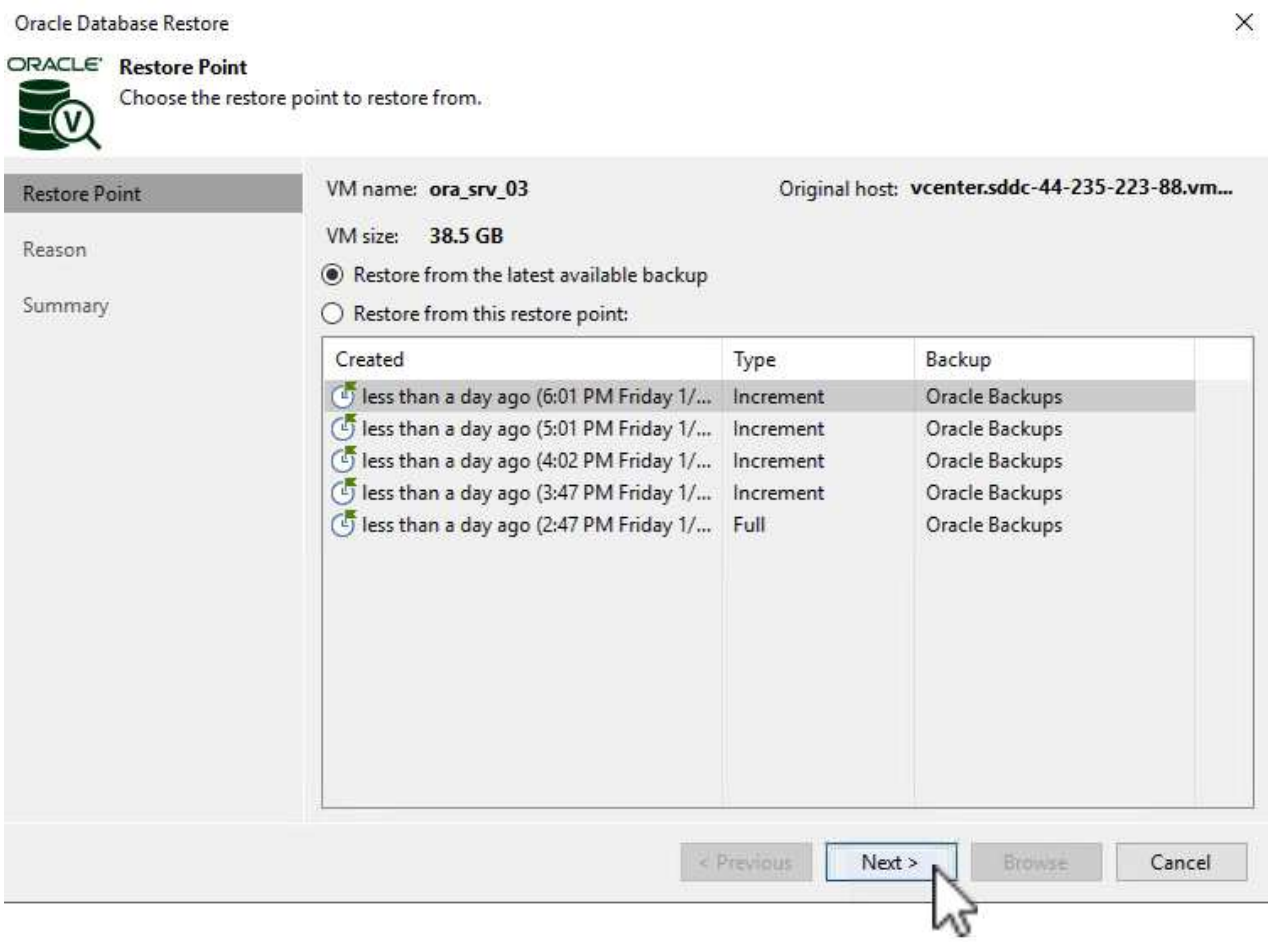
Veeam Explorer로 Oracle 데이터베이스를 복원합니다

이 섹션에서는 Veeam Explorer를 사용하여 다른 서버로 Oracle 데이터베이스를 복구하는 방법에 대해 설명합니다.

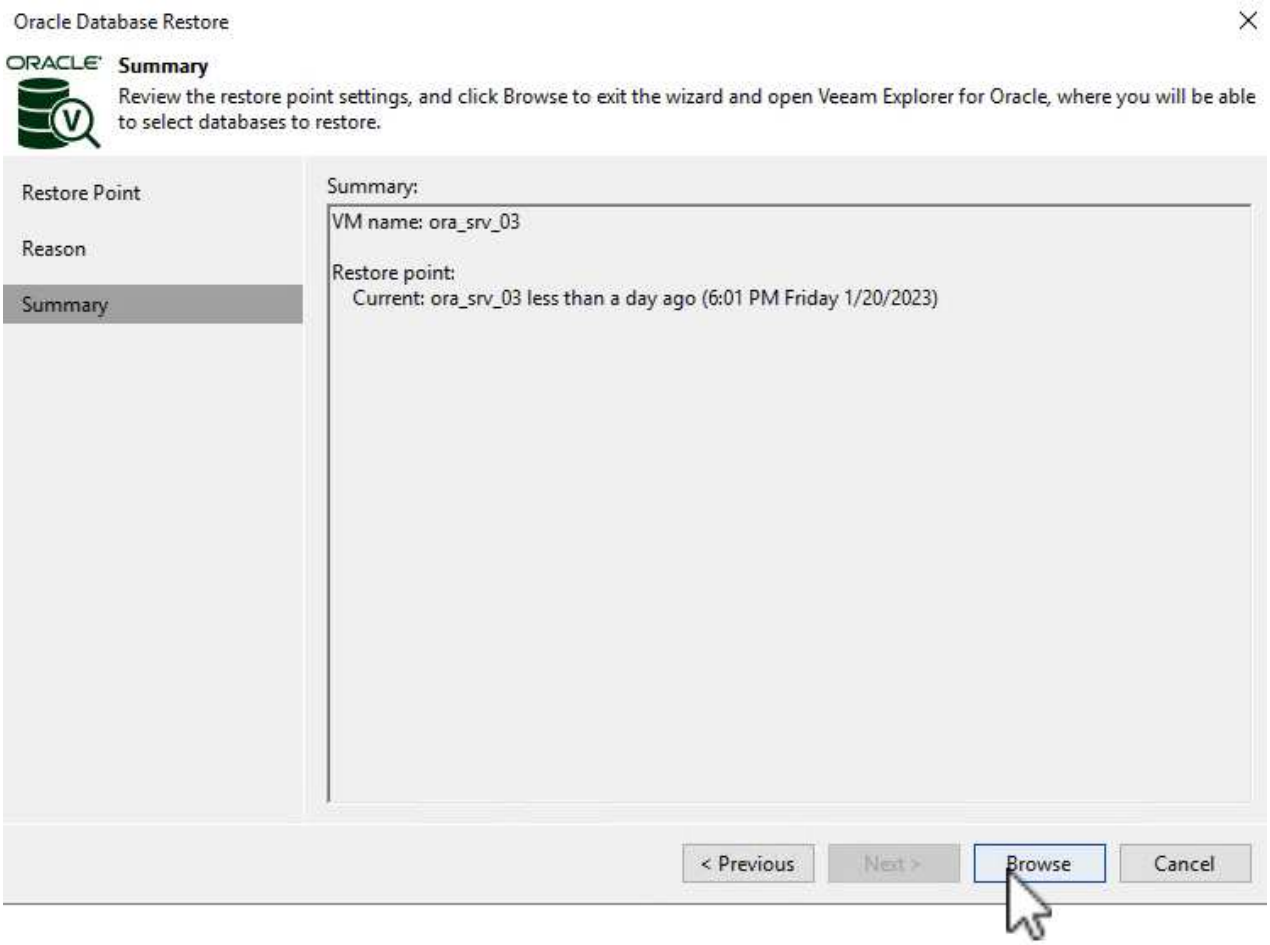
1. Veeam Backup and Replication 콘솔에서 Oracle 백업 목록으로 이동하여 서버를 마우스 오른쪽 버튼으로 클릭하고 * Restore application items * 를 선택한 다음 * oracle databases… * 를 선택합니다.



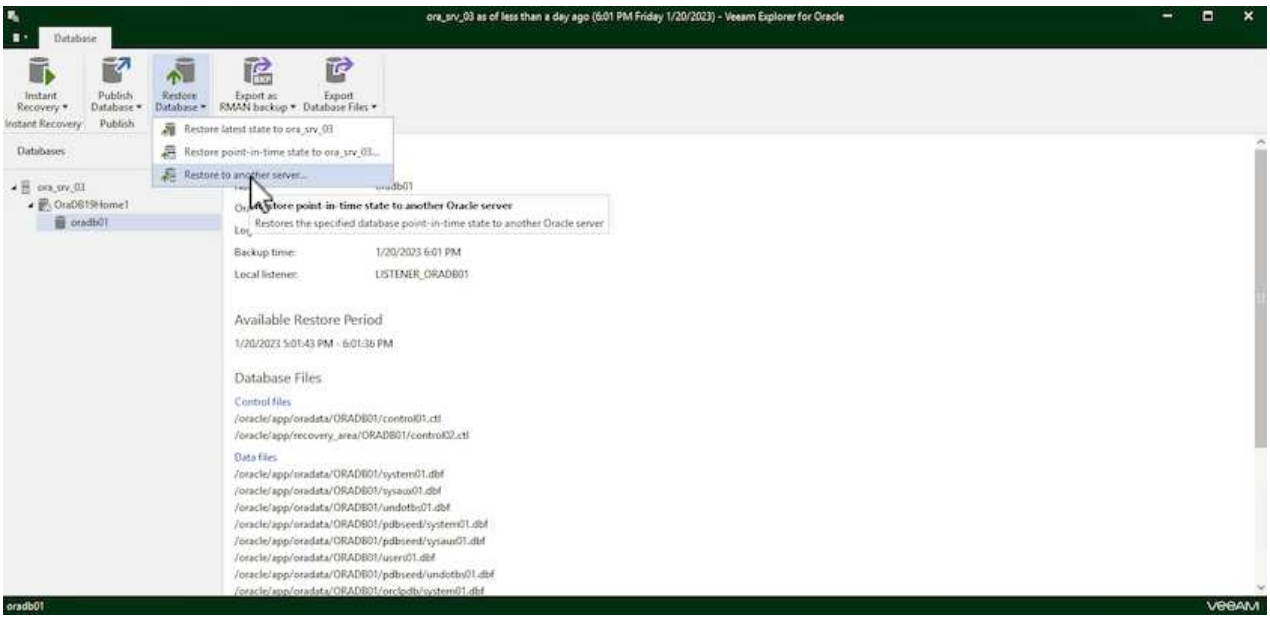
2. Oracle Database Restore Wizard의 목록에서 복원 지점을 선택하고 * Next * 를 클릭합니다.



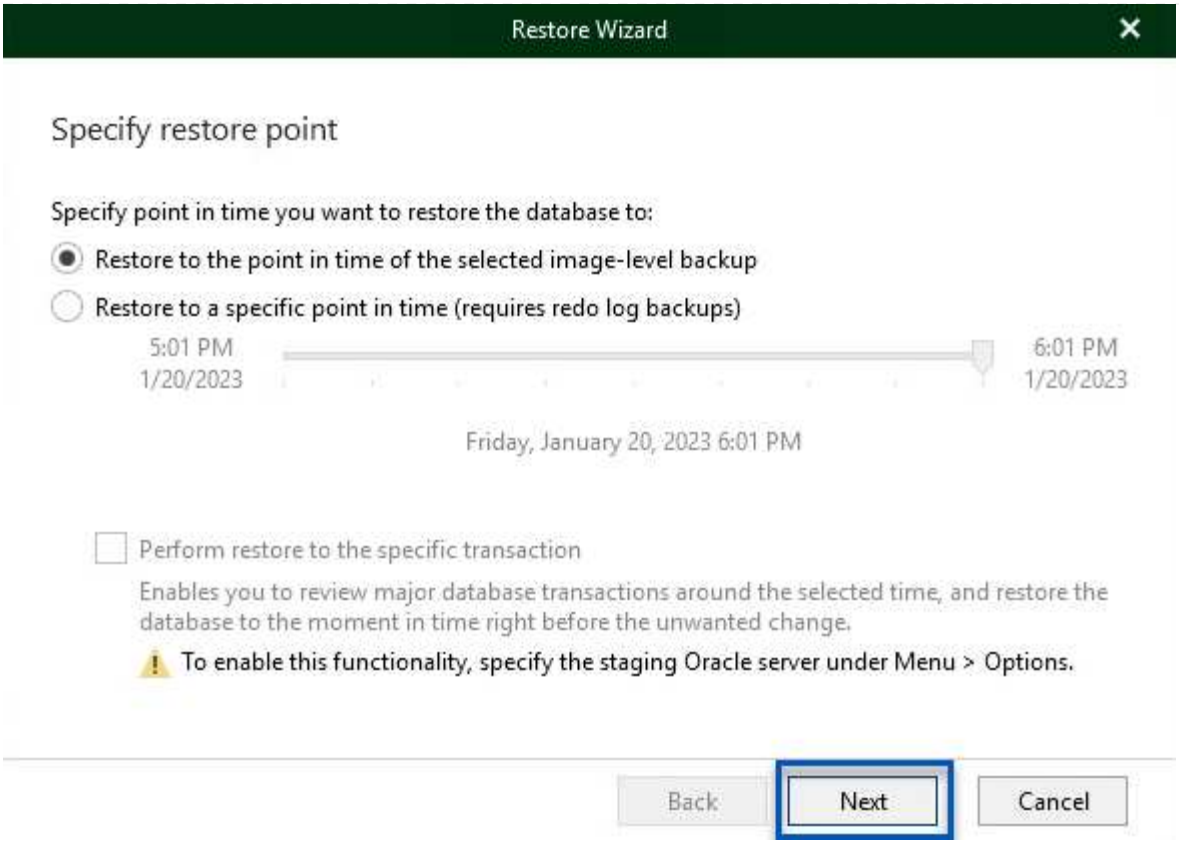
3. 원하는 경우 * Restore Reason * 을 입력한 다음 Summary 페이지에서 * Browse * 버튼을 클릭하여 Veeam Explorer for Oracle을 시작합니다.



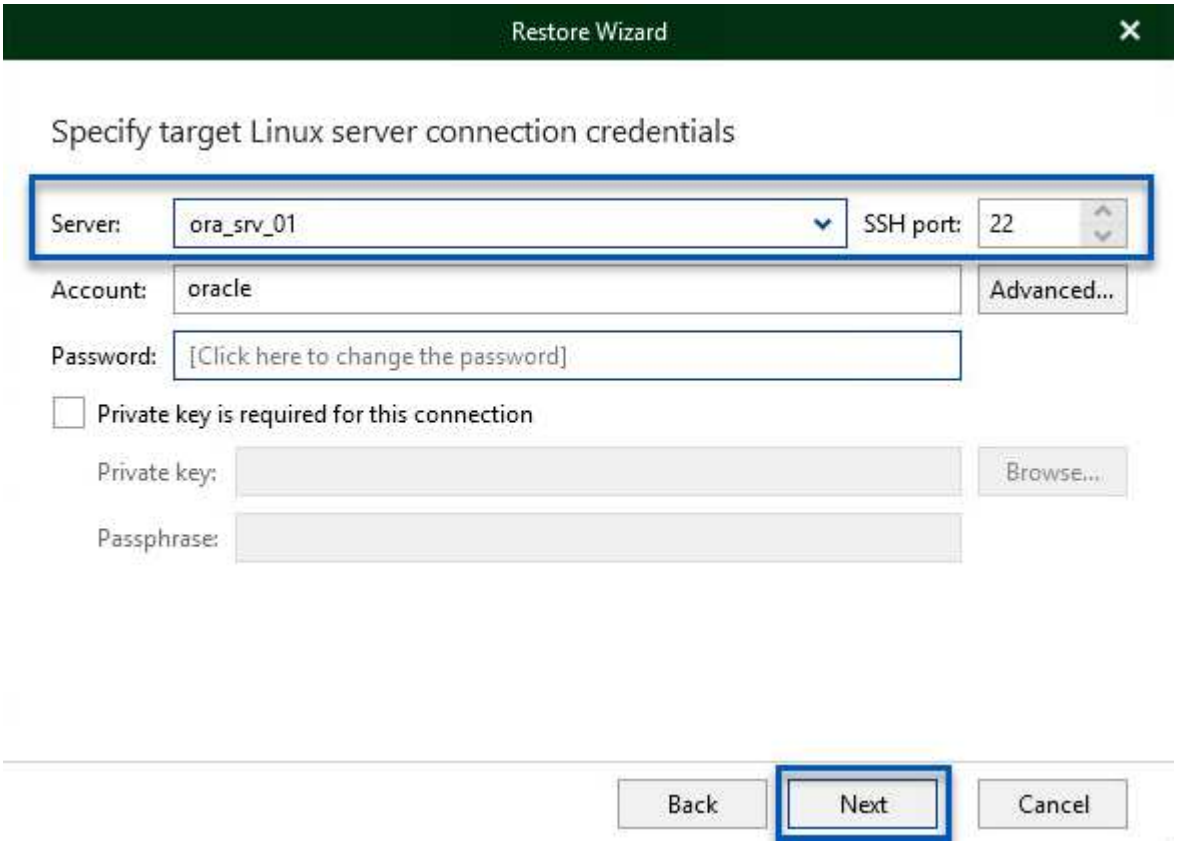
4. Veeam Explorer에서 데이터베이스 인스턴스 목록을 확장하고 복원할 데이터베이스를 클릭한 다음 상단의 * Restore Database * 드롭다운 메뉴에서 * Restore to another server… * 를 선택합니다.



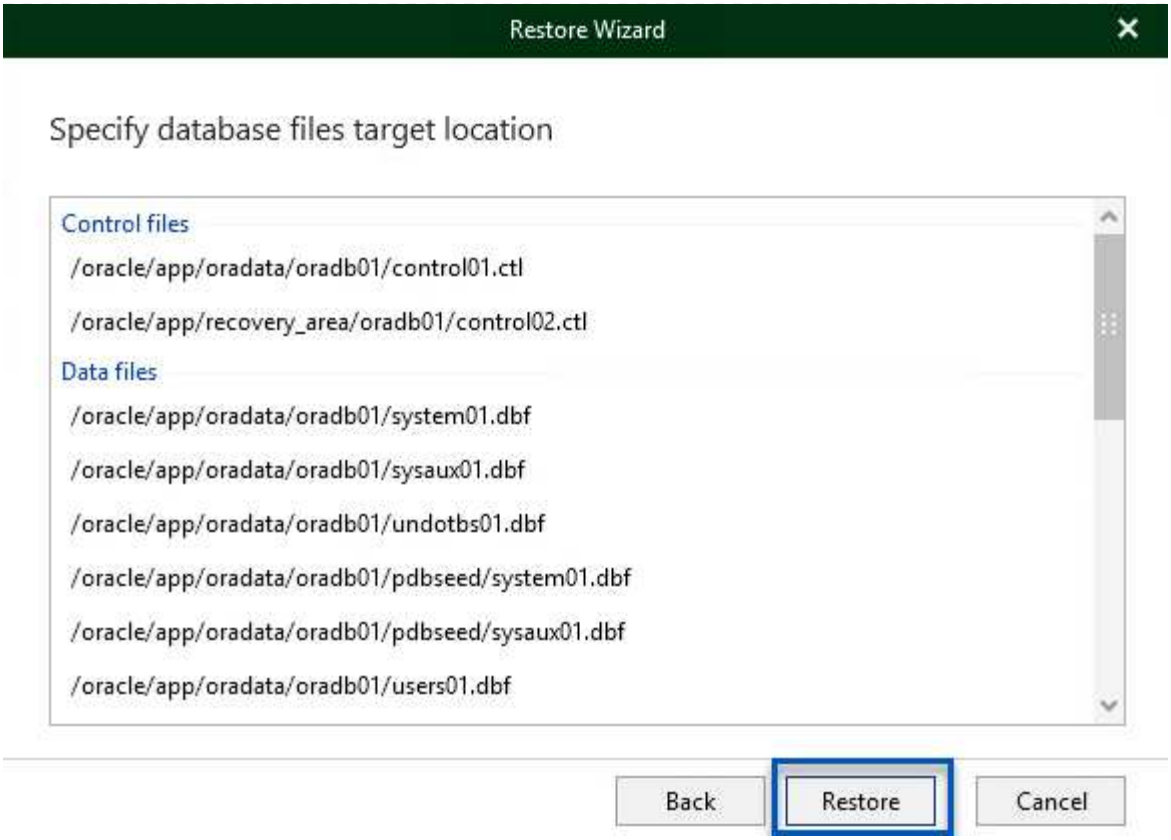
5. 복원 마법사에서 복원할 복원 지점을 지정하고 * 다음 * 을 클릭합니다.



6. 데이터베이스를 복원할 대상 서버와 계정 자격 증명을 지정하고 * 다음 * 을 클릭합니다.



7. 마지막으로 데이터베이스 파일 대상 위치를 지정하고 * 복원 * 버튼을 클릭하여 복원 프로세스를 시작합니다.

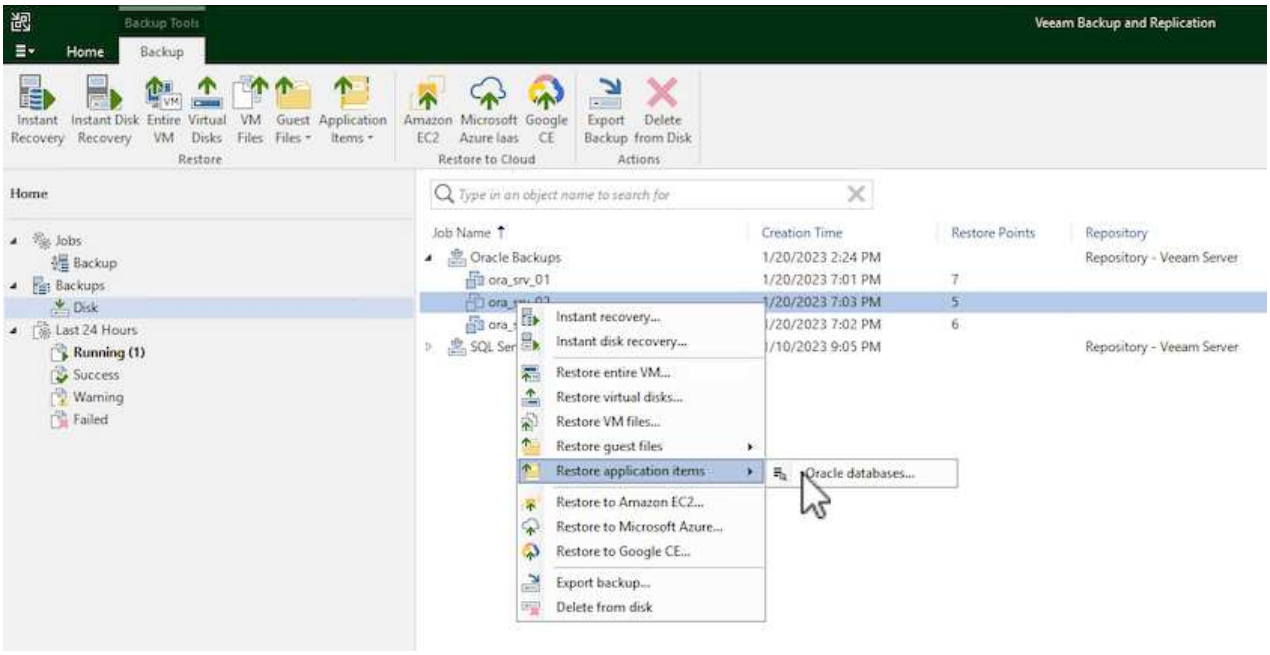


8. 데이터베이스 복구가 완료되면 서버에서 Oracle 데이터베이스가 올바르게 시작되는지 확인합니다.

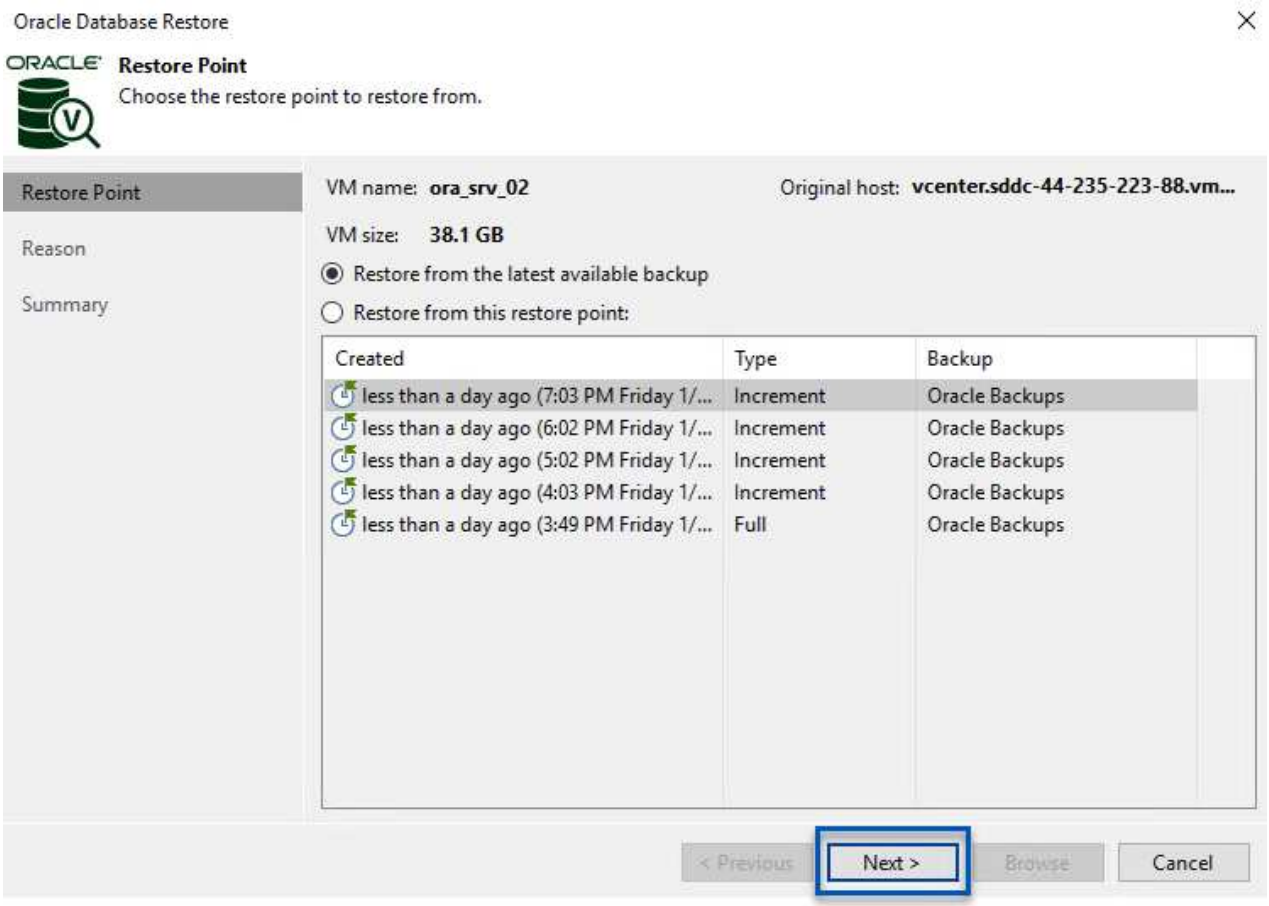
Oracle 데이터베이스를 대체 서버에 게시합니다

이 섹션에서는 전체 복원을 시작하지 않고 빠르게 액세스할 수 있도록 데이터베이스를 대체 서버에 게시합니다.

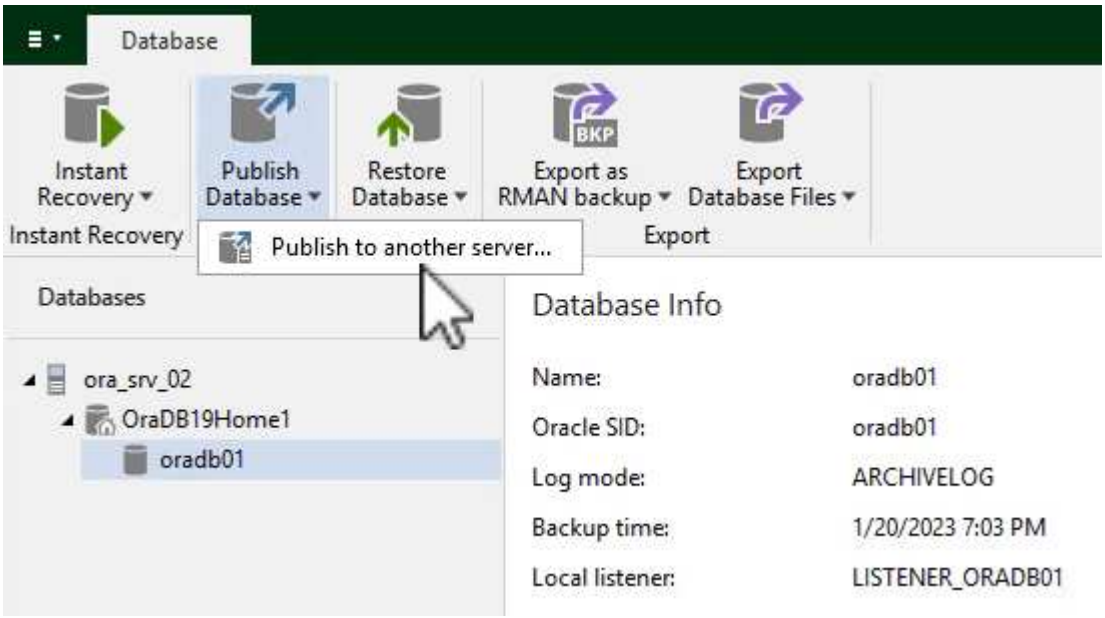
1. Veeam Backup and Replication 콘솔에서 Oracle 백업 목록으로 이동하여 서버를 마우스 오른쪽 버튼으로 클릭하고 * Restore application items * 를 선택한 다음 * oracle databases… * 를 선택합니다.



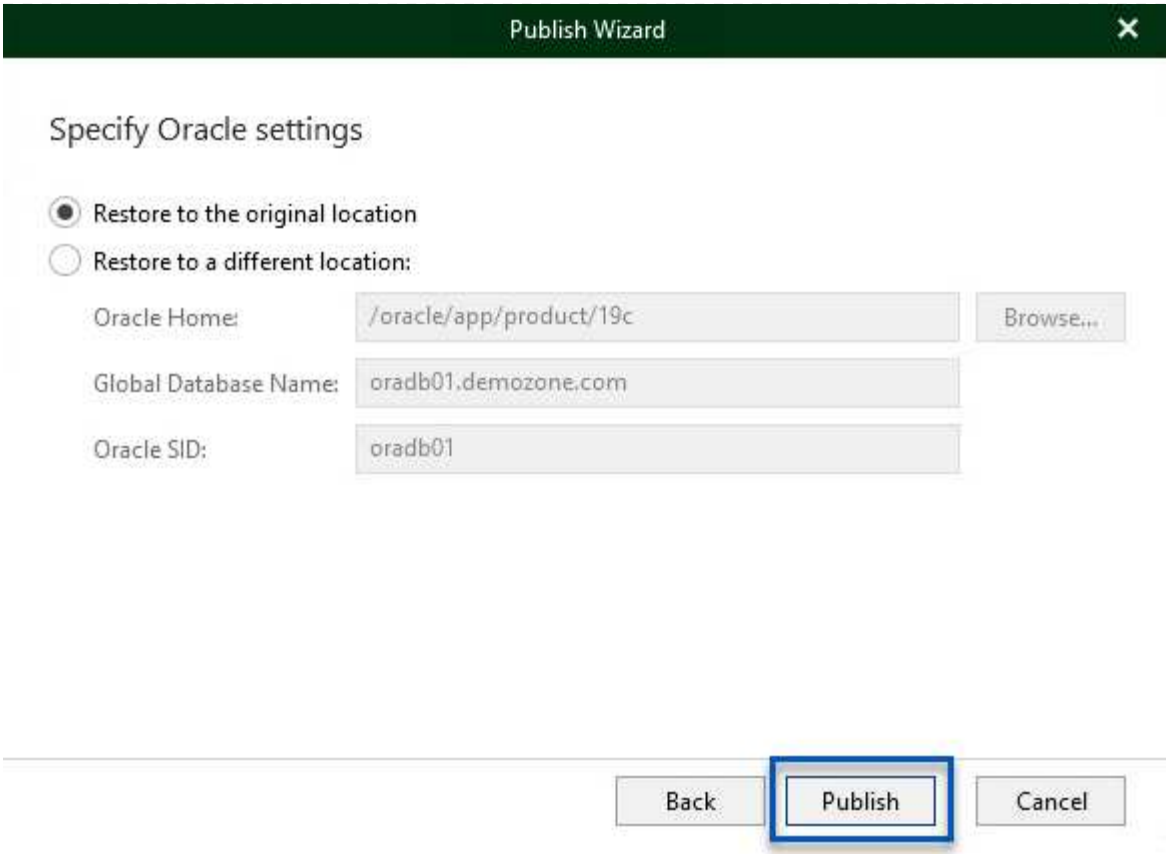
2. Oracle Database Restore Wizard의 목록에서 복원 지점을 선택하고 * Next * 를 클릭합니다.



3. 원하는 경우 * Restore Reason * 을 입력한 다음 Summary 페이지에서 * Browse * 버튼을 클릭하여 Veeam Explorer for Oracle을 시작합니다.
4. Veeam Explorer에서 데이터베이스 인스턴스 목록을 확장하고 복원할 데이터베이스를 클릭한 다음 상단의 * Publish Database * 드롭다운 메뉴에서 * Publish to another server… * 를 선택합니다.



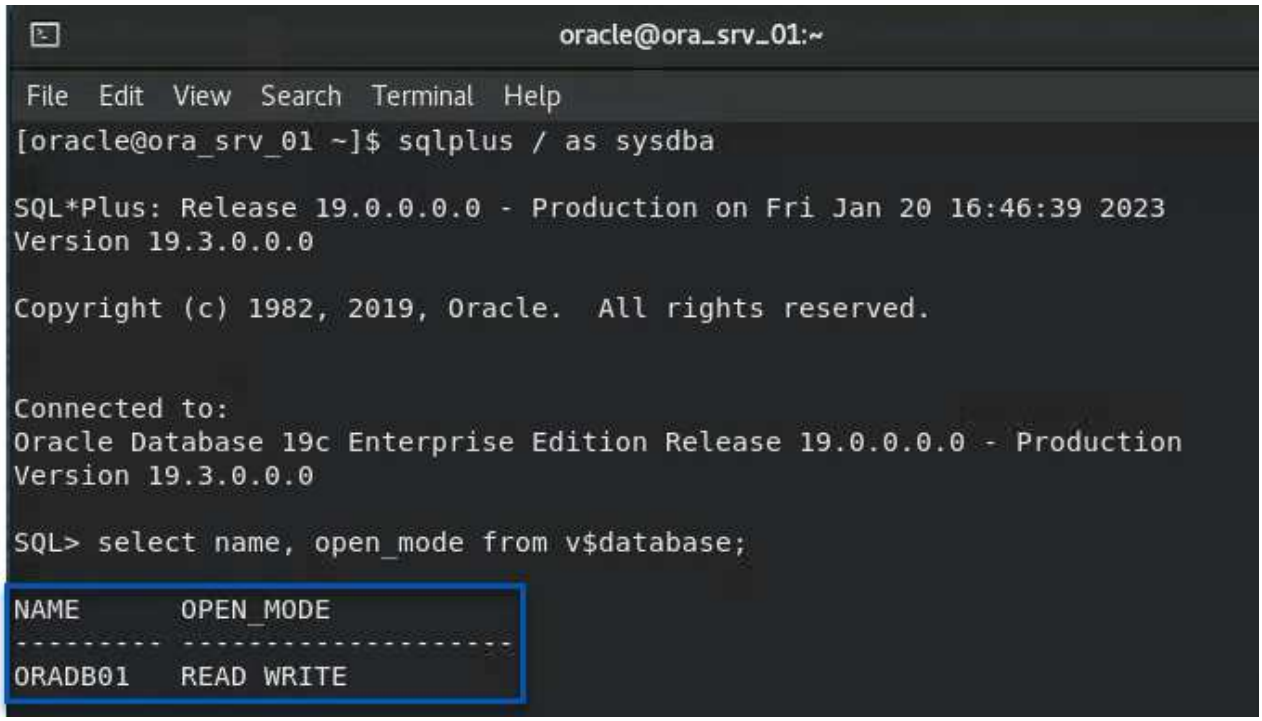
5. 게시 마법사에서 데이터베이스를 게시할 복원 지점을 지정하고 * 다음 * 을 클릭합니다.
6. 마지막으로 대상 Linux 파일 시스템 위치를 지정하고 * 게시 * 를 클릭하여 복원 프로세스를 시작합니다.



7. 게시가 완료되면 대상 서버에 로그인하고 다음 명령을 실행하여 데이터베이스가 실행 중인지 확인합니다.

```
oracle@ora_srv_01> sqlplus / as sysdba
```

```
SQL> select name, open_mode from v$database;
```



결론

VMware Cloud는 비즈니스 크리티컬 애플리케이션을 실행하고 중요한 데이터를 저장할 수 있는 강력한 플랫폼입니다. 비즈니스 연속성을 보장하고 사이버 위협 및 데이터 손실을 방지하기 위해 VMware Cloud를 사용하는 기업에게 보안 데이터 보호 솔루션은 필수적입니다. 안정적이고 강력한 데이터 보호 솔루션을 선택함으로써 기업은 중요한 데이터가 무엇에 관계없이 안전하고 안전하다는 확신을 가질 수 있습니다.

이 문서에 제공된 사용 사례는 NetApp, VMware, Veeam의 통합을 강조하는 검증된 데이터 보호 기술에 중점을 둡니다. ONTAP용 FSX는 AWS에서 VMware Cloud를 위한 보조 NFS 데이터 저장소로 지원되며 모든 가상 머신 및 애플리케이션 데이터에 사용됩니다. Veeam Backup & Replication은 기업이 백업 및 복구 프로세스를 개선, 자동화 및 간소화할 수 있도록 설계된 포괄적인 데이터 보호 솔루션입니다. Veeam을 ONTAP용 FSx에서 호스팅되는 iSCSI 백업 타겟 볼륨과 함께 사용하면 VMware Cloud에 상주하는 애플리케이션 데이터를 안전하고 쉽게 관리할 수 있는 데이터 보호 솔루션을 제공할 수 있습니다.

추가 정보

이 솔루션에 제공되는 기술에 대한 자세한 내용은 다음 추가 정보를 참조하십시오.

- "ONTAP용 FSX 사용 설명서"
- "Veeam Help Center 기술 문서"
- "AWS의 VMware Cloud 지원: 고려 사항 및 제한 사항"

TR-4955: ONTAP 및 **VMC(AWS VMware Cloud)**용 **FSx**를 통한 재해 복구

Niyaz Mohamed, NetApp

개요

클라우드로 재해 복구는 사이트 운영 중단 및 데이터 손상 이벤트(예: 랜섬웨어)로부터 워크로드를 보호하는 복원력이

있고 비용 효율적인 방법입니다. NetApp SnapMirror 기술을 사용하면 사내 VMware 워크로드를 AWS에서 실행되는 ONTAP의 FSx에 복제할 수 있습니다.

DRO(재해 복구 오케스트레이터, UI를 포함한 스크립팅된 솔루션)를 사용하여 사내에서 ONTAP용 FSx로 복제된 워크로드를 원활하게 복구할 수 있습니다. DRO는 VM 등록을 통해 SnapMirror 레벨에서 VMC로 복구를 자동화하고 NSX-T에서 직접 네트워크 매핑을 수행합니다 이 기능은 모든 VMC 환경에 포함되어 있습니다.

시작하기

AWS에서 **VMware Cloud**를 구축 및 구성합니다

"AWS 기반 VMware 클라우드" AWS 에코시스템의 VMware 기반 워크로드에 클라우드 네이티브 경험을 제공합니다. 각 VMware SDDC(소프트웨어 정의 데이터 센터)는 VPC(Amazon Virtual Private Cloud)에서 실행되며 전체 VMware 스택(vCenter Server 포함), NSX-T 소프트웨어 정의 네트워킹, vSAN 소프트웨어 정의 스토리지 및 워크로드에 컴퓨팅 및 스토리지 리소스를 제공하는 하나 이상의 ESXi 호스트를 제공합니다. AWS에서 VMC 환경을 구성하려면 다음 단계를 수행하십시오 "링크". DR 목적으로도 파일럿 라이트 클러스터를 사용할 수 있습니다.

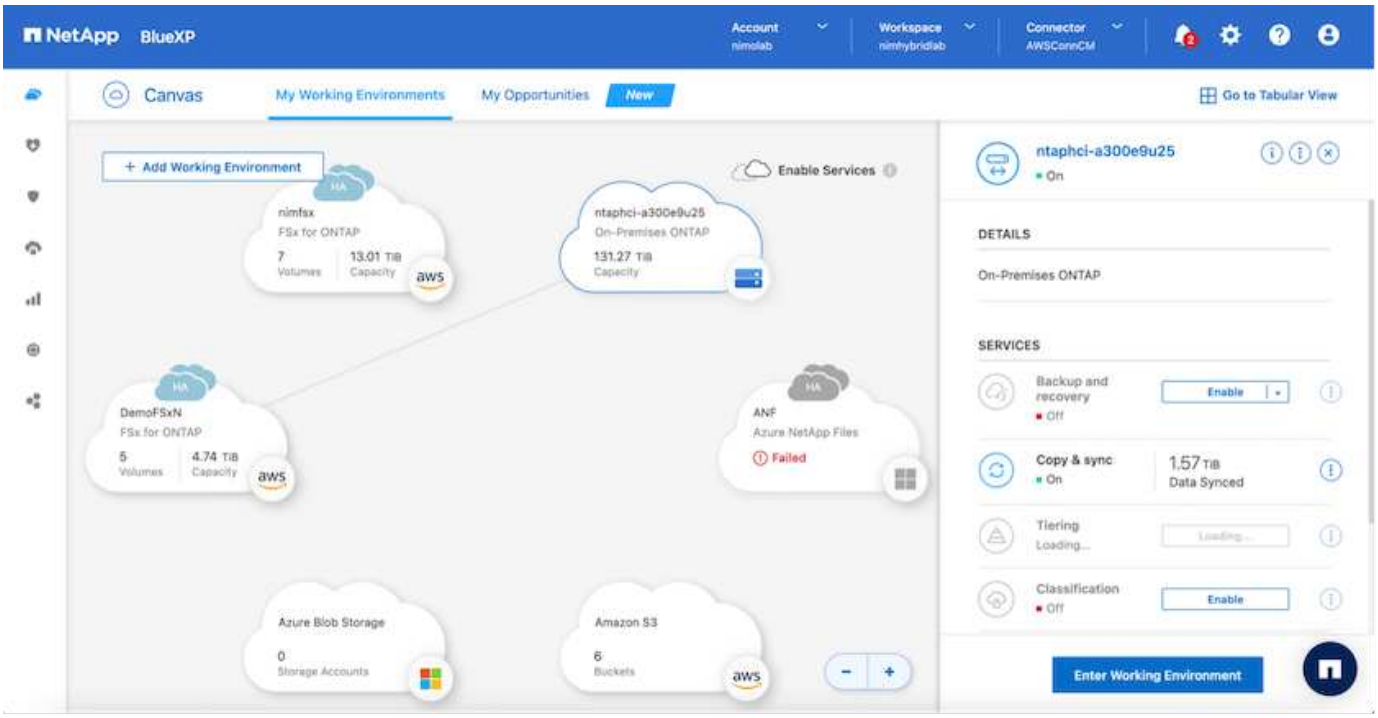
> 최초 릴리즈에서 DRO는 기존의 파일럿 라이트 클러스터를 지원합니다. 온디맨드 SDDC 작성은 향후 릴리스에서 제공될 예정입니다.

ONTAP용 **FSx**를 프로비저닝하고 구성합니다

NetApp ONTAP용 Amazon FSx는 널리 사용되는 NetApp ONTAP 파일 시스템에 구축된 매우 안정적이고 확장 가능하며 고성능의 풍부한 기능 파일 스토리지를 제공하는 완전 관리형 서비스입니다. 이 단계를 따릅니다 "링크" ONTAP용 FSx를 프로비저닝하고 구성하려면 다음을 수행합니다.

ONTAP용 **FSx**에 **SnapMirror**를 구축하고 구성합니다

다음 단계는 NetApp BlueXP를 사용하고 AWS에서 ONTAP용 프로비저닝된 FSx 인스턴스를 검색하고 적절한 빈도와 NetApp 스냅샷 복사본 보존을 사용하여 원하는 데이터 저장소 볼륨을 사내 환경에서 ONTAP용 FSx로 복제하는 것입니다.



이 링크의 단계에 따라 BlueXP를 구성합니다. NetApp ONTAP CLI를 사용하여 이 링크 이후의 복제를 예약할 수도 있습니다.

SnapMirror 관계는 전제 조건이며 미리 만들어야 합니다.

DRO 설치

DRO를 시작하려면 지정된 EC2 인스턴스 또는 가상 시스템에서 Ubuntu 운영 체제를 사용하여 필수 구성 요소를 충족하는지 확인합니다. 그런 다음 패키지를 설치합니다.

필수 구성 요소

- 소스 및 대상 vCenter 및 스토리지 시스템에 대한 접속이 있는지 확인합니다.
- DNS 이름을 사용하는 경우 DNS 확인이 필요합니다. 그렇지 않으면 vCenter 및 스토리지 시스템의 IP 주소를 사용해야 합니다.
- 루트 권한이 있는 사용자를 생성합니다. EC2 인스턴스에서 sudo를 사용할 수도 있습니다.

OS 요구 사항

- 최소 2GB 및 4개의 vCPU가 있는 Ubuntu 20.04(LTS
- 지정된 에이전트 VM에 다음 패키지를 설치해야 합니다.
  - Docker 를 참조하십시오
  - Docker-Compose
  - JQ

의 사용 권한을 변경합니다 `docker.sock`: `sudo chmod 666 /var/run/docker.sock`.

를 클릭합니다 `deploy.sh` 스크립트는 필요한 모든 필수 구성 요소를 실행합니다.

패키지를 설치합니다

1. 지정된 가상 머신에 설치 패키지를 다운로드합니다.

```
git clone https://github.com/NetApp/DRO-AWS.git
```

이 에이전트는 사내에 설치하거나 AWS VPC 내에 설치할 수 있습니다.

2. 패키지의 압축을 풀고 배포 스크립트를 실행한 다음 호스트 IP(예: 10.10.10)를 입력합니다.

```
tar xvf DRO-prereq.tar
```

3. 디렉토리로 이동하고 다음과 같이 배포 스크립트를 실행합니다.

```
sudo sh deploy.sh
```

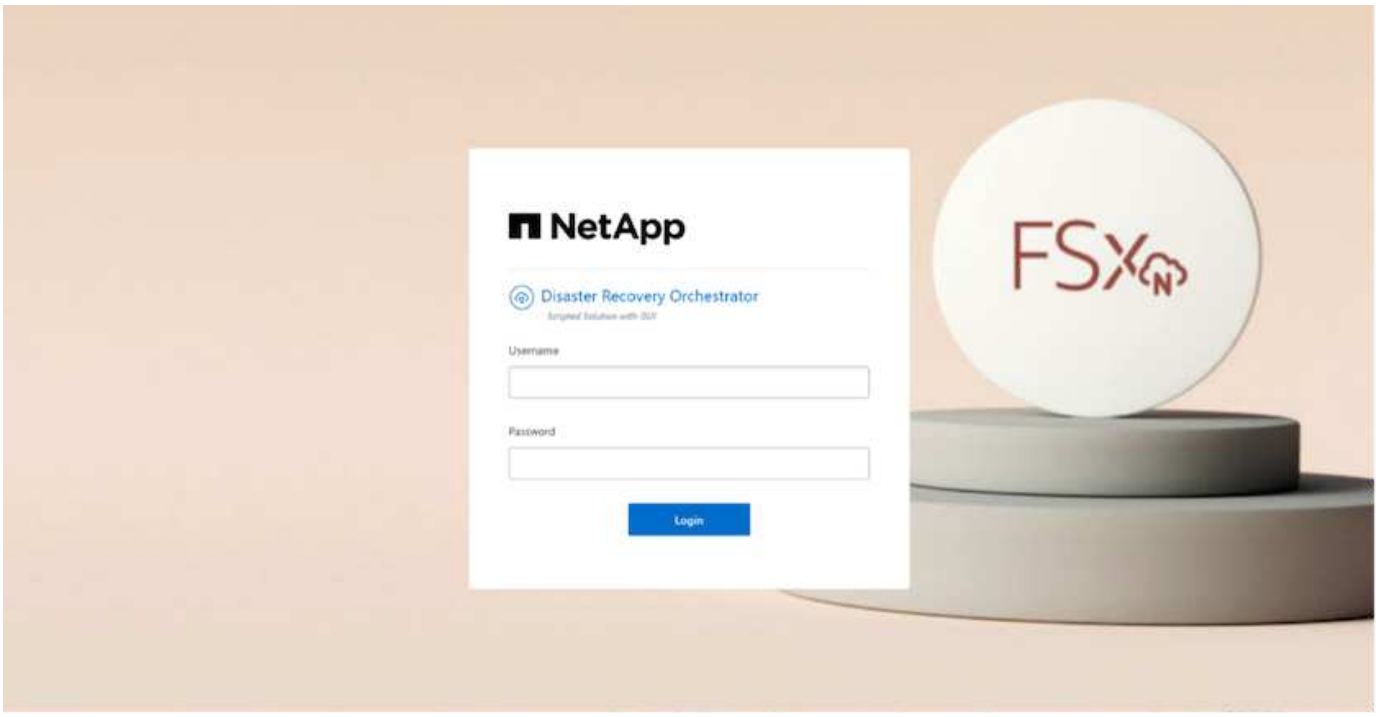
4. 다음을 사용하여 UI에 액세스합니다.

```
https://<host-ip-address>
```

다음 기본 자격 증명을 사용합니다.

```
Username: admin
Password: admin
```

암호는 "암호 변경" 옵션을 사용하여 변경할 수 있습니다.



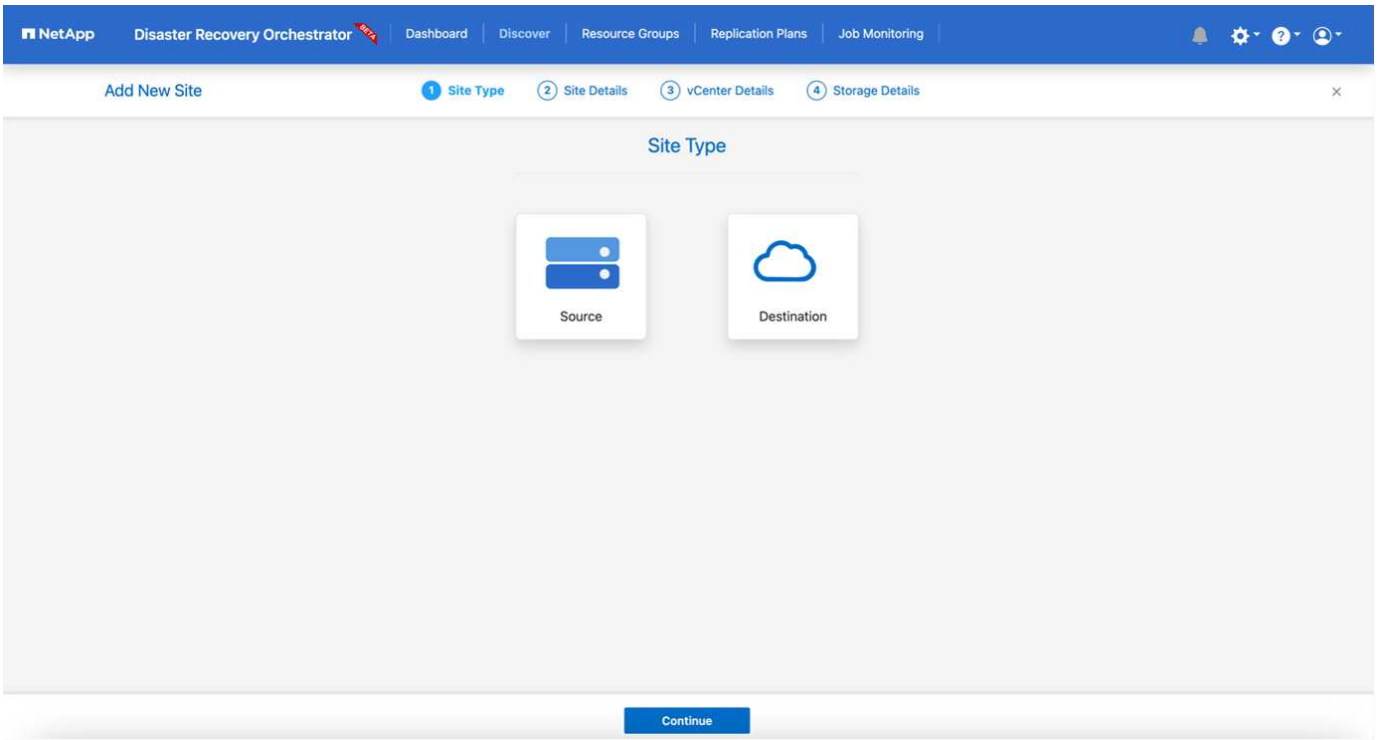
DRO 구성

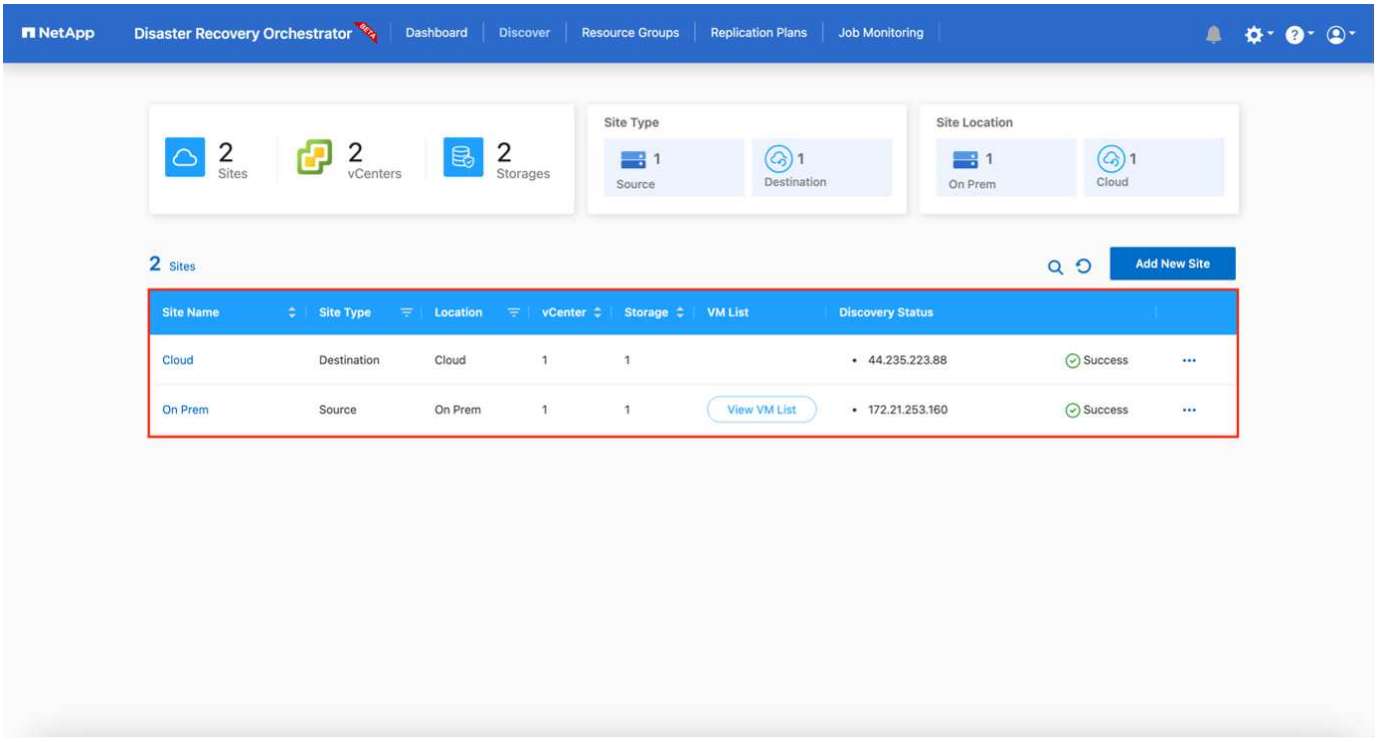
ONTAP 및 VMC용 FSx가 올바르게 구성된 후에는 ONTAP용 FSx에서 읽기 전용 SnapMirror 복사본을 사용하여 VMC로 온-프레미스 워크로드의 복구를 자동화하도록 DRO를 구성할 수 있습니다.

ONTAP용 FSx가 구축된 AWS 및 동일한 VPC에 DRO 에이전트를 구축하는 것이 좋습니다(피어 연결도 가능). DRO 에이전트가 네트워크를 통해 온-프레미스 구성 요소와 ONTAP 및 VMC용 FSx 리소스와 통신할 수 있도록 합니다.

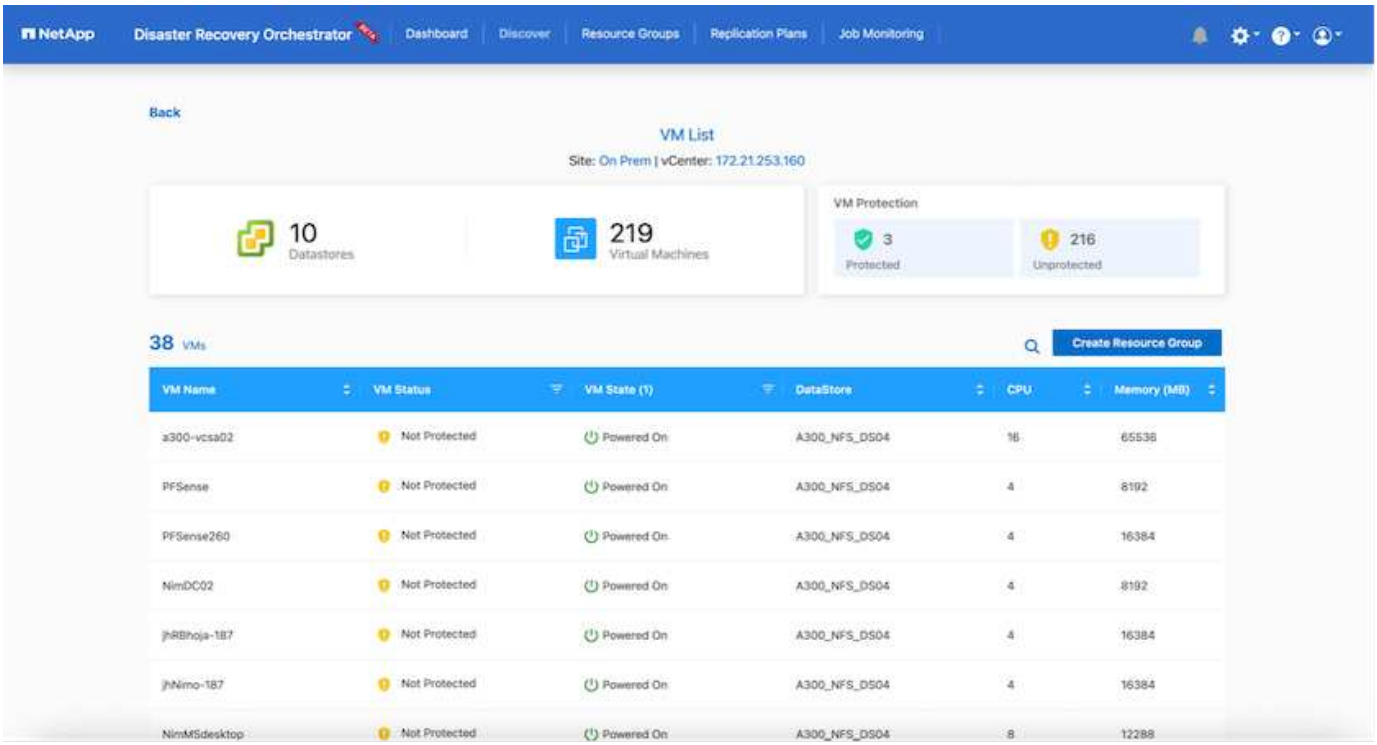
첫 번째 단계는 온프레미스 및 클라우드 리소스(vCenter 및 스토리지 모두)를 DRO에 검색하고 추가하는 것입니다. 지원되는 브라우저에서 DRO를 열고 기본 사용자 이름 및 암호(admin/admin)와 사이트 추가를 사용합니다. 검색 옵션을 사용하여 사이트를 추가할 수도 있습니다. 다음 플랫폼을 추가합니다.

- 온프레미스
  - 사내 vCenter
  - ONTAP 스토리지 시스템
- 클라우드
  - VMC vCenter
  - ONTAP용 FSX





추가된 DRO는 자동 검색을 수행하고 소스 스토리지에서 ONTAP용 FSx로 해당 SnapMirror 복제본이 있는 VM을 표시합니다. DRO는 VM에서 사용하는 네트워크 및 포트 그룹을 자동으로 감지하여 채웁니다.



다음 단계는 필요한 VM을 기능 그룹으로 그룹화하여 리소스 그룹 역할을 하는 것입니다.

리소스 그룹화

플랫폼을 추가한 후 복구할 VM을 리소스 그룹으로 그룹화할 수 있습니다. DRO 리소스 그룹을 사용하면 종속 VM 집합을 부팅 순서, 부팅 지연 및 복구 시 실행할 수 있는 선택적 응용 프로그램 유효성 검사가 포함된 논리 그룹으로 그룹화할 수 있습니다.

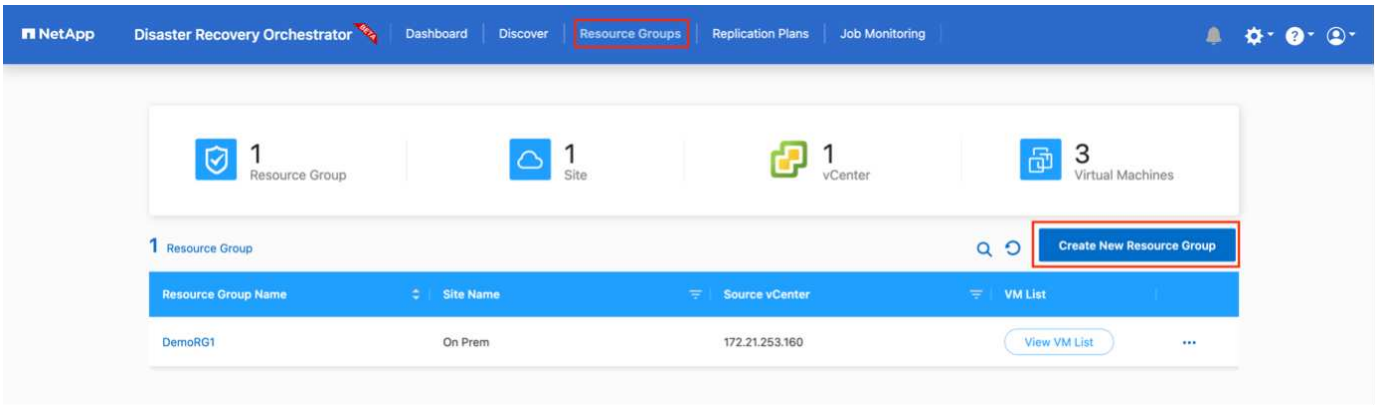
리소스 그룹 생성을 시작하려면 다음 단계를 수행하십시오.

1. 리소스 그룹 * 에 액세스하여 * 새 리소스 그룹 생성 * 을 클릭합니다.
2. 새 리소스 그룹 * 의 드롭다운에서 소스 사이트를 선택하고 * 만들기 * 를 클릭합니다.
3. 리소스 그룹 세부 정보 * 를 입력하고 * 계속 * 을 클릭합니다.
4. 검색 옵션을 사용하여 적절한 VM을 선택합니다.
5. 선택한 VM의 부팅 순서 및 부팅 지연(초)을 선택합니다. 각 VM을 선택하고 우선 순위를 설정하여 전원 켜기 순서의 순서를 설정합니다. 모든 VM의 기본값은 3입니다.

   옵션은 다음과 같습니다.

   1 – 전원을 켤 첫 번째 가상 머신 3 – 기본값 5 – 전원을 켤 마지막 가상 머신

6. 리소스 그룹 만들기 * 를 클릭합니다.

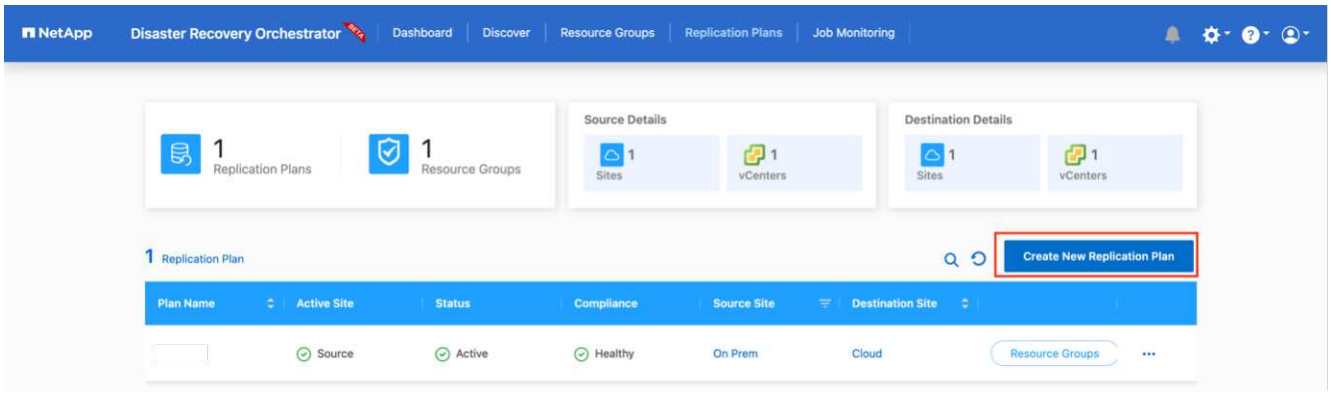


복제 계획

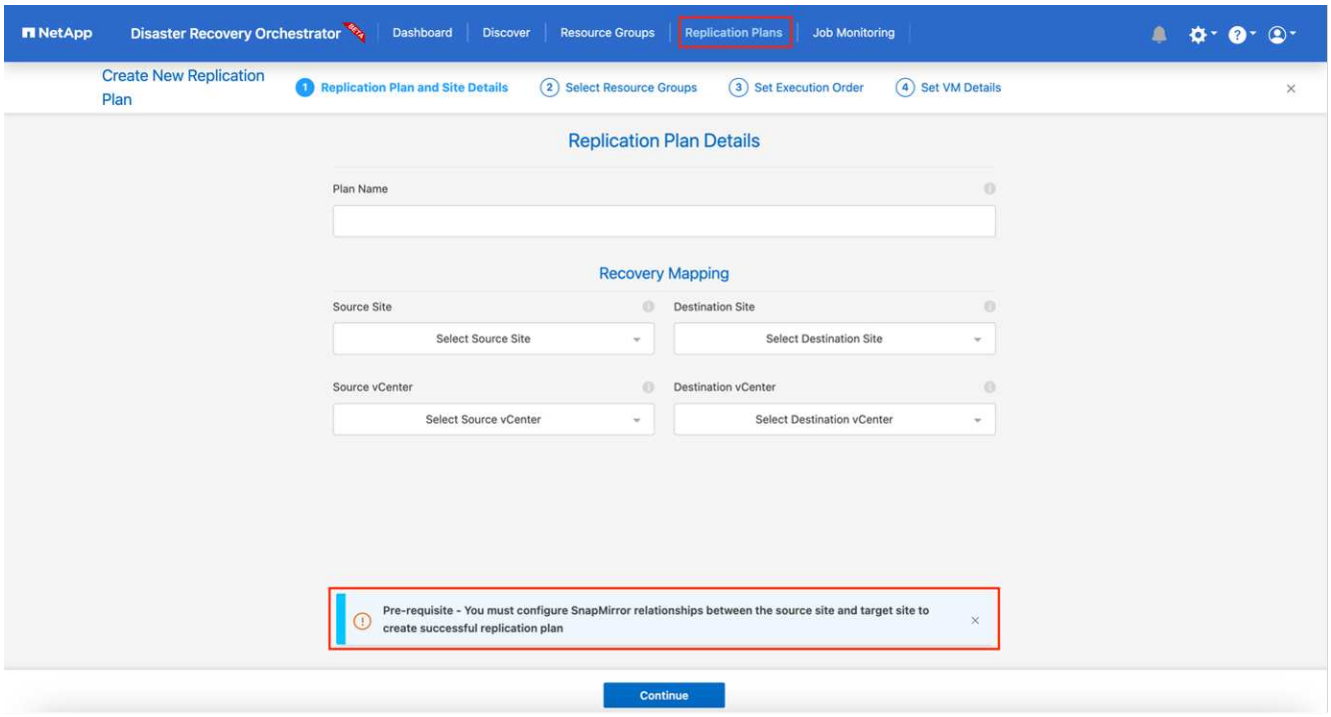
재해가 발생할 경우 애플리케이션을 복구할 계획이 필요합니다. 드롭다운에서 소스 및 대상 vCenter 플랫폼을 선택하고 이 계획에 포함할 리소스 그룹을 선택하고, 애플리케이션 복구 및 전원 켜기 방법(예: 도메인 컨트롤러, 계층 1, 계층 2 등)을 그룹화합니다. 이러한 계획을 청사진이라고도 합니다. 복구 계획을 정의하려면 * Replication Plan * 탭으로 이동하여 * New Replication Plan * 을 클릭합니다.

복제 계획 생성을 시작하려면 다음 단계를 수행하십시오.

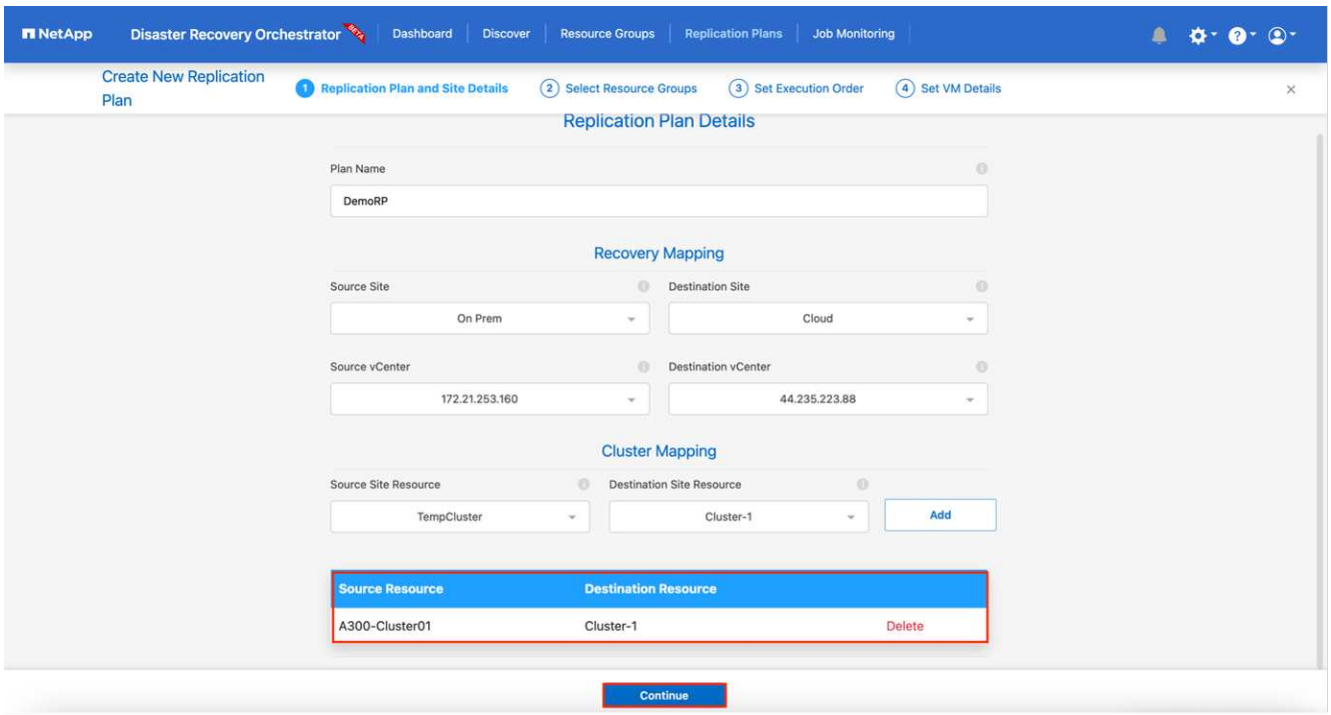
1. Replication Plans * 에 액세스하여 * Create New Replication Plan * 을 클릭합니다.



2. 새 복제 계획 * 에서 소스 사이트, 연결된 vCenter, 대상 사이트 및 연결된 vCenter를 선택하여 계획 이름을 제공하고 복구 매핑을 추가합니다.

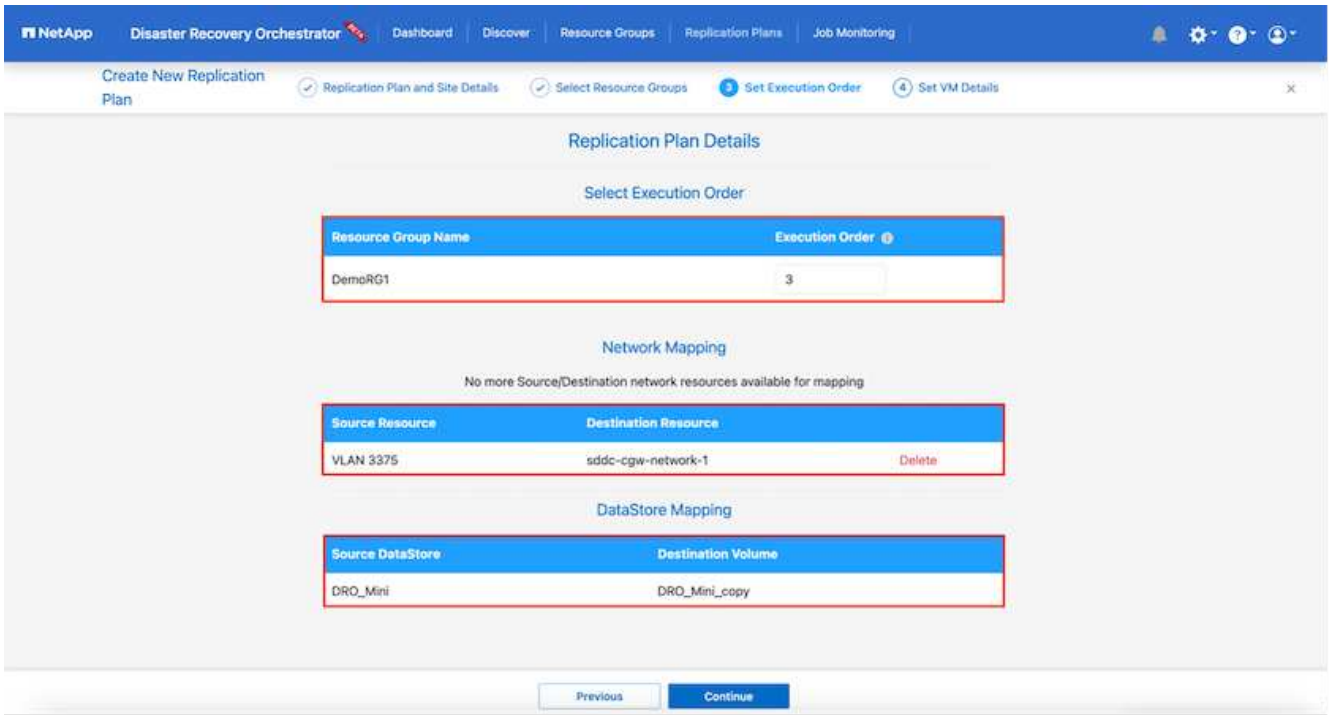


3. 복구 매핑이 완료되면 클러스터 매핑을 선택합니다.

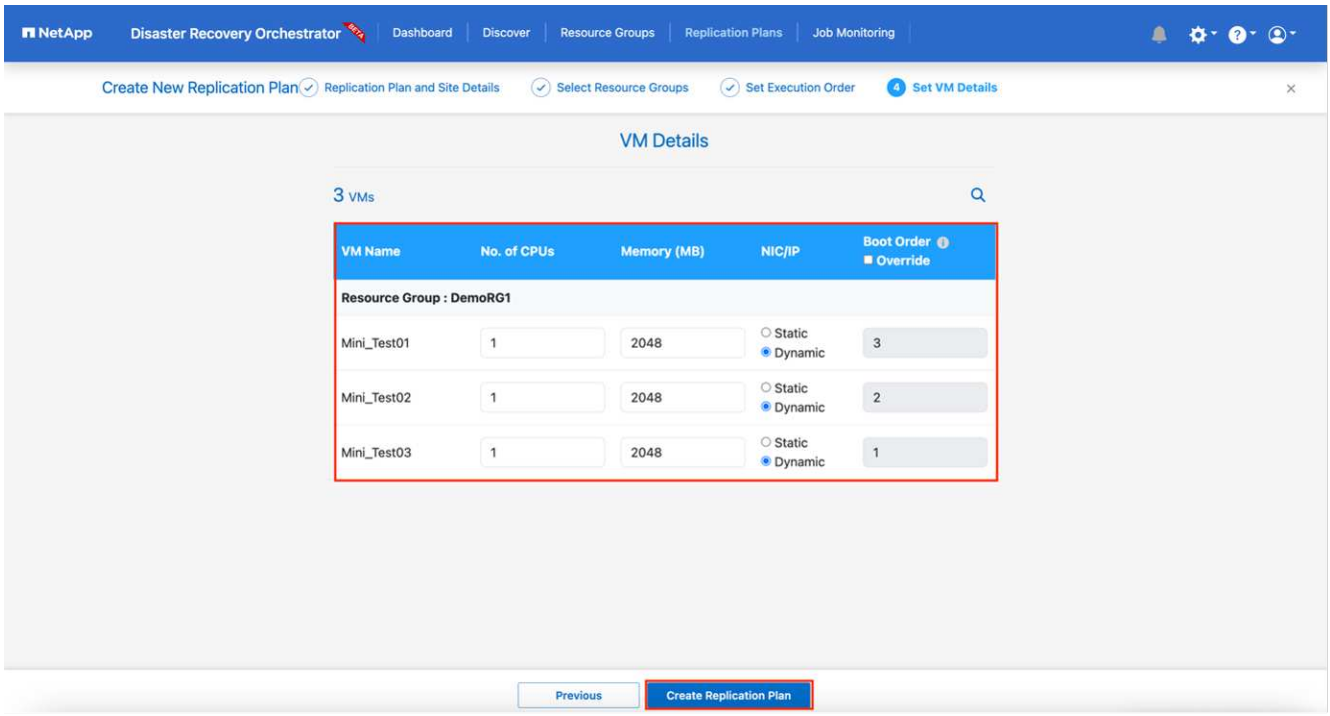


4. 리소스 그룹 세부 정보 * 를 선택하고 * 계속 * 을 클릭합니다.
5. 리소스 그룹의 실행 순서를 설정합니다. 이 옵션을 사용하면 여러 리소스 그룹이 있을 때 작업 순서를 선택할 수 있습니다.
6. 작업을 완료한 후 해당 세그먼트에 대한 네트워크 매핑을 선택합니다. 세그먼트는 VMC 내에서 이미 프로비저닝되어야 하므로 VM을 매핑할 적절한 세그먼트를 선택하십시오.
7. 선택한 VM에 따라 데이터 저장소 매핑이 자동으로 선택됩니다.

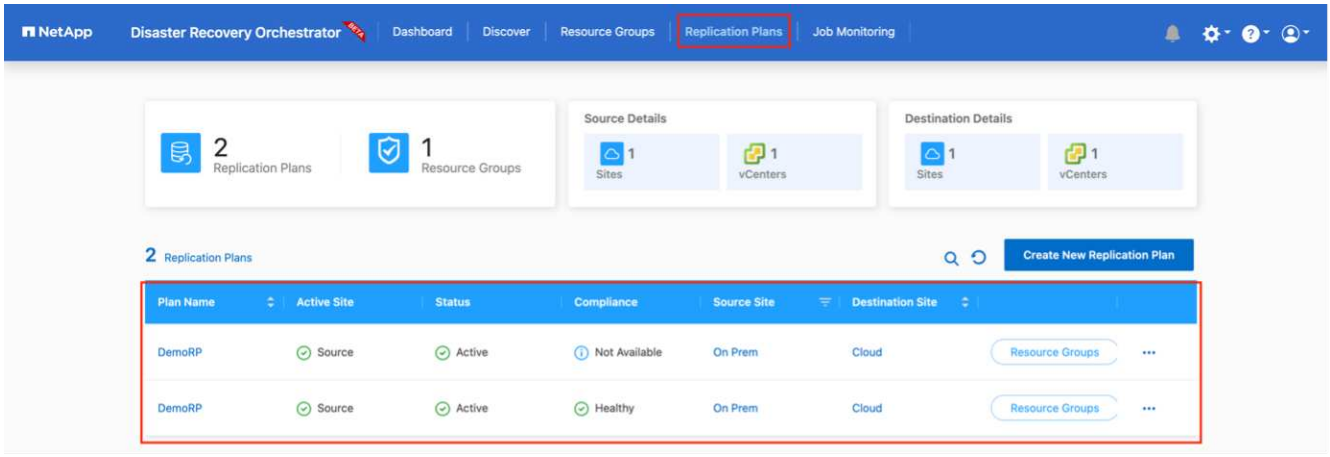
SnapMirror가 볼륨 레벨에 있습니다. 따라서 모든 VM이 복제 대상에 복제됩니다. 데이터 저장소에 속한 모든 VM을 선택해야 합니다. 이 옵션을 선택하지 않으면 복제 계획에 포함된 VM만 처리됩니다.



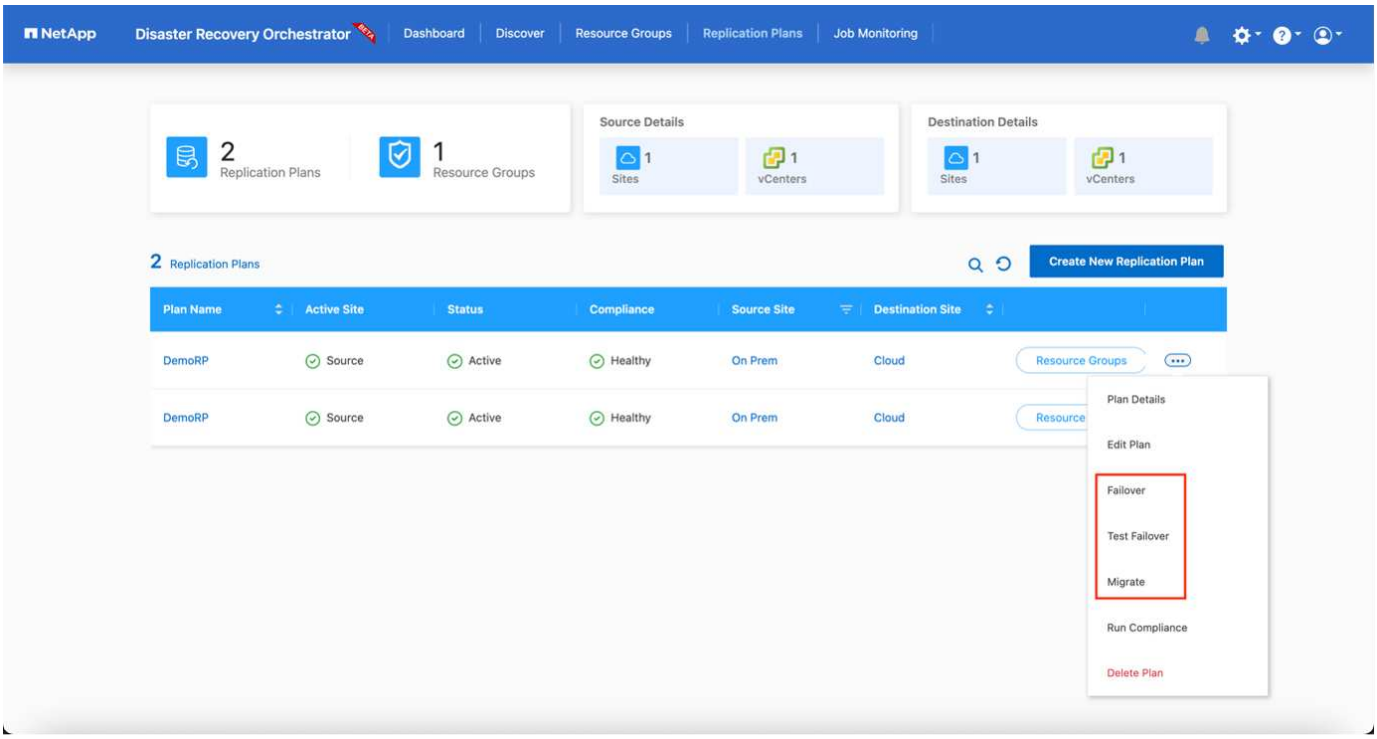
8. VM 세부 정보 아래에서 VM의 CPU 및 RAM 매개 변수의 크기를 선택적으로 조정할 수 있습니다. 이는 대규모 환경을 소규모 타겟 클러스터로 복구하거나 일대일 물리적 VMware 인프라를 프로비저닝하지 않고도 DR 테스트를 수행할 때 매우 유용합니다. 또한 리소스 그룹에서 선택한 모든 VM에 대한 부팅 순서 및 부팅 지연(초)을 수정할 수 있습니다. 리소스 그룹 부팅 순서 선택 중에 선택한 변경 사항에서 필요한 변경 사항이 있는 경우 부팅 순서를 수정하는 추가 옵션이 있습니다. 기본적으로 리소스 그룹을 선택하는 동안 선택한 부팅 순서가 사용되지만 이 단계에서는 모든 수정 작업을 수행할 수 있습니다.

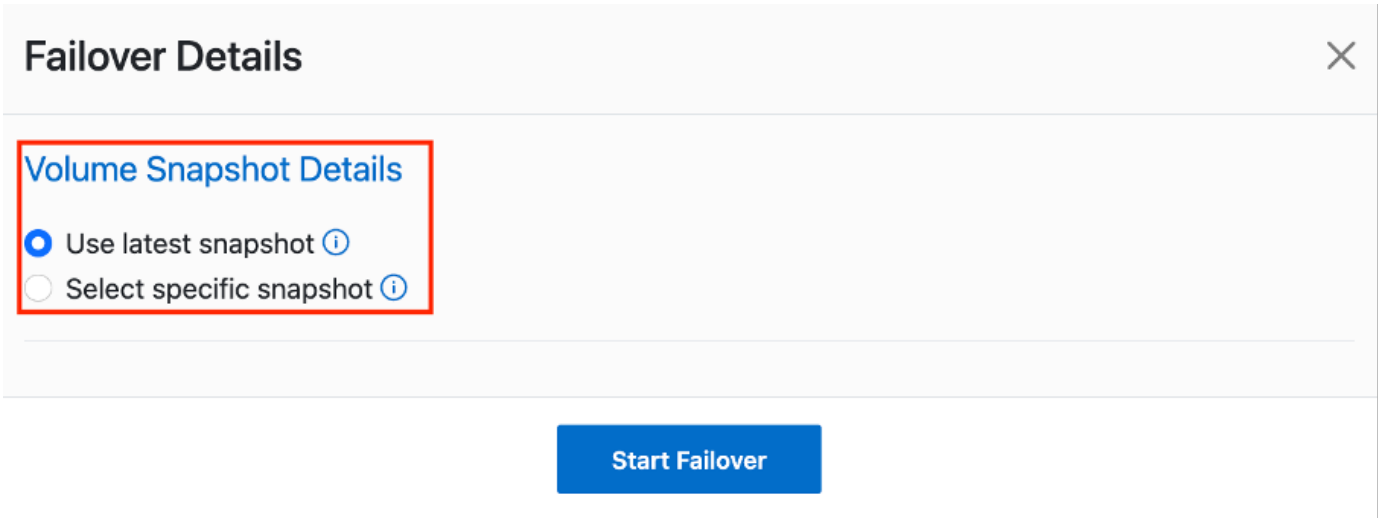


9. Create Replication Plan * 을 클릭합니다.

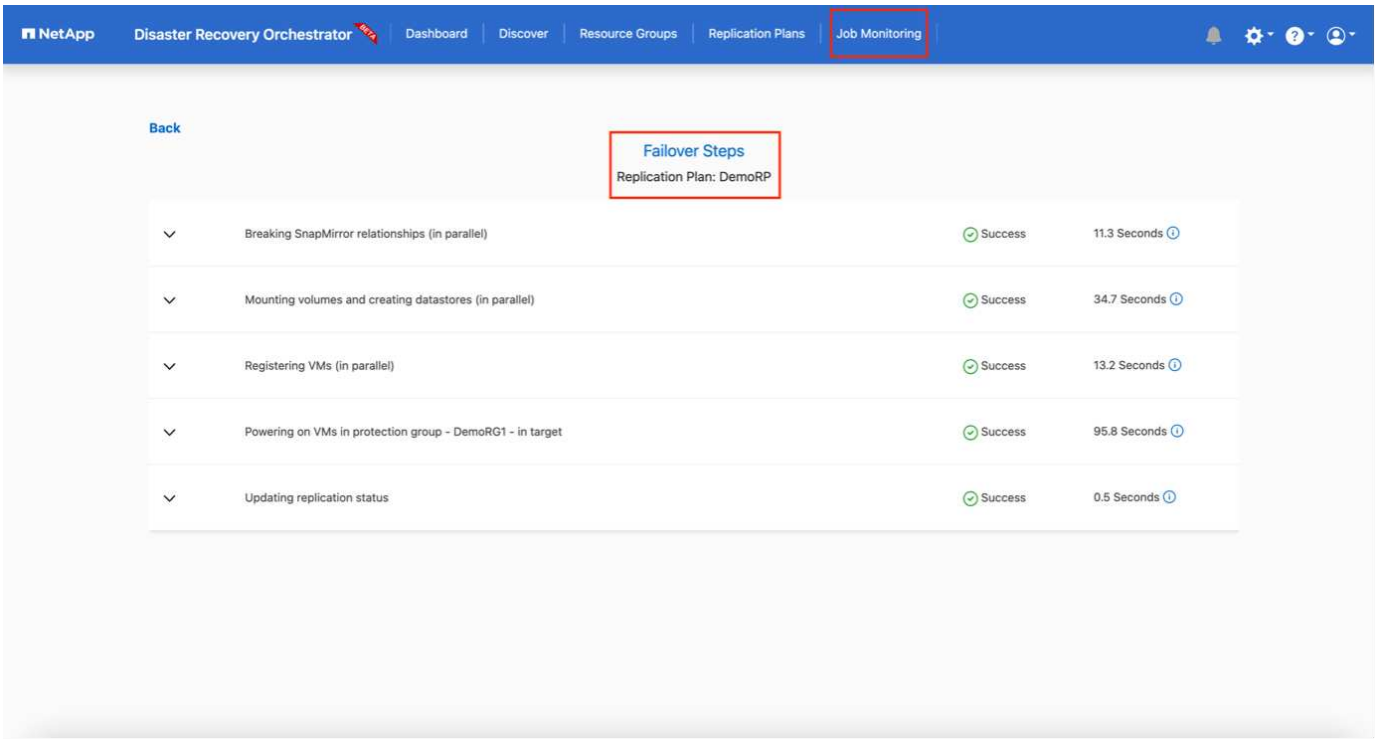


복제 계획이 생성되면 요구 사항에 따라 페일오버 옵션, 테스트 페일오버 옵션 또는 마이그레이션 옵션을 사용할 수 있습니다. 페일오버 및 테스트 페일오버 옵션 중에 최신 SnapMirror 스냅샷 복사본이 사용되거나, SnapMirror의 보존 정책에 따라 특정 시점의 Snapshot 복사본에서 특정 스냅샷 복사본을 선택할 수 있습니다. 가장 최근의 복제본이 이미 손상 또는 암호화된 상태에서 랜섬웨어와 같은 손상 이벤트가 발생할 경우 시점 옵션이 매우 유용할 수 있습니다. DRO는 사용 가능한 모든 시점을 표시합니다. 복제 계획에 지정된 구성으로 대체 작동을 트리거하거나 테스트 대체 작동을 트리거하려면 * 장애 조치 * 또는 * 테스트 대체 작동 * 을 클릭합니다.

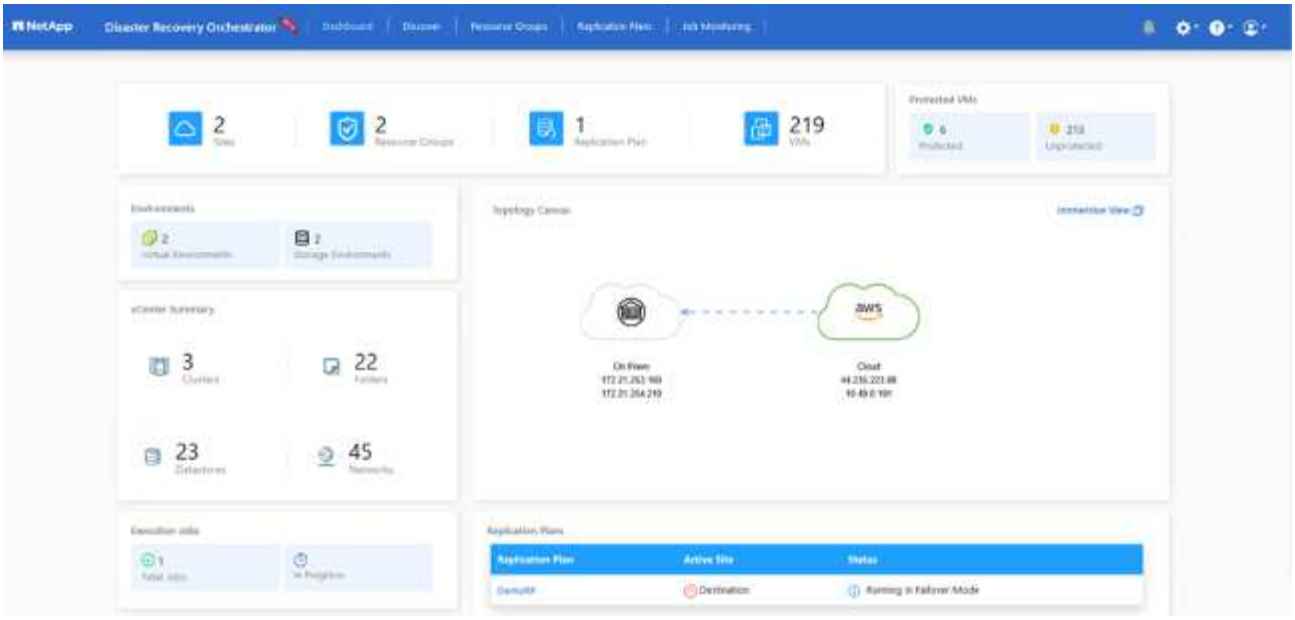




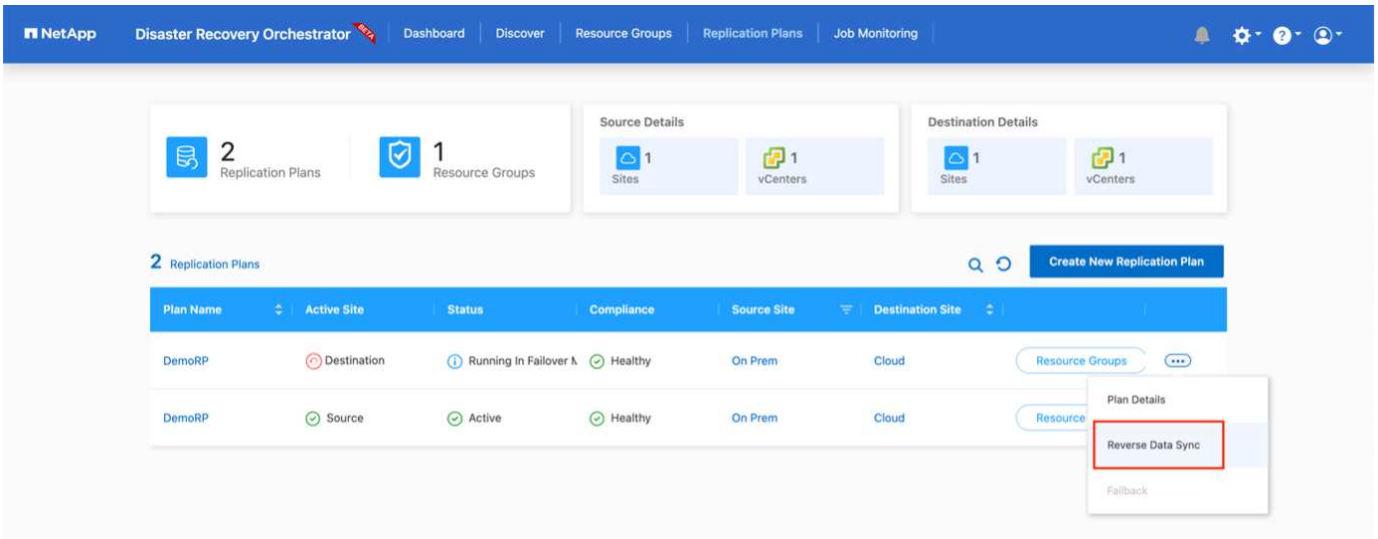
복제 계획은 작업 메뉴에서 모니터링할 수 있습니다.

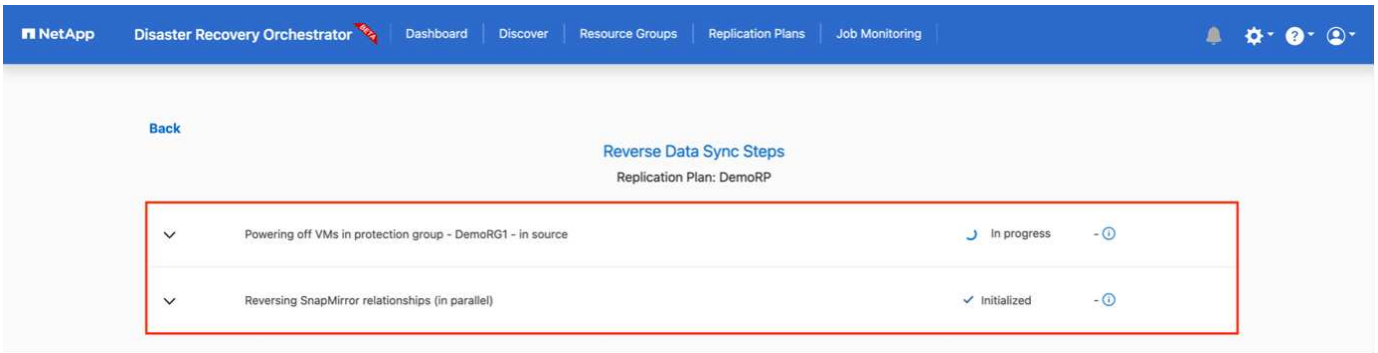


페일오버가 트리거된 후 복구된 항목이 VMC vCenter(VM, 네트워크, 데이터 저장소)에서 표시될 수 있습니다. 기본적으로 VM은 Workload 폴더로 복구됩니다.

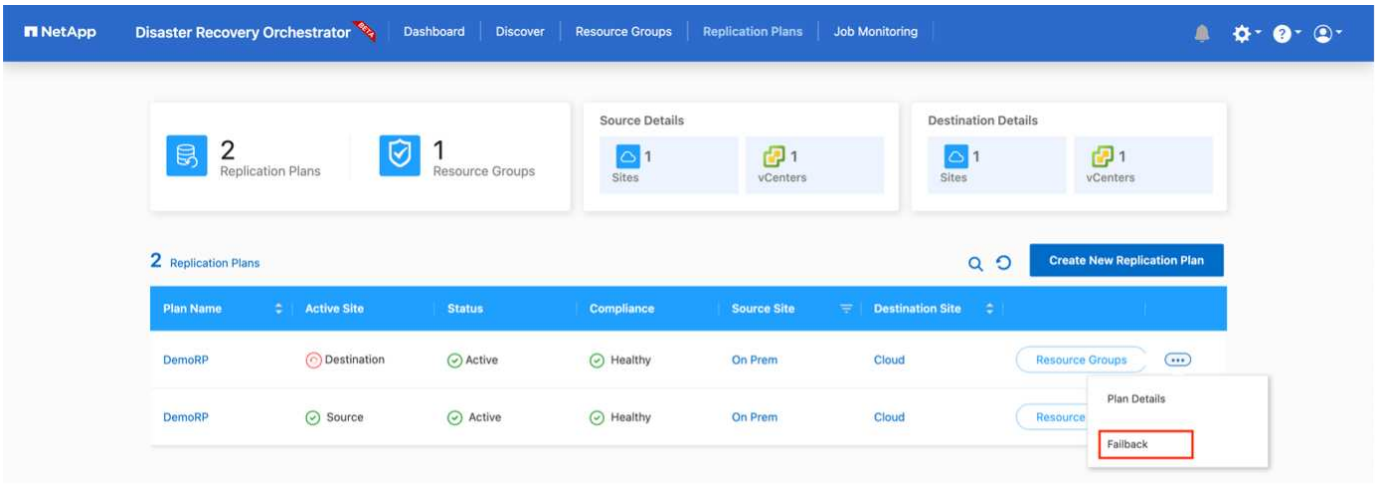


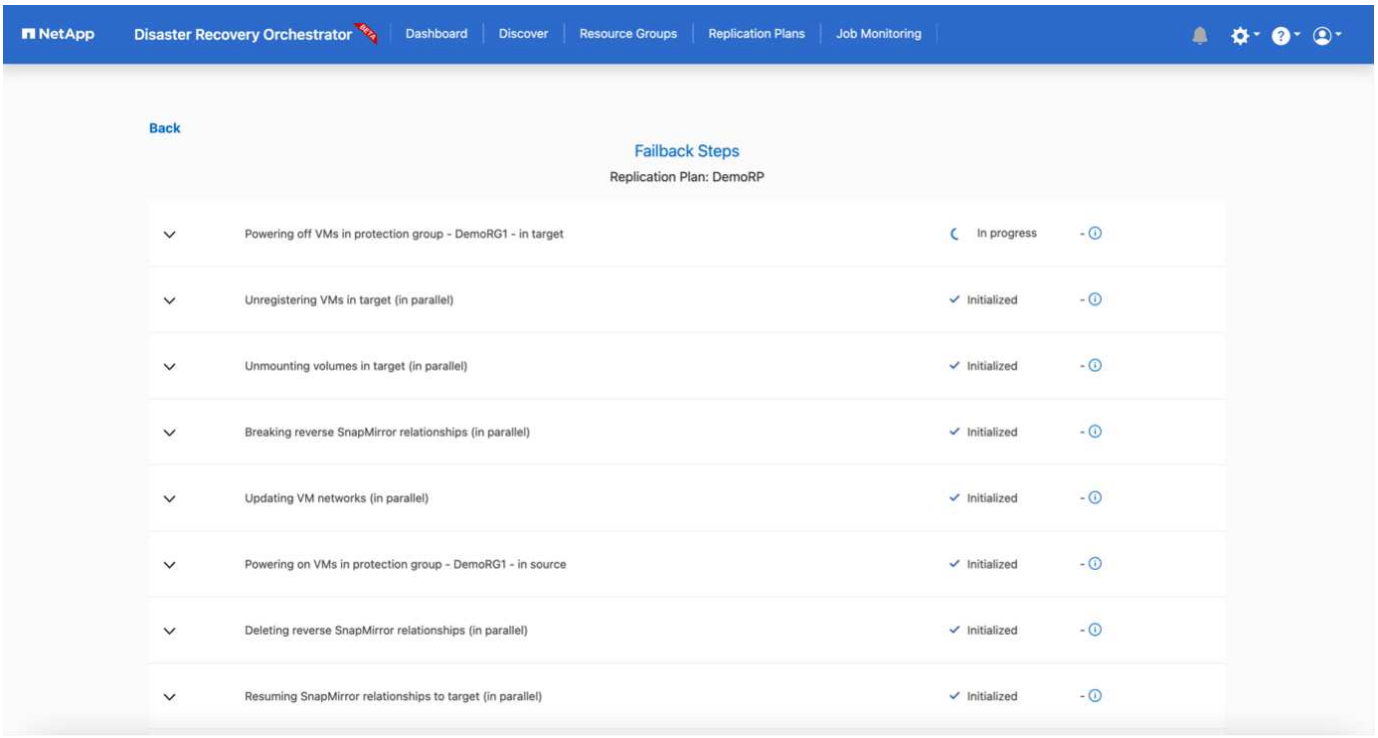
페일백은 복제 계획 레벨에서 트리거될 수 있습니다. 테스트 페일오버의 경우 최분해 옵션을 사용하여 변경 사항을 롤백하고 FlexClone 관계를 제거할 수 있습니다. 페일오버와 관련된 페일백은 2단계 프로세스입니다. 복제 계획을 선택하고 * Reverse data sync * 를 선택합니다.



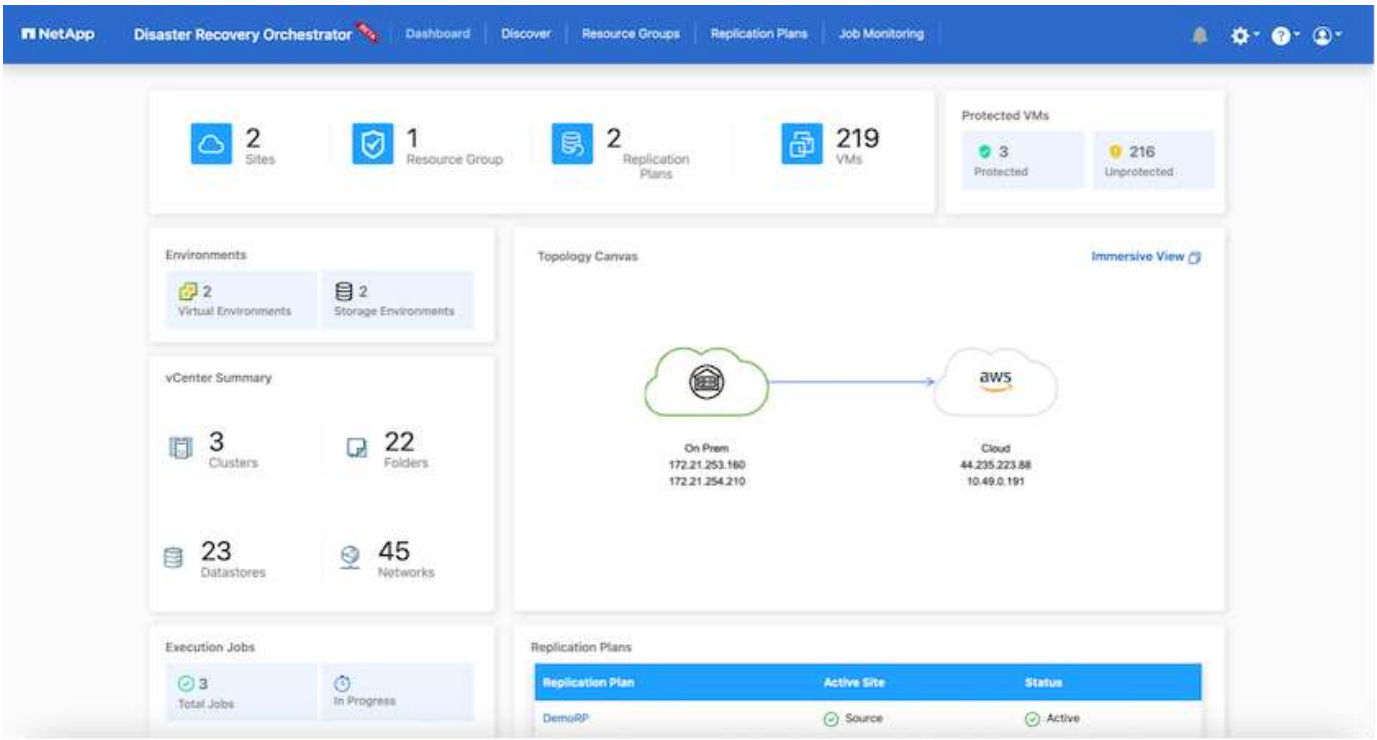


완료되면 페일백을 트리거하여 원래 운영 사이트로 다시 이동할 수 있습니다.





NetApp BlueXP에서는 복제 상태가 적절한 볼륨(VMC에 읽기-쓰기 볼륨으로 매핑된 볼륨)에 대해 끊어지는 것을 볼 수 있습니다. 테스트 페일오버 중에 DRO는 대상 또는 복제본 볼륨을 매핑하지 않습니다. 대신 필요한 SnapMirror(또는 Snapshot) 인스턴스의 FlexClone 복사본을 만들고 FlexClone 인스턴스를 노출합니다. FlexClone 인스턴스는 ONTAP용 FSx의 추가 물리적 용량을 소비하지 않습니다. 이 프로세스를 통해 DR 테스트 또는 분류 워크플로우 중에도 볼륨을 수정하지 않고 복제 작업을 계속할 수 있습니다. 또한 이 프로세스를 통해 오류가 발생하거나 손상된 데이터가 복구되면 복제본을 제거할 위험 없이 복구를 정리할 수 있습니다.



랜섬웨어 복구

랜섬웨어에서 복구하는 것은 매우 힘든 작업이 될 수 있습니다. 특히, IT 조직은 안전한 반환 지점이 어디인지 정확히 파악하기가 어려우며, 일단 결정된 후에는 침낭성 맬웨어 또는 취약한 응용 프로그램 등의 재발생 공격으로부터 복구된 워크로드를 보호하기가 어려울 수 있습니다.

DRO는 사용 가능한 모든 시점에서 시스템을 복구할 수 있도록 함으로써 이러한 문제를 해결합니다. 또한 작업 부하를 기능적이면서도 격리된 네트워크로 복구할 수 있으므로 응용 프로그램이 남북 트래픽에 노출되지 않은 위치에서 상호 작동하고 통신할 수 있습니다. 이를 통해 보안 팀은 법의학 조사를 안전하게 수행할 수 있으며, 숨겨진 악성 코드나 잠자는 맬웨어가 없는지 확인할 수 있습니다.

이점

- 효율적이고 복원력이 뛰어난 SnapMirror 복제 사용:
- Snapshot 복사본 보존을 통해 사용 가능한 모든 시점으로 복구합니다.
- 스토리지, 컴퓨팅, 네트워크 및 애플리케이션 검증 단계에서 수백 또는 수천 개의 VM을 복구하는 데 필요한 모든 단계를 완벽하게 자동화
- ONTAP FlexClone 기술을 사용하여 복제된 볼륨을 변경하지 않는 방법으로 워크로드 복구
  - 볼륨 또는 스냅샷 복사본에 대한 데이터 손상 위험을 방지합니다.
  - DR 테스트 워크플로우 중에 복제 중단 방지
  - DevTest, 보안 테스트, 패치 또는 업그레이드 테스트, 수정 테스트 등과 같은 DR 이외의 다른 워크플로우에 클라우드 컴퓨팅 리소스를 사용하여 DR 데이터를 사용할 수 있습니다.
- CPU 및 RAM 최적화를 통해 보다 작은 컴퓨팅 클러스터로 복구할 수 있으므로 클라우드 비용을 절감할 수 있습니다.

저자: Niyaz Mohamed-NetApp Solutions Engineering

개요

Amazon FSx for NetApp ONTAP와 AWS의 VMware Cloud의 통합은 SDDC의 클러스터에 연결할 수 있는 NetApp ONTAP 파일 시스템 기반의 AWS 관리형 외부 NFS 데이터 저장소입니다. 컴퓨팅 리소스와 독립적으로 확장이 가능한 유연한 고성능 가상화 스토리지 인프라를 고객에게 제공합니다.

AWS SDDC 기반 VMware Cloud를 재해 복구 타겟으로 사용하려는 고객은 VM 복제 기능을 제공하는 검증된 타사 솔루션을 사용하여 온프레미스에서 데이터를 복제하는 데 FSx for ONTAP 데이터 저장소를 사용할 수 있습니다. FSx for ONTAP 데이터 저장소를 추가하면 스토리지를 수용하기 위해 엄청난 양의 ESXi 호스트를 사용하여 AWS SDDC에 VMware 클라우드를 구축하는 것보다 비용 최적화된 배포를 실현할 수 있습니다.

또한 이 접근 방식은 고객이 VMC에서 FSx for ONTAP 데이터 저장소와 함께 파일럿 라이트 클러스터를 사용하여 VM 복제본을 호스팅할 수 있도록 지원합니다. 복제 계획을 정상적으로 페일오버하여 AWS 기반 VMware Cloud로의 마이그레이션 옵션으로 같은 프로세스를 확장할 수도 있습니다.

문제 설명

이 문서에서는 FSx for ONTAP 데이터 저장소와 Veeam 백업 및 복제를 사용하여 VM 복제 기능을 사용하여 온프레미스 VMware VM의 재해 복구를 AWS 기반의 VMware Cloud로 설정하는 방법을 설명합니다.

Veeam Backup & Replication을 사용하면 재해 복구(DR)를 위해 온사이트 및 원격 복제를 수행할 수 있습니다. 가상 머신을 복제할 때 Veeam Backup & Replication은 타겟 VMware Cloud on AWS SDDC 클러스터에 기본 VMware vSphere 형식으로 VM의 정확한 복제본을 생성하고 복제본을 원래 VM과 동기화된 상태로 유지합니다.

READY-TO-START 상태에 있는 VM의 복제본이 있기 때문에 복제는 최상의 RTO(Recovery Time Objective) 값을 제공합니다. 이 복제 메커니즘은 재해 발생 시 VMware Cloud on AWS SDDC에서 워크로드를 신속하게 시작할 수 있도록 보장합니다. Veeam Backup & Replication 소프트웨어는 또한 WAN을 통한 복제 및 느린 연결을 위해 트래픽 전송을 최적화합니다. 또한 중복 데이터 블록, 제로 데이터 블록, 스왑 파일 및 제외된 VM 게스트 OS 파일을 필터링하고 복제 트래픽을 압축합니다.

복제 작업이 전체 네트워크 대역폭을 소비하는 것을 방지하기 위해 WAN 가속기 및 네트워크 조절 규칙을 적용할 수 있습니다. Veeam Backup & Replication의 복제 프로세스는 작업 중심으로 수행되므로 복제 작업을 구성하여 복제가 수행됩니다. 재해가 발생할 경우 해당 복제본 복제본으로 장애 조치를 수행하여 VM을 복구하기 위해 장애 조치를 트리거할 수 있습니다.

페일오버가 수행되면 복제된 VM이 원래 VM의 역할을 대신합니다. 페일오버는 복제본의 최신 상태 또는 알려진 정상 복구 지점으로 수행할 수 있습니다. 따라서 필요에 따라 랜섬웨어 복구 또는 격리된 테스트가 가능합니다. Veeam Backup & Replication에서 페일오버와 페일백은 임시 중간 단계로, 이 단계는 추가로 완료해야 합니다. Veeam Backup & Replication은 다양한 재해 복구 시나리오를 처리할 수 있는 다양한 옵션을 제공합니다.

[Veeam Replication 및 FSx ONTAP for VMC를 사용하는 DR 시나리오의 다이어그램]

솔루션 구축

고급 단계

1. Veeam Backup and Replication 소프트웨어는 적절한 네트워크 연결을 통해 사내 환경에서 실행됩니다.
2. VMware Cloud on AWS 구성 에 대한 자세한 내용은 VMware Cloud Tech Zone 문서를 참조하십시오 "AWS

기반 VMware Cloud와 Amazon FSx for NetApp ONTAP 구축 가이드 의 통합" 구축하려면 AWS SDDC에 VMware Cloud를, FSx for ONTAP를 NFS 데이터 저장소로 구성합니다. (최소 구성으로 설정된 파일럿 라이트 환경을 DR 목적으로 사용할 수 있습니다. 장애 발생 시 VM이 이 클러스터로 페일오버되고 추가 노드를 추가할 수 있습니다.)

3. Veeam Backup and Replication을 사용하여 VM 복제본을 생성하도록 복제 작업을 설정합니다.
4. 페일오버 계획을 만들고 페일오버를 수행합니다.
5. 재해 이벤트가 완료되고 운영 사이트가 가동되면 운영 VM으로 다시 전환합니다.

Veeam VM을 **VMC** 및 **FSx for ONTAP** 데이터 저장소로 복제하기 위한 사전 요구 사항

1. Veeam Backup & Replication 백업 VM이 소스 vCenter와 AWS SDDC 클러스터의 타겟 VMware 클라우드에 연결되어 있는지 확인합니다.
2. 백업 서버는 짧은 이름을 확인하고 소스 및 타겟 vCenter에 연결할 수 있어야 합니다.
3. 대상 FSx for ONTAP 데이터 저장소에는 복제된 VM의 VMDK를 저장할 수 있는 충분한 여유 공간이 있어야 합니다

자세한 내용은 "고려 사항 및 제한 사항"을 참조하십시오 "여기".

배포 세부 정보

1단계**: VM** 복제

Veeam Backup & Replication은 VMware vSphere 스냅샷 기능을 활용하며, 복제하는 동안 Veeam Backup & Replication은 VMware vSphere에 VM 스냅샷을 생성하도록 요청합니다. VM 스냅샷은 가상 디스크, 시스템 상태, 구성 등을 포함하는 VM의 시점 복제본입니다. Veeam Backup & Replication은 이 스냅샷을 복제용 데이터 소스로 사용합니다.

VM을 복제하려면 다음 단계를 수행하십시오.

1. Veeam Backup & Replication Console을 엽니다.
2. 홈 보기에서 복제 작업 > 가상 머신 > VMware vSphere 를 선택합니다.
3. 작업 이름을 지정하고 해당 고급 제어 확인란을 선택합니다. 다음 을 클릭합니다.
   - 온-프레미스와 AWS 간의 접속 대역폭이 제한된 경우 복제 시드 확인란을 선택합니다.
   - VMware Cloud on AWS SDDC의 세그먼트가 사내 사이트 네트워크의 세그먼트와 일치하지 않으면 Network remapping (다른 네트워크를 가진 AWS VMC 사이트의 경우) 확인란을 선택합니다.
   - 온프레미스 운영 사이트의 IP 주소 지정 체계가 AWS VMC 사이트의 체계와 다른 경우 복제 Re-IP(IP 주소 지정 체계가 다른 DR 사이트의 경우) 확인란을 선택합니다.

     [DR Veeam FSx 이미지 2] | *dr-veeam-fsx-image2.png*
4. AWS SDDC 기반 VMware Cloud에 연결된 FSx for ONTAP 데이터 저장소에 복제해야 하는 VM을 * 가상 머신 * 단계에서 선택합니다. vSAN에 가상 머신을 배치하여 사용 가능한 vSAN 데이터스토어 용량을 채울 수 있습니다. 파일럿 라이트 클러스터에서는 3노드 클러스터의 가용 용량이 제한됩니다. 나머지 데이터를 FSx for ONTAP 데이터 저장소에 복제할 수 있습니다. Add * 를 클릭한 다음 * Add Object * 창에서 필요한 VM 또는 VM 컨테이너를 선택하고 * Add * 를 클릭합니다. 다음 * 을 클릭합니다.

   [DR Veeam FSx 이미지 3] | *dr-veeam-fsx-image3.png*
5. 그런 다음 대상을 AWS SDDC 클러스터/호스트의 VMware Cloud 및 VM 복제본용 적절한 리소스 풀, VM 폴더 및 FSx for ONTAP 데이터 저장소로 선택합니다. 그런 다음 * 다음 * 을 클릭합니다.

   [DR Veeam FSx 이미지 4] | *dr-veeam-fsx-image4.png*
6. 다음 단계에서는 필요에 따라 소스 및 대상 가상 네트워크 간의 매핑을 생성합니다.

   [DR Veeam FSx 이미지5] | *dr-veeam-fsx-image5.png*
7. 작업 설정 * 단계에서 VM 복제본, 보존 정책 등에 대한 메타데이터를 저장할 백업 리포지토리를 지정합니다.
8. 데이터 전송 * 단계에서 * 원본 * 및 * 대상 * 프록시 서버를 업데이트하고 * 자동 * 선택(기본값)을 그대로 두고 * 직접 * 옵션을 선택한 후 * 다음 * 을 클릭합니다.
9. Guest Processing * 단계에서 필요에 따라 * Enable application-aware processing * 옵션을 선택합니다. 다음 * 을 클릭합니다.

   [DR Veeam FSx 이미지6] | *dr-veeam-fsx-image6.png*
10. 정기적으로 실행할 복제 작업을 실행할 복제 스케줄을 선택합니다.
11. 마법사의 * Summary * 단계에서 복제 작업의 세부 정보를 검토합니다. 마법사를 닫은 후 바로 작업을 시작하려면 * 마침을 클릭하면 작업 실행 * 확인란을 선택하고, 그렇지 않으면 확인란을 선택하지 않은 상태로 둡니다. 그런 다음 * 마침 * 을 클릭하여 마법사를 닫습니다.

[DR Veeam FSx 이미지7] | *dr-veeam-fsx-image7.png*

복제 작업이 시작되면 접미사가 지정된 VM이 대상 VMC SDDC 클러스터/호스트에 채워집니다.

[DR Veeam FSx 이미지8] | *dr-veeam-fsx-image8.png*

Veeam 복제에 대한 자세한 내용은 을 참조하십시오 "복제 작동 방법".

2단계**:** 장애 조치 계획을 만듭니다

초기 복제 또는 시드가 완료되면 페일오버 계획을 생성합니다. 페일오버 계획은 종속 VM에 대해 하나씩 또는 그룹으로 자동 페일오버를 수행하는 데 도움이 됩니다. 페일오버 계획은 부팅 지연을 포함하여 VM이 처리되는 순서에 대한 청사진입니다. 또한 페일오버 계획은 중요한 종속 VM이 이미 실행 중인지 확인하는 데 도움이 됩니다.

계획을 생성하려면 Replicas라는 새 하위 섹션으로 이동하고 Failover Plan을 선택합니다. 적절한 VM을 선택합니다. Veeam Backup & Replication은 이 시점에 가장 가까운 복원 지점을 찾아 VM 복제를 시작하는 데 사용합니다.

ⓘ 초기 복제가 완료되고 VM 복제본이 준비 상태가 된 후에만 페일오버 계획을 추가할 수 있습니다.

ⓘ 페일오버 계획을 실행할 때 동시에 시작할 수 있는 최대 VM 수는 10개입니다.

ⓘ 페일오버 프로세스 중에는 소스 VM의 전원이 꺼지지 않습니다.

장애 조치 계획 * 을 만들려면 다음을 수행합니다.

1. 홈 보기에서 * 페일오버 계획 > VMware vSphere * 를 선택합니다.
2. 그런 다음 계획에 이름과 설명을 입력합니다. 필요에 따라 사전 및 사후 페일오버 스크립트를 추가할 수 있습니다. 예를 들어 복제된 VM을 시작하기 전에 VM을 종료하는 스크립트를 실행합니다.

   [DR Veeam FSx 이미지9] | *dr-veeam-fsx-image9.png*

3. VM을 계획에 추가하고 애플리케이션 종속성을 충족하도록 VM 부팅 순서 및 부팅 지연을 수정합니다.

   [DR Veeam FSx 이미지 10] | *dr-veeam-fsx-image10.png*

복제 작업 생성에 대한 자세한 내용은 을 참조하십시오 "복제 작업을 생성하는 중입니다".

3단계**:** 페일오버 계획을 실행합니다

페일오버 중에 프로덕션 사이트의 소스 VM이 재해 복구 사이트의 해당 복제본으로 전환됩니다. 페일오버 프로세스의 일부로 Veeam Backup & Replication은 VM 복제본을 필요한 복구 지점으로 복구하고 소스 VM의 모든 입출력 작업을 해당 복제본으로 이동합니다. 복제본은 재해 발생 시에만 사용할 수 있으며 DR 드릴을 시뮬레이션하는 데도 사용할 수 있습니다. 페일오버 시뮬레이션 중에는 소스 VM이 계속 실행 중입니다. 필요한 모든 테스트가 수행되면 페일오버를 취소하고 정상 작업으로 돌아갈 수 있습니다.

DR 훈련 중에 IP 충돌을 피하기 위해 네트워크 분할이 제대로 수행되었는지 확인하십시오.

장애 조치 계획을 시작하려면 * 장애 조치 계획 * 탭을 클릭하고 장애 조치 계획을 마우스 오른쪽 버튼으로 클릭합니다. 시작 * 을 선택합니다. 이렇게 하면 VM 복제본의 최신 복구 지점을 사용하여 장애 조치가 수행됩니다. VM 복제본의 특정 복원 지점으로 페일오버하려면 * 시작 * 을 선택합니다.

[DR Veeam FSx 이미지 11] | *dr-veeam-fsx-image11.png*

[DR Veeam FSx 이미지12] | *dr-veeam-fsx-image12.png*

VM 복제본의 상태가 Ready에서 Failover로 변경되고 VM은 대상 VMware Cloud on AWS SDDC 클러스터 /호스트에서 시작됩니다.

[DR Veeam FSx 이미지 13] | *dr-veeam-fsx-image13.png*

페일오버가 완료되면 VM의 상태가 "페일오버"로 변경됩니다.

[DR Veeam FSx 이미지14] | *dr-veeam-fsx-image14.png*

Veeam Backup & Replication은 소스 VM의 복제본이 준비 상태로 돌아갈 때까지 소스 VM에 대한 모든 복제 작업을 중지합니다.

페일오버 계획에 대한 자세한 내용은 을 참조하십시오 "페일오버 계획".

4단계**:** 프로덕션 사이트로 페일백합니다

장애 조치 계획이 실행 중인 경우 중간 단계로 간주되며 요구 사항에 따라 확정되어야 합니다. 다음과 같은 옵션이 있습니다.

- * Failback to Production * - 원래 VM으로 다시 전환하고 VM 복제본이 실행되는 동안 발생한 모든 변경 사항을 원래 VM으로 전송합니다.

> ⓘ 페일백을 수행하면 변경 내용이 전송되지만 게시되지는 않습니다. 원래 VM이 예상대로 작동하지 않는 경우 * 페일백 커밋 * (원래 VM이 예상대로 작동하는 것으로 확인된 경우) 또는 * 페일백 실행 취소 * 를 선택하여 VM 복제본으로 돌아갑니다.

- * 장애 조치 실행 취소 * - 원래 VM으로 다시 전환하고 실행 중에 VM 복제본의 모든 변경 사항을 취소합니다.
- * 영구 장애 조치 * - 원래 VM에서 VM 복제본으로 영구적으로 전환하고 이 복제본을 원래 VM으로 사용합니다.

이 데모에서는 Failback to Production을 선택했습니다. 마법사의 대상 단계에서 원래 VM으로 페일백이 선택되었고 "복원 후 VM 전원 켜기" 확인란이 활성화되었습니다.

[DR Veeam FSx 이미지15] | *dr-veeam-fsx-image15.png*

[DR Veeam FSx 이미지 16] | *dr-veeam-fsx-image16.png*

페일백 커밋은 페일백 작업을 완료하는 방법 중 하나입니다. 페일백이 커밋되면 장애가 발생한 VM(운영 VM)에 전송된 변경 사항이 예상대로 작동하는지 확인합니다. 커밋 작업 후에 Veeam Backup & Replication은 운영 VM에 대한 복제 작업을 재개합니다.

페일백 프로세스에 대한 자세한 내용은 의 Veeam 문서를 참조하십시오 "복제를 위한 페일오버 및 페일백".

[DR Veeam FSx 이미지17] | *dr-veeam-fsx-image17.png*

[DR Veeam FSx 이미지 18] | *dr-veeam-fsx-image18.png*

운영 환경으로 페일백이 성공한 후 VM이 모두 원래 운영 사이트로 복구됩니다.

[DR Veeam FSx 이미지 19] | *dr-veeam-fsx-image19.png*

결론

FSx for ONTAP 데이터 저장소 기능을 통해 Veeam 또는 검증된 타사 툴이 파일럿 라이트 클러스터를 사용하고, 클러스터에 VM 복제 복사본을 수용하기 위해 다수의 호스트를 보유하지 않고 경제적인 DR 솔루션을 제공할 수 있습니다. 이 제품은 맞춤형 재해 복구 계획을 처리할 수 있는 강력한 솔루션을 제공합니다. 또한 기존 백업 제품을 사내에서 재사용하여 DR 요구사항을 충족할 수 있으므로, 사내에서 DR 데이터 센터를 종료하여 클라우드 기반 재해 복구가 가능합니다. 재해가 발생한 경우 버튼 클릭 한 번으로 계획된 페일오버 또는 페일오버로 페일오버를 수행할 수 있으며 DR 사이트를 활성화하기로 결정합니다.

이 프로세스에 대해 자세히 알아보려면 자세한 단계별 안내 비디오를 참조하십시오.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a

AWS/VMC에서 워크로드 마이그레이션

TR 4942: VMware HCX를 사용하여 워크로드를 FSx ONTAP 데이터 저장소로 마이그레이션합니다

저자: NetApp 솔루션 엔지니어링

개요: VMware HCX, FSx ONTAP 보조 데이터 저장소 및 VMware Cloud를 사용하여 가상 시스템 마이그레이션

AWS(Amazon Web Services)의 VMware 클라우드(VMC)에 대한 일반적인 사용 사례로서, NetApp ONTAP용 Amazon FSx의 보조 NFS 데이터 저장소가 포함된 VMware 워크로드를 마이그레이션합니다. VMware HCX가 선호되는 옵션이며, VMware에서 지원하는 모든 데이터 저장소에서 실행되는 사내 VM(가상 머신)과 해당 데이터를 ONTAP용 FSx의 보조 NFS 데이터 저장소를 포함하는 VMC 데이터 저장소로 이동하는 다양한 마이그레이션 방법을 제공합니다.

VMware HCX는 주로 클라우드 전반에서 워크로드 마이그레이션, 워크로드 재조정 및 비즈니스 연속성을 간소화하도록 설계된 모바일 플랫폼입니다. 이 제품은 AWS 기반 VMware Cloud의 일부로 포함되어 있으며 워크로드를 다양한 방법으로 마이그레이션하여 DR(재해 복구) 작업에 사용할 수 있습니다.

이 문서에서는 모든 주요 구성 요소, 온프레미스 및 클라우드 데이터 센터 측 등 다양한 VM 마이그레이션 메커니즘을 지원하는 VMware HCX를 구축 및 구성하기 위한 단계별 지침을 제공합니다.

자세한 내용은 을 참조하십시오 "HCX 구축 소개" 및 "AWS SDDC 대상 환경에서 VMware 클라우드를 사용하여 체크리스트 B-HCX를 설치합니다".

높은 수준의 단계

이 목록에는 VMware HCX를 설치하고 구성하는 단계가 수록되어 있습니다.

1. VMware Cloud Services Console을 통해 VMC SDDC(소프트웨어 정의 데이터 센터)에 대한 HCX를 활성화합니다.
2. 온-프레미스 vCenter Server에서 HCX Connector OVA 설치 프로그램을 다운로드하여 구축합니다.
3. 라이센스 키를 사용하여 HCX를 활성화합니다.
4. 온프레미스 VMware HCX Connector를 VMC HCX Cloud Manager와 페어링합니다.
5. 네트워크 프로파일, 컴퓨팅 프로파일 및 서비스 메시를 구성합니다.
6. (선택 사항) 네트워크 확장을 수행하여 네트워크를 확장하고 재IP를 방지합니다.
7. 어플라이언스 상태를 확인하고 마이그레이션이 가능한지 확인합니다.
8. VM 워크로드를 마이그레이션합니다.

필수 구성 요소

시작하기 전에 다음 필수 구성 요소가 충족되었는지 확인하십시오. 자세한 내용은 을 참조하십시오 "HCX 설치 준비 중". 연결을 포함하여 사전 요구 사항이 충족되면 VMC의 VMware HCX 콘솔에서 라이센스 키를 생성하여 HCX를 구성하고 활성화합니다. HCX가 활성화되면 vCenter 플러그인이 구축되며 관리를 위해 vCenter 콘솔을 사용하여 액세스할 수 있습니다.

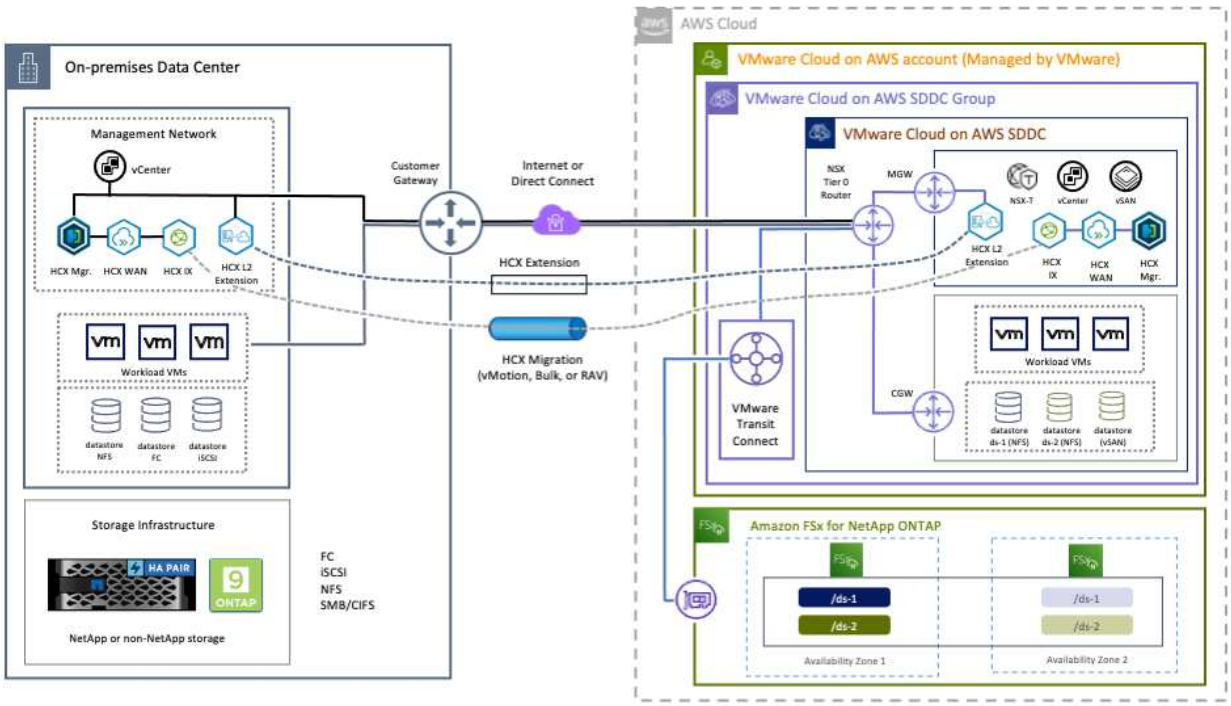
HCX 활성화 및 배포를 진행하기 전에 다음 설치 단계를 완료해야 합니다.

1. 기존 VMC SDDC를 사용하거나 다음 새 SDDC를 생성합니다 "NetApp 링크" 또는 이 "VMware 링크".
2. 사내 vCenter 환경에서 VMC SDDC로의 네트워크 경로는 vMotion을 사용하여 VM 마이그레이션을 지원해야 합니다.
3. 필수 를 확인하십시오 "방화벽 규칙 및 포트" 온-프레미스 vCenter Server와 SDDC vCenter 간에 vMotion 트래픽이 허용됩니다.
4. ONTAP NFS 볼륨용 FSx는 VMC SDDC에 보조 데이터 저장소로 마운트되어야 합니다. NFS 데이터 저장소를 적절한 클러스터에 연결하려면 여기에 설명된 단계를 따르십시오 "NetApp 링크" 또는 이 "VMware 링크".

고급 아키텍처

테스트 목적으로, 이 검증에 사용된 온프레미스 랩 환경은 사이트 간 VPN을 통해 AWS VPC에 연결되었으며, 외부 전송 게이트웨이를 통해 AWS와 VMware 클라우드 SDDC에 사내 연결을 가능하게 했습니다. HCX 마이그레이션 및 네트워크 확장 트래픽은 온프레미스 및 VMware 클라우드 대상 SDDC 사이에서 인터넷을 통해 흐릅니다. Direct Connect 프라이빗 가상 인터페이스를 사용하도록 이 아키텍처를 수정할 수 있습니다.

다음 이미지는 높은 수준의 아키텍처를 보여 줍니다.



솔루션 구축

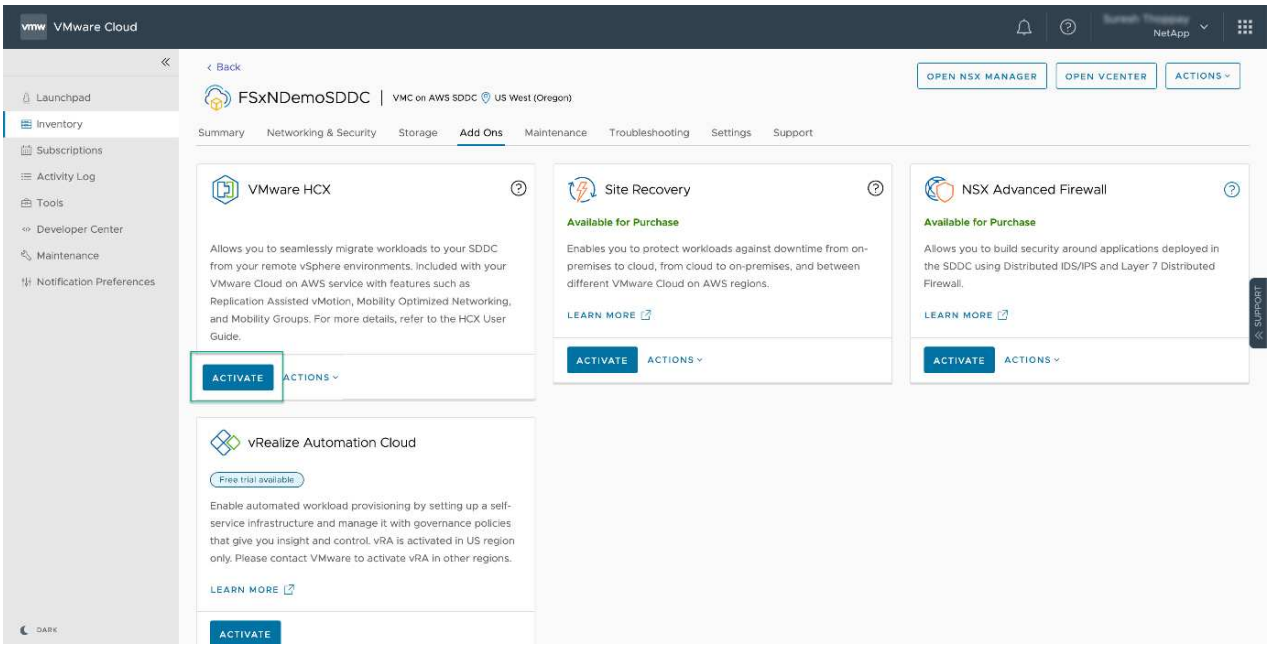
이 솔루션의 배포를 완료하려면 다음 단계를 따르십시오.

1단계**:** 애드온 옵션을 사용하여 **VMC SDDC**를 통해 **HCX**를 활성화합니다

설치를 수행하려면 다음 단계를 수행하십시오.

1. 에서 VMC 콘솔에 로그인합니다 "vmc.vmware.com" 재고 에 액세스할 수 있습니다.
2. 적절한 SDDC를 선택하고 Add-On에 액세스하려면 SDDC에서 View Details를 클릭하고 Add On 탭을 선택합니다.
3. VMware HCX에 대해 활성화 를 클릭합니다.

   이 단계를 완료하는 데 최대 25분이 소요됩니다.

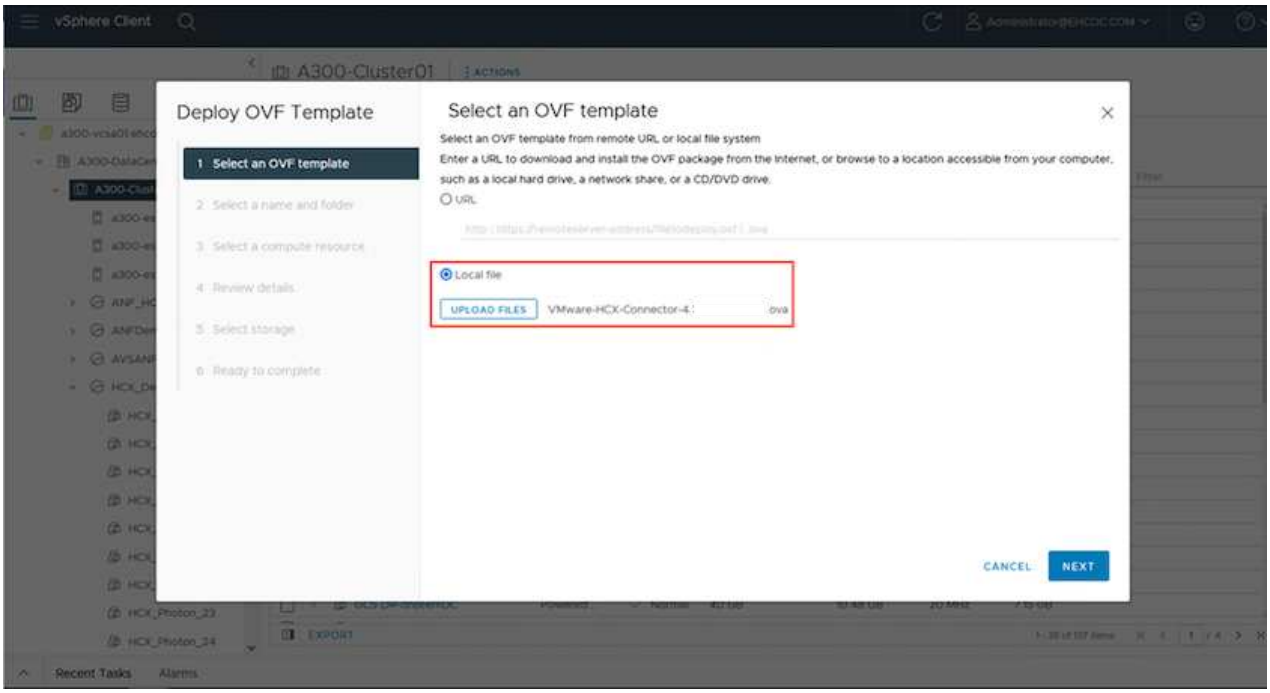


4. 구축이 완료되면 vCenter Console에서 HCX Manager 및 관련 플러그인을 사용할 수 있는지 확인하여 구축을 검증합니다.
5. 적절한 관리 게이트웨이 방화벽을 만들어 HCX Cloud Manager에 액세스하는 데 필요한 포트를 엽니다. 이제 HCX Cloud Manager가 HCX 작업을 수행할 준비가 되었습니다.

2단계**:** 온**-**프레미스 **vCenter Server**에 설치 관리자 **OVA**를 구축합니다

온프레미스 커넥터가 VMC의 HCX Manager와 통신하려면 적절한 방화벽 포트가 온-프레미스 환경에서 열려 있는지 확인합니다.

1. VMC 콘솔에서 HCX 대시보드로 이동하고 관리 로 이동한 다음 시스템 업데이트 탭을 선택합니다. HCX 커넥터 OVA 이미지에 대한 다운로드 링크 요청 을 클릭합니다.
2. HCX Connector를 다운로드한 후 온-프레미스 vCenter Server에 OVA를 구축합니다. vSphere Cluster를 마우스 오른쪽 버튼으로 클릭하고 Deploy OVF Template 옵션을 선택합니다.

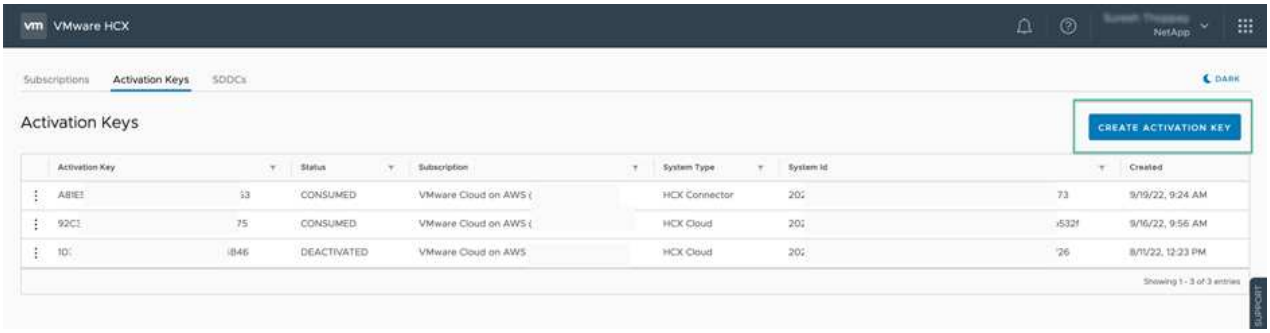


3. Deploy OVF Template 마법사에 필요한 정보를 입력하고 Next를 클릭한 다음 Finish를 클릭하여 VMware HCX Connector OVA를 구축합니다.
4. 가상 어플라이언스의 전원을 수동으로 켭니다. 단계별 지침을 보려면 로 이동하십시오 "VMware HCX 사용자 가이드".

3단계**:** 라이센스 키로 **HCX** 커넥터를 활성화합니다

VMware HCX 커넥터 OVA를 온-프레미스로 배포하고 어플라이언스를 시작한 후 다음 단계를 수행하여 HCX 커넥터를 활성화하십시오. VMC의 VMware HCX 콘솔에서 라이센스 키를 생성하고 VMware HCX Connector 설정 중에 라이센스를 입력합니다.

1. VMware Cloud Console에서 Inventory로 이동하여 SDDC를 선택하고 View Details를 클릭합니다. 추가 기능 탭의 VMware HCX 타일에서 Open HCX를 클릭합니다.
2. 활성화 키 탭에서 활성화 키 생성 을 클릭합니다. 시스템 유형을 HCX 커넥터로 선택하고 확인을 클릭하여 키를 생성합니다. 활성화 키를 복사합니다.



사내에 구축된 각 HCX Connector에는 별도의 키가 필요합니다.

3. 사내 VMware HCX Connector 에 로그인합니다 "https://hcxconnectorIP:9443" 관리자 자격 증명을 사용합니다.

OVA 배포 중에 정의된 암호를 사용합니다.

4. Licensing 섹션에서 2단계에서 복사한 활성화 키를 입력하고 Activate를 클릭합니다.

활성화를 성공적으로 완료하려면 온-프레미스 HCX 커넥터에 인터넷 액세스가 있어야 합니다.

5. Datacenter Location(데이터 센터 위치) 에서 VMware HCX Manager를 설치할 위치를 지정합니다. 계속 을 클릭합니다.
6. 시스템 이름 에서 이름을 업데이트하고 계속 을 클릭합니다.
7. 예 를 선택한 다음 계속 을 선택합니다.
8. vCenter 연결 에서 vCenter Server에 대한 IP 주소 또는 FQDN(정규화된 도메인 이름) 및 자격 증명을 제공하고 계속 을 클릭합니다.

나중에 통신 문제를 방지하려면 FQDN을 사용합니다.

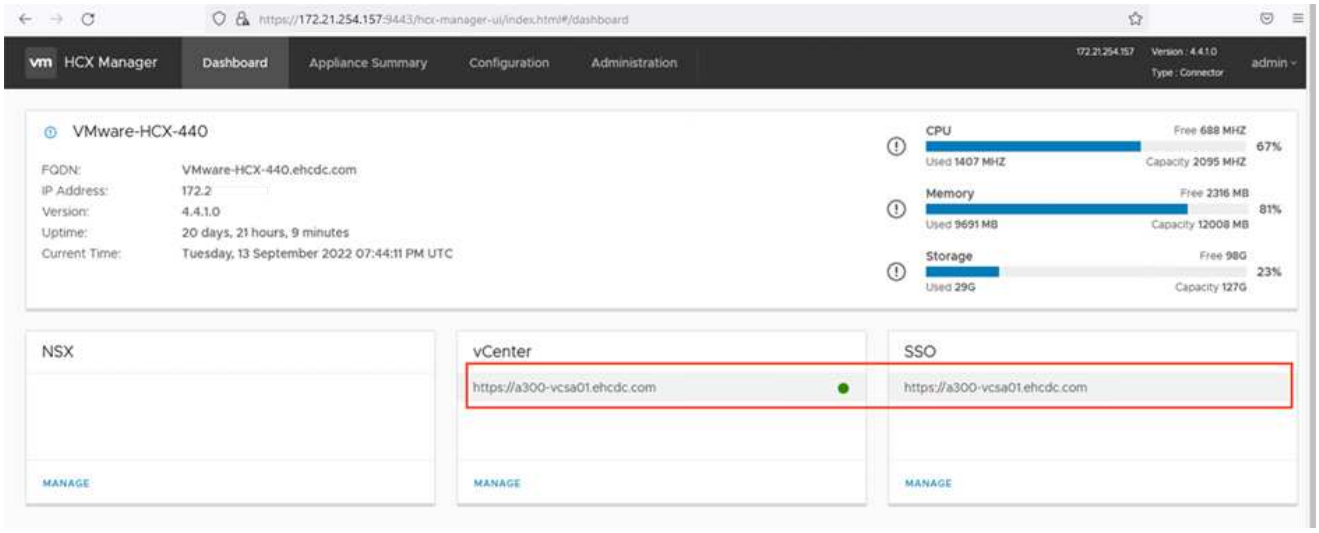
9. SSO/PSC 구성에서 플랫폼 서비스 컨트롤러의 FQDN 또는 IP 주소를 제공하고 계속을 클릭합니다.

vCenter Server의 IP 주소 또는 FQDN을 입력합니다.

10. 정보가 올바르게 입력되었는지 확인하고 다시 시작 을 클릭합니다.
11. 완료되면 vCenter Server가 녹색으로 표시됩니다. vCenter Server와 SSO 모두 올바른 구성 매개 변수를

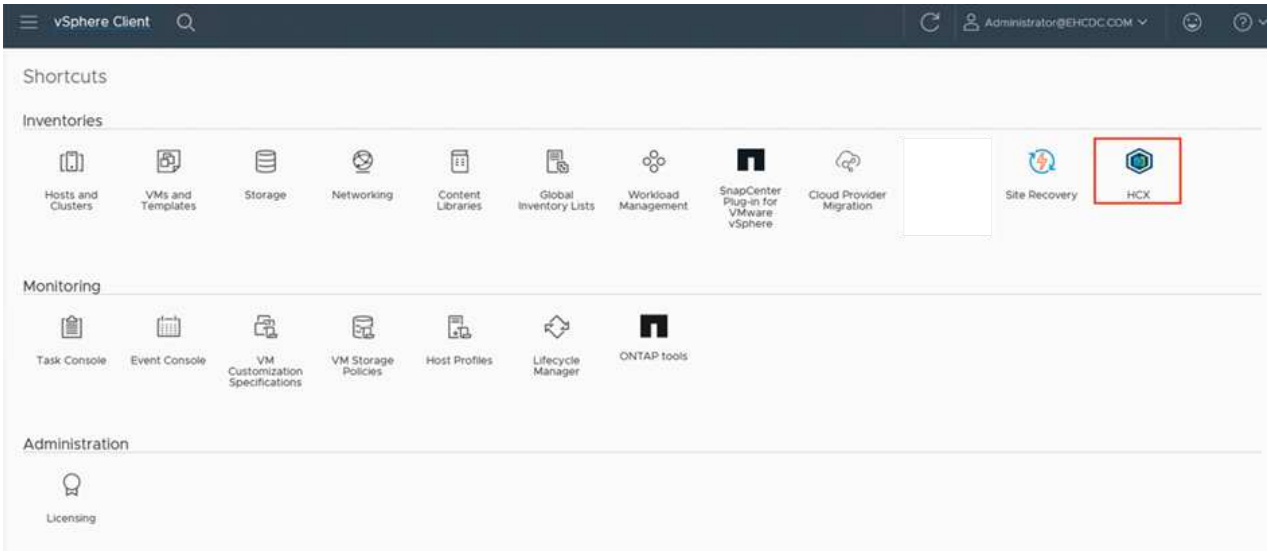
가져야 하며, 이는 이전 페이지와 동일해야 합니다.

이 프로세스는 약 10~20분 정도 소요되며 플러그인이 vCenter Server에 추가되어야 합니다.

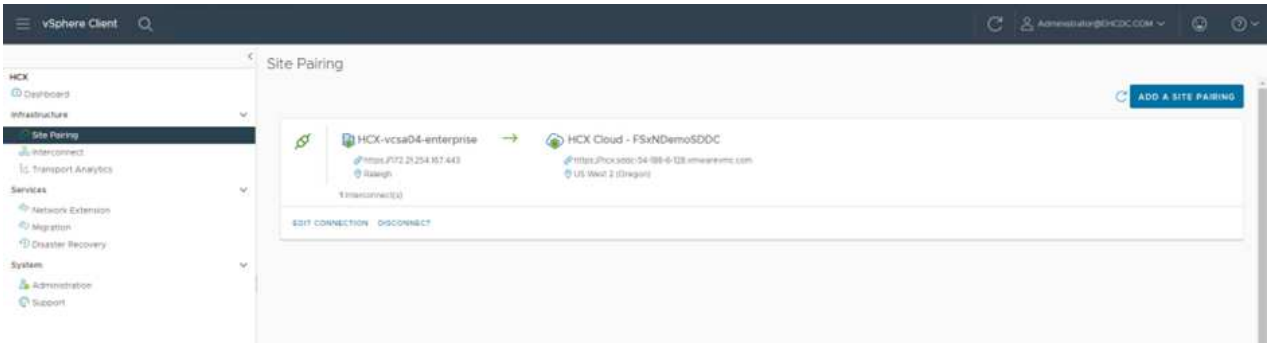


4단계**:** 사내 **VMware HCX Connector**와 **VMC HCX Cloud Manager**를 페어링합니다

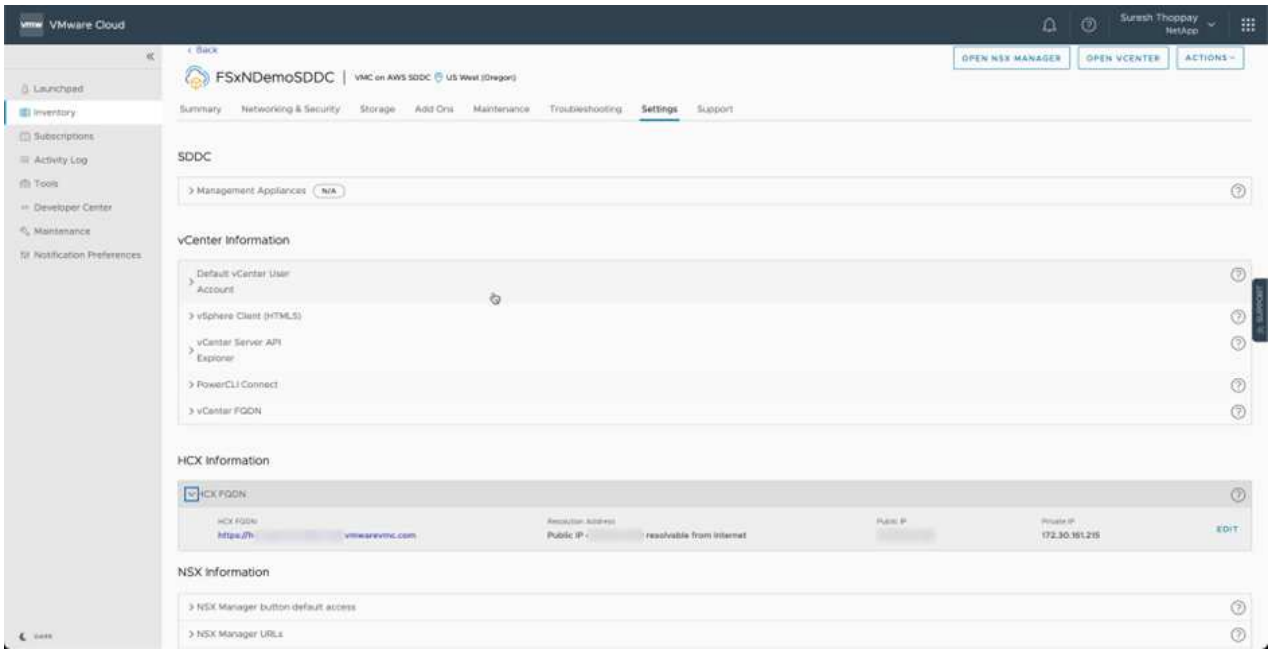
1. 온-프레미스 vCenter Server와 VMC SDDC 간에 사이트 쌍을 생성하려면 온-프레미스 vCenter Server에 로그인하고 HCX vSphere Web Client 플러그인에 액세스합니다.

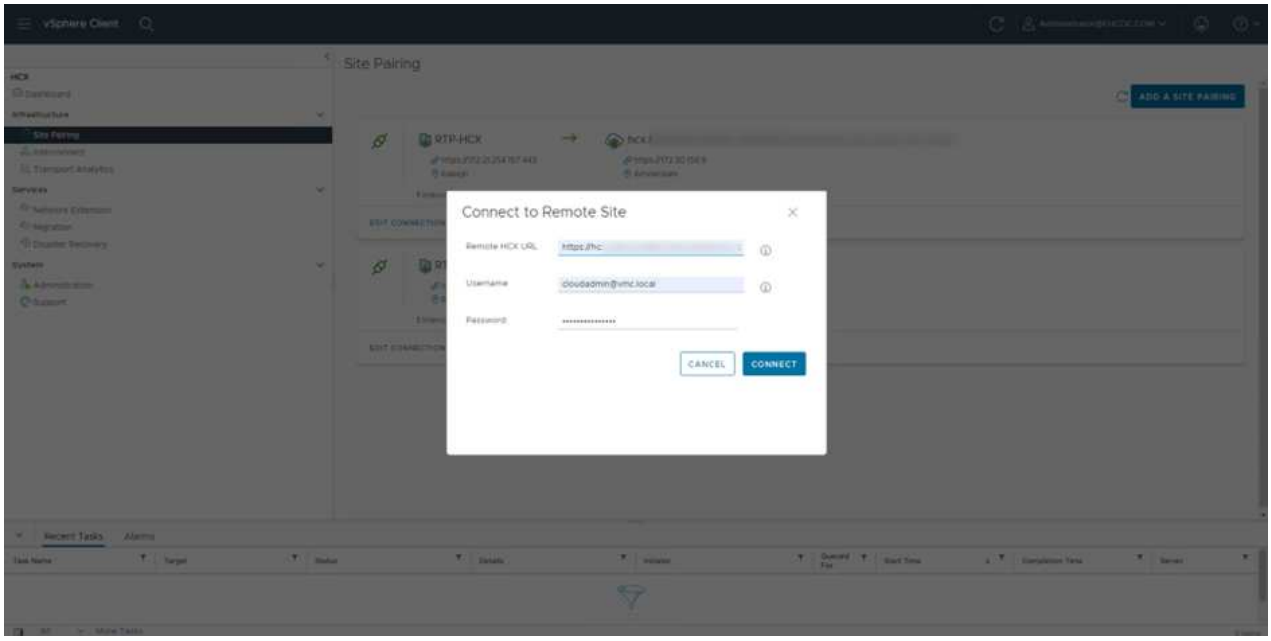


2. 인프라 에서 사이트 페어링 추가 를 클릭합니다. 원격 사이트를 인증하려면 VMC HCX Cloud Manager URL 또는 IP 주소와 CloudAdmin 역할의 자격 증명을 입력합니다.



HCX 정보는 SDDC 설정 페이지에서 검색할 수 있습니다.





3. 사이트 페어링을 시작하려면 연결 을 클릭합니다.

> VMware HCX Connector는 포트 443을 통해 HCX Cloud Manager IP와 통신할 수 있어야 합니다.

4. 페어링이 생성된 후에는 새로 구성된 사이트 페어링을 HCX 대시보드에서 사용할 수 있습니다.

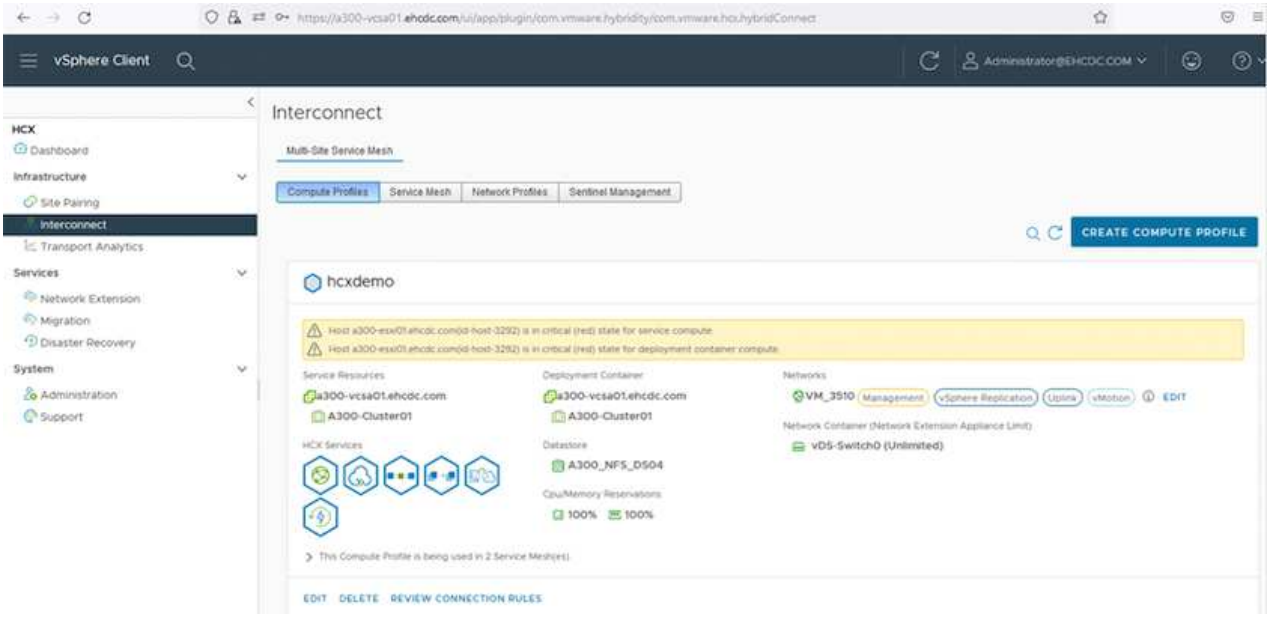
5단계**:** 네트워크 프로파일**,** 컴퓨팅 프로파일 및 서비스 메시를 구성합니다

VMware HCX-IX(HCX Interconnect) 어플라이언스는 인터넷을 통해 보안 터널 기능을 제공하고 타겟 사이트에 대한 프라이빗 연결을 통해 복제 및 vMotion 기반 기능을 지원합니다. 상호 연결은 암호화, 트래픽 엔지니어링 및 SD-WAN을 제공합니다. HCI-IX 상호 연결 어플라이언스를 생성하려면 다음 단계를 수행하십시오.

1. 인프라 에서 상호 연결 > 다중 사이트 서비스 메시 > 컴퓨팅 프로파일 > 컴퓨팅 프로파일 생성 을 선택합니다.

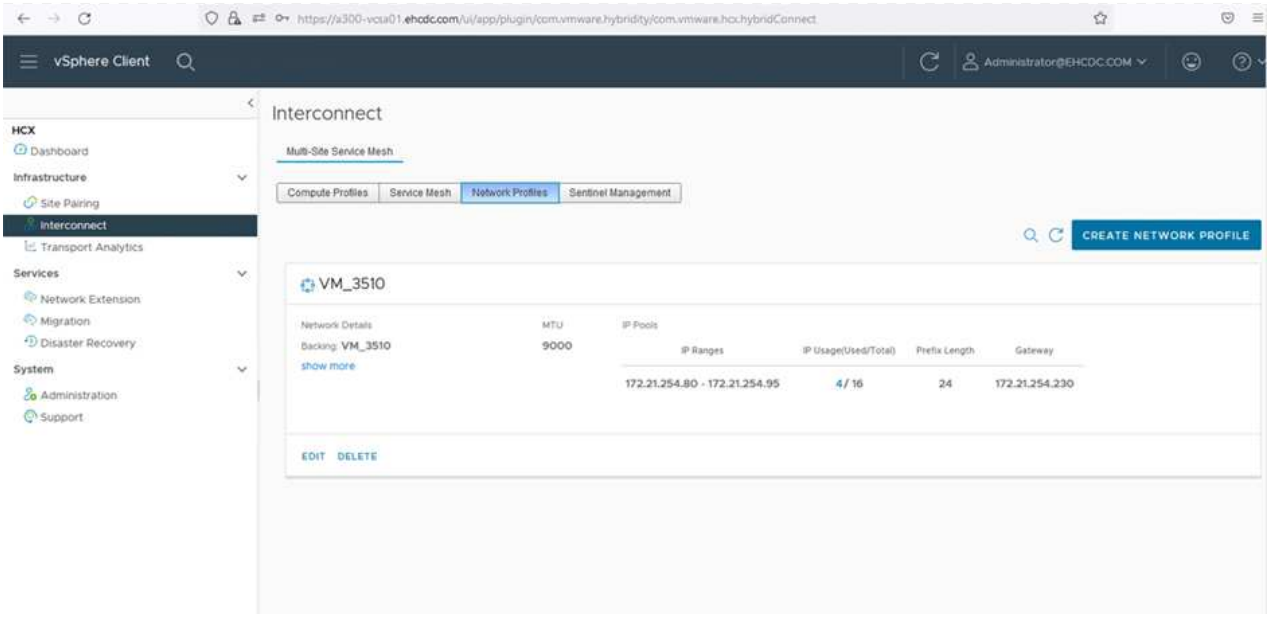
   컴퓨팅 프로파일에는 상호 연결 가상 어플라이언스를 구축하는 데 필요한 컴퓨팅, 스토리지 및 네트워크 구축 매개 변수가 포함됩니다. 또한 VMware 데이터 센터의 어떤 부분을 HCX 서비스에 액세스할 수 있는지도 지정합니다.

   자세한 지침은 을 참조하십시오 "컴퓨팅 프로파일 생성".



2. 컴퓨팅 프로파일을 만든 후 다중 사이트 서비스 메시 > 네트워크 프로파일 > 네트워크 프로파일 만들기를 선택하여 네트워크 프로파일을 만듭니다.
3. 네트워크 프로파일은 HCX가 가상 어플라이언스에 사용할 IP 주소 및 네트워크의 범위를 정의합니다.

   이 경우 두 개 이상의 IP 주소가 필요합니다. 이러한 IP 주소는 관리 네트워크에서 가상 어플라이언스로 할당됩니다.

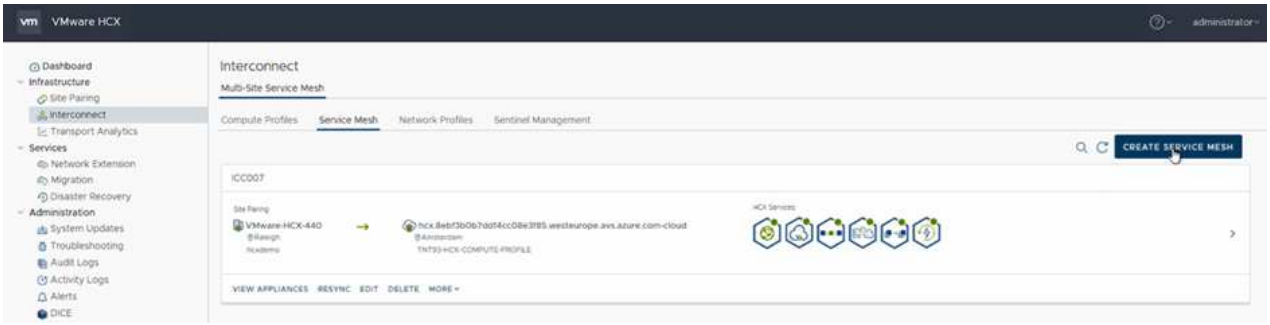


자세한 지침은 을 참조하십시오 "네트워크 프로파일 만들기".

> 인터넷을 통해 SD-WAN에 연결하는 경우 네트워킹 및 보안 섹션에서 공용 IP를 예약해야 합니다.

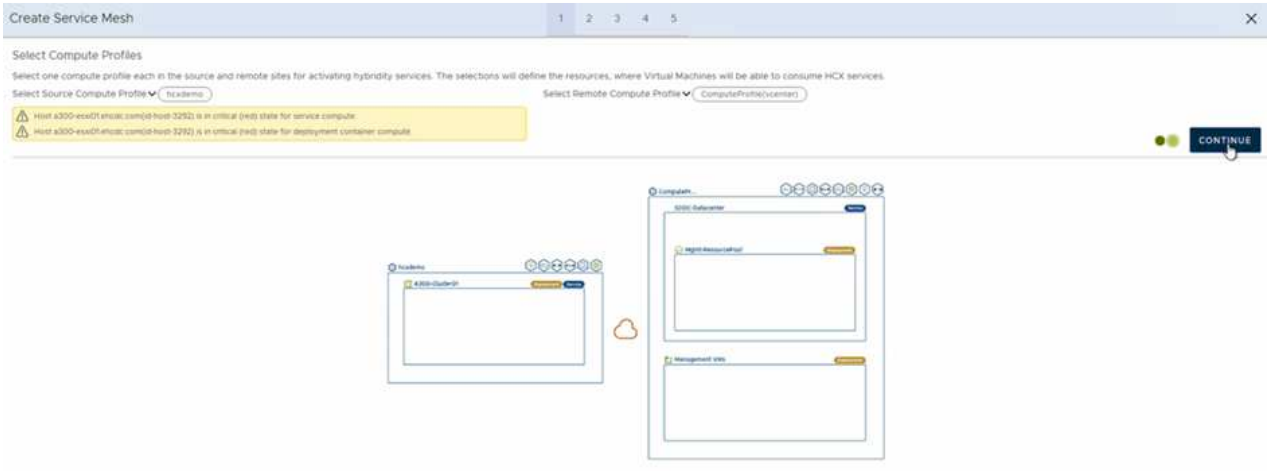
4. 서비스 메시를 생성하려면 상호 연결 옵션에서 서비스 메시 탭을 선택하고 온-프레미스 및 VMC SDDC 사이트를 선택합니다.

   서비스 메시는 로컬 및 원격 계산 및 네트워크 프로파일 쌍을 설정합니다.

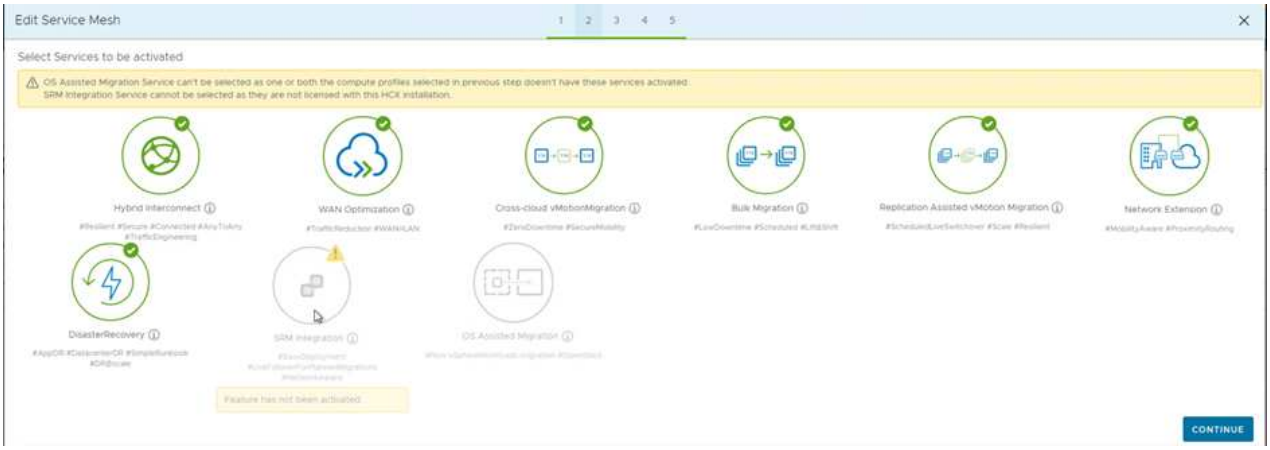


> 이 프로세스의 일환으로 소스 사이트와 타겟 사이트 모두에서 자동으로 구성되는 HCX 어플라이언스를 구축하여 안전한 전송 패브릭을 생성합니다.

5. 소스 및 원격 컴퓨팅 프로파일을 선택하고 계속을 클릭합니다.

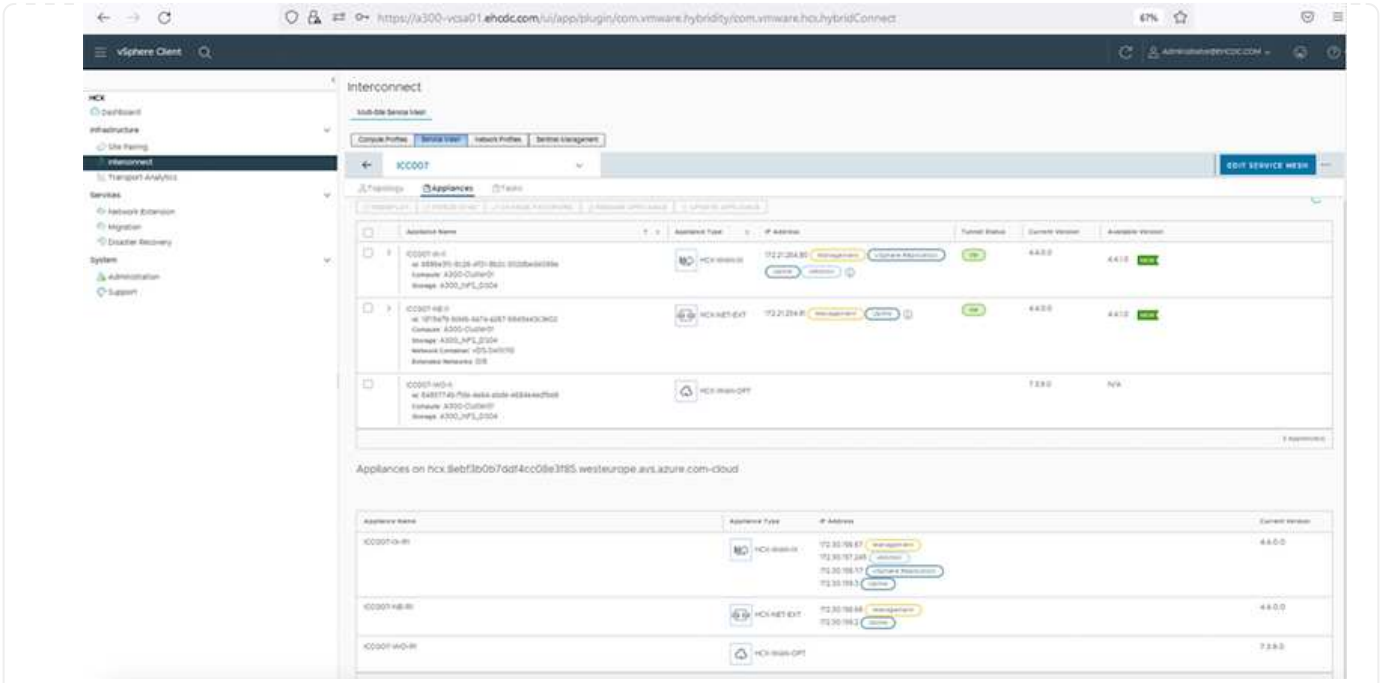


6. 활성화할 서비스를 선택하고 계속 을 클릭합니다.



> Replication Assisted vMotion 마이그레이션, SRM 통합 및 OS 지원 마이그레이션에는 HCX Enterprise 라이센스가 필요합니다.

7. 서비스 메시의 이름을 작성하고 마침을 클릭하여 작성 프로세스를 시작합니다. 배포를 완료하는 데 약 30분이 소요됩니다. 서비스 메시를 구성한 후 워크로드 VM을 마이그레이션하는 데 필요한 가상 인프라 및 네트워킹이 생성되었습니다.


vSphere Client
Interconnect
ICC007
EDIT SERVICE MESH
Appliances
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

6단계: 워크로드 마이그레이션

HCX는 사내 및 VMC SDDC와 같은 둘 이상의 서로 다른 환경 간에 양방향 마이그레이션 서비스를 제공합니다. HCX 대량 마이그레이션, HCX vMotion, HCX 콜드 마이그레이션, HCX Replication Assisted vMotion(HCX Enterprise Edition에서 사용 가능) 및 HCX OS 지원 마이그레이션(HCX Enterprise Edition에서 사용 가능)과 같은 다양한 마이그레이션 기술을 사용하여 HCX 활성 사이트로 애플리케이션 워크로드를 마이그레이션할 수 있습니다.

사용 가능한 HCX 마이그레이션 기술에 대한 자세한 내용은 을 참조하십시오 "VMware HCX 마이그레이션 유형"

HCX-IX 어플라이언스는 Mobility Agent 서비스를 사용하여 vMotion, Cold 및 RAV(Replication Assisted vMotion) 마이그레이션을 수행합니다.

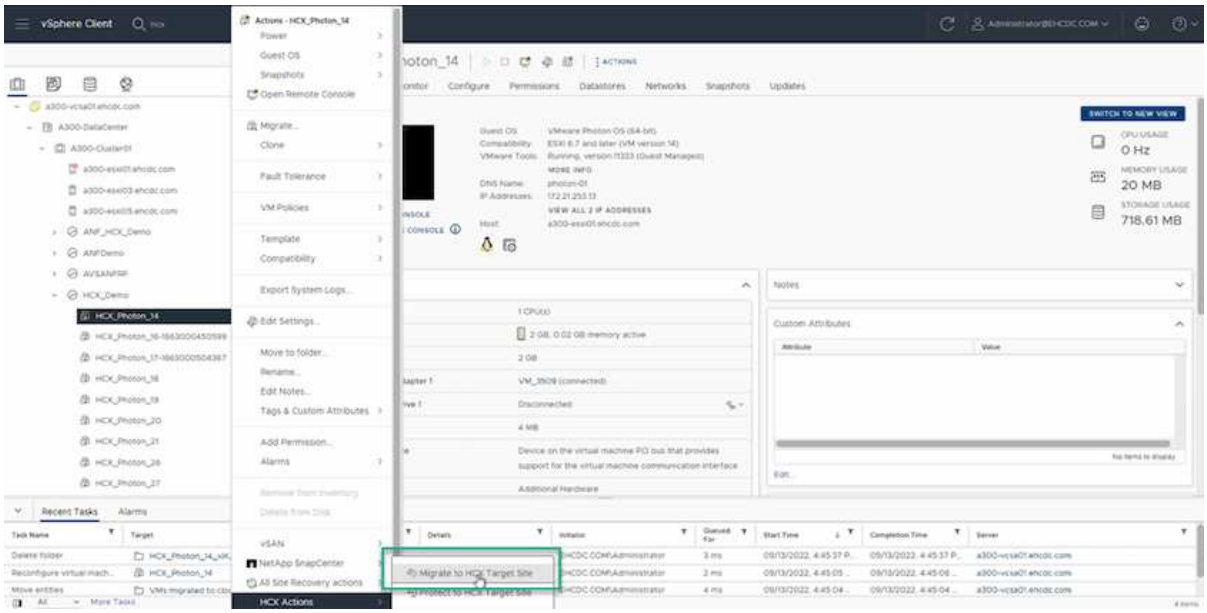
HCX-IX 어플라이언스는 vCenter Server에서 Mobility Agent 서비스를 호스트 개체로 추가합니다. 이 개체에 표시되는 프로세서, 메모리, 스토리지 및 네트워킹 리소스는 IX 어플라이언스를 호스팅하는 물리적 하이퍼바이저의 실제 소비량을 나타내지 않습니다.

VMware HCX vMotion

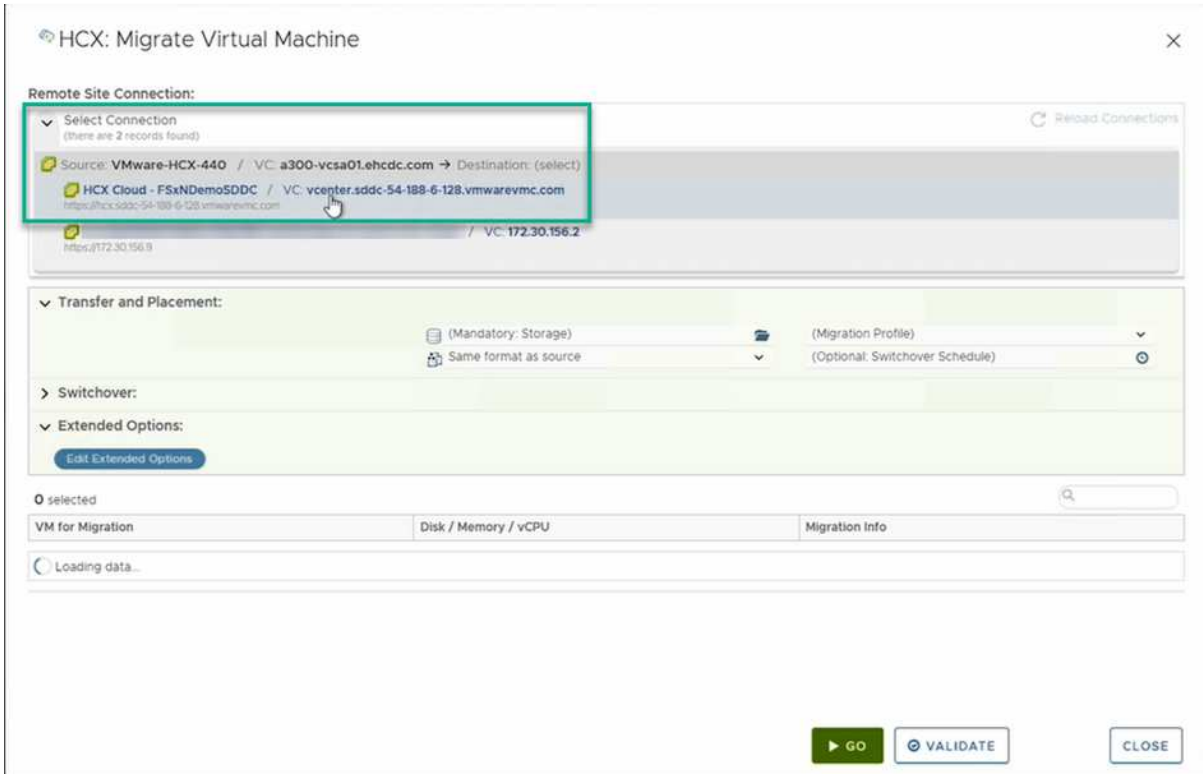
이 섹션에서는 HCX vMotion 메커니즘을 설명합니다. 이 마이그레이션 기술은 VMware vMotion 프로토콜을 사용하여 VM을 VMC SDDC로 마이그레이션합니다. vMotion 마이그레이션 옵션은 한 번에 하나의 VM의 VM 상태를 마이그레이션하는 데 사용됩니다. 이 마이그레이션 방법 중에는 서비스가 중단되지 않습니다.

IP 주소를 변경할 필요 없이 VM을 마이그레이션하려면 네트워크 확장이 있어야 합니다 (VM이 연결된 포트 그룹의 경우).

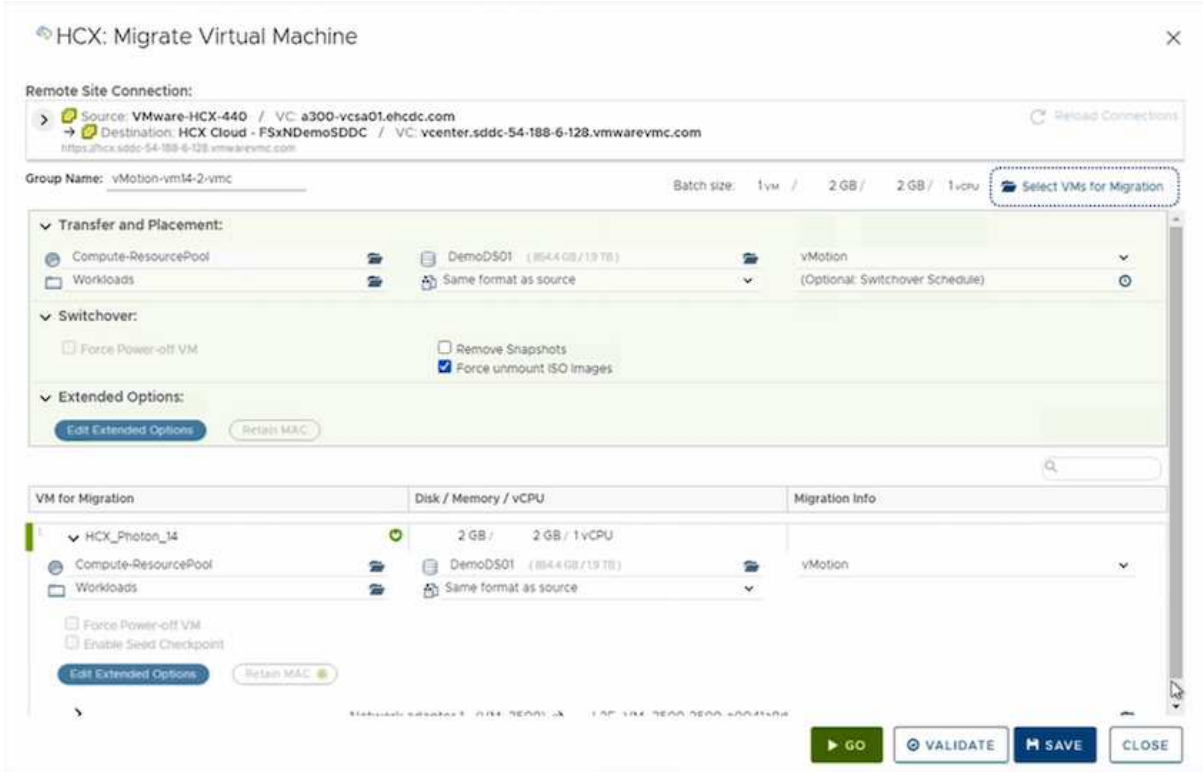
1. 온-프레미스 vSphere Client에서 Inventory로 이동하여 마이그레이션할 VM을 마우스 오른쪽 버튼으로 클릭하고 HCX Actions > Migrate to HCX Target Site를 선택합니다.



2. 가상 시스템 마이그레이션 마법사에서 원격 사이트 연결(타겟 VMC SDDC)을 선택합니다.



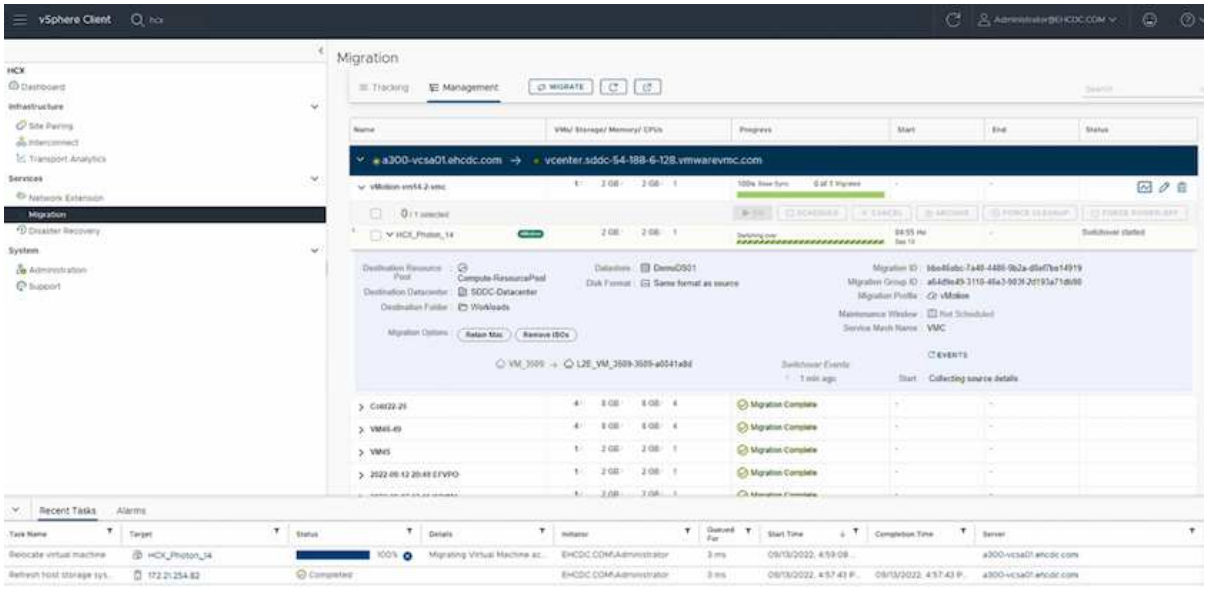
3. 그룹 이름을 추가하고 전송 및 배치에서 필수 필드(클러스터, 스토리지 및 대상 네트워크)를 업데이트한 후 유효성 검사를 클릭합니다.



4. 유효성 검사가 완료된 후 이동을 클릭하여 마이그레이션을 시작합니다.

vMotion 전송은 VM 활성 메모리, 실행 상태, IP 주소 및 MAC 주소를 캡처합니다. HCX vMotion의 요구 사항 및 제한 사항에 대한 자세한 내용은 을 참조하십시오 "VMware HCX vMotion 및 콜드 마이그레이션 이해".

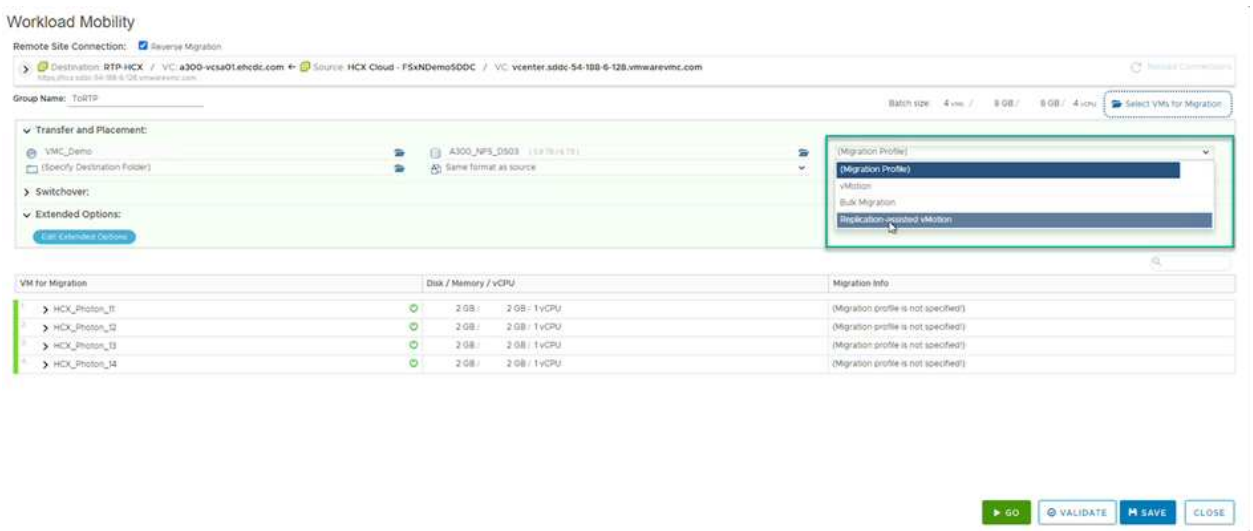
5. HCX > 마이그레이션 대시보드에서 vMotion의 진행 상황과 완료 상태를 모니터링할 수 있습니다.



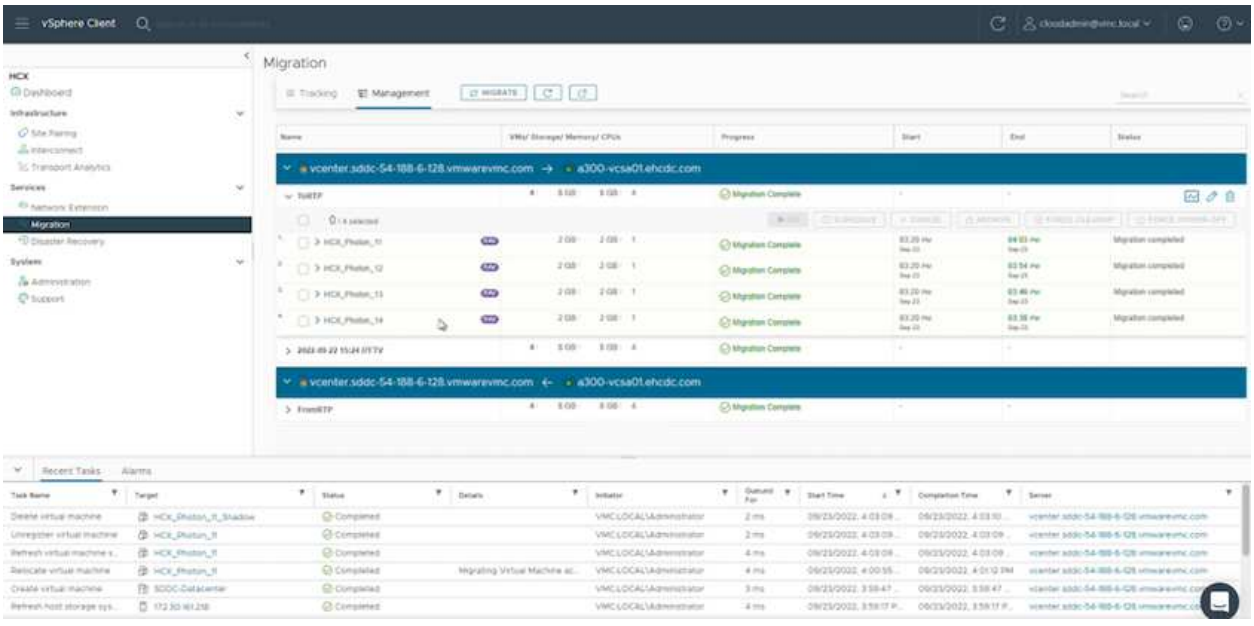
VMware Replication Assisted vMotion을 참조하십시오

VMware 문서에서 이미 알아보았듯이 VMware HCX RAV(Replication Assisted vMotion)는 대량 마이그레이션과 vMotion의 이점을 결합합니다. 대량 마이그레이션에서는 vSphere Replication을 사용하여 여러 VM을 병렬로 마이그레이션합니다. 전환 중에 VM이 재부팅됩니다. HCX vMotion은 다운타임 없이 마이그레이션되지만 복제 그룹에서 한 번에 한 VM에 대해 순차적으로 수행됩니다. RAV는 VM을 병렬로 복제하며 절체 윈도우가 될 때까지 동기화 상태를 유지합니다. 전환 프로세스 중에 VM의 다운타임 없이 한 번에 하나의 VM을 마이그레이션합니다.

다음 스크린샷은 마이그레이션 프로필을 Replication Assisted vMotion으로 보여 줍니다.



복제 기간은 소수의 VM의 vMotion에 비해 더 길어질 수 있습니다. RAV에서는 델타만 동기화하고 메모리 내용을 포함시키십시오. 다음은 마이그레이션 상태의 스크린샷입니다. 이 스크린샷은 마이그레이션의 시작 시간이 동일하고 각 VM에 대한 종료 시간이 어떻게 다른지 보여 줍니다.



HCX 마이그레이션 옵션 및 HCX를 사용하여 워크로드를 온프레미스에서 VMware Cloud on AWS로 마이그레이션하는 방법에 대한 자세한 내용은 를 참조하십시오 "VMware HCX 사용자 가이드".

VMware HCX vMotion에는 100Mbps 이상의 처리량 기능이 필요합니다.

ONTAP 데이터 저장소용 타겟 VMC FSx에 마이그레이션을 수용할 수 있는 충분한 공간이 있어야 합니다.

결론

사내 모든 유형/공급업체 스토리지에 상주하는 데이터를 클라우드 또는 하이브리드 클라우드에 배치하든, AWS ONTAP용 Amazon FSx와 HCX는 애플리케이션 계층에 대한 데이터 요구 사항을 원활하게 만들어 워크로드를 구축 및 마이그레이션하는 동시에 TCO를 절감하는 탁월한 옵션을 제공합니다. 어떤 사용 사례에서든 VMC와 FSx for ONTAP 데이터 저장소를 함께 사용하여 사내 및 멀티 클라우드 전체의 클라우드 이점, 일관된 인프라 및 운영을 빠르게 실현하고, 워크로드의 양방향 이동성을 실현하며, 엔터프라이즈급 용량과 성능을 실현할 수 있습니다. VMware vSphere 복제, VMware vMotion 또는 NFC 복사를 사용하여 스토리지를 연결하고 VM을 마이그레이션하는 데 사용되는 익숙한 프로세스와 절차가 동일합니다.

이점

이 문서의 핵심 사항은 다음과 같습니다.

- 이제 Amazon FSx ONTAP를 VMC SDDC의 데이터 저장소로 사용할 수 있습니다.
- 모든 사내 데이터 센터에서 FSx for ONTAP 데이터 저장소를 사용하여 실행 중인 VMC로 데이터를 쉽게 마이그레이션할 수 있습니다
- 마이그레이션 작업 중에 용량 및 성능 요구 사항을 충족하도록 FSx ONTAP 데이터 저장소를 쉽게 확장 및 축소할 수 있습니다.

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 웹 사이트 링크를 참조하십시오.

- VMware 클라우드 설명서

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- NetApp ONTAP용 Amazon FSx 문서

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  VMware HCX 사용자 가이드

- "https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

지역 가용성 **– VMC**용 보조 **NFS** 데이터 저장소

AWS/VMC에서 보조 NFS 데이터 저장소를 사용할 수 있는 가용성은 Amazon에서 정의합니다. 먼저, VMC와 FSxN을 모두 지정된 지역에서 사용할 수 있는지 확인해야 합니다. 그런 다음 해당 지역에서 FSxN 보조 NFS 데이터 저장소가 지원되는지 여부를 확인해야 합니다.

- VMC의 가용성을 확인합니다 "여기".

- 아마존의 가격 책정 가이드에서는 FSxN(FSx ONTAP)을 사용할 수 있는 위치에 대한 정보를 제공합니다. 해당 정보를 찾을 수 있습니다 "여기".
- VMC에 대한 FSxN 보조 NFS 데이터 저장소의 가용성이 곧 제공될 예정입니다.

정보가 아직 릴리즈되는 동안 다음 차트는 VMC, FSxN 및 FSxN에 대한 현재 지원을 보조 NFS 데이터 저장소로 식별합니다.

미주

* AWS 지역 *	* VMC 가용성 *	* FSx ONTAP 가용성 *	* NFS 데이터 저장소 가용성 *
미국 동부(노던 버지니아)	예	예	예
미국 동부(오하이오)	예	예	예
미국 서부(캘리포니아 북부)	예	아니요	아니요
미국 서부(오리건주)	예	예	예
GovCloud(미국 서부)	예	예	예
캐나다(중부)	예	예	예
남아메리카(상파울루)	예	예	예

마지막 업데이트: 2022년 6월 2일.

유럽

* AWS 지역 *	* VMC 가용성 *	* FSx ONTAP 가용성 *	* NFS 데이터 저장소 가용성 *
유럽(아일랜드)	예	예	예
유럽(런던)	예	예	예
유럽(프랑크푸르트)	예	예	예
유럽(파리)	예	예	예
유럽(밀라노)	예	예	예
유럽(스톡홀름)	예	예	예

마지막 업데이트: 2022년 6월 2일.

아시아 태평양

* AWS 지역 *	* VMC 가용성 *	* FSx ONTAP 가용성 *	* NFS 데이터 저장소 가용성 *
아시아 태평양(시드니)	예	예	예
아시아 태평양(도쿄)	예	예	예
아시아 태평양(오사카)	예	아니요	아니요
아시아 태평양(싱가포르)	예	예	예
아시아 태평양(서울)	예	예	예
아시아 태평양(뭄바이)	예	예	예
아시아 태평양(자카르타)	아니요	아니요	아니요
아시아 태평양(홍콩)	예	예	예

마지막 업데이트: 2022년 9월 28일.

Azure AVS용 NetApp 기능

NetApp이 AVS(Azure VMware Solution)에 제공하는 기능에 대해 자세히 알아보십시오. NetApp은 게스트 연결 스토리지 장치로, 보충 NFS 데이터 저장소에서 마이그레이션 워크플로우에 전환, 클라우드로 확장/버스팅, 백업/복원, 재해 복구까지 지원합니다.

다음 옵션 중 하나를 선택하여 원하는 콘텐츠의 섹션으로 이동합니다.

- "Azure에서 AVS 구성"
- "AVS용 NetApp 스토리지 옵션"
- "NetApp/VMware 클라우드 솔루션"

Azure에서 AVS 구성

온프레미스에서와 마찬가지로 클라우드 기반 가상화 환경을 계획하는 것은 VM 및 마이그레이션을 생성할 수 있는 성공적인 프로덕션 준비 환경에 매우 중요합니다.

이 섹션에서는 Azure VMware 솔루션을 설정 및 관리하고 NetApp 스토리지를 연결하는 데 사용할 수 있는 옵션과 함께 사용하는 방법을 설명합니다.

게스트 내 스토리지는 Cloud Volumes ONTAP를 Azure VMware 솔루션에 연결하는 유일한 지원 방법입니다.

설치 프로세스는 다음 단계로 나눌 수 있습니다.

- 리소스 공급자를 등록하고 프라이빗 클라우드를 생성합니다
- 새 또는 기존 ExpressRoute 가상 네트워크 게이트웨이에 연결합니다
- 네트워크 연결을 확인하고 프라이빗 클라우드에 액세스합니다

자세한 내용을 확인하십시오 "AVS의 구성 단계".

AVS용 NetApp 스토리지 옵션

NetApp 스토리지는 Azure AVS에서 guess Connected 또는 보충 NFS 데이터 저장소로 여러 가지 방법으로 활용할 수 있습니다.

를 방문하십시오 "지원되는 NetApp 스토리지 옵션" 를 참조하십시오.

Azure는 다음과 같은 구성에서 NetApp 스토리지를 지원합니다.

- 게스트 연결 스토리지로서의 Azure NetApp Files(ANF)
- CVO(Cloud Volumes ONTAP)를 게스트 연결 스토리지로 사용합니다
- Azure NetApp Files(ANF)를 보조 NFS 데이터 저장소로 사용합니다

자세한 내용을 확인하십시오 "AVS용 게스트 연결 스토리지 옵션". 자세한 내용을 확인하십시오 "AVS용 보조 NFS

데이터 저장소 옵션".

솔루션 사용 사례

NetApp 및 VMware 클라우드 솔루션을 사용하면 많은 사용 사례를 Azure AVS에서 간단하게 구축할 수 있습니다. SE 사례는 VMware에서 정의한 각 클라우드 영역에 대해 정의됩니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 확장
- 마이그레이션

"Azure AVS용 NetApp 솔루션을 찾아보십시오"

Azure/AVS에서 워크로드 보호

ANF 및 **Jetstream**을 통한 재해 복구

클라우드로 재해 복구는 사이트 운영 중단 및 데이터 손상 이벤트(예: 랜섬웨어)로부터 워크로드를 보호하는 복원력이 있고 비용 효율적인 방법입니다. VMware VAIO 프레임워크를 사용하여 온프레미스 VMware 워크로드를 Azure Blob 스토리지에 복제하고 복구하여 데이터 손실과 제로급 RTO를 최소화하거나 최소화할 수 있습니다.

Jetstream DR을 사용하면 사내에서 AVS로, 특히 Azure NetApp Files로 복제된 워크로드를 원활하게 복구할 수 있습니다. DR 사이트에서 최소한의 리소스와 비용 효율적인 클라우드 스토리지를 사용하여 비용 효율적으로 재해 복구를 수행할 수 있습니다. Jetstream DR은 Azure Blob Storage를 통해 ANF 데이터 저장소에 대한 복구를 자동화합니다. Jetstream DR은 네트워크 매핑에 따라 독립적인 VM 또는 관련 VM 그룹을 복구 사이트 인프라로 복구하고 랜섬웨어 보호를 위한 시점 복구를 제공합니다.

이 문서에서는 Jetstream DR 운영 원리 및 주요 구성 요소에 대해 설명합니다.

1. 사내 데이터 센터에 Jetstream DR 소프트웨어를 설치합니다.
   a. Azure Marketplace(ZIP)에서 Jetstream DR 소프트웨어 번들을 다운로드하고 지정된 클러스터에 Jetstream DR MSA(OVA)를 배포합니다.
   b. I/O 필터 패키지를 사용하여 클러스터를 구성합니다(Jetstream VIB 설치).
   c. DR AVS 클러스터와 동일한 영역에서 Azure Blob(Azure Storage Account)를 프로비저닝합니다.
   d. DRVA 어플라이언스를 구축하고 복제 로그 볼륨(기존 데이터 저장소 또는 공유 iSCSI 스토리지의 VMDK)을 할당합니다.
   e. 보호된 도메인(관련 VM 그룹)을 생성하고 DRVA 및 Azure Blob Storage/ANF를 할당합니다.
   f. 보호를 시작합니다.
2. Azure VMware Solution 프라이빗 클라우드에 Jetstream DR 소프트웨어를 설치합니다.
   a. 실행 명령을 사용하여 Jetstream DR을 설치 및 구성합니다.
   b. 동일한 Azure Blob 컨테이너를 추가하고 Scan Domains 옵션을 사용하여 도메인을 검색합니다.
   c. 필요한 DRVA 어플라이언스를 배포합니다.
   d. 사용 가능한 vSAN 또는 ANF 데이터 저장소를 사용하여 복제 로그 볼륨을 생성합니다.
   e. 보호된 도메인을 가져오고 RockVA(복구 VA)를 구성하여 VM 배치에 ANF 데이터 저장소를 사용합니다.
   f. 적절한 페일오버 옵션을 선택하고 제로급 RTO 도메인 또는 VM에 대한 연속 재수화를 시작합니다.
3. 재해 이벤트 중에 지정된 AVS DR 사이트에서 Azure NetApp Files 데이터 저장소로 장애 조치를 트리거합니다.
4. 보호된 사이트를 복구한 후 보호된 사이트에 대한 페일백을 호출합니다. 시작하기 전에 이 지침에 따라 사전 요구 사항이 충족되는지 확인합니다 "링크" 또한 Jetstream Software에서 제공하는 BWT(대역폭 테스트 도구)를 실행하여 Jetstream DR 소프트웨어와 함께 사용할 경우 Azure Blob 스토리지의 잠재적 성능과 해당 복제 대역폭을 평가합니다. 연결을 포함한 사전 요구 사항이 준비된 후에는 에서 Jetstream DR for AVS를 설정하고 구독하십시오 "Azure 마켓플레이스 를 참조하십시오". 소프트웨어 번들을 다운로드한 후 위에 설명된 설치 프로세스를 진행합니다.

많은 수의 VM(예: 100+)에 대한 보호를 계획하고 시작할 때는 Jetstream DR Automation Toolkit의 CPT(Capacity Planning Tool)를 사용하십시오. RTO 및 복구 그룹 기본 설정과 함께 보호할 VM 목록을 제공한 다음 CPT를 실행합니다.

CPT는 다음과 같은 기능을 수행합니다.

- RTO에 따라 VM을 보호 도메인에 결합합니다.
- 최적의 DRVA 수 및 해당 리소스 정의
- 필요한 복제 대역폭을 추정하는 중입니다.
- 복제 로그 볼륨 특성(용량, 대역폭 등) 식별
- 필요한 오브젝트 스토리지 용량을 예측하는 등

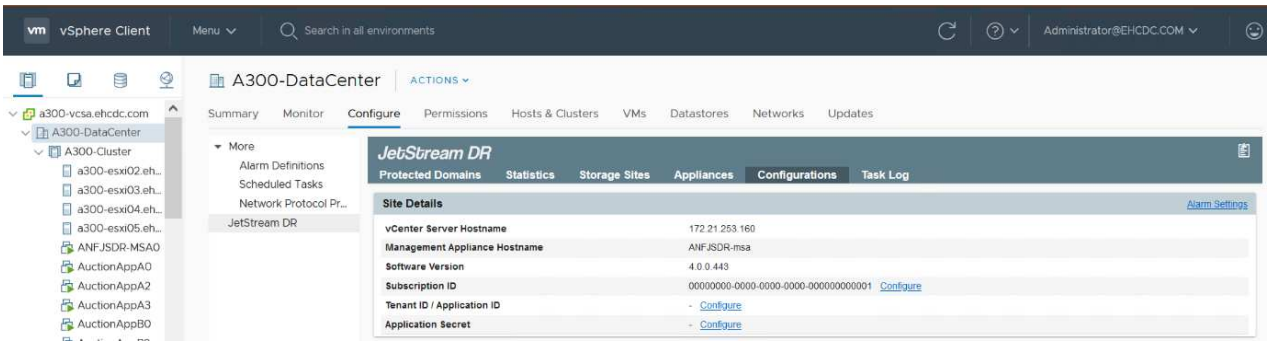
규정된 도메인의 수와 컨텐츠는 평균 IOPS, 총 용량, 우선 순위(페일오버 순서를 정의하는 경우), RTO 등과 같은 다양한 VM 특성에 따라 달라집니다.

온프레미스 데이터 센터에 **Jetstream DR**을 설치합니다

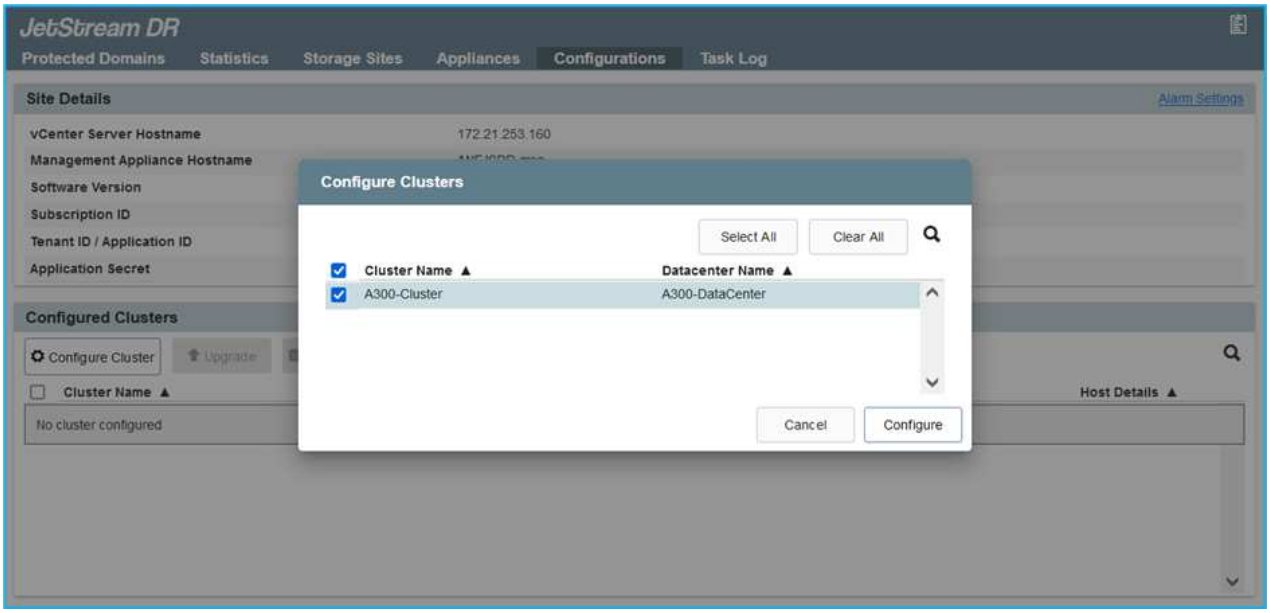
Jetstream DR 소프트웨어는 Jetstream DR Management Server Virtual Appliance(MSA), DR 가상 어플라이언스(DRVA) 및 호스트 구성 요소(I/O 필터 패키지)의 세 가지 주요 구성 요소로 구성됩니다. MSA는 컴퓨팅 클러스터에 호스트 구성 요소를 설치 및 구성한 다음 Jetstream DR 소프트웨어를 관리하는 데 사용됩니다. 다음 목록에는 설치 프로세스에 대한 자세한 설명이 나와 있습니다.

구내 **Jetstream DR**을 설치하는 방법

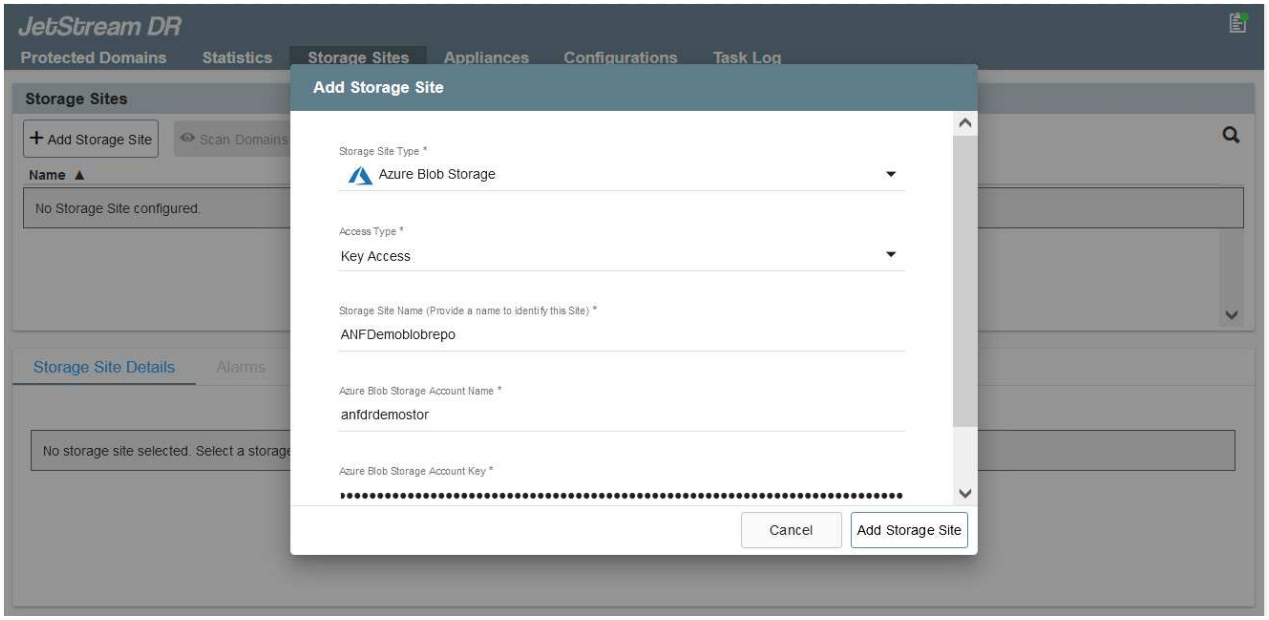
1. 필수 구성 요소를 확인하십시오.
2. 리소스 및 구성 권장 사항에 대해 용량 계획 툴을 실행합니다(선택 사항이지만 개념 증명 평가에는 권장됨).
3. Jetstream DR MSA를 지정된 클러스터의 vSphere 호스트에 구축합니다.
4. 브라우저에서 DNS 이름을 사용하여 MSA를 실행합니다.
5. MSA에 vCenter Server를 등록합니다. 설치를 수행하려면 다음 세부 단계를 완료하십시오.
6. Jetstream DR MSA를 구축하고 vCenter Server를 등록한 후에는 vSphere Web Client를 사용하여 Jetstream DR 플러그인에 액세스합니다. 이 작업은 데이터 센터 > 구성 > Jetstream DR로 이동하여 수행할 수 있습니다.



7. Jetstream DR 인터페이스에서 적절한 클러스터를 선택합니다.



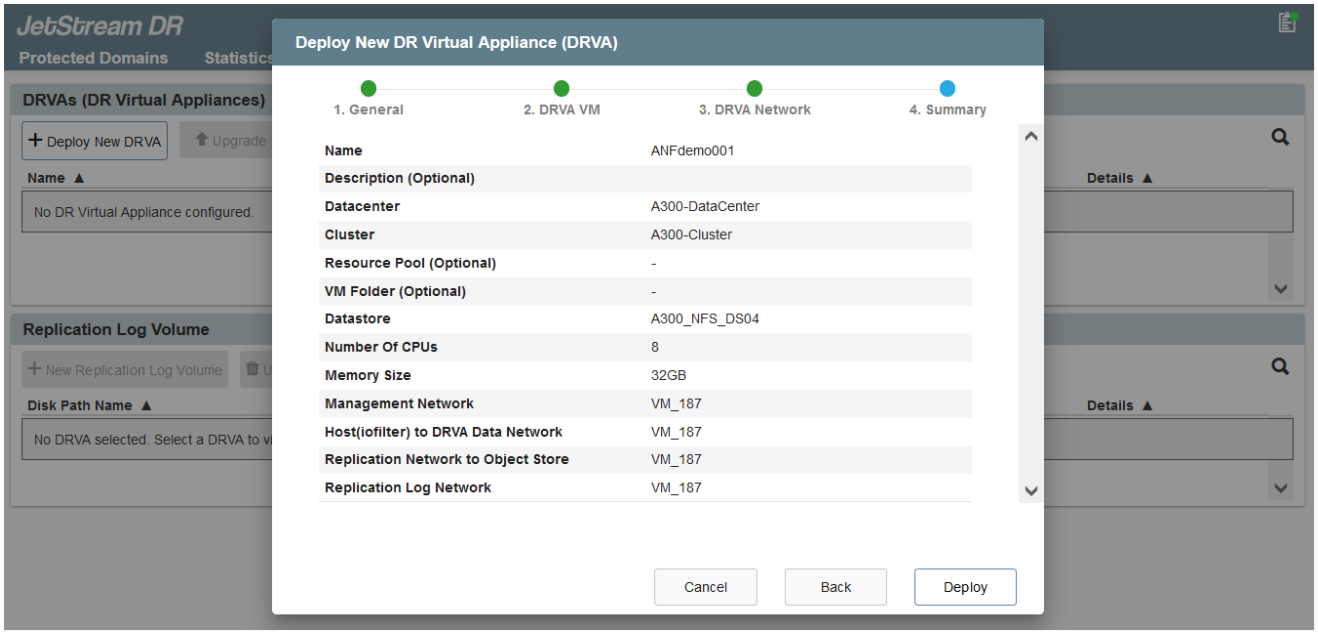
8. I/O 필터 패키지를 사용하여 클러스터를 구성합니다.



9. 복구 사이트에 있는 Azure Blob Storage를 추가합니다.
10. Appliances(어플라이언스) 탭에서 DR Virtual Appliance(DRVA)를 구축합니다.

> DRVA는 CPT에 의해 자동으로 생성될 수 있지만 POC 평가에서는 DR 주기를 수동으로 구성 및 실행하는 것이 좋습니다(시작 보호 > 장애 조치 > 장애 복구).

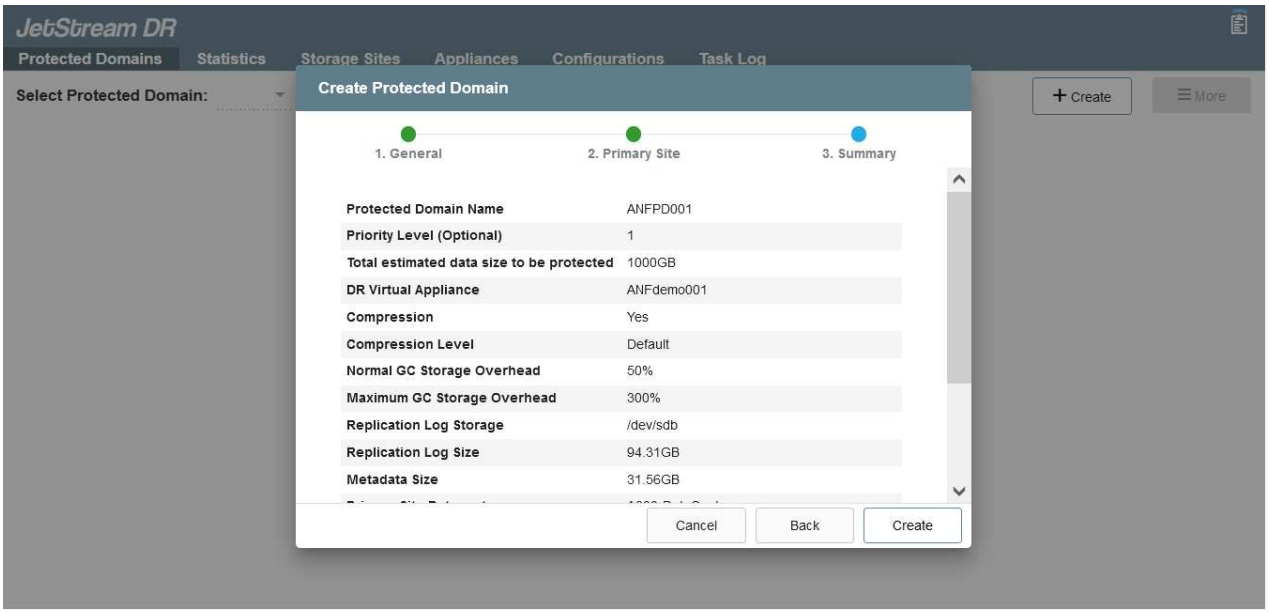
Jetstream DRVA는 데이터 복제 프로세스의 주요 기능을 용이하게 하는 가상 어플라이언스입니다. 보호되는 클러스터에는 DRVA가 하나 이상 포함되어야 하며, 일반적으로 호스트당 DRVA가 하나씩 구성됩니다. 각 DRVA는 여러 개의 보호된 도메인을 관리할 수 있습니다.



이 예에서는 80개의 가상 머신에 대해 4개의 DRVA가 생성되었습니다.

1. 사용 가능한 데이터 저장소 또는 독립 공유 iSCSI 스토리지 풀에서 VMDK를 사용하여 각 DRVA에 대한 복제 로그 볼륨을 생성합니다.

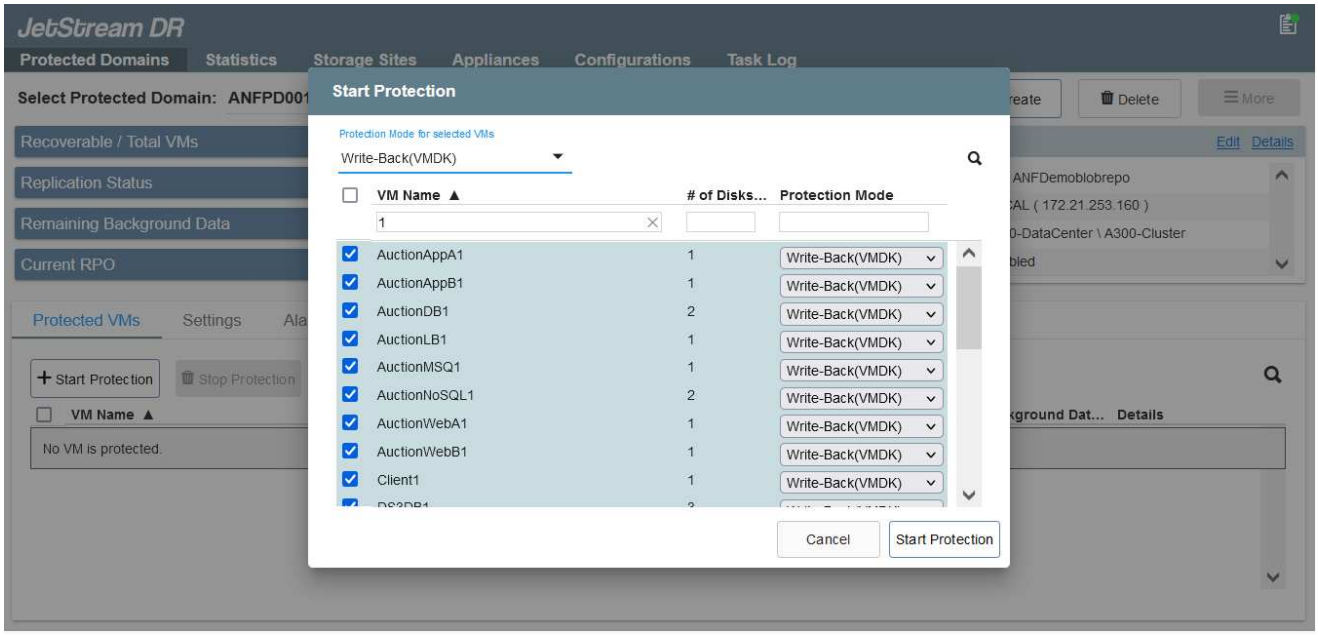
2. 보호 도메인 탭에서 Azure Blob 저장소 사이트, DRVA 인스턴스 및 복제 로그에 대한 정보를 사용하여 필요한 수의 보호된 도메인을 만듭니다. 보호 도메인은 함께 보호되고 장애 조치/장애 복구 작업에 우선 순위가 할당된 클러스터 내의 특정 VM 또는 VM 집합을 정의합니다.



3. 보호할 VM을 선택하고 보호된 도메인의 VM 보호를 시작합니다. 그러면 지정된 Blob 저장소에 대한 데이터 복제가 시작됩니다.

ⓘ 보호 도메인의 모든 VM에 동일한 보호 모드가 사용되는지 확인합니다.

ⓘ VMDK(Write-Back) 모드에서는 더 높은 성능을 제공할 수 있습니다.



복제 로그 볼륨이 고성능 스토리지에 배치되었는지 확인합니다.

페일오버 실행 도서를 구성하여 VM(복구 그룹)을 그룹화하고 부팅 순서 시퀀스를 설정하고 IP 구성과 함께 CPU/메모리 설정을 수정할 수 있습니다.

실행 명령을 사용하여 **Azure VMware** 솔루션 프라이빗 클라우드에 **AVS**용 **Jetstream DR**을 설치합니다

복구 사이트(AVS)의 모범 사례는 3노드 파일럿 라이트 클러스터를 미리 생성하는 것입니다. 이렇게 하면 다음 항목을 포함하여 복구 사이트 인프라를 사전 구성할 수 있습니다.

- 대상 네트워킹 세그먼트, 방화벽, DHCP 및 DNS 등의 서비스 등
- AVS용 Jetstream DR 설치
- ANF 볼륨을 데이터 저장소로 구성하고, moreJetStream DR은 미션 크리티컬 도메인에 대해 제로급 RTO 모드를 지원합니다. 이러한 도메인의 경우 대상 스토리지가 사전 설치되어 있어야 합니다. ANF는 이 경우 권장되는 스토리지 유형입니다.

세그먼트 생성을 포함한 네트워크 구성은 AVS 클러스터에서 사내 요구 사항과 일치하도록 구성해야 합니다.

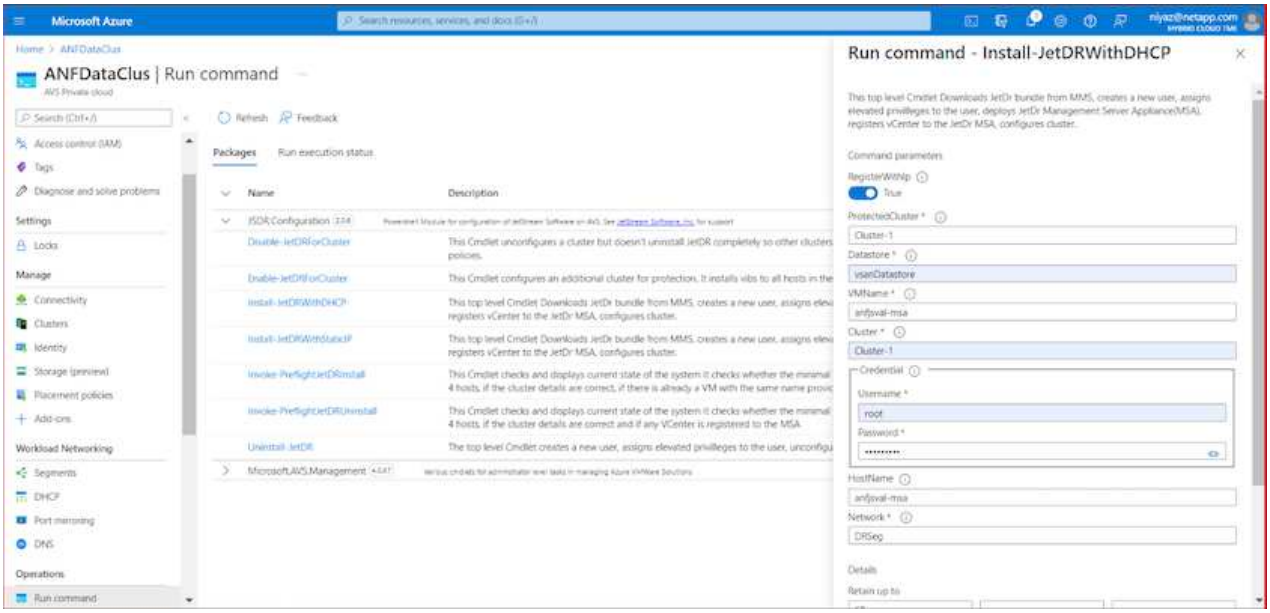
SLA 및 RTO 요구 사항에 따라 지속적인 페일오버 또는 일반(표준) 페일오버 모드를 사용할 수 있습니다. 제로급 RTO의 경우 복구 사이트에서 연속 재수화를 시작해야 합니다.

Azure VMware 솔루션 프라이빗 클라우드에 AVS용 Jetstream DR을 설치하려면 다음 단계를 수행하십시오.

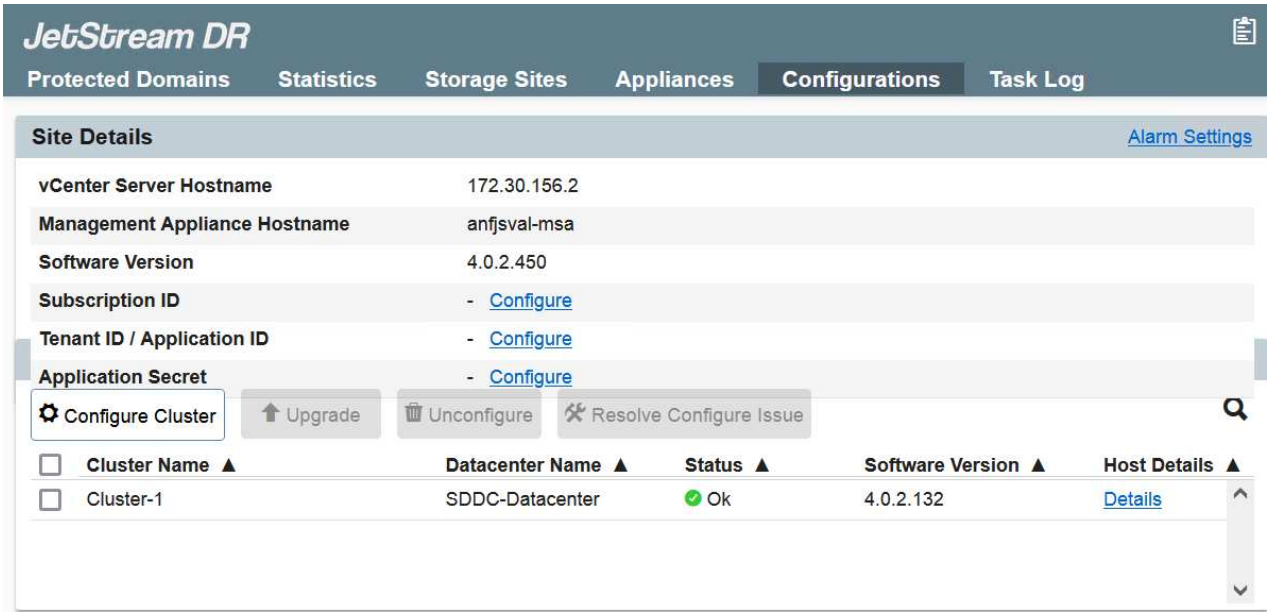
1. Azure 포털에서 Azure VMware 솔루션으로 이동하여 프라이빗 클라우드를 선택한 다음 명령 실행 > 패키지 > JSDR.Configuration을 선택합니다.

> Azure VMware 솔루션의 기본 CloudAdmin 사용자는 AVS용 Jetstream DR을 설치할 권한이 없습니다. Azure VMware 솔루션을 사용하면 Jetstream DR용 Azure VMware 솔루션 실행 명령을 호출하여 Jetstream DR을 간단하고 자동으로 설치할 수 있습니다.

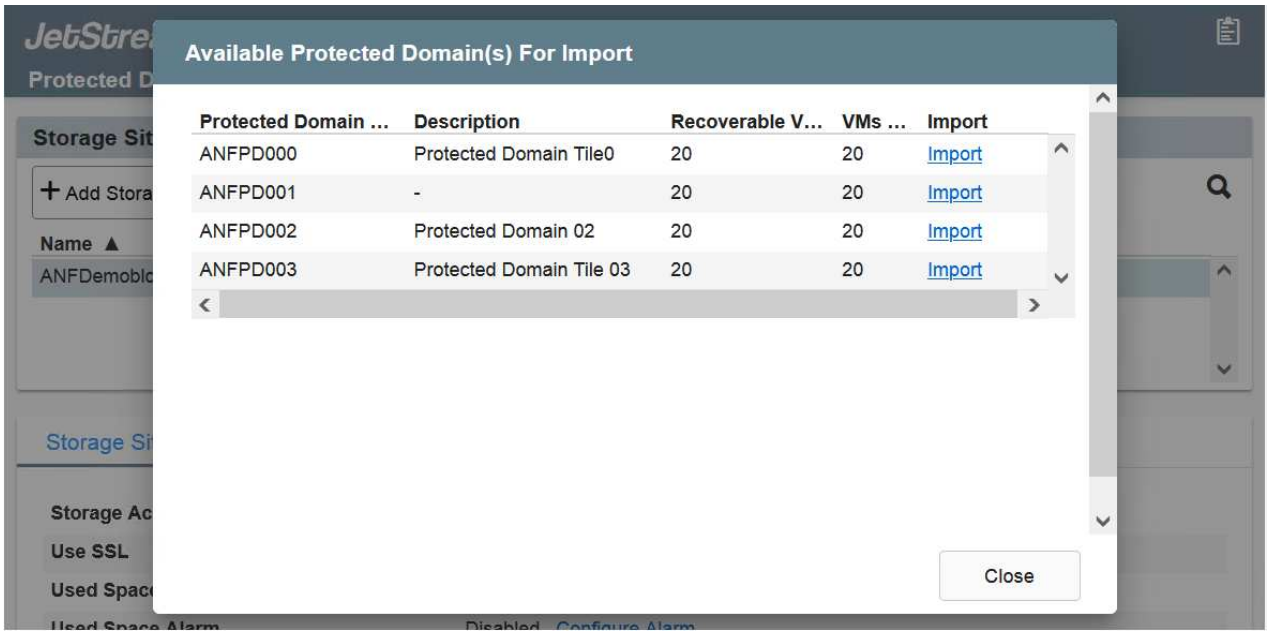
다음 스크린샷은 DHCP 기반 IP 주소를 사용한 설치를 보여 줍니다.



2. AVS 설치를 위한 Jetstream DR이 완료되면 브라우저를 새로 고칩니다. Jetstream DR UI에 액세스하려면 SDDC 데이터 센터 > 구성 > Jetstream DR로 이동하십시오.



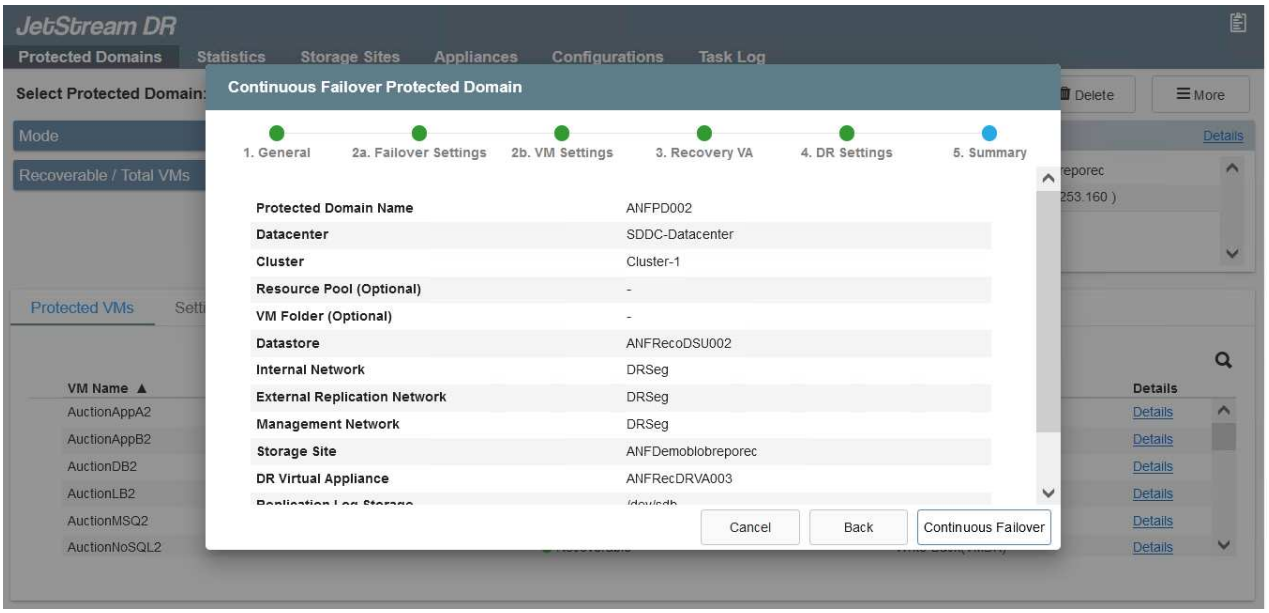
3. Jetstream DR 인터페이스에서 온프레미스 클러스터를 저장소 사이트로 보호하는 데 사용된 Azure Blob 저장소 계정을 추가한 다음 도메인 검사 옵션을 실행합니다.



4. 보호된 도메인을 가져온 후 DRVA 어플라이언스를 구축합니다. 이 예에서는 Jetstream DR UI를 사용하여 복구 사이트에서 수동으로 연속 재수화를 시작합니다.

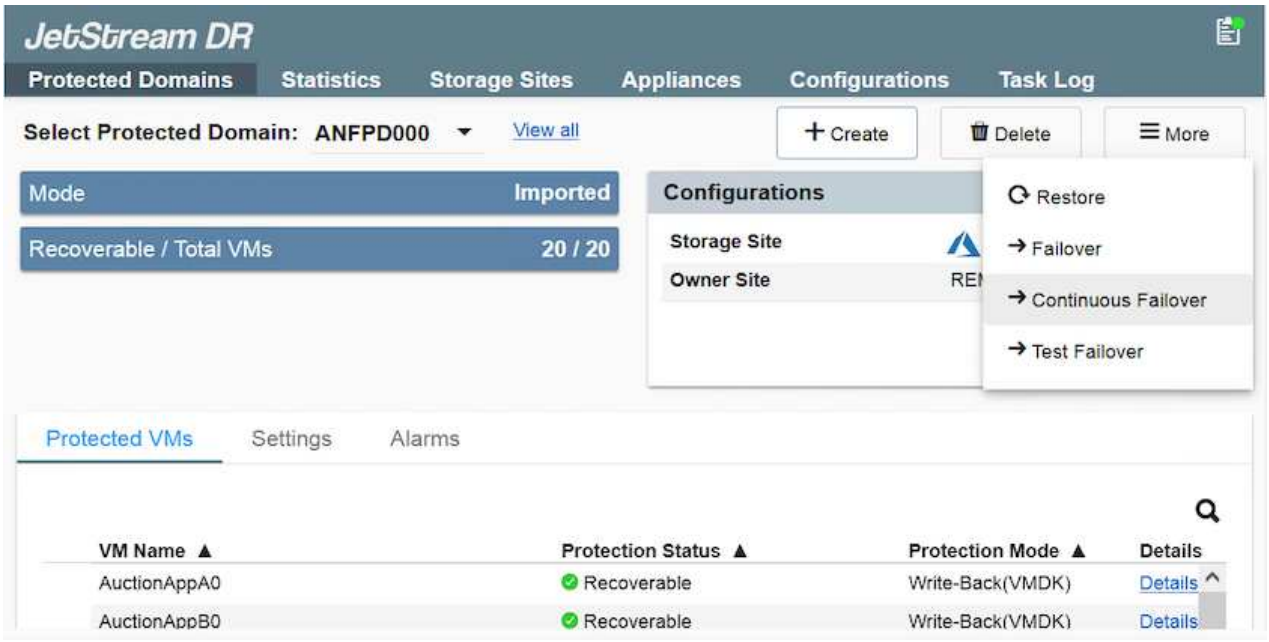
> CPT 생성 계획을 사용하여 이러한 단계를 자동화할 수도 있습니다.

5. 사용 가능한 vSAN 또는 ANF 데이터 저장소를 사용하여 복제 로그 볼륨을 생성합니다.
6. 보호된 도메인을 가져오고 VM 배치에 ANF 데이터 저장소를 사용하도록 복구 VA를 구성합니다.



선택한 세그먼트에서 DHCP가 활성화되어 있고 사용 가능한 IP가 충분한지 확인합니다. 도메인이 복구되는 동안 동적 IP가 일시적으로 사용됩니다. 복구 중인 각 VM(연속 재수화 포함)에는 개별 동적 IP가 필요합니다. 복구가 완료되면 IP가 해제되고 다시 사용할 수 있습니다.

7. 적절한 페일오버 옵션(무중단 페일오버 또는 페일오버)을 선택합니다. 이 예에서는 연속 재수화(연속 페일오버)가 선택됩니다.

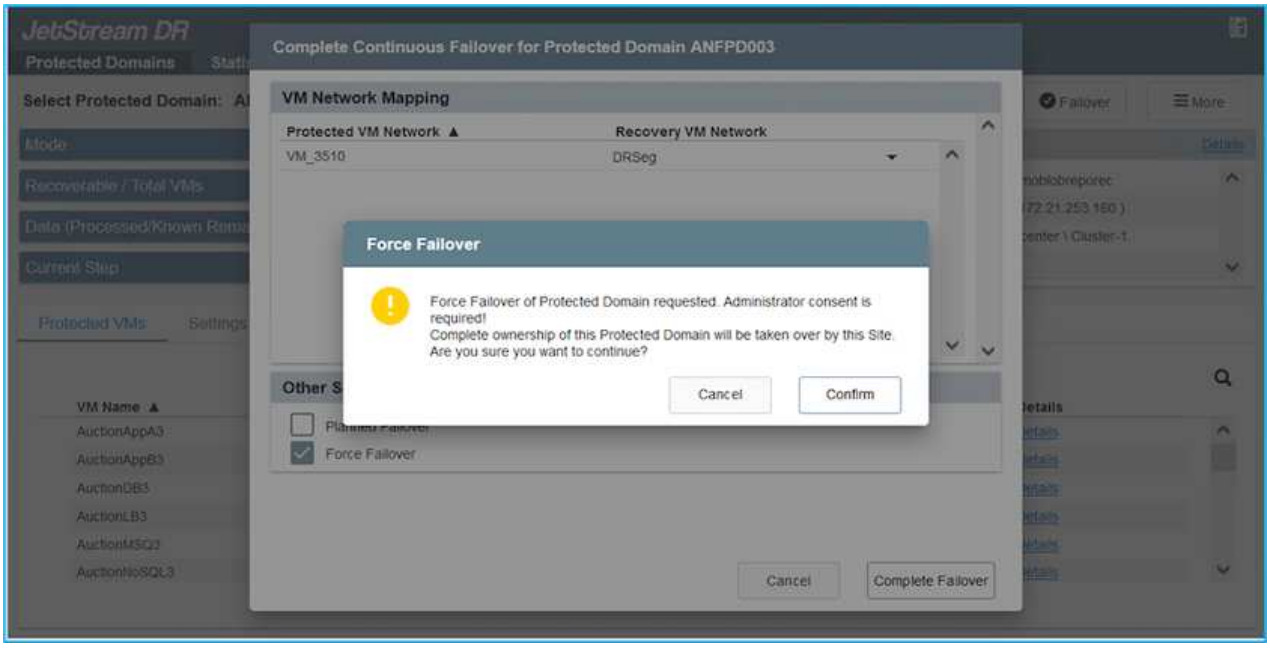


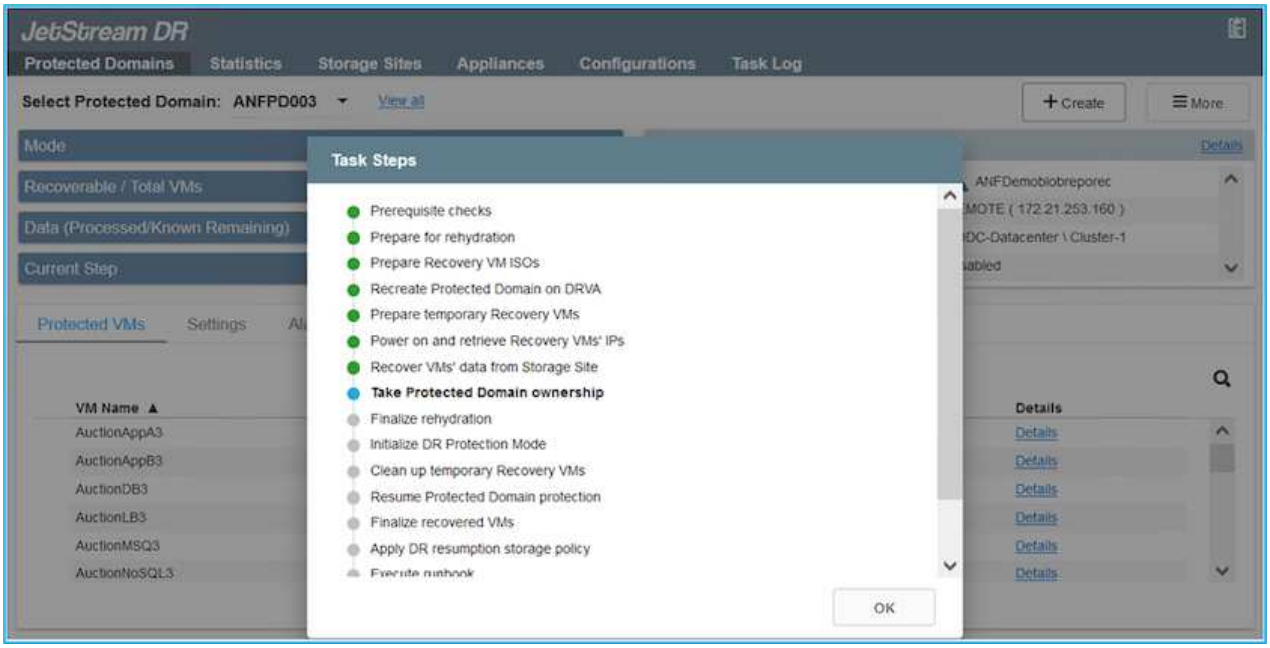
페일오버/페일백 수행

1. 사내 환경의 보호 클러스터에서 재해가 발생한 후(부분 장애 또는 전체 장애) 페일오버를 트리거합니다.

   CPT를 사용하여 Azure Blob Storage에서 AVS 클러스터 복구 사이트로 VM을 복구하는 페일오버 계획을 실행할 수 있습니다.

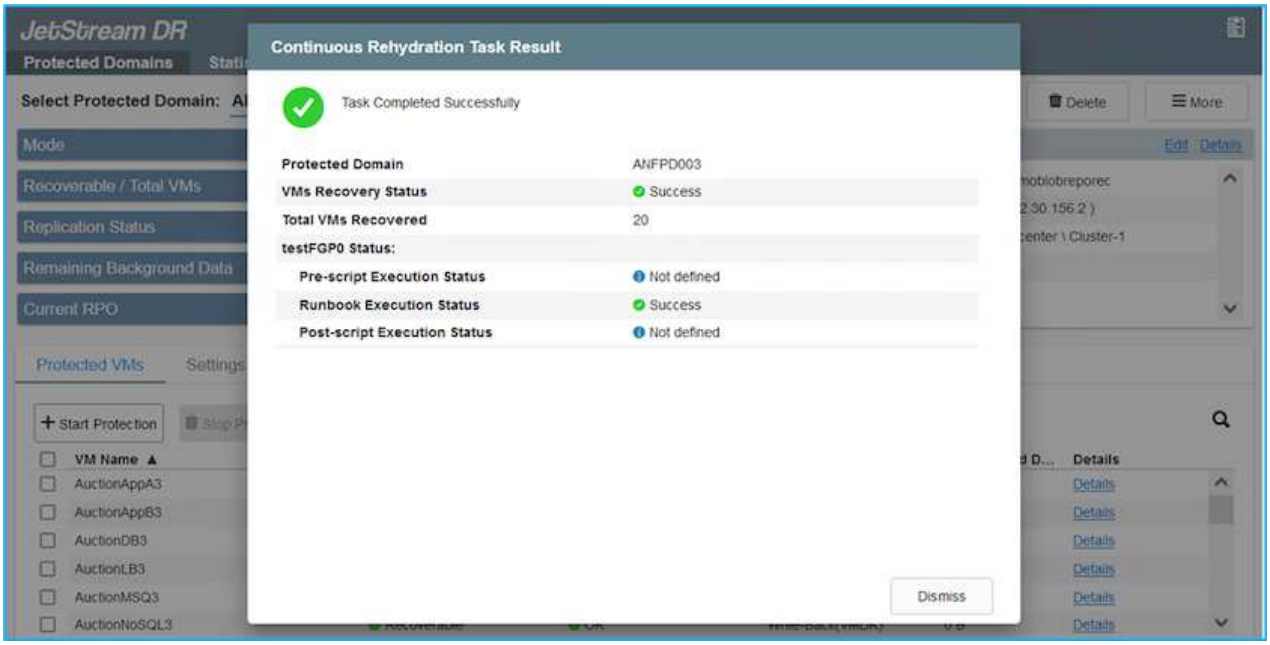
   AVS에서 보호된 VM이 시작될 때 장애 조치(연속 또는 표준 재수화) 후 보호가 자동으로 재개되고 Jetstream DR은 Azure Blob Storage의 해당/원래 컨테이너로 데이터를 계속 복제합니다.





   작업 표시줄에 장애 조치 작업의 진행률이 표시됩니다.

2. 작업이 완료되면 복구된 VM에 액세스하고 비즈니스가 정상적으로 계속됩니다.

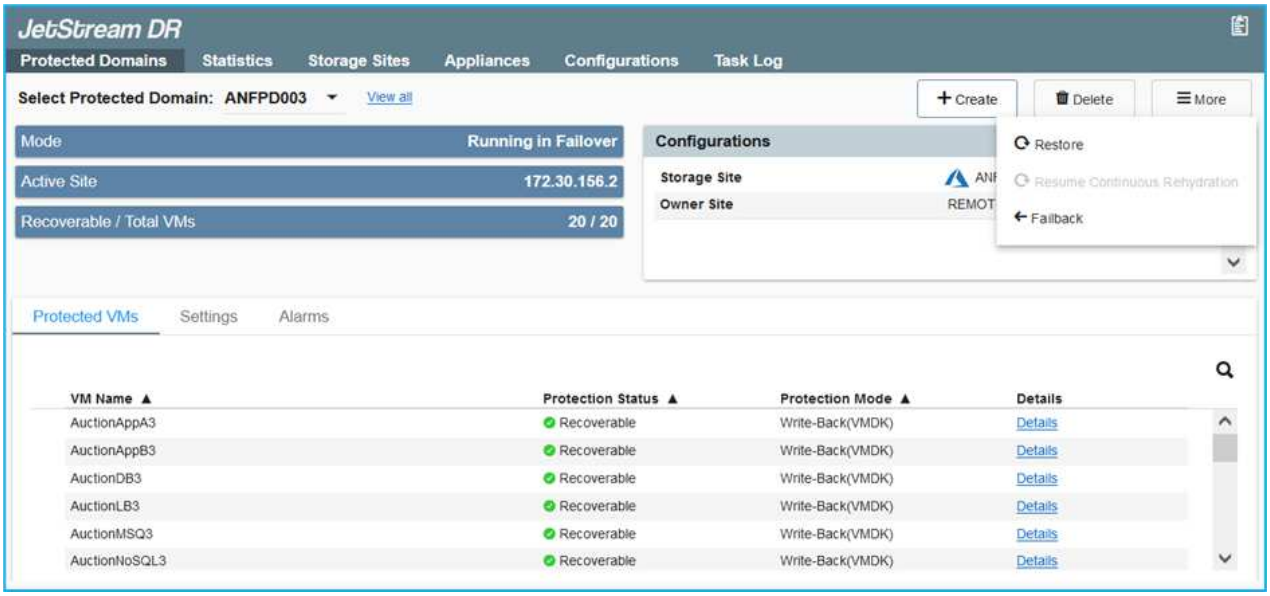


운영 사이트가 다시 가동된 후 페일백을 수행할 수 있습니다. VM 보호가 재개되고 데이터 일관성을 확인해야 합니다.

3. 사내 환경을 복원합니다. 재해 발생 유형에 따라 보호 클러스터의 구성을 복원 및/또는 확인해야 할 수도 있습니다. 필요한 경우 Jetstream DR 소프트웨어를 재설치해야 할 수 있습니다.

> 참고: 자동화 툴킷에 제공된 RECOVERY_UTILITY_Prepare_failback" 스크립트를 사용하여 오래된 VM, 도메인 정보 등의 원래 보호 사이트를 정리할 수 있습니다.

4. 복원된 온프레미스 환경에 액세스하고 Jetstream DR UI로 이동한 다음 적절한 보호 도메인을 선택합니다. 보호 사이트가 페일백될 준비가 되면 UI에서 페일백 옵션을 선택합니다.



CPT에서 생성한 페일백 계획을 사용하여 VM과 해당 데이터를 오브젝트 저장소에서 원래 VMware 환경으로 되돌릴 수도 있습니다.

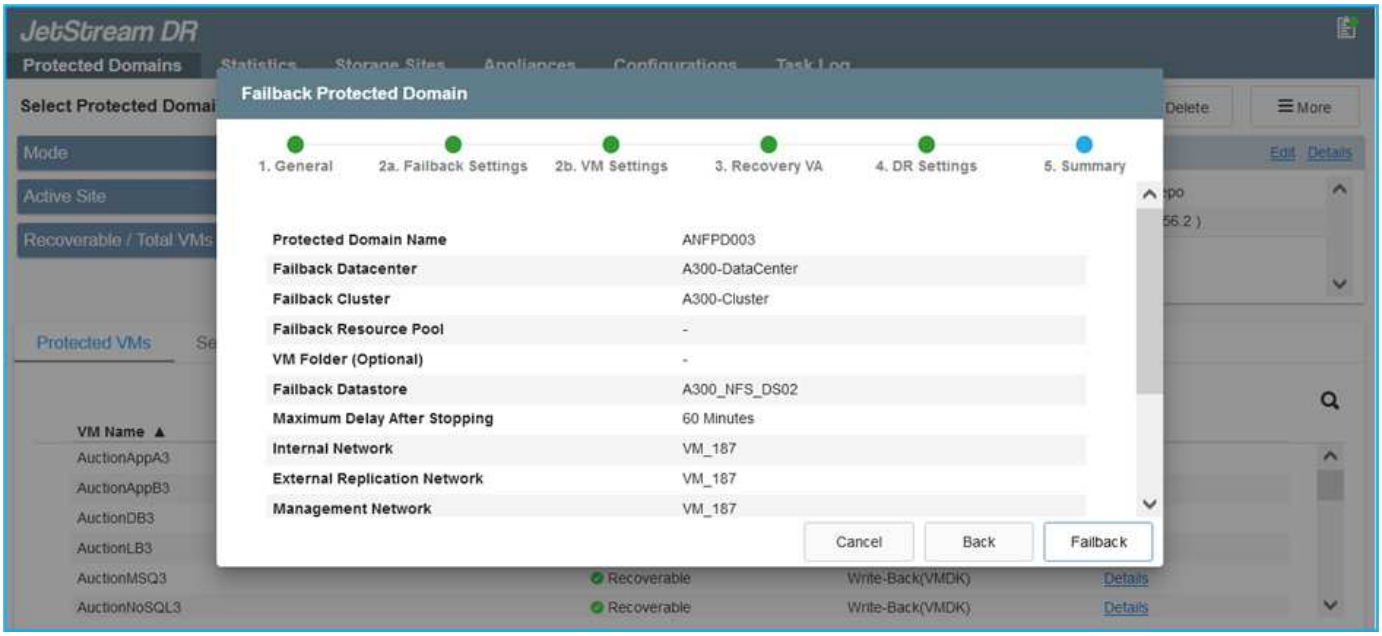
복구 사이트에서 VM을 일시 중지하고 보호 사이트에서 다시 시작한 후 최대 지연 시간을 지정합니다. 여기에는 대체 작동 VM 중지 후 복제 완료, 복구 사이트를 정리하기 위한 시간, 보호 사이트에서 VM을 다시 만드는 시간이 포함됩니다. NetApp이 권장하는 값은 10분입니다.

페일백 프로세스를 완료한 다음 VM 보호 및 데이터 정합성 재개를 확인합니다.

Ransomeware 복구

랜섬웨어에서 복구하는 것은 매우 힘든 작업이 될 수 있습니다. 특히, IT 조직이 안전한 반환 지점을 결정하고 결정된 후에는 복구된 워크로드가 재발생하는 공격으로부터 보호하는 방법(휴면 맬웨어로부터 또는 취약한 응용 프로그램을 통해)을 확인하기 어려울 수 있습니다.

Azure NetApp Files 데이터 저장소와 함께 AVS용 Jetstream DR을 사용하면 조직에서 사용 가능한 시점으로부터 복구할 수 있으므로 필요에 따라 분리된 기능적 네트워크로 워크로드를 복구할 수 있습니다. 복구 기능을 사용하면 애플리케이션이 기능을 수행하고 서로 통신하면서 남북의 트래픽에 노출되지 않도록 함으로써 보안 팀이 법의학 및 기타 필요한 조치를 수행할 수 있는 안전한 장소를 제공할 수 있습니다.



CVO 및 **AVS(**게스트 연결 스토리지**)**를 통한 재해 복구

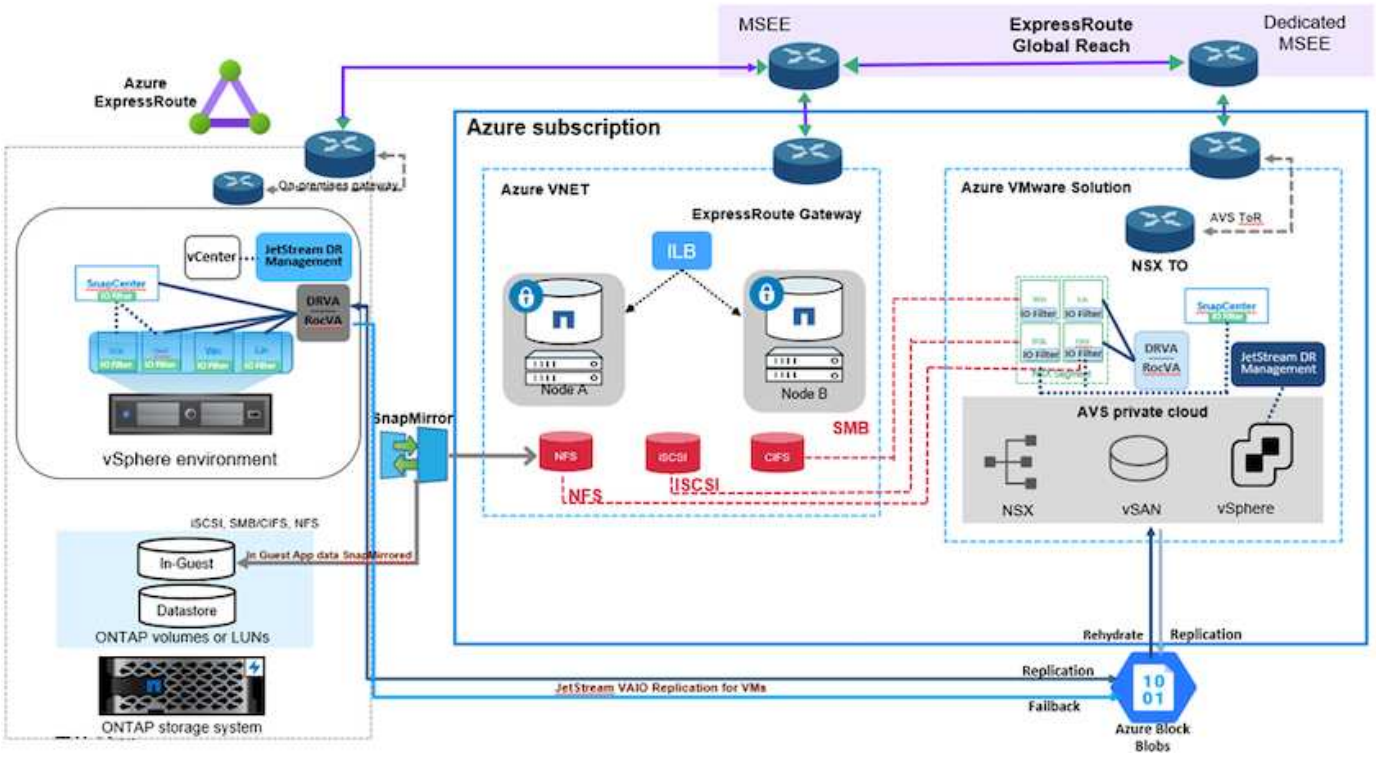
개요

저자: Ravi BCB, Niyaz Mohamed, NetApp

클라우드로 재해 복구는 랜섬웨어 등 사이트 운영 중단 및 데이터 손상 이벤트로부터 워크로드를 보호하는 복원력이 있는 비용 효율적인 방법입니다. NetApp SnapMirror를 사용하면 게스트 연결 스토리지를 사용하는 사내 VMware 워크로드를 Azure에서 실행되는 NetApp Cloud Volumes ONTAP에 복제할 수 있습니다. 여기에는 애플리케이션 데이터가 포함됩니다. 하지만 실제 VM 자체는 어떻습니까? 재해 복구는 가상 머신, VMDK, 애플리케이션 데이터 등을 비롯한 모든 종속 구성 요소를 포함해야 합니다. 이를 위해 Jetstream과 함께 SnapMirror를 사용하면 VM VMDK에 vSAN 스토리지를 사용하는 동시에 사내에서 Cloud Volumes ONTAP로 복제된 워크로드를 원활하게 복구할 수

있습니다.

이 문서에서는 NetApp SnapMirror, Jetstream 및 AVS(Azure VMware Solution)를 사용하여 재해 복구를 설정하고 수행하기 위한 단계별 접근 방식을 제공합니다.



가정

이 문서에서는 애플리케이션 데이터(게스트 연결)를 위한 게스트 내 스토리지에 초점을 두고 사내 환경에서 애플리케이션 정합성 보장 백업을 위해 SnapCenter를 사용하고 있다고 가정합니다.

> 이 문서는 타사 백업 또는 복구 솔루션에 적용됩니다. 환경에 사용된 솔루션에 따라 Best Practice를 따라 조직 SLA를 충족하는 백업 정책을 생성합니다.

온프레미스 환경과 Azure 가상 네트워크 간의 연결을 위해 고속 경로 글로벌 도달 범위 또는 VPN 게이트웨이가 있는 가상 WAN을 사용합니다. 세그먼트는 사내 VLAN 설계를 기반으로 생성해야 합니다.

> 온프레미스 데이터 센터를 Azure에 연결하는 여러 가지 옵션이 있어 이 문서의 특정 워크플로 개요를 볼 수 없습니다. Azure 설명서를 참조하여 적절한 Azure-사내와 Azure 간 연결 방법을 확인하십시오.

DR 솔루션 구축

솔루션 구축 개요

1. 필요한 RPO 요구 사항에 따라 SnapCenter를 사용하여 애플리케이션 데이터를 백업했는지 확인합니다.
2. 적절한 서브스크립션 및 가상 네트워크 내에서 Cloud Manager를 사용하여 올바른 인스턴스 크기로 Cloud Volumes ONTAP를 프로비저닝합니다.
    a. 관련 애플리케이션 볼륨에 대해 SnapMirror를 구성합니다.

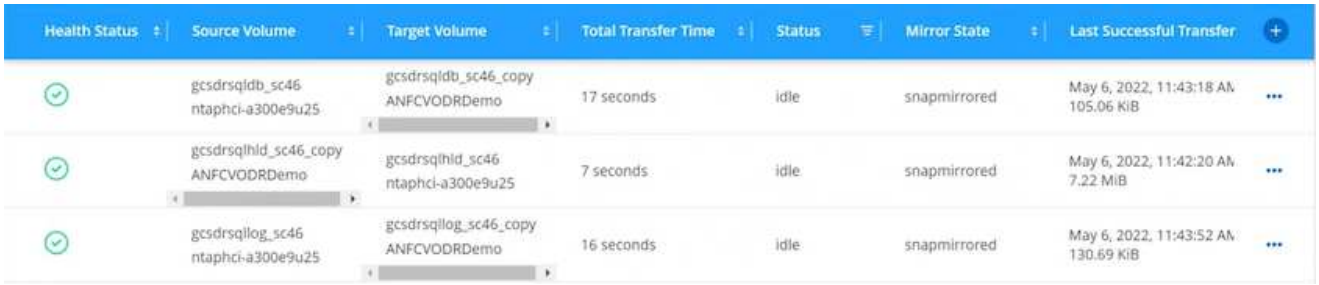
b. 예약된 작업 후 SnapMirror 업데이트를 트리거하도록 SnapCenter의 백업 정책을 업데이트합니다.

3. Jetstream DR 소프트웨어를 사내 데이터 센터에 설치하고 가상 시스템을 보호합니다.
4. Azure VMware Solution 프라이빗 클라우드에 Jetstream DR 소프트웨어를 설치합니다.
5. 재해 이벤트 중에 Cloud Manager를 사용하여 SnapMirror 관계를 중단시키고 지정된 AVS DR 사이트의 Azure NetApp Files 또는 vSAN 데이터스토어로 가상 시스템의 페일오버를 트리거합니다.
   a. 애플리케이션 VM에 대한 iSCSI LUN 및 NFS 마운트를 다시 연결합니다.
6. 운영 사이트가 복구된 후 SnapMirror를 다시 동기화하여 보호 사이트에 대한 페일백을 호출합니다.

배포 세부 정보

Azure에서 **CVO**를 구성하고 볼륨을 **CVO**로 복제합니다

첫 번째 단계는 Cloud Volumes ONTAP Azure("링크")를 사용하여 원하는 볼륨을 Cloud Volumes ONTAP에 복제하고 원하는 빈도와 스냅샷 보존 기능을 사용할 수 있습니다.



AVS 호스트 및 **CVO** 데이터 액세스를 구성합니다

SDDC를 구축할 때 고려해야 할 두 가지 중요한 요소는 Azure VMware 솔루션에서 SDDC 클러스터의 크기와 SDDC를 사용할 수 있는 기간을 결정하는 것입니다. 재해 복구 솔루션의 두 가지 주요 고려 사항은 전체 운영 비용을 절감하는 데 도움이 됩니다. SDDC는 최대 3개의 호스트까지 구성할 수 있으며, 전체 구축 환경에서 다중 호스트 클러스터까지 가능합니다.

AVS 클러스터의 구축 결정은 주로 RPO/RTO 요구 사항을 기반으로 합니다. Azure VMware 솔루션을 사용하면 SDDC를 테스트 또는 실제 재해 이벤트에 대비하여 적시에 프로비저닝할 수 있습니다. SDDC를 적시에 구축하면 재해 발생 시 ESXi 호스트 비용을 절감할 수 있습니다. 그러나 이러한 구축 형태는 SDDC를 프로비저닝하는 동안 RTO에 몇 시간 정도 영향을 줍니다.

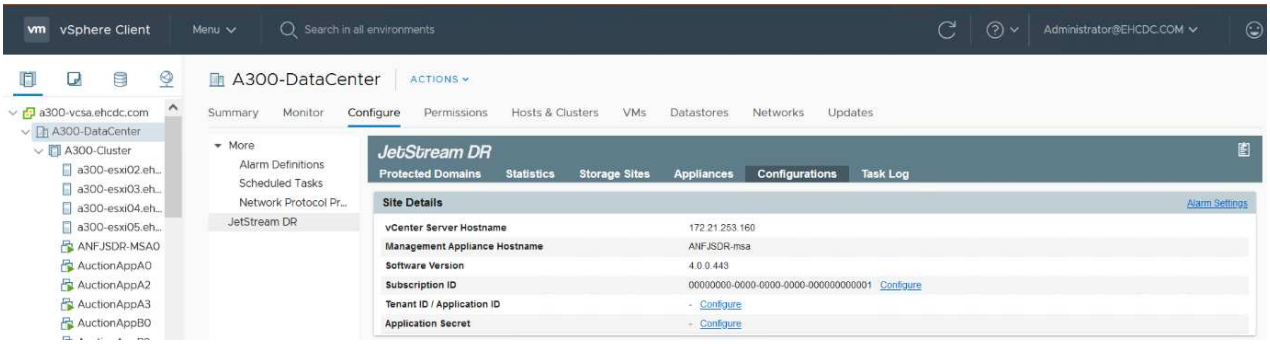
가장 일반적인 구축 옵션은 SDDC를 상시 작동, 파일럿 라이트 모드로 실행하는 것입니다. 이 옵션은 항상 사용 가능한 호스트 세 개로 구성된 작은 공간을 제공하며 시뮬레이션 활동 및 규정 준수 검사를 위한 실행 기준을 제공하여 복구 작업 속도를 높이고 운영 사이트와 DR 사이트 간의 운영 드리프트가 발생하지 않도록 합니다. 실제 DR 이벤트를 처리하는 데 필요한 경우 파일럿 라이트 클러스터를 원하는 레벨로 신속하게 확장할 수 있습니다.

AVS SDDC를 구성하려면(온디맨드 또는 파일럿 라이트 모드여야 함) 을 참조하십시오 "Azure에서 가상화 환경을 구축하고 구성합니다". 사전 요구 사항으로, 연결이 설정된 후 AVS 호스트에 상주하는 게스트 VM이 Cloud Volumes ONTAP의 데이터를 사용할 수 있는지 확인합니다.

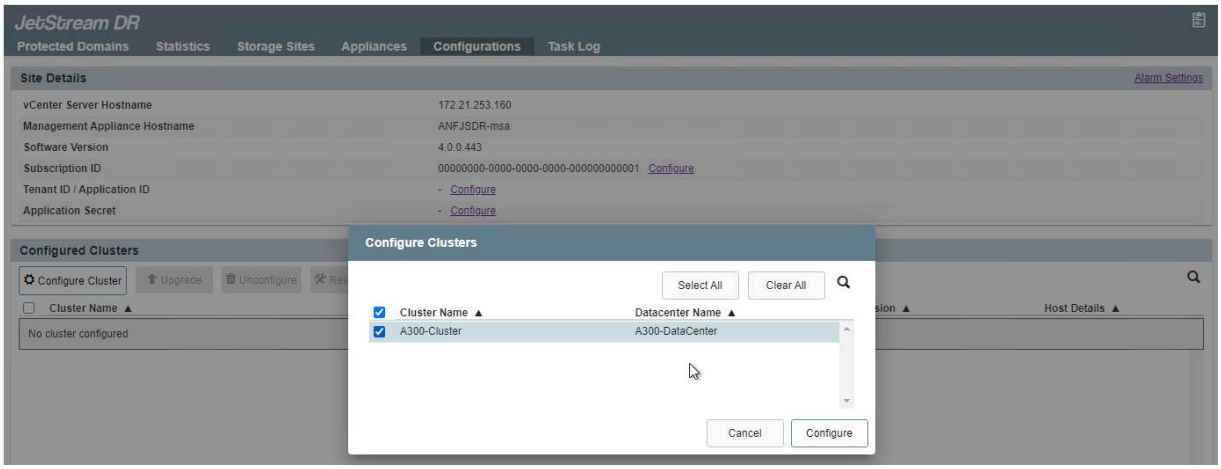
Cloud Volumes ONTAP 및 AVS를 올바르게 구성한 후에는 VAIO 메커니즘을 사용하고 Cloud Volumes ONTAP에 애플리케이션 볼륨 복사본을 위한 SnapMirror를 활용하여 Jetstream을 구성하여 온프레미스 워크로드를 AVS(게스트 내 스토리지가 있는 응용 프로그램 VMDK 및 VM이 있는 VM)로 자동으로 복구합니다.

Jetstream DR 소프트웨어는 Jetstream DR Management Server Virtual Appliance(MSA), DR 가상 어플라이언스(DRVA) 및 호스트 구성 요소(I/O 필터 패키지)의 세 가지 주요 구성 요소로 구성됩니다. MSA는 컴퓨팅 클러스터에 호스트 구성 요소를 설치 및 구성한 다음 Jetstream DR 소프트웨어를 관리하는 데 사용됩니다. 설치 프로세스는 다음과 같습니다.

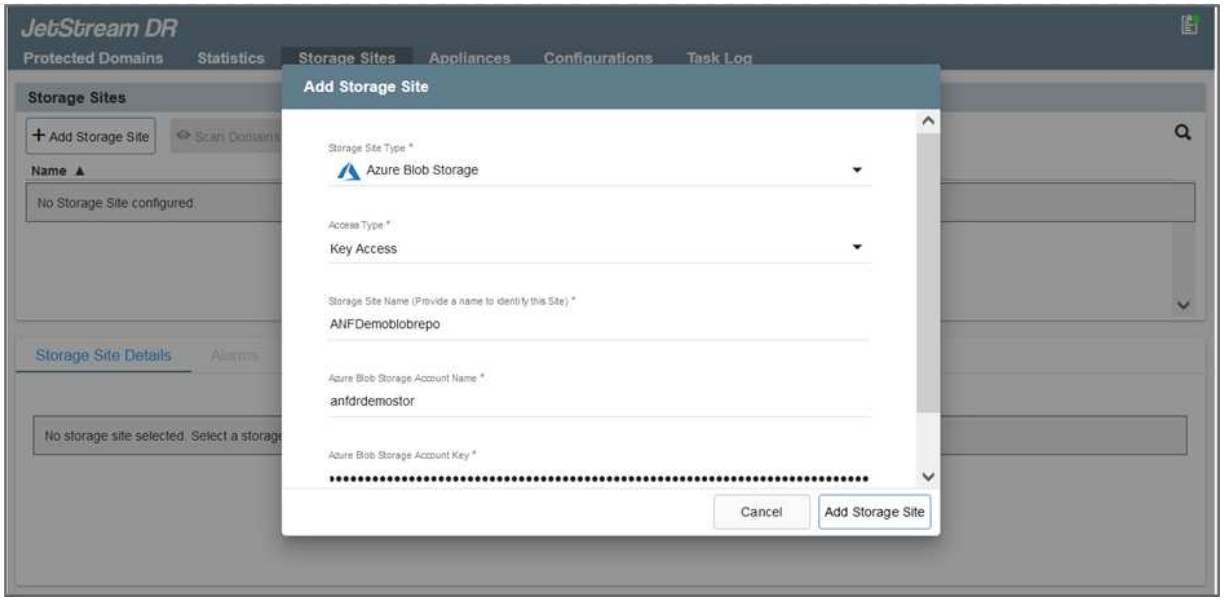
1. 필수 구성 요소를 확인하십시오.
2. 리소스 및 구성 권장 사항에 대해 용량 계획 툴을 실행합니다.
3. Jetstream DR MSA를 지정된 클러스터의 각 vSphere 호스트에 구축합니다.
4. 브라우저에서 DNS 이름을 사용하여 MSA를 실행합니다.
5. MSA에 vCenter Server를 등록합니다.
6. Jetstream DR MSA를 구축하고 vCenter Server를 등록한 후 vSphere Web Client를 사용하여 Jetstream DR 플러그인으로 이동합니다. 이 작업은 데이터 센터 > 구성 > Jetstream DR로 이동하여 수행할 수 있습니다.



7. Jetstream DR 인터페이스에서 다음 작업을 완료합니다.
   a. I/O 필터 패키지를 사용하여 클러스터를 구성합니다.

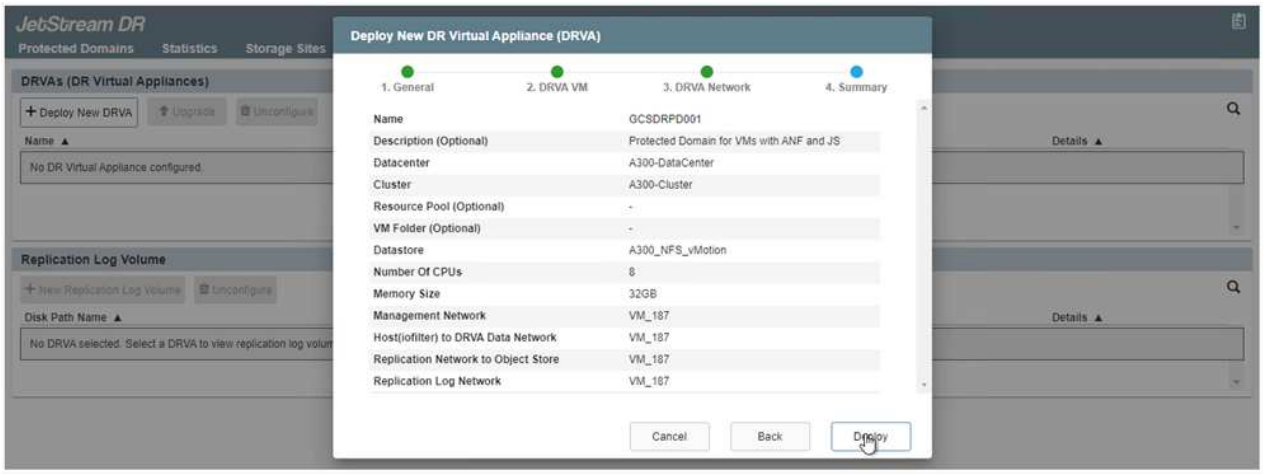


   b. 복구 사이트에 있는 Azure Blob 저장소를 추가합니다.

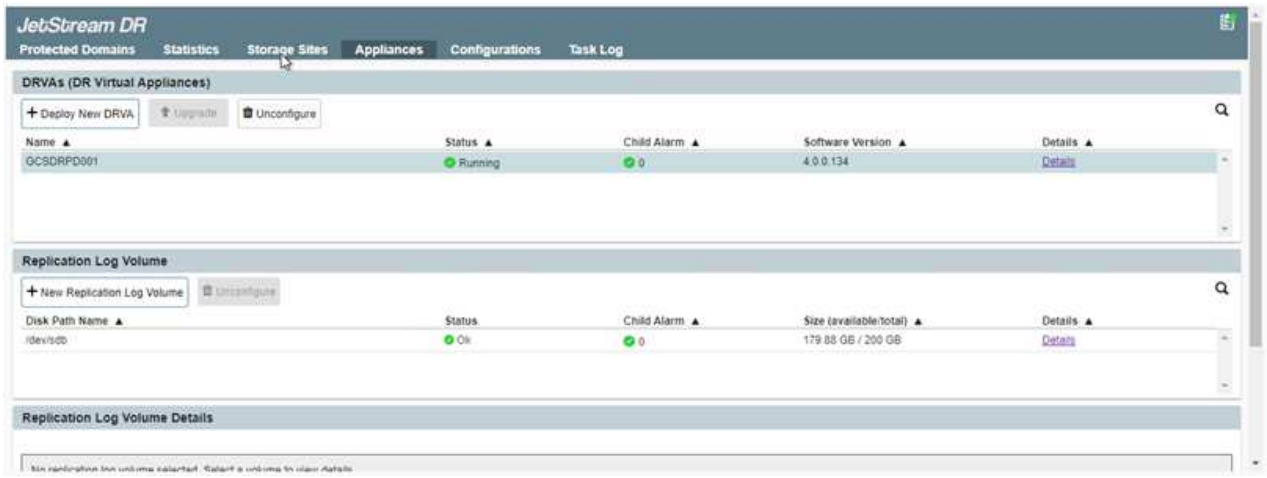


8. Appliances 탭에서 필요한 수의 DR 가상 어플라이언스(DRVA)를 구축합니다.

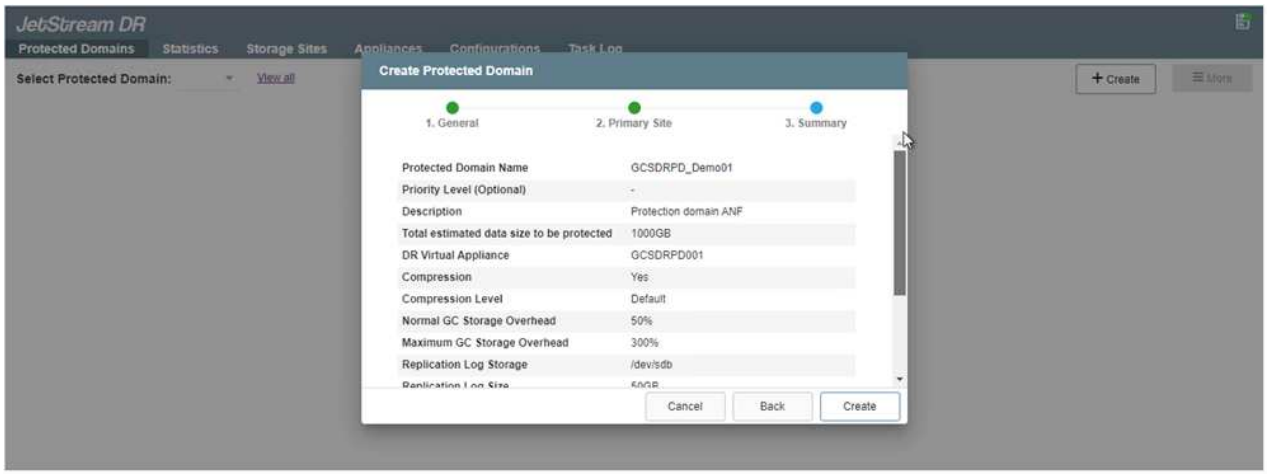
   용량 계획 툴을 사용하여 필요한 DRVA의 수를 추정합니다.

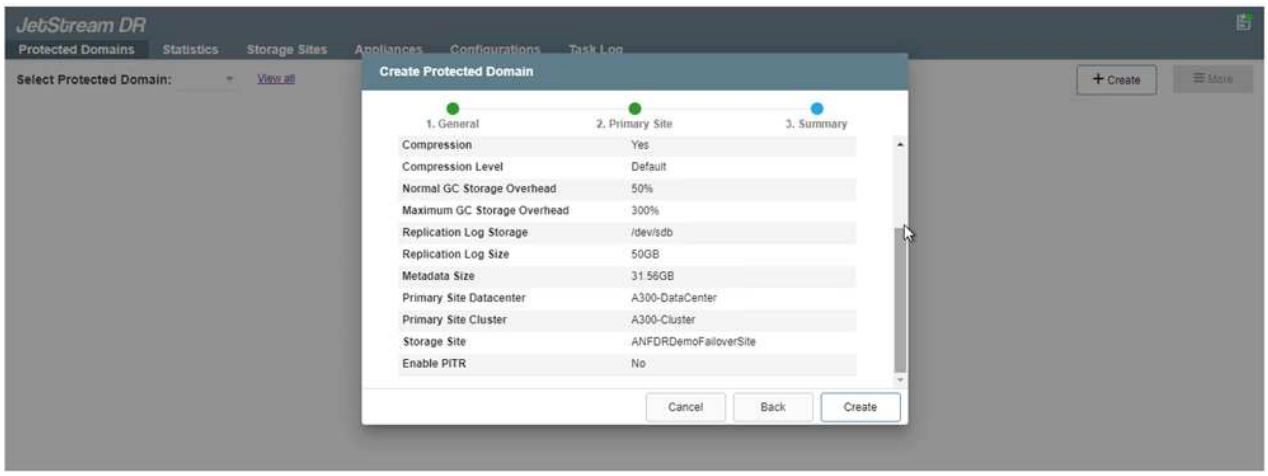


9. 사용 가능한 데이터 저장소 또는 독립 공유 iSCSI 스토리지 풀에서 VMDK를 사용하여 각 DRVA에 대한 복제 로그 볼륨을 생성합니다.



10. 보호 도메인 탭에서 Azure Blob 저장소 사이트, DRVA 인스턴스 및 복제 로그에 대한 정보를 사용하여 필요한 수의 보호된 도메인을 만듭니다. 보호 도메인은 함께 보호되고 장애 조치/장애 복구 작업에 우선 순위 순서를 할당하는 클러스터 내의 특정 VM 또는 애플리케이션 VM 세트를 정의합니다.

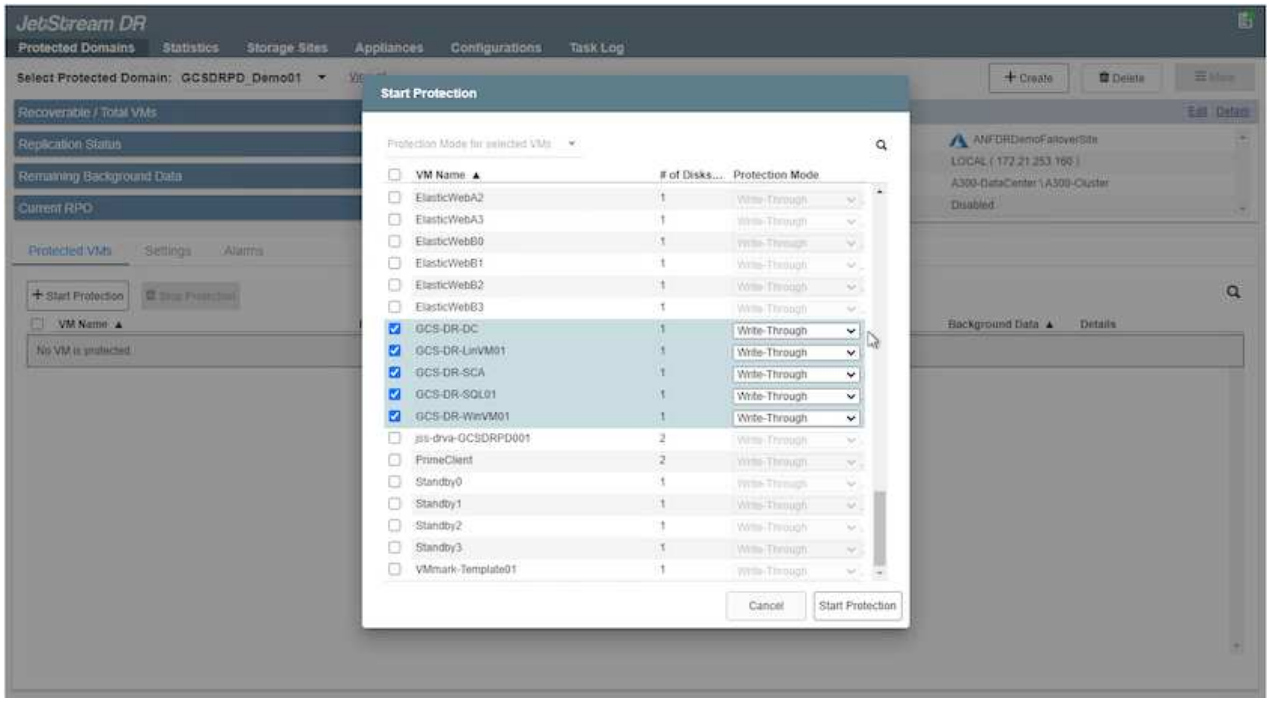




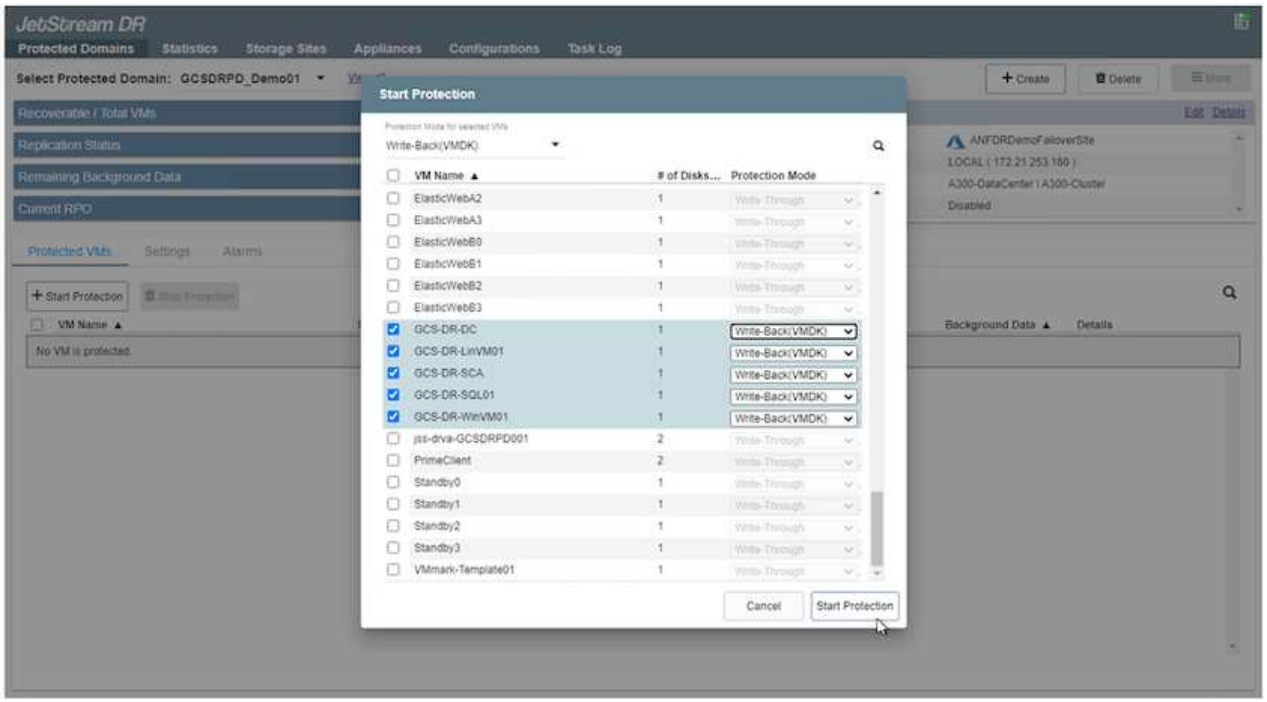
11. 보호할 VM을 선택하고 종속성을 기반으로 VM을 애플리케이션 그룹으로 그룹화합니다. 애플리케이션 정의를 사용하면 VM 세트를 부팅 순서, 부팅 지연 및 복구 시 실행할 수 있는 선택적 애플리케이션 검증을 포함하는 논리 그룹으로 그룹화할 수 있습니다.

보호 도메인의 모든 VM에 동일한 보호 모드가 사용되는지 확인합니다.

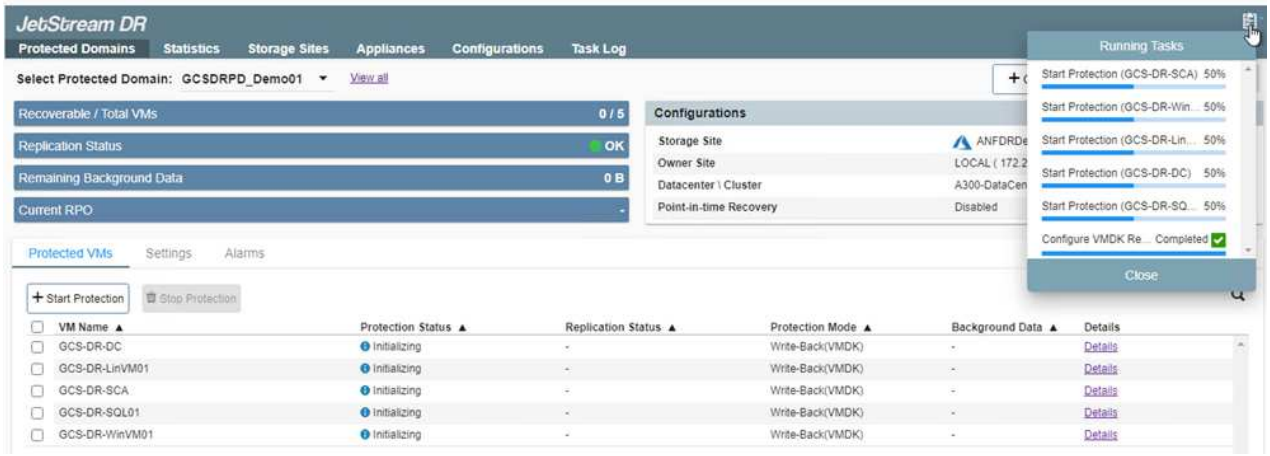
VMDK(Write-Back) 모드는 더 높은 성능을 제공합니다.



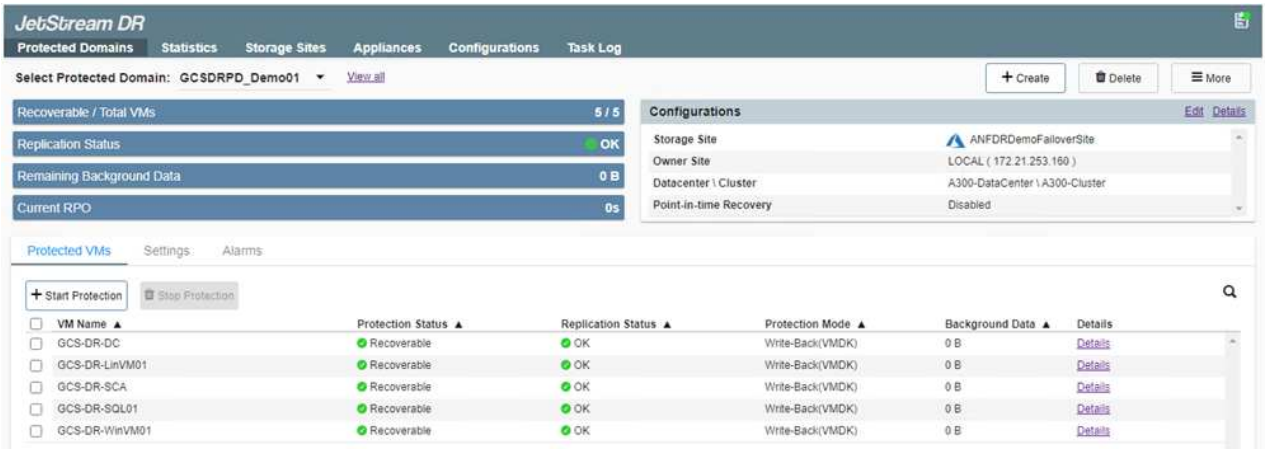
12. 복제 로그 볼륨이 고성능 스토리지에 배치되었는지 확인합니다.



13. 작업을 완료한 후 보호 도메인에 대한 보호 시작 을 클릭합니다. 그러면 선택한 VM에 대한 데이터 복제가 지정된 Blob 저장소로 시작됩니다.



14. 복제가 완료되면 VM 보호 상태가 복구 가능으로 표시됩니다.

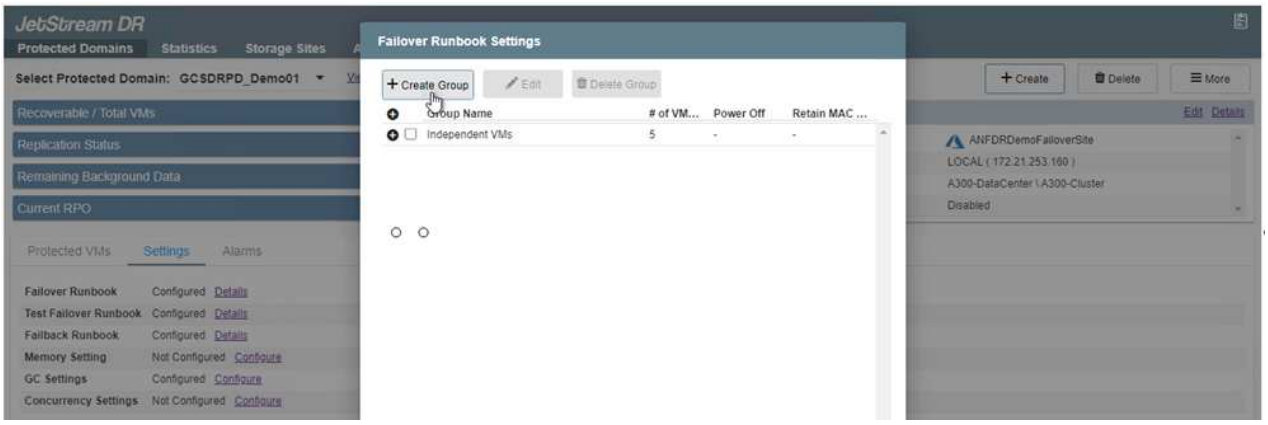


> 페일오버 런북은 VM(복구 그룹이라고 함)을 그룹화하고 부팅 순서 시퀀스를 설정하고 IP 구성과 함께 CPU/메모리 설정을 수정하도록 구성할 수 있습니다.

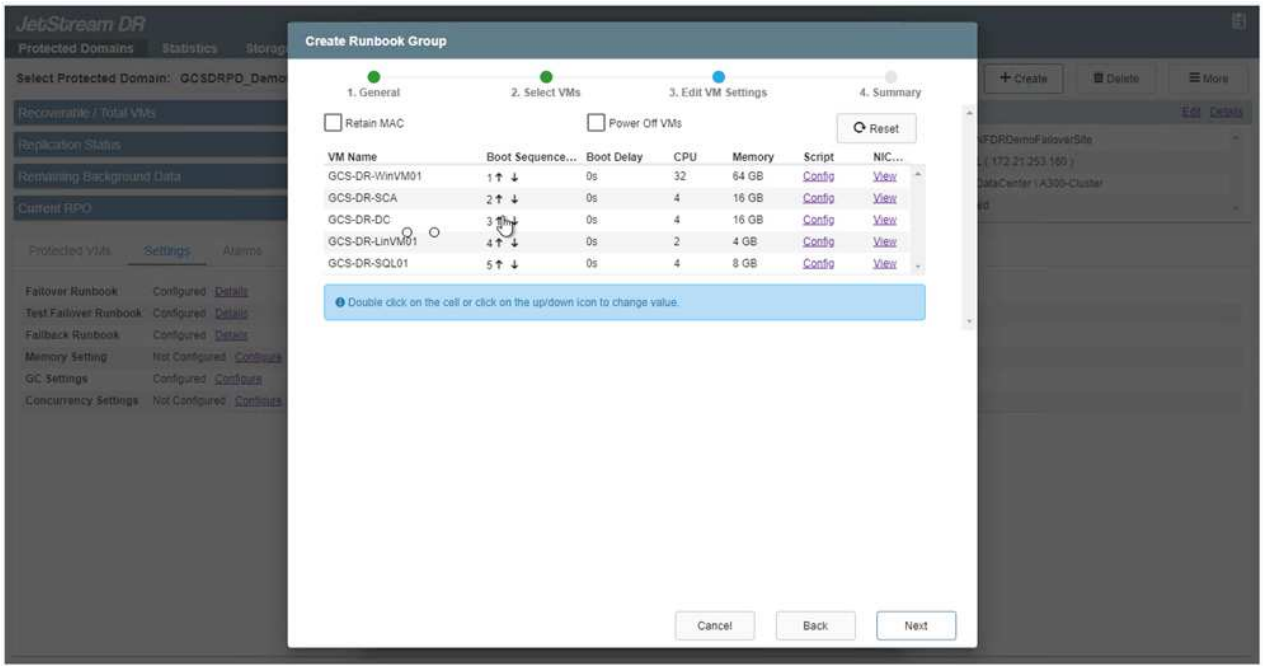
15. 설정 을 클릭한 다음 Runbook 구성 링크를 클릭하여 Runbook 그룹을 구성합니다.

16. 새 Runbook 그룹을 생성하려면 Create Group 버튼을 클릭합니다.

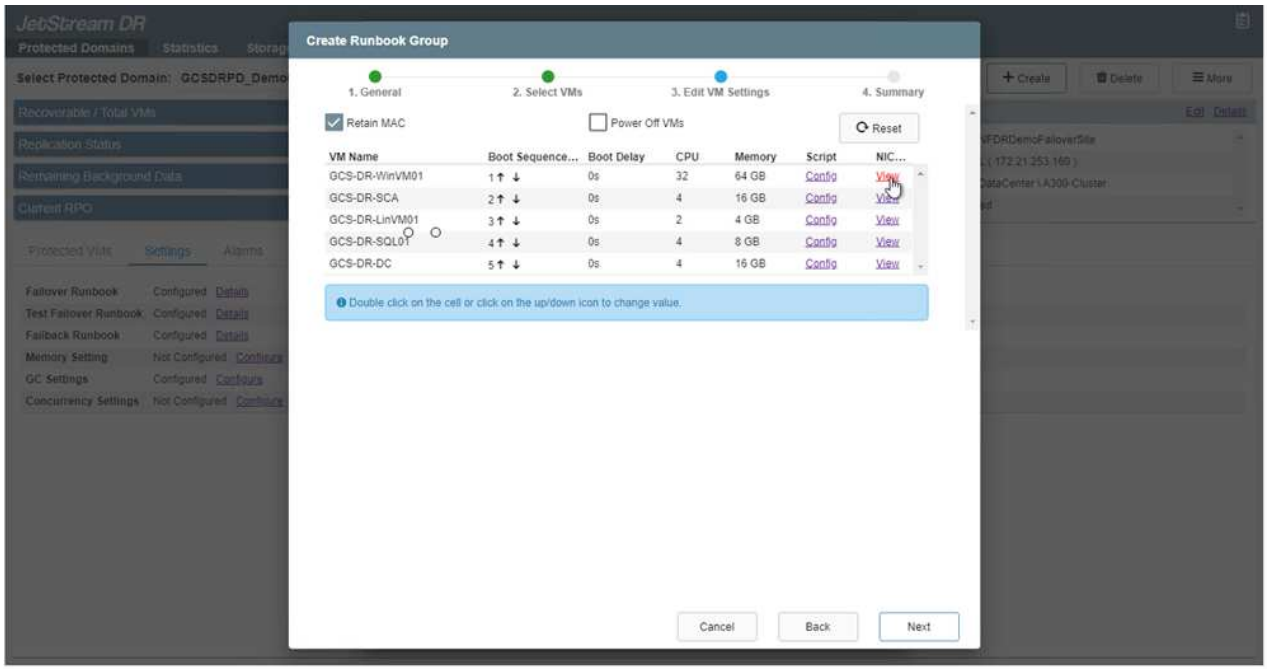
필요한 경우 화면 아래쪽에 사용자 지정 사전 스크립트 및 사후 스크립트를 적용하여 Runbook 그룹의 작업 전후에 자동으로 실행합니다. Runbook 스크립트가 관리 서버에 있는지 확인합니다.



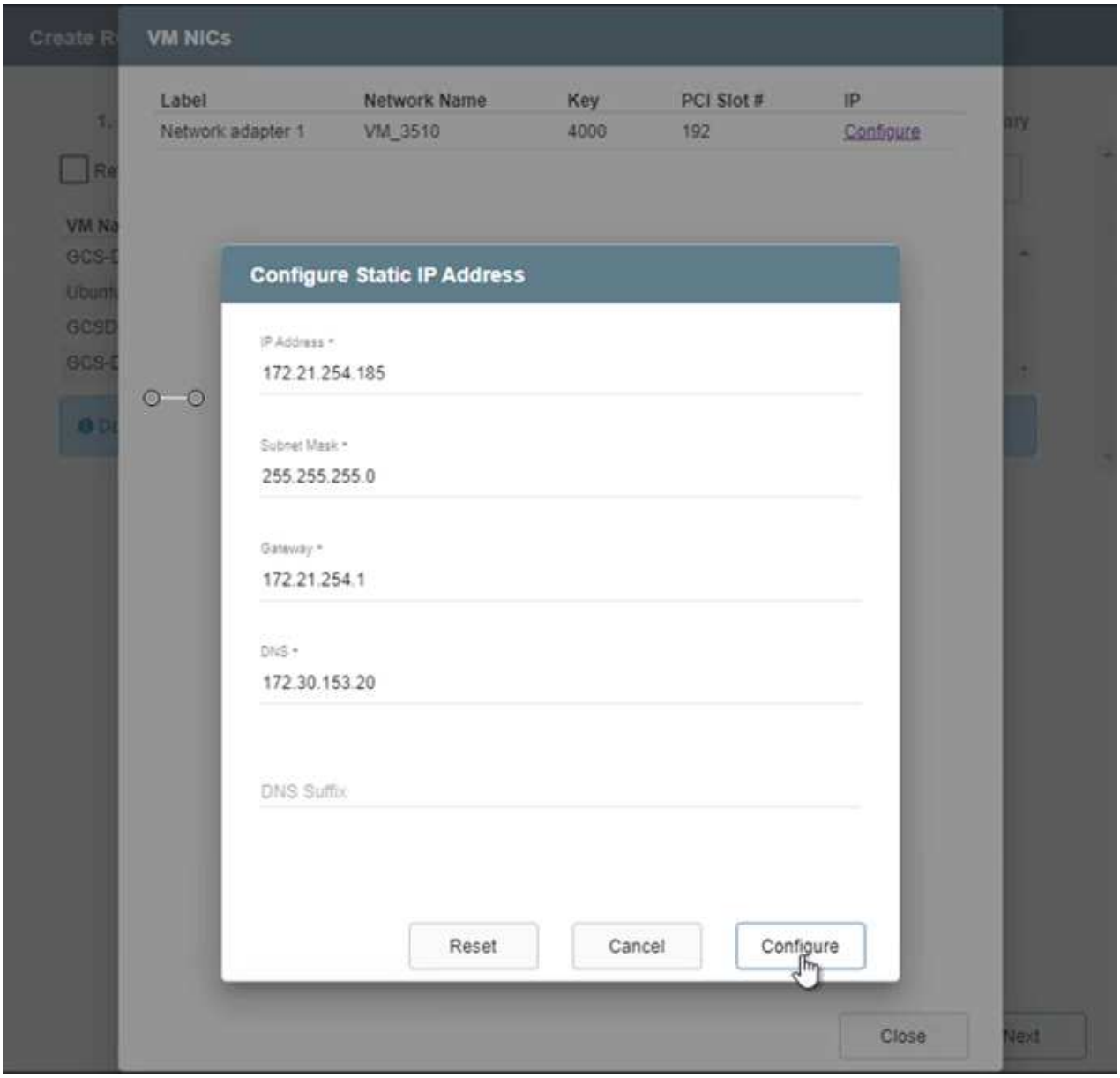
17. 필요에 따라 VM 설정을 편집합니다. 부팅 순서, 부팅 지연(초 단위로 지정), CPU 수 및 할당할 메모리 양을 포함하여 VM을 복구하기 위한 매개 변수를 지정합니다. 위쪽 또는 아래쪽 화살표를 클릭하여 VM의 부팅 순서를 변경합니다. MAC를 유지하기 위한 옵션도 제공됩니다.

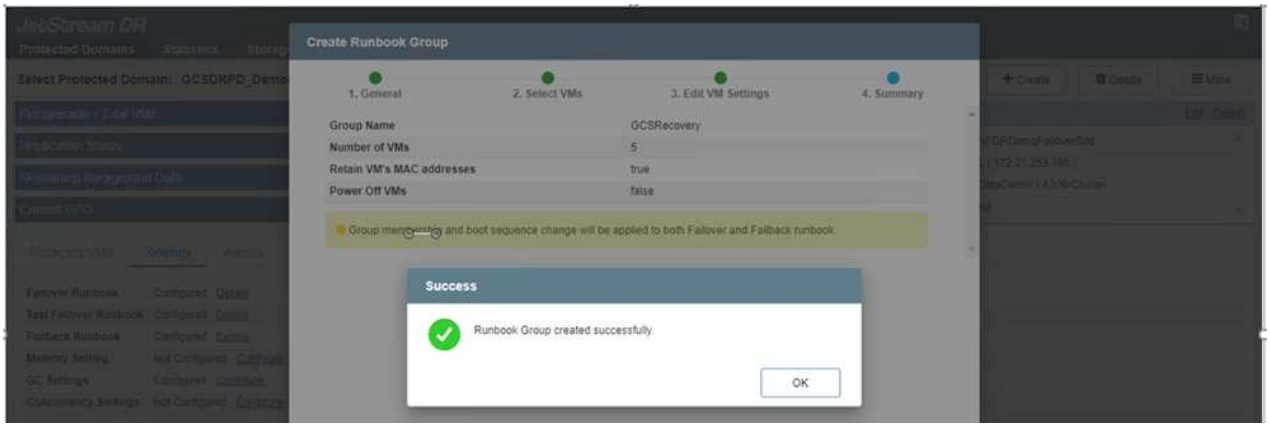


18. 정적 IP 주소는 그룹의 개별 VM에 대해 수동으로 구성할 수 있습니다. VM의 NIC View 링크를 클릭하여 IP 주소 설정을 수동으로 구성합니다.



19. 구성 버튼을 클릭하여 해당 VM에 대한 NIC 설정을 저장합니다.





이제 페일오버 및 페일백 Runbook의 상태가 모두 Configured로 표시됩니다. 페일오버 및 페일백 Runbook 그룹은 동일한 초기 VM 및 설정 그룹을 사용하여 쌍으로 생성됩니다. 필요한 경우 각 Runbook 그룹의 세부 정보 링크를 클릭하고 설정을 변경하여 Runbook 그룹의 설정을 개별적으로 사용자 지정할 수 있습니다.

복구 사이트(AVS)의 모범 사례는 3노드 파일럿 라이트 클러스터를 미리 생성하는 것입니다. 이를 통해 다음을 포함하여 복구 사이트 인프라를 사전 구성할 수 있습니다.

- 대상 네트워킹 세그먼트, 방화벽, DHCP 및 DNS 등의 서비스 등
- AVS용 Jetstream DR 설치
- 데이터 저장소 등을 사용하여 ANF 볼륨 구성

Jetstream DR은 미션 크리티컬 도메인에 대해 제로급 RTO 모드를 지원합니다. 이러한 도메인의 경우 대상 스토리지가 사전 설치되어 있어야 합니다. ANF는 이 경우 권장되는 스토리지 유형입니다.

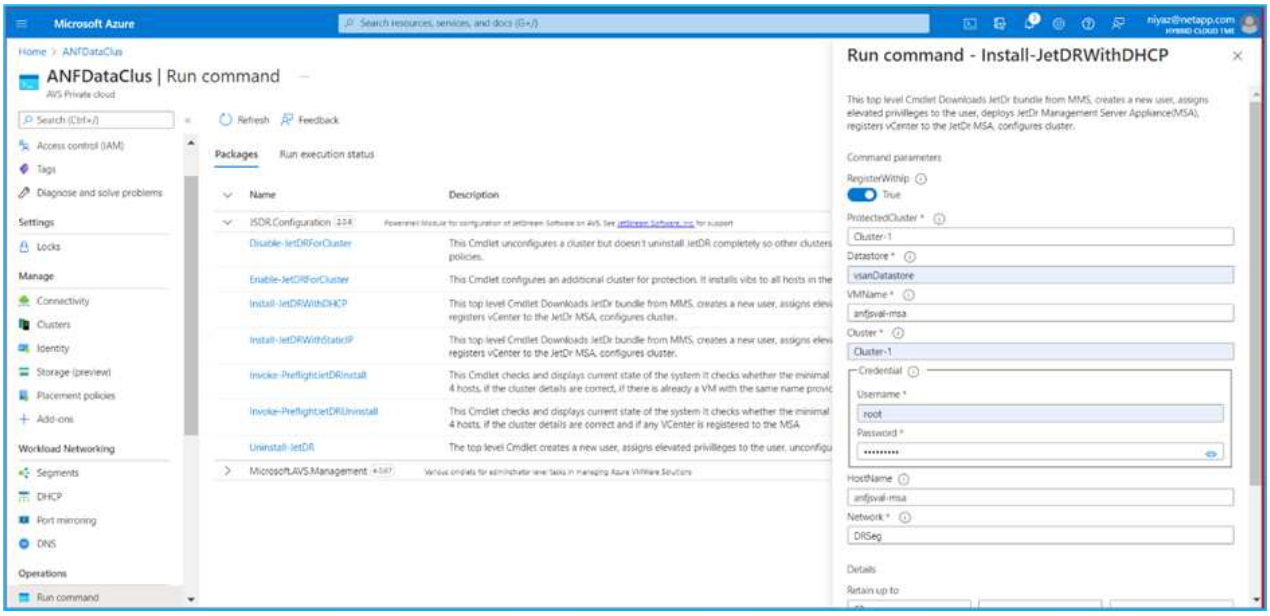
세그먼트 생성을 포함한 네트워크 구성은 AVS 클러스터에서 사내 요구 사항과 일치하도록 구성해야 합니다.

SLA 및 RTO 요구 사항에 따라 연속 페일오버 또는 일반(표준) 페일오버 모드를 사용할 수 있습니다. 제로급 RTO의 경우 복구 사이트에서 연속 재수화를 시작해야 합니다.

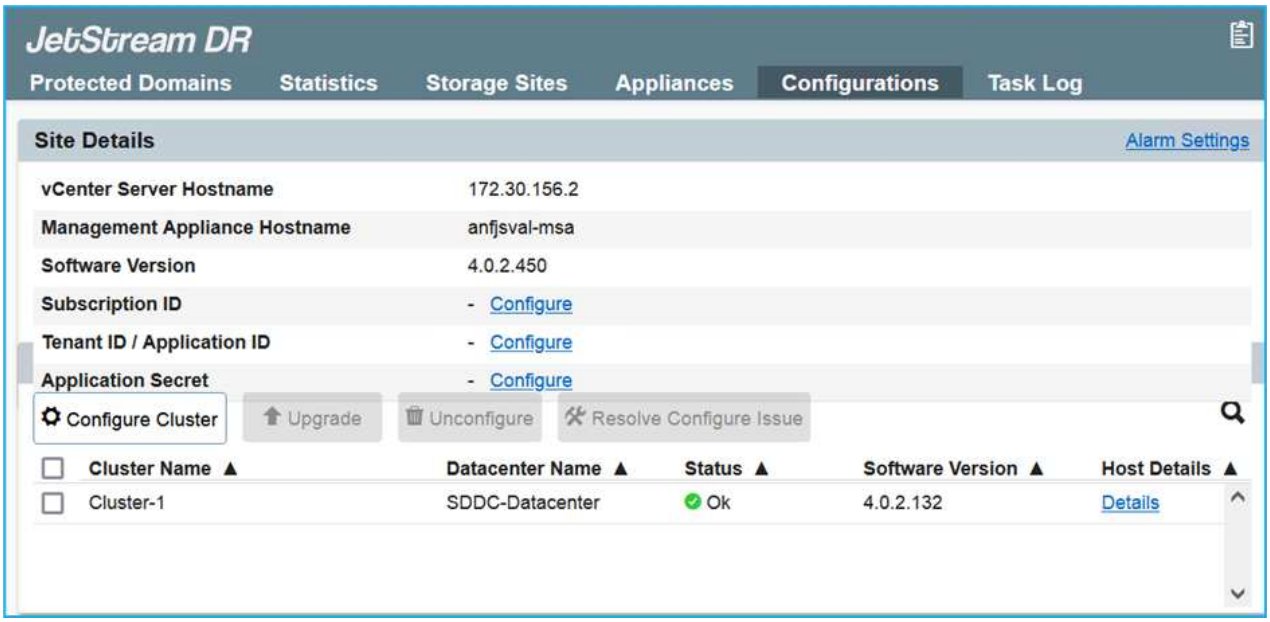
1. Azure VMware 솔루션 프라이빗 클라우드에 AVS용 Jetstream DR을 설치하려면 실행 명령을 사용하십시오. Azure 포털에서 Azure VMware 솔루션으로 이동하고 프라이빗 클라우드를 선택한 다음 명령 실행 > 패키지 > JSDR.Configuration을 선택합니다.

   Azure VMware 솔루션의 기본 CloudAdmin 사용자는 AVS용 Jetstream DR을 설치할 권한이 없습니다. Azure VMware 솔루션을 사용하면 Jetstream DR용 Azure VMware 솔루션 실행 명령을 호출하여 Jetstream DR을 간단하고 자동으로 설치할 수 있습니다.

   다음 스크린샷은 DHCP 기반 IP 주소를 사용한 설치를 보여 줍니다.

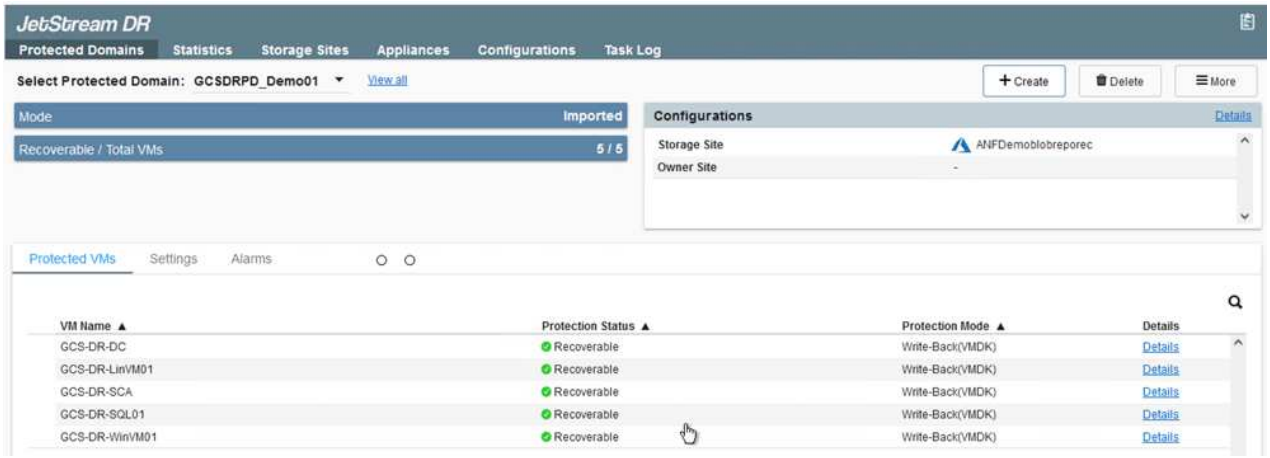


2. AVS 설치를 위한 Jetstream DR이 완료되면 브라우저를 새로 고칩니다. Jetstream DR UI에 액세스하려면 SDDC 데이터 센터 > 구성 > Jetstream DR로 이동하십시오.



3. Jetstream DR 인터페이스에서 다음 작업을 완료합니다.
   a. 온-프레미스 클러스터를 저장소 사이트로 보호하는 데 사용된 Azure Blob 저장소 계정을 추가한 다음 도메인 검사 옵션을 실행합니다.
   b. 나타나는 팝업 대화 상자에서 가져올 보호된 도메인을 선택한 다음 해당 가져오기 링크를 클릭합니다.

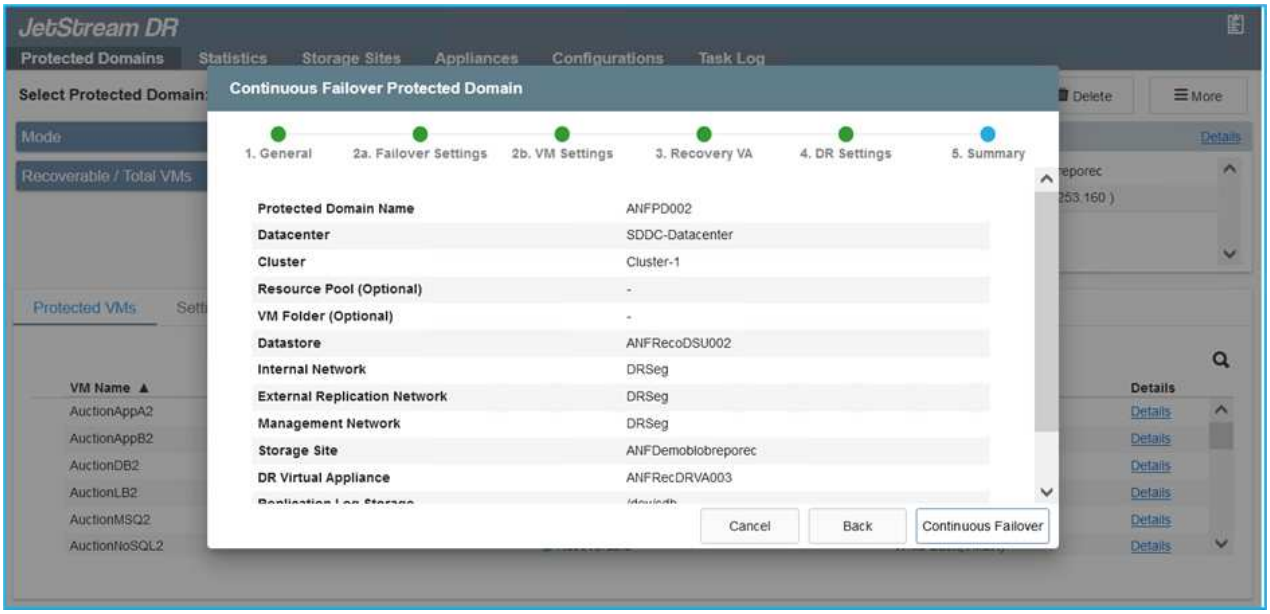
4. 복구를 위해 도메인을 가져옵니다. 보호 도메인 탭으로 이동하여 원하는 도메인이 선택되었는지 확인하거나 보호 도메인 선택 메뉴에서 원하는 도메인을 선택합니다. 보호된 도메인에 있는 복구 가능한 VM 목록이 표시됩니다.



5. 보호된 도메인을 가져온 후 DRVA 어플라이언스를 구축합니다.

CPT 생성 계획을 사용하여 이러한 단계를 자동화할 수도 있습니다.

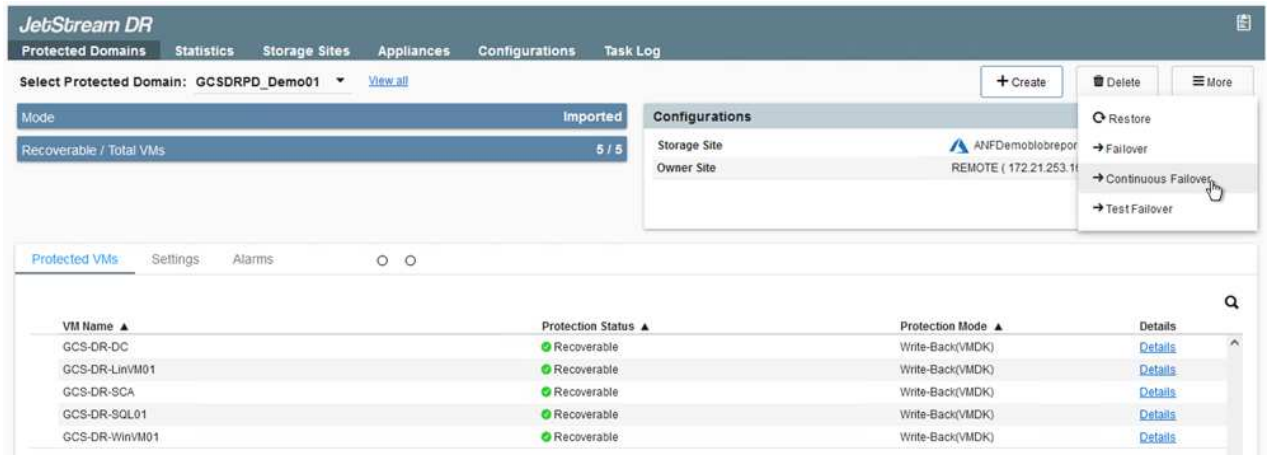
6. 사용 가능한 vSAN 또는 ANF 데이터 저장소를 사용하여 복제 로그 볼륨을 생성합니다.
7. 보호된 도메인을 가져오고 VM 배치에 ANF 데이터 저장소를 사용하도록 복구 VA를 구성합니다.



> 선택한 세그먼트에서 DHCP가 활성화되어 있고 사용 가능한 IP가 충분한지 확인합니다. 도메인이 복구되는 동안 동적 IP가 일시적으로 사용됩니다. 복구 중인 각 VM(연속 재수화 포함)에는 개별 동적 IP가 필요합니다. 복구가 완료되면 IP가 해제되고 다시 사용할 수 있습니다.

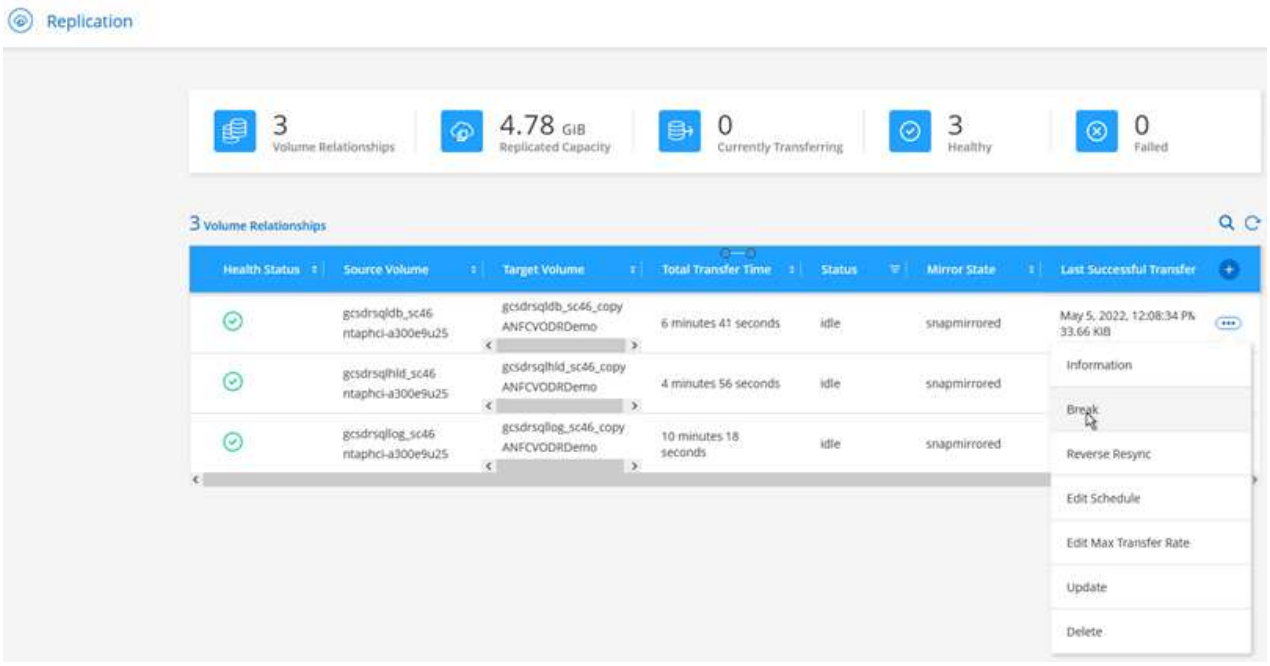
8. 적절한 페일오버 옵션(무중단 페일오버 또는 페일오버)을 선택합니다. 이 예에서는 연속 재수화(연속 페일오버)가 선택됩니다.

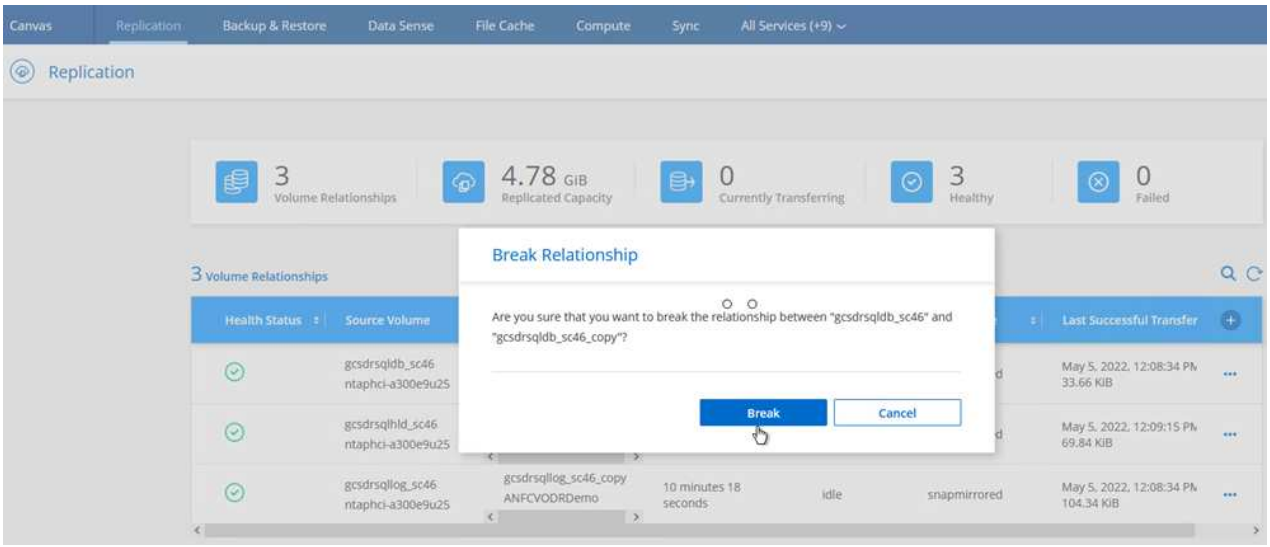
> 연속 페일오버 모드와 페일오버 모드는 구성이 수행될 때 다르지만, 두 페일오버 모드는 동일한 단계를 사용하여 구성됩니다. 장애 조치 단계는 재해 이벤트에 따라 함께 구성 및 수행됩니다. 지속적인 페일오버는 언제든지 구성할 수 있으며, 이후 정상적인 시스템 작동 중에 백그라운드에서 실행될 수 있습니다. 재해 이벤트가 발생한 후 지속적인 페일오버가 완료되어 보호된 VM의 소유권을 복구 사이트로 즉시 전송합니다(제로급 RTO).



지속적인 장애 조치 프로세스가 시작되고 UI에서 진행 상태를 모니터링할 수 있습니다. 현재 단계 섹션에서 파란색 아이콘을 클릭하면 페일오버 프로세스의 현재 단계에 대한 세부 정보를 보여주는 팝업 창이 표시됩니다.

1. 사내 환경의 보호된 클러스터에서 재해가 발생한 후(일부 또는 전체 장애) 해당 애플리케이션 볼륨에 대한 SnapMirror 관계를 끊은 후 Jetstream을 사용하여 VM에 대한 페일오버를 트리거할 수 있습니다.

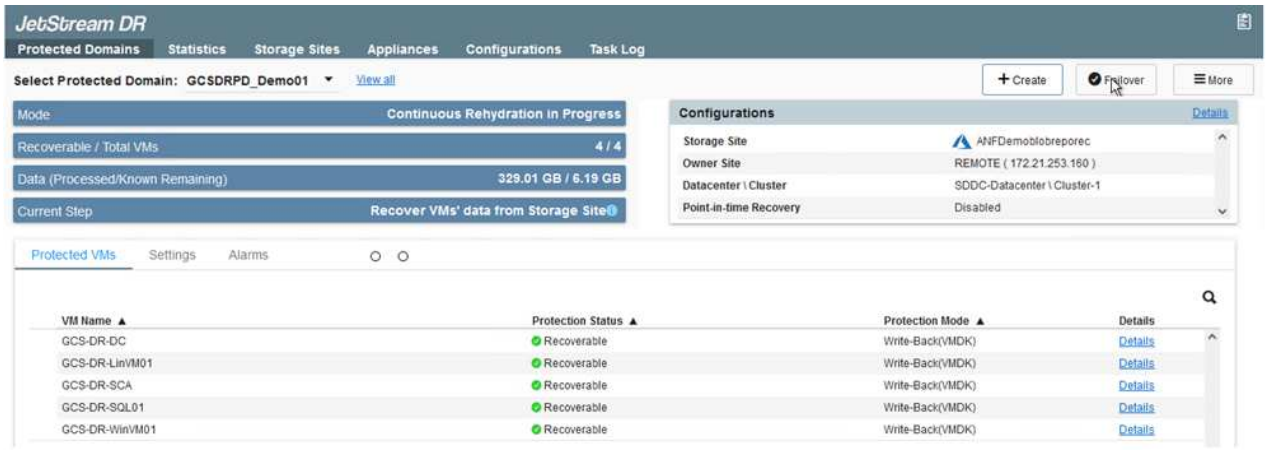


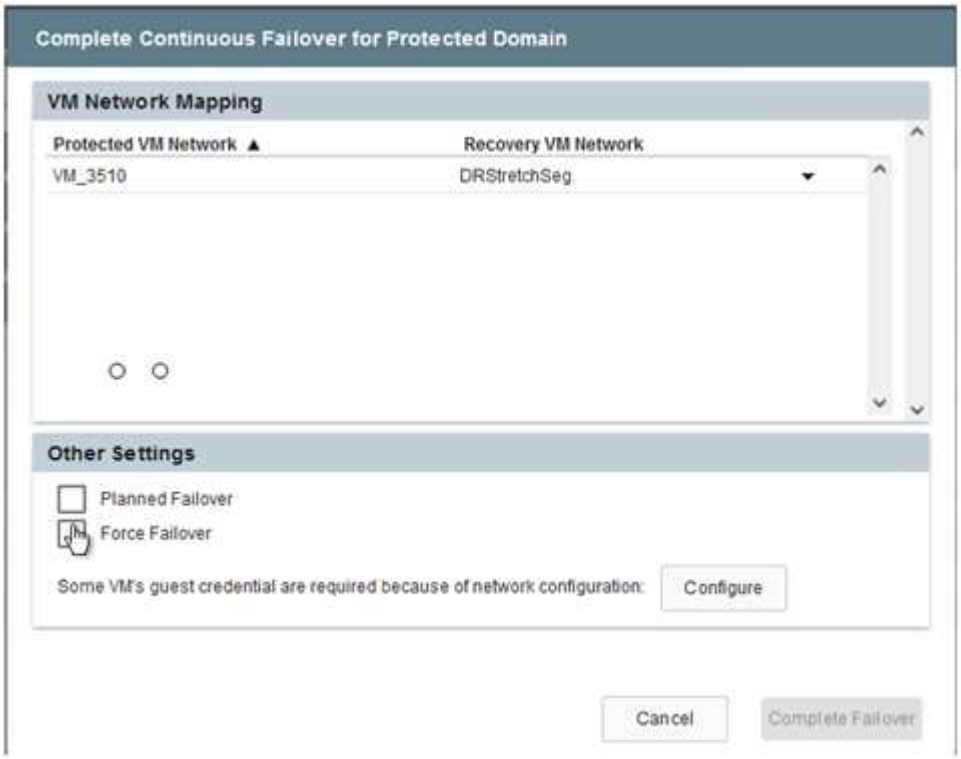


이 단계는 복구 프로세스를 용이하게 하기 위해 쉽게 자동화할 수 있습니다.

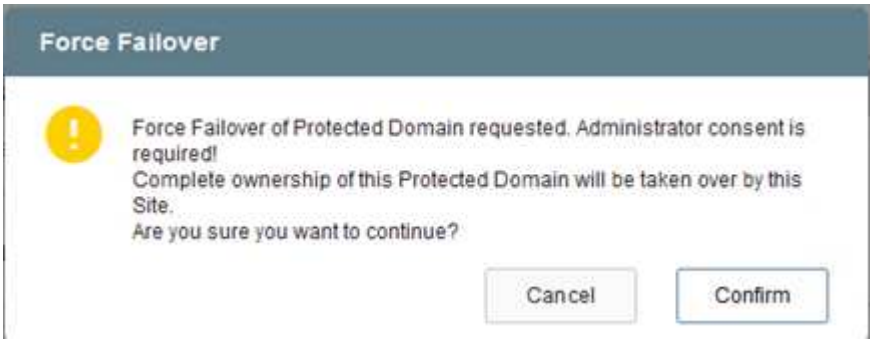
2. AVS SDDC(대상 측)에서 Jetstream UI에 액세스하고 페일오버 옵션을 트리거하여 페일오버를 완료합니다. 작업 표시줄에 장애 조치 작업의 진행률이 표시됩니다.

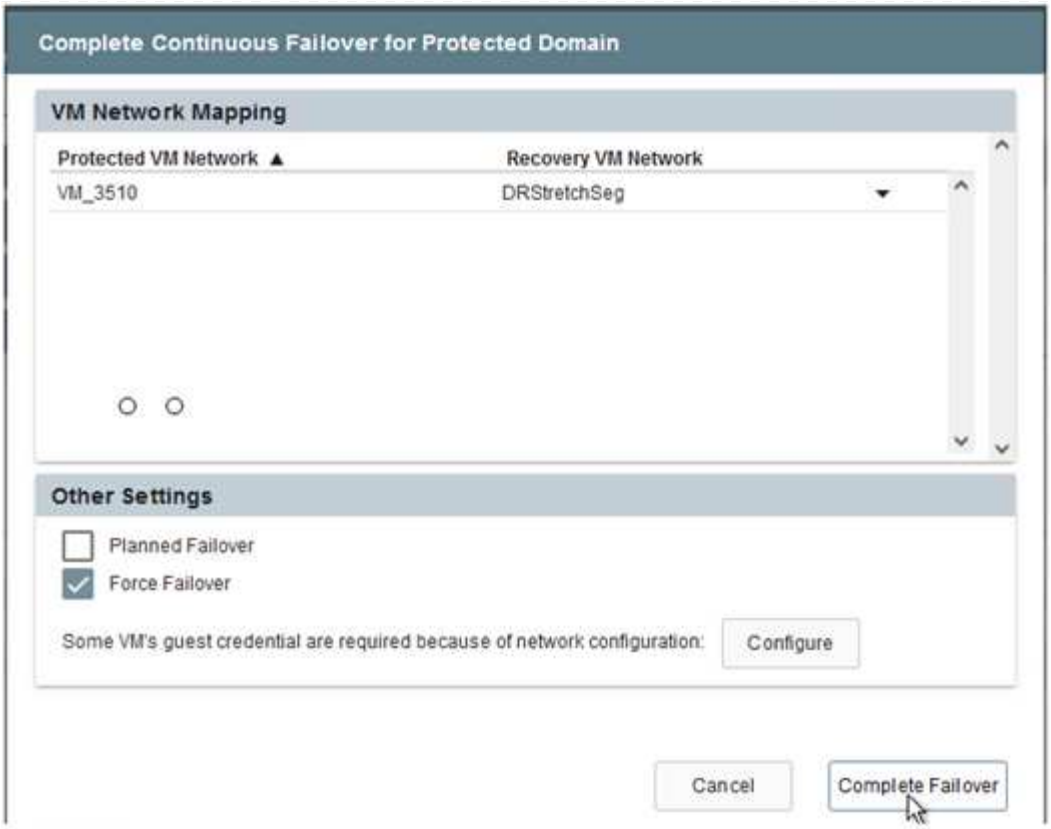
   페일오버를 완료할 때 나타나는 대화 상자에서 페일오버 작업을 계획대로 지정하거나 강제 작업으로 가정할 수 있습니다.





강제 대체 작동 에서는 운영 사이트에 더 이상 액세스할 수 없으며 보호 도메인의 소유권이 복구 사이트에 의해 직접 가정되어야 한다고 가정합니다.





3. 연속 페일오버가 완료되면 작업 완료를 확인하는 메시지가 나타납니다. 작업이 완료되면 복구된 VM에 액세스하여 iSCSI 또는 NFS 세션을 구성합니다.

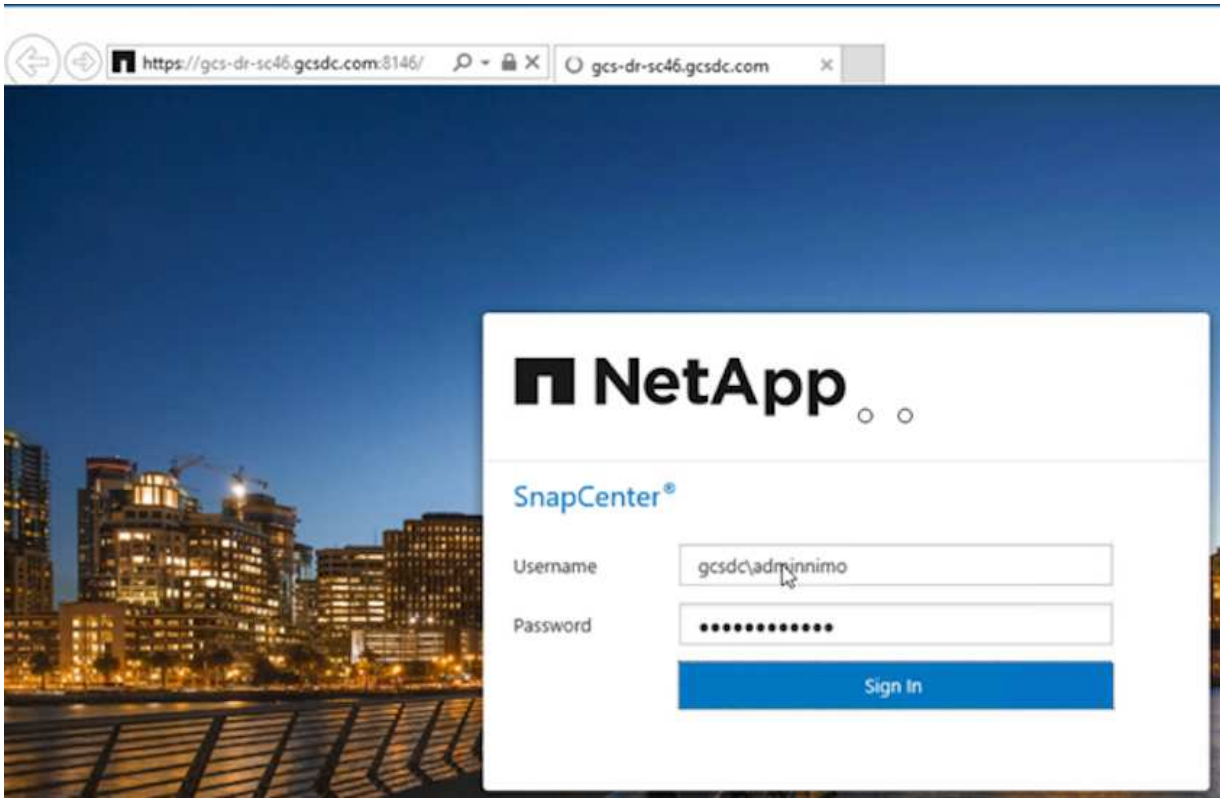
페일오버 모드가 페일오버에서 실행 중으로 변경되고 VM 상태는 복구 가능합니다. 이제 보호 도메인의 모든 VM이 페일오버 Runbook 설정에 지정된 상태의 복구 사이트에서 실행됩니다.

장애 조치 구성 및 인프라를 확인하기 위해 Jetstream DR을 테스트 모드(장애 조치 테스트 옵션)로 작동하여 가상 시스템 및 해당 데이터가 개체 저장소에서 테스트 복구 환경으로 복구되는 것을 관찰할 수 있습니다. 테스트 모드에서 페일오버 절차를 실행하면 실제 페일오버 프로세스와 비슷합니다.

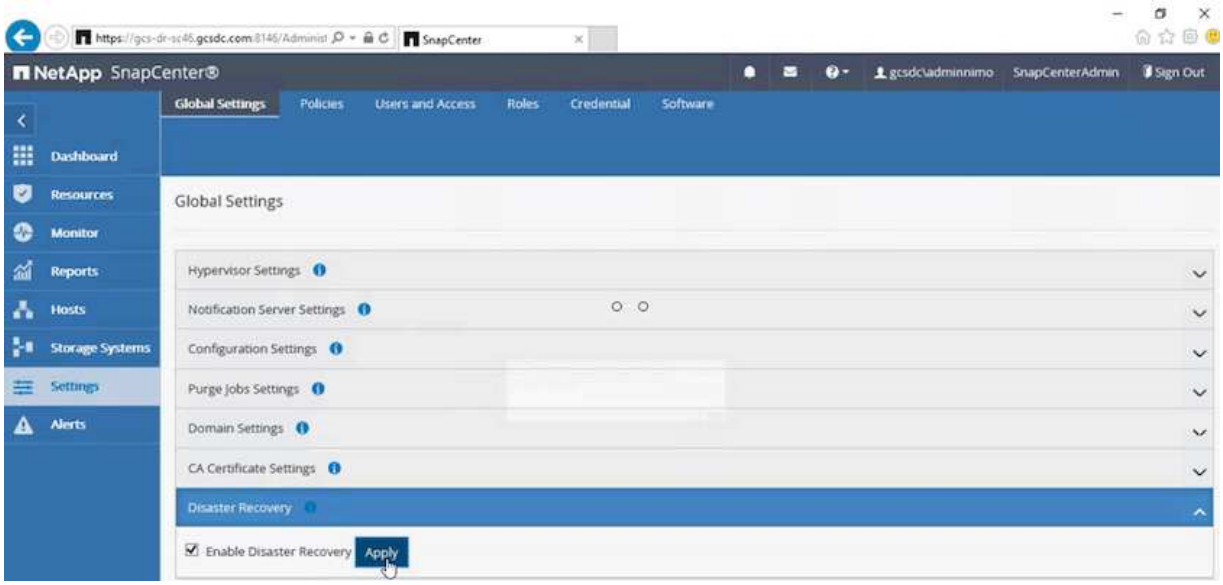
4. 가상 머신이 복구된 후 게스트 내 스토리지에 스토리지 재해 복구를 사용합니다. 이 프로세스를 시연하기 위해

이 예에서는 SQL Server가 사용됩니다.

5. AVS SDDC에서 복구된 SnapCenter VM에 로그인하고 DR 모드를 활성화합니다.
   a. browserN을 사용하여 SnapCenter UI에 액세스합니다.



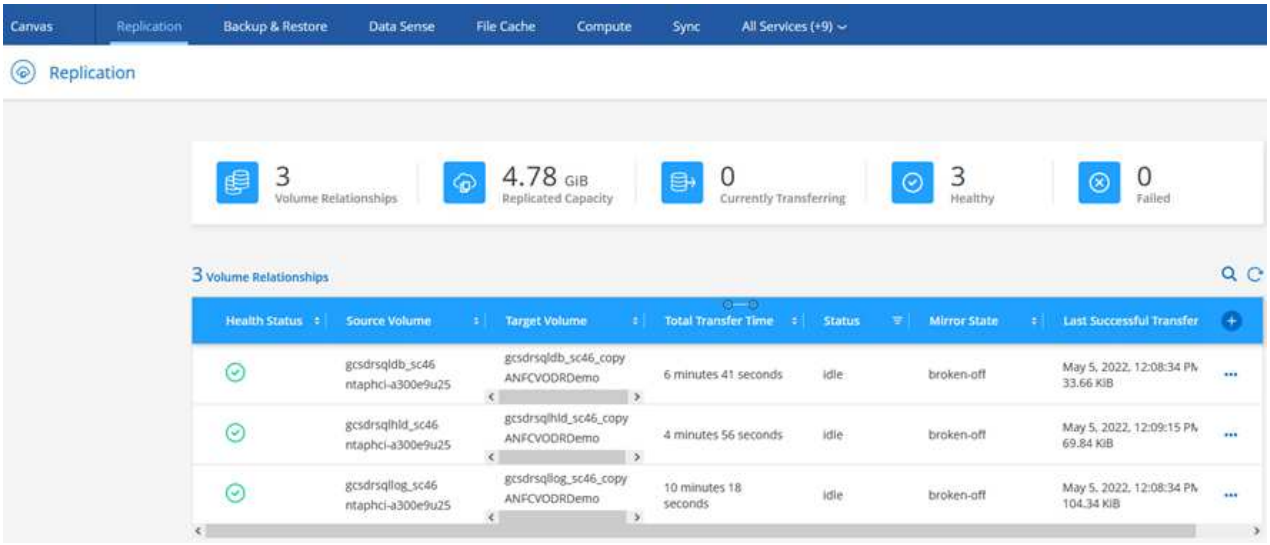
   b. 설정 페이지에서 설정 > 글로벌 설정 > 재해 복구 로 이동합니다.
   c. 재해 복구 활성화 를 선택합니다.
   d. 적용 을 클릭합니다.



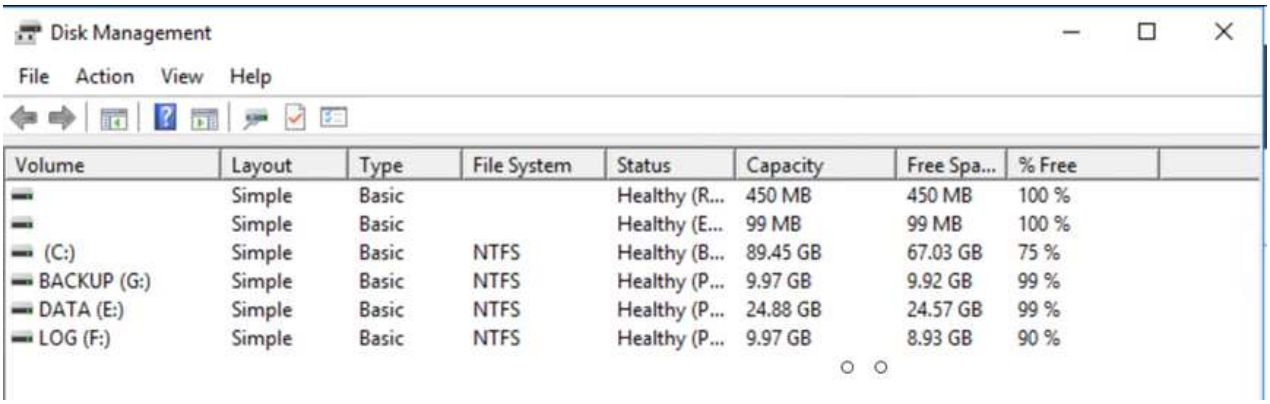
   e. 모니터 > 작업 을 클릭하여 DR 작업이 활성화되었는지 확인합니다.

스토리지 재해 복구에 NetApp SnapCenter 4.6 이상을 사용해야 합니다. 이전 버전의 경우 SnapMirror를 사용하여 복제된 애플리케이션 정합성 보장 스냅샷을 사용해야 하며, 재해 복구 사이트에서 이전 백업을 복구해야 하는 경우 수동 복구를 실행해야 합니다.

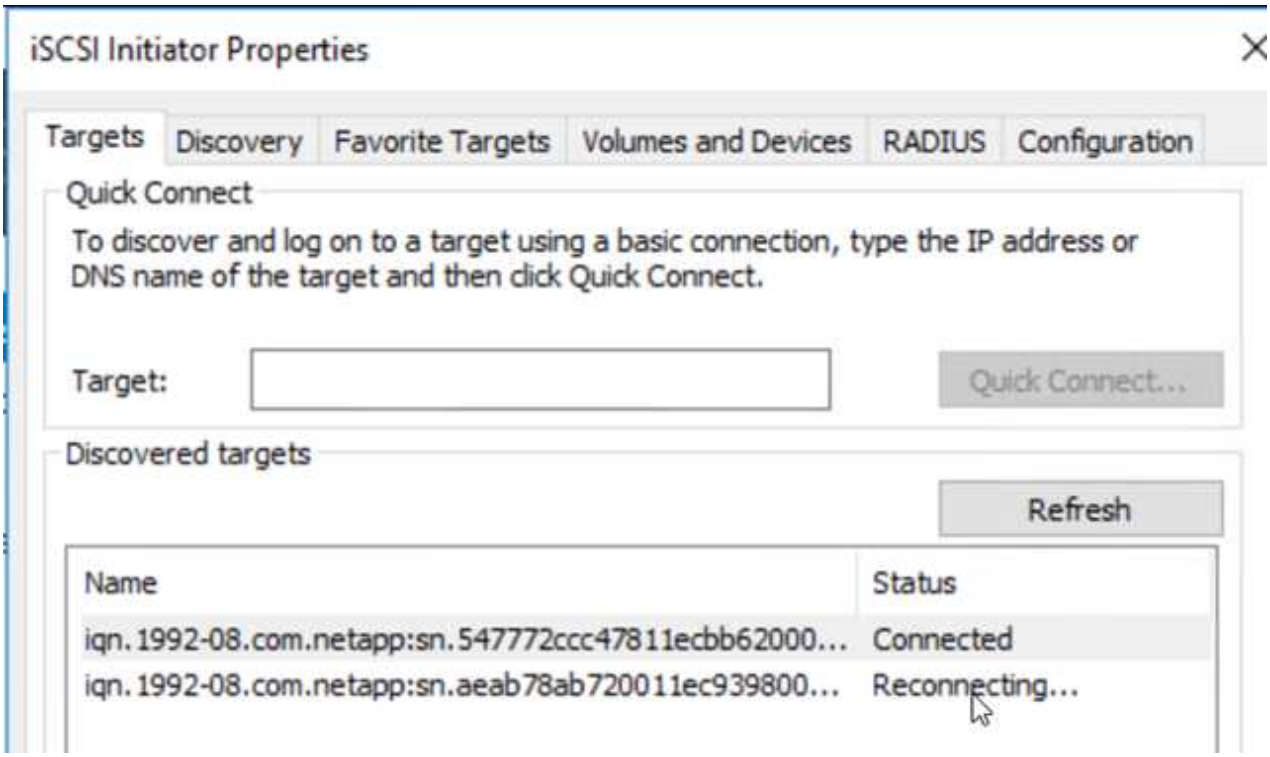
6. SnapMirror 관계가 끊어져 있는지 확인합니다.



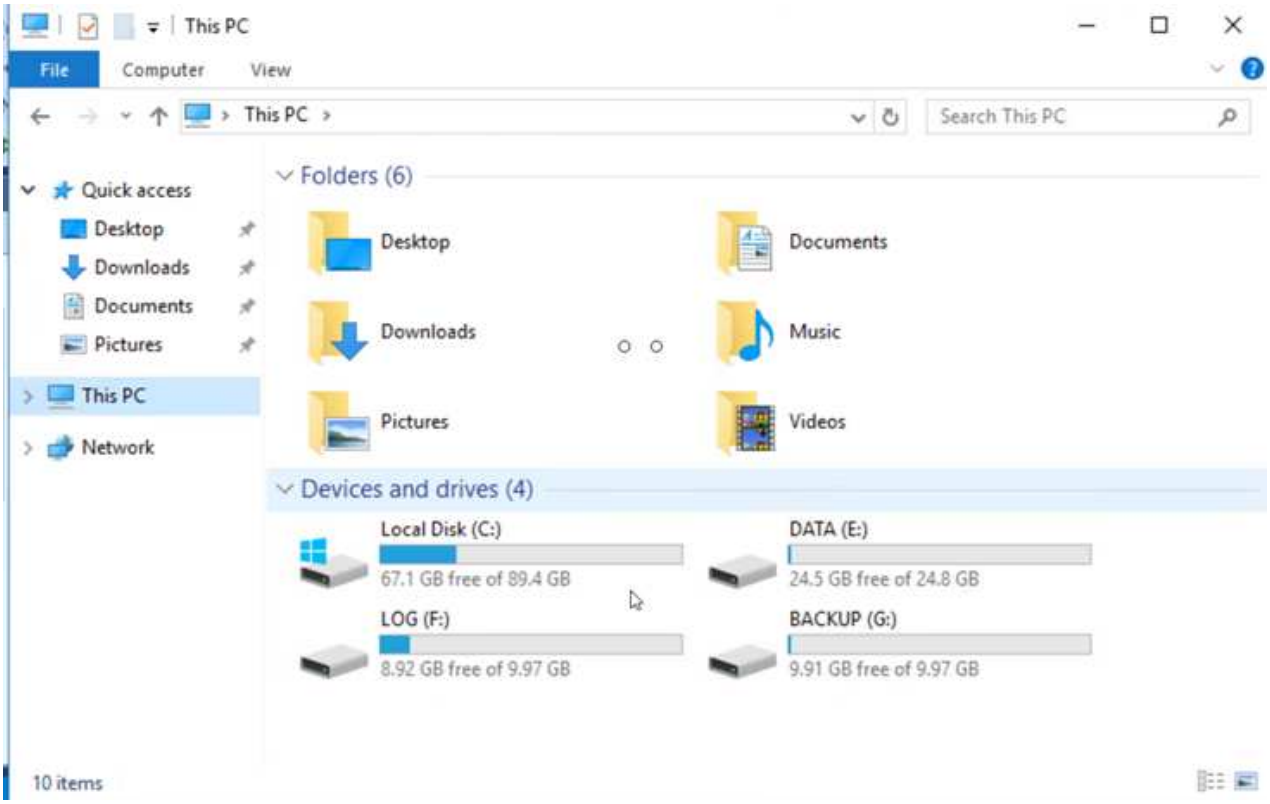
7. Cloud Volumes ONTAP의 LUN을 동일한 드라이브 문자로 복구된 SQL 게스트 VM에 연결합니다.



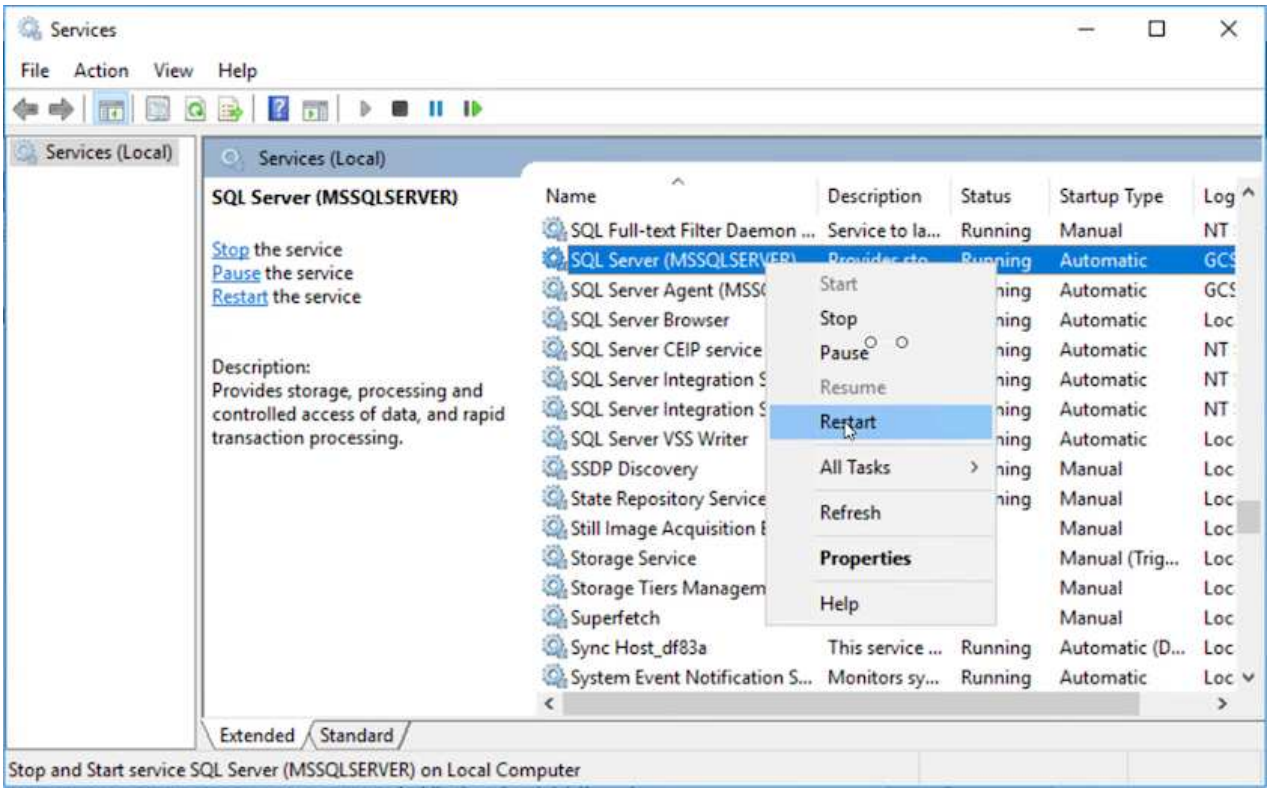
8. iSCSI 초기자를 열고, 이전에 연결이 끊긴 세션을 지우고, 복제된 Cloud Volumes ONTAP 볼륨에 대한 다중 경로와 함께 새 대상을 추가합니다.



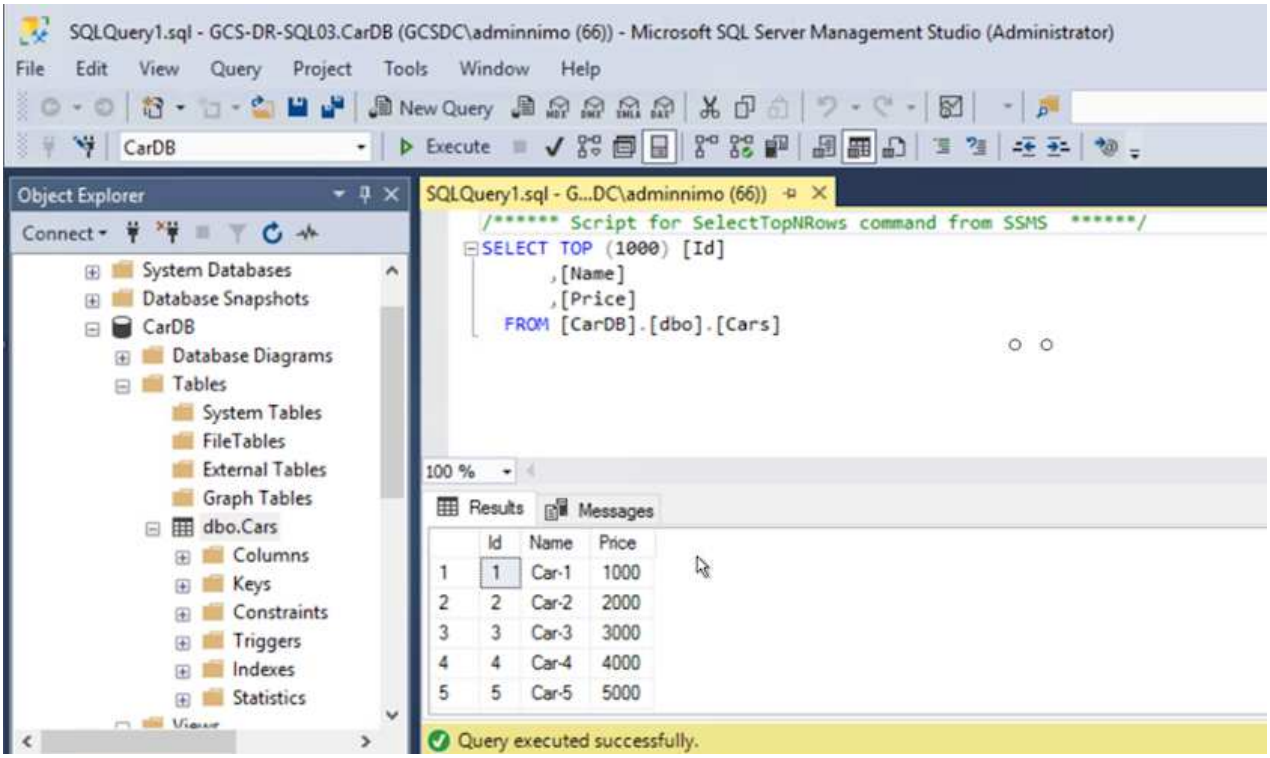
9. DR 이전에 사용한 드라이브 문자와 동일한 드라이브 문자를 사용하여 모든 디스크가 연결되어 있는지 확인합니다.



10. MSSQL 서버 서비스를 다시 시작합니다.



11. SQL 리소스가 다시 온라인 상태인지 확인합니다.



NFS의 경우 mount 명령을 사용하여 볼륨을 연결하고 '/etc/fstab' 항목을 업데이트합니다.

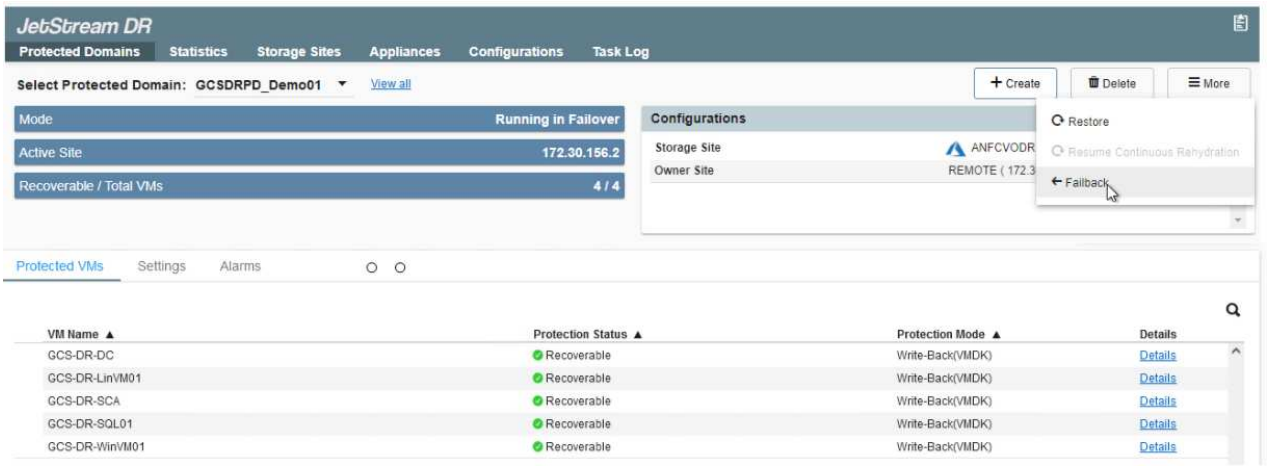
이 시점에서는 작업을 실행하고 정상적으로 비즈니스를 계속할 수 있습니다.

NSX-T 엔드에서는 페일오버 시나리오를 시뮬레이션하기 위해 별도의 전용 Tier-1 게이트웨이를 생성할 수 있습니다. 이렇게 하면 모든 워크로드가 서로 통신할 수 있지만, 트래픽이 환경 내외부로 라우팅될 수는 없으므로 교차 오염의 위험 없이 모든 분류, 억제 또는 강화 작업을 수행할 수 있습니다. 이 작업은 이 문서의 범위를 벗어나지만 격리 시뮬레이션을 위해 쉽게 수행할 수 있습니다.

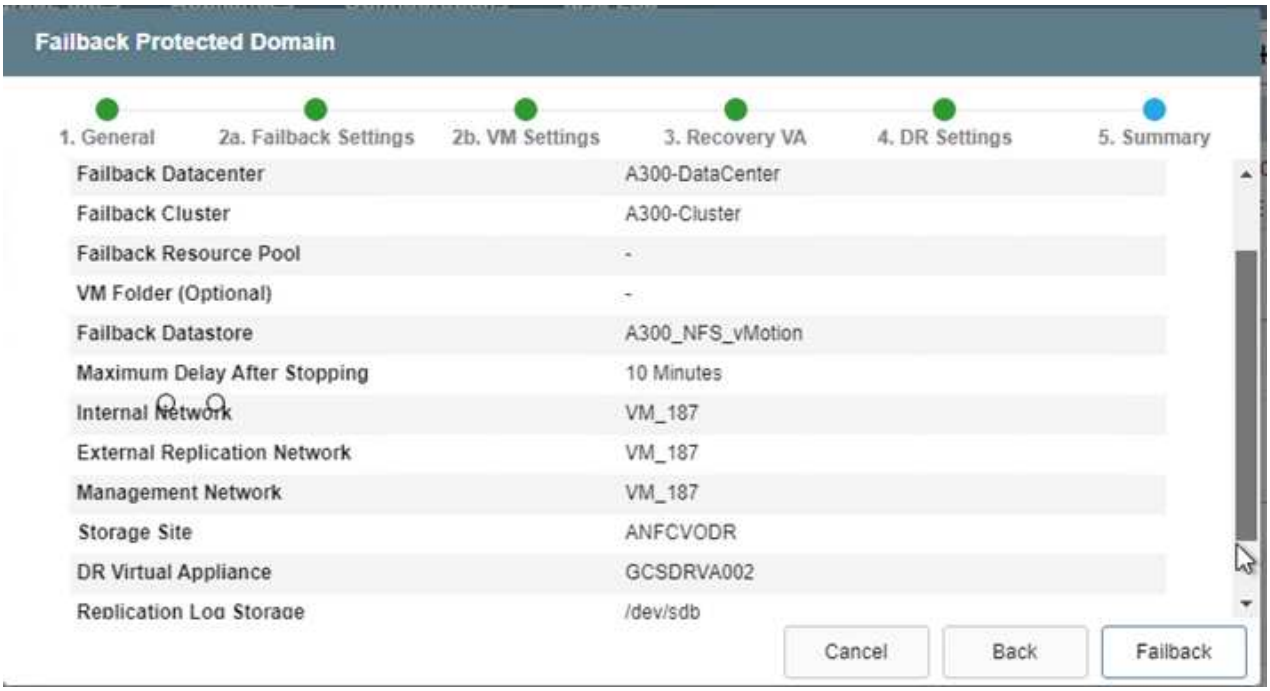
운영 사이트가 다시 가동된 후 페일백을 수행할 수 있습니다. Jetstream에 의해 VM 보호가 재개되고 SnapMirror 관계가 역전되어야 합니다.

1. 사내 환경을 복원합니다. 재해 발생 유형에 따라 보호 클러스터의 구성을 복원 및/또는 확인해야 할 수도 있습니다. 필요한 경우 Jetstream DR 소프트웨어를 재설치해야 할 수 있습니다.
2. 복원된 온프레미스 환경에 액세스하고 Jetstream DR UI로 이동한 다음 적절한 보호 도메인을 선택합니다. 보호 사이트가 페일백될 준비가 되면 UI에서 페일백 옵션을 선택합니다.

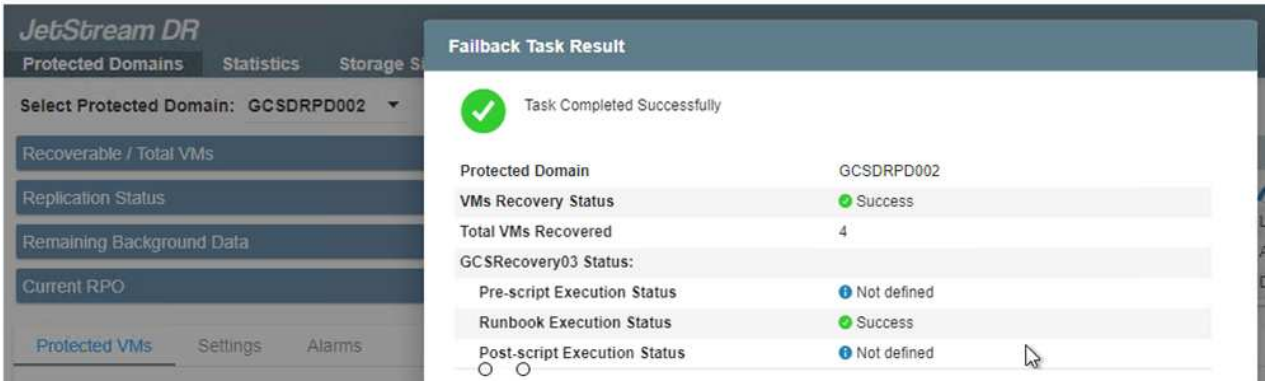
CPT에서 생성한 페일백 계획을 사용하여 VM과 해당 데이터를 오브젝트 저장소에서 원래 VMware 환경으로 되돌릴 수도 있습니다.



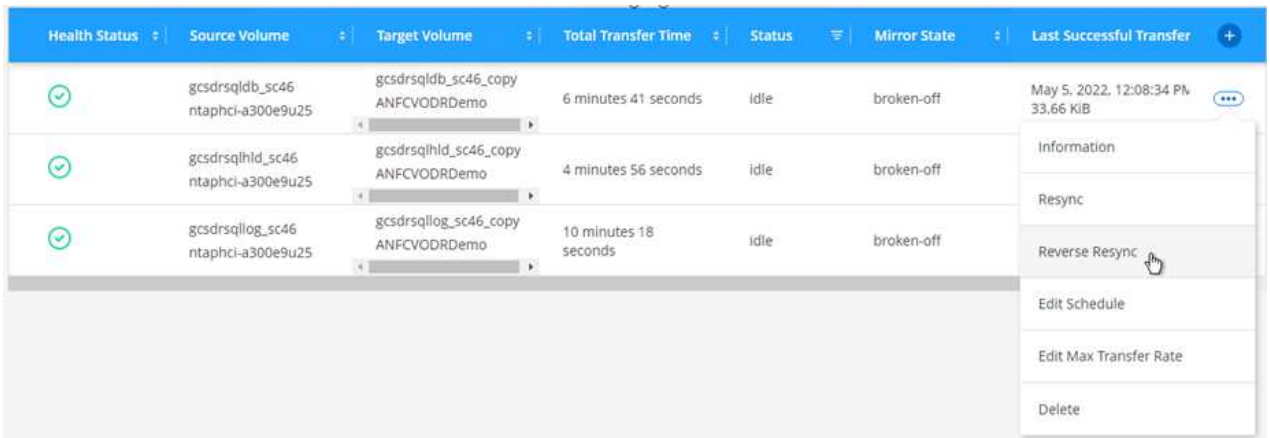
복구 사이트에서 VM을 일시 중지하고 보호 사이트에서 다시 시작한 후 최대 지연 시간을 지정합니다. 이 프로세스를 완료하는 데 필요한 시간은 장애 조치 VM을 중지한 후 복제 완료, 복구 사이트를 청소하는 데 필요한 시간, 보호 사이트에서 VM을 다시 만드는 데 필요한 시간 등을 포함합니다. 10분을 권장합니다.

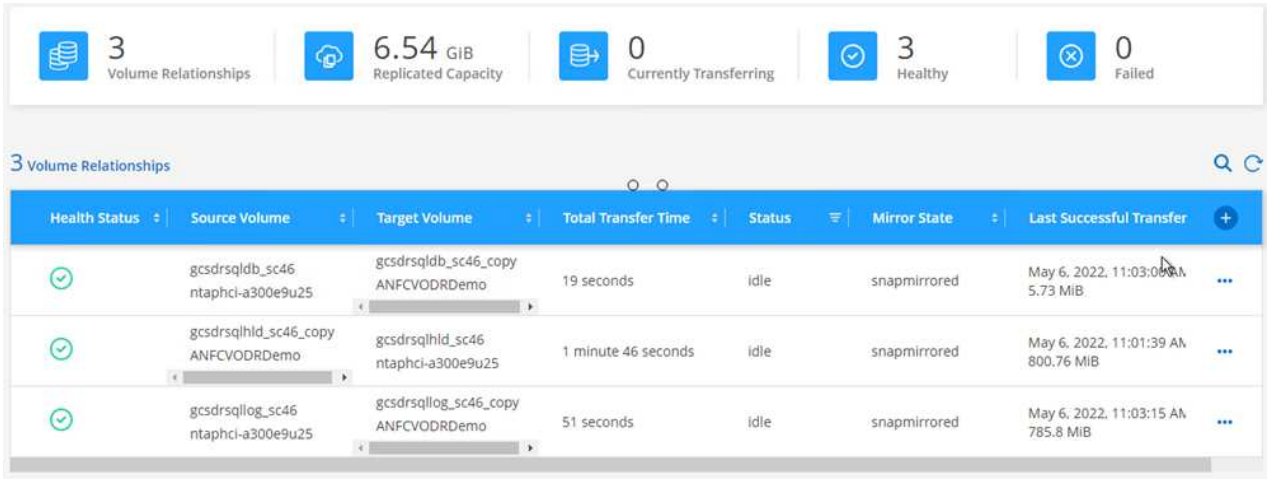


3. 페일백 프로세스를 완료한 다음 VM 보호 및 데이터 정합성 재개를 확인합니다.

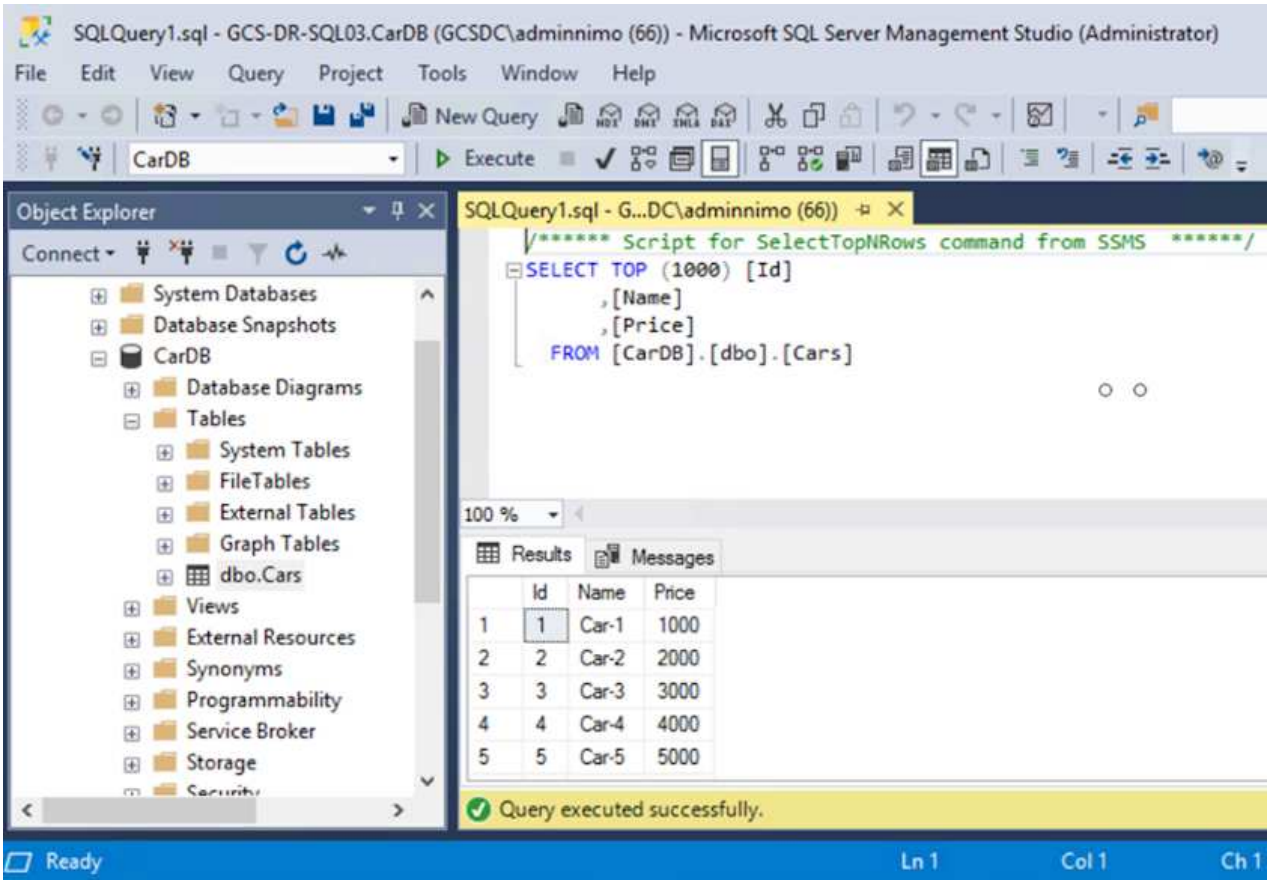


4. VM이 복구된 후 호스트에서 보조 스토리지를 분리하고 운영 스토리지에 접속합니다.





5. MSSQL 서버 서비스를 다시 시작합니다.
6. SQL 리소스가 다시 온라인 상태인지 확인합니다.



운영 스토리지로 페일백하려면 역방향 재동기화 작업을 수행하여 페일오버 전과 관계 방향이 동일한지 확인합니다.

역재동기화 작업 후 운영 스토리지와 보조 스토리지의 역할을 유지하려면 역방향 재동기화 작업을 다시 수행하십시오.

이 프로세스는 Oracle과 같은 다른 애플리케이션, 유사한 데이터베이스 유형 및 게스트 연결 스토리지를 사용하는

다른 애플리케이션에 적용됩니다.

항상 그렇듯이 중요한 워크로드를 운영 환경으로 포팅하기 전에 해당 워크로드를 복구하는 단계를 테스트하십시오.

이 솔루션의 이점

- SnapMirror의 효율적이고 복원력이 뛰어난 복제를 사용합니다.
- ONTAP 스냅샷 보존을 사용하여 사용 가능한 모든 시점 복구
- 스토리지, 컴퓨팅, 네트워크 및 애플리케이션 검증 단계에서 수백 또는 수천 개의 VM을 복구하는 데 필요한 모든 단계에서 완전한 자동화가 가능합니다.
- SnapCenter는 복제된 볼륨을 변경하지 않는 클론 생성 메커니즘을 사용합니다.
  - 이렇게 하면 볼륨 및 스냅숏에 대한 데이터 손상 위험이 방지됩니다.
  - DR 테스트 워크플로우 중에 복제 중단 방지
  - 개발/테스트, 보안 테스트, 패치 및 업그레이드 테스트, 수정 테스트 등 DR 이외의 워크플로우에 DR 데이터를 활용합니다.
- CPU 및 RAM 최적화를 통해 보다 작은 컴퓨팅 클러스터로 복구할 수 있으므로 클라우드 비용을 절감할 수 있습니다.

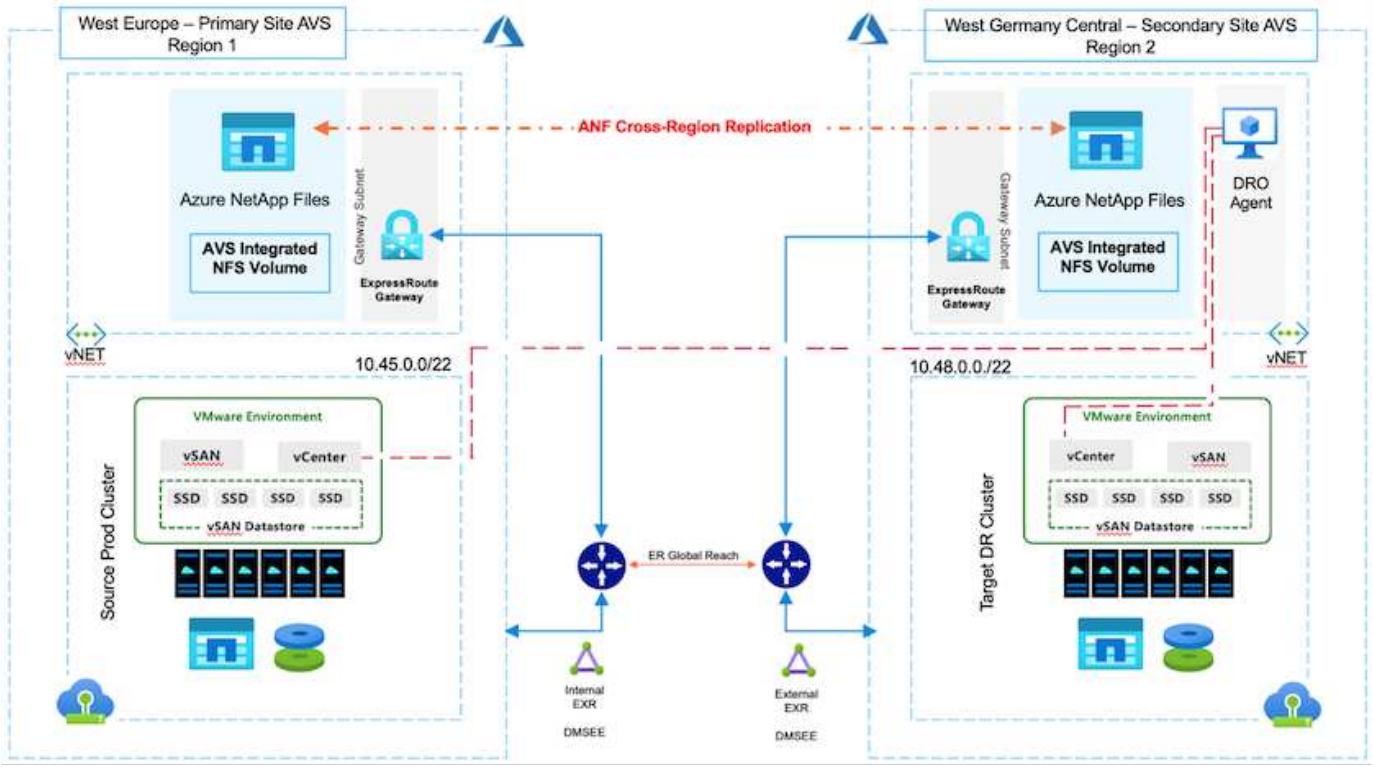
TR-4955: ANF(Azure NetApp Files) 및 **AVS(Azure VMware Solution)**를 통한 재해 복구

저자: Niyaz Mohamed, NetApp 솔루션 엔지니어링

개요

클라우드 내 영역 간의 블록 레벨 복제를 사용하는 재해 복구는 사이트 중단 및 데이터 손상 이벤트(예: 랜섬웨어)로부터 워크로드를 보호하는 복원력이 있고 비용 효율적인 방법입니다. ANF(Azure NetApp Files) 교차 지역 볼륨 복제를 사용하면 Azure NetApp Files 볼륨을 기본 AVS 사이트의 NFS 데이터 저장소로 사용하는 AVS(Azure VMware Solution) SDDC 사이트에서 실행되는 VMware 워크로드를 대상 복구 영역의 지정된 보조 AVS 사이트로 복제할 수 있습니다.

DRO(재해 복구 오케스트레이터)(UI가 포함된 스크립팅된 솔루션)를 사용하여 AVS SDDC 간에 복제된 워크로드를 원활하게 복구할 수 있습니다. DRO는 복제 피어링을 끊은 다음 AVS에 VM 등록을 통해 대상 볼륨을 데이터 저장소로 마운트하고 NSX-T(모든 AVS 프라이빗 클라우드에 포함)에서 직접 네트워크 매핑을 실행하여 복구를 자동화합니다.



필수 구성 요소 및 일반 권장 사항

- 복제 피어링을 생성하여 지역 간 복제를 활성화했는지 확인합니다. 을 참조하십시오 "Azure NetApp Files에 대한 볼륨 복제를 생성합니다".
- 소스 클라우드와 타겟 Azure VMware 솔루션 프라이빗 클라우드 간에 ExpressRoute Global Reach를 구성해야 합니다.
- 리소스에 액세스할 수 있는 서비스 보안 주체가 있어야 합니다.
- 기본 AVS 사이트에서 보조 AVS 사이트로 연결되는 토폴로지는 다음과 같습니다.
- 를 구성합니다 "복제" 비즈니스 요구 및 데이터 변경률에 따라 각 볼륨에 대한 일정을 적절히 조정합니다.

계단식 및 팬인 및 팬아웃 토폴로지는 지원되지 않습니다.

시작하기

Azure VMware 솔루션을 구축합니다

를 클릭합니다 "Azure VMware 솔루션" AVS(AVS)는 Microsoft Azure 퍼블릭 클라우드 내에 완벽하게 작동하는 VMware SDDC를 제공하는 하이브리드 클라우드 서비스입니다. AVS는 Microsoft에서 완벽하게 관리 및 지원하고 Azure 인프라를 사용하는 VMware에서 검증한 최초의 솔루션입니다. 따라서 고객은 컴퓨팅 가상화를 위한 VMware ESXi, 하이퍼 컨버지드 스토리지를 위한 vSAN 및 네트워킹 및 보안을 위한 NSX를 얻는 동시에 Microsoft Azure의 세계적인 입지, 동급 최고의 데이터 센터 시설 및 네이티브 Azure 서비스 및 솔루션의 풍부한 에코시스템에 근접할 수 있는 이점을 누릴 수 있습니다. Azure VMware 솔루션 SDDC와 Azure NetApp Files를 함께 사용하면 네트워크 지연 시간을 최소화하면서 최상의 성능을 얻을 수 있습니다.

Azure에서 AVS 프라이빗 클라우드를 구성하려면 이 단계를 수행하십시오 "링크" NetApp 제품 설명서를 참조하십시오 "링크" Microsoft 설명서를 참조하십시오. 최소 구성으로 설정된 파일럿 라이트 환경을 DR 용도로 사용할 수 있습니다. 이 설정에는 중요한 애플리케이션을 지원하는 핵심 구성 요소만 포함되며, 페일오버가 발생하는 경우 더 많은 호스트를

확장하고 확장하여 대량의 로드를 처리할 수 있습니다.

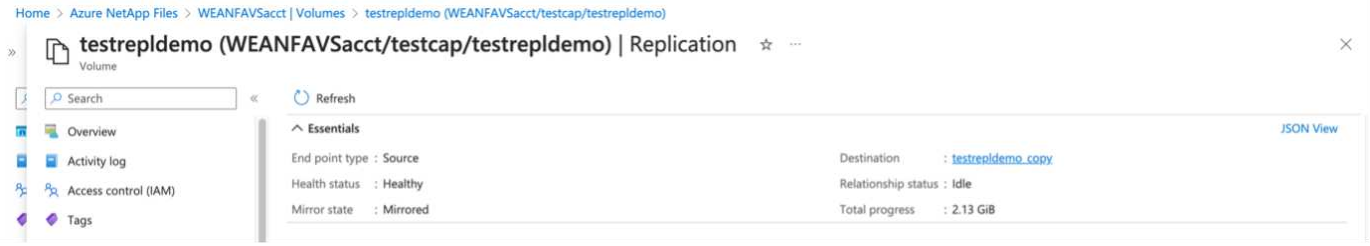
최초 릴리즈에서 DRO는 기존 AVS SDDC 클러스터를 지원합니다. 온디맨드 SDDC 작성은 향후 릴리스에서 제공될 예정입니다.

Azure NetApp Files 프로비저닝 및 구성

"Azure NetApp Files" 는 엔터프라이즈급 고성능 용량제 파일 스토리지 서비스입니다. 이 단계를 따릅니다 "링크" AVS 프라이빗 클라우드 구축을 최적화하기 위해 Azure NetApp Files를 NFS 데이터 저장소로 프로비저닝 및 구성합니다.

Azure NetApp Files 기반 데이터 저장소 볼륨에 대한 볼륨 복제를 생성합니다

첫 번째 단계는 AVS 기본 사이트에서 AVS 보조 사이트로 원하는 데이터 저장소 볼륨에 대한 교차 지역 복제를 적절한 빈도와 보존 기능으로 설정하는 것입니다.



이 단계를 따릅니다 "링크" 복제 피어링을 생성하여 지역 간 복제를 설정합니다. 대상 용량 풀의 서비스 수준은 소스 용량 풀의 서비스 수준과 일치할 수 있습니다. 그러나 이러한 특정 사용 사례에서 표준 서비스 수준을 선택한 다음 "서비스 수준을 수정합니다" 실제 재해 또는 DR 시뮬레이션이 발생하는 경우

교차 지역 복제 관계는 사전 요구 사항으로, 미리 만들어야 합니다.

DRO 설치

DRO를 시작하려면 지정된 Azure 가상 시스템에서 Ubuntu 운영 체제를 사용하고 필수 구성 요소를 충족하는지 확인하십시오. 그런 다음 패키지를 설치합니다.

- 필수 구성 요소: *
- 리소스에 액세스할 수 있는 서비스 보안 주체
- 소스 및 대상 SDDC 및 Azure NetApp Files 인스턴스에 대한 적절한 연결이 있는지 확인합니다.
- DNS 이름을 사용하는 경우 DNS 확인이 필요합니다. 그렇지 않으면 vCenter에 IP 주소를 사용합니다.
- OS 요구 사항: *
- Ubuntu Focal 20.04 (LTS) 지정된 에이전트 가상 머신에 다음 패키지를 설치해야 합니다.
- Docker 를 참조하십시오
- Docker-Compose
- JqChange `docker.sock` 이 새 권한에 대한 설명: `sudo chmod 666 /var/run/docker.sock`.

를 클릭합니다 `deploy.sh` 스크립트는 필요한 모든 필수 구성 요소를 실행합니다.

단계는 다음과 같습니다.

1. 지정된 가상 머신에 설치 패키지를 다운로드합니다.

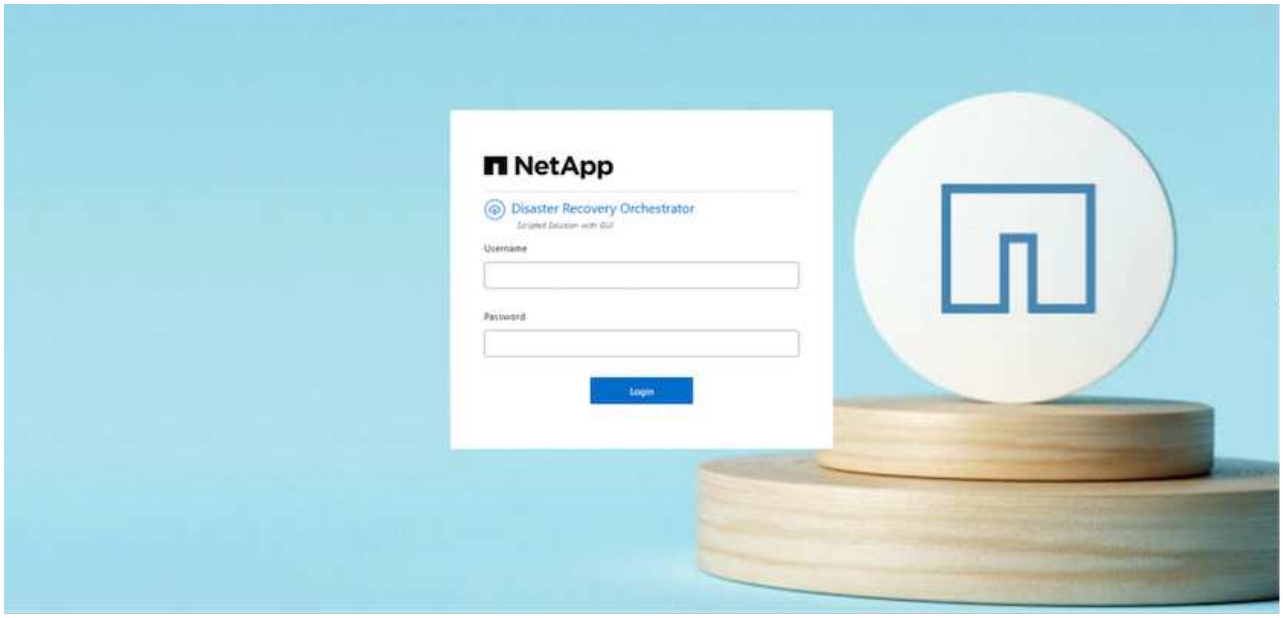
```
git clone https://github.com/NetApp/DRO-Azure.git
```

에이전트는 SDDC와 별도로 AVS 사이트 영역이나 기본 AVS 사이트 영역에 설치해야 합니다.

2. 패키지의 압축을 풀고 배포 스크립트를 실행한 다음 호스트 IP를 입력합니다(예: `10.10.10.10`)를 클릭합니다.

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. 다음 자격 증명을 사용하여 UI에 액세스합니다.
   - 사용자 이름: `admin`
   - 암호: `admin`



DRO 구성

Azure NetApp Files 및 AVS가 올바르게 구성된 후 운영 AVS 사이트에서 보조 AVS 사이트로 워크로드 복구를 자동화하도록 DRO 구성을 시작할 수 있습니다. DRO 에이전트가 네트워크를 통해 적절한 AVS 및 Azure NetApp Files 구성 요소와 통신할 수 있도록 보조 AVS 사이트에 DRO 에이전트를 구축하고 ExpressRoute 게이트웨이 연결을 구성하는 것이 좋습니다.

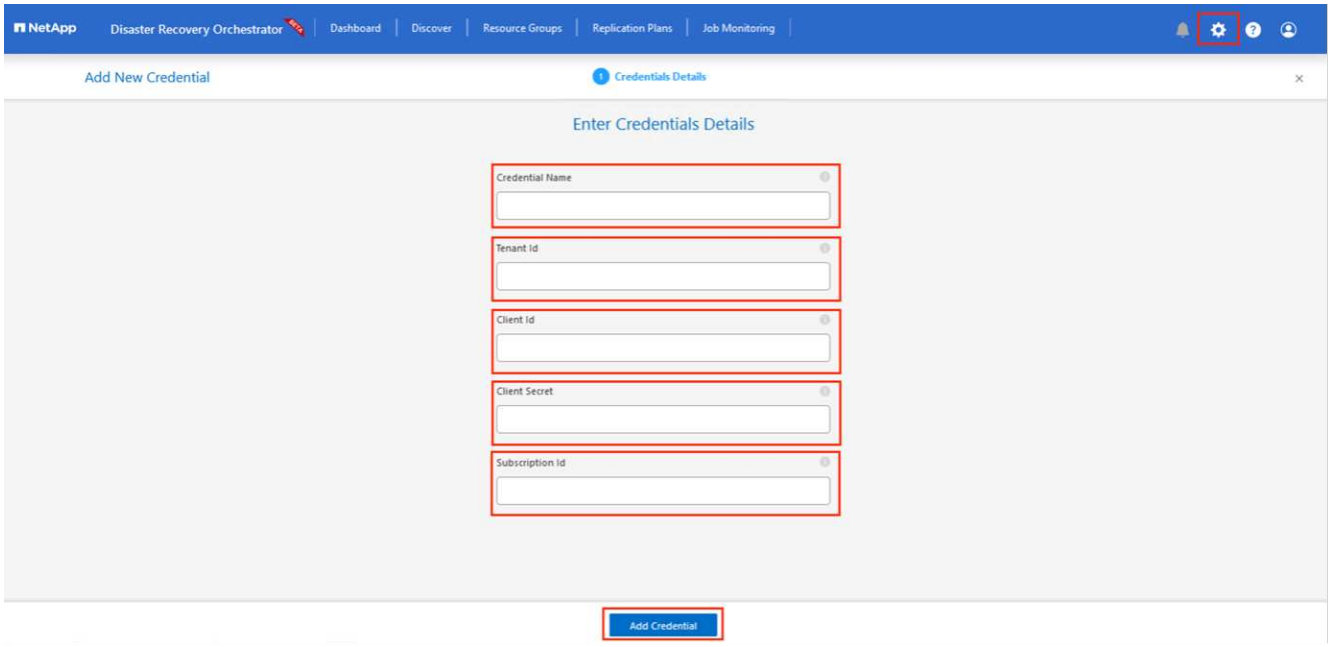
첫 번째 단계는 자격 증명을 추가하는 것입니다. DRO는 Azure NetApp Files 및 Azure VMware 솔루션을 검색할 수 있는 권한이 필요합니다. Azure AD(Active Directory) 응용 프로그램을 생성 및 설정하고 DRO에 필요한 Azure 자격 증명을 획득하여 Azure 계정에 필요한 권한을 부여할 수 있습니다. 서비스 보안 주체를 Azure 구독에 바인딩하고 필요한 관련 권한이 있는 사용자 지정 역할을 할당해야 합니다. 소스 및 대상 환경을 추가하면 서비스 보안 주체와

연결된 자격 증명을 선택하라는 메시지가 표시됩니다. 새 사이트 추가를 클릭하기 전에 이러한 자격 증명을 DRO에 추가해야 합니다.

이 작업을 수행하려면 다음 단계를 수행하십시오.

1. 지원되는 브라우저에서 DRO를 열고 기본 사용자 이름과 암호를 사용합니다 /admin/admin)를 클릭합니다. 암호는 암호 변경 옵션을 사용하여 처음 로그인한 후 재설정할 수 있습니다.
2. DRO 콘솔의 오른쪽 상단에서 * 설정 * 아이콘을 클릭하고 * 자격 증명 * 을 선택합니다.
3. 새 자격 증명 추가 를 클릭하고 마법사의 단계를 따릅니다.
4. 자격 증명을 정의하려면 필요한 권한을 부여하는 Azure Active Directory 서비스 보안 주체에 대한 정보를 입력합니다.
   - 자격 증명 이름입니다
   - 테넌트 ID입니다
   - 클라이언트 ID입니다
   - 클라이언트 암호
   - 구독 ID입니다

     AD 응용 프로그램을 만들 때 이 정보를 캡처해야 합니다.
5. 새 자격 증명에 대한 세부 정보를 확인하고 자격 증명 추가 를 클릭합니다.

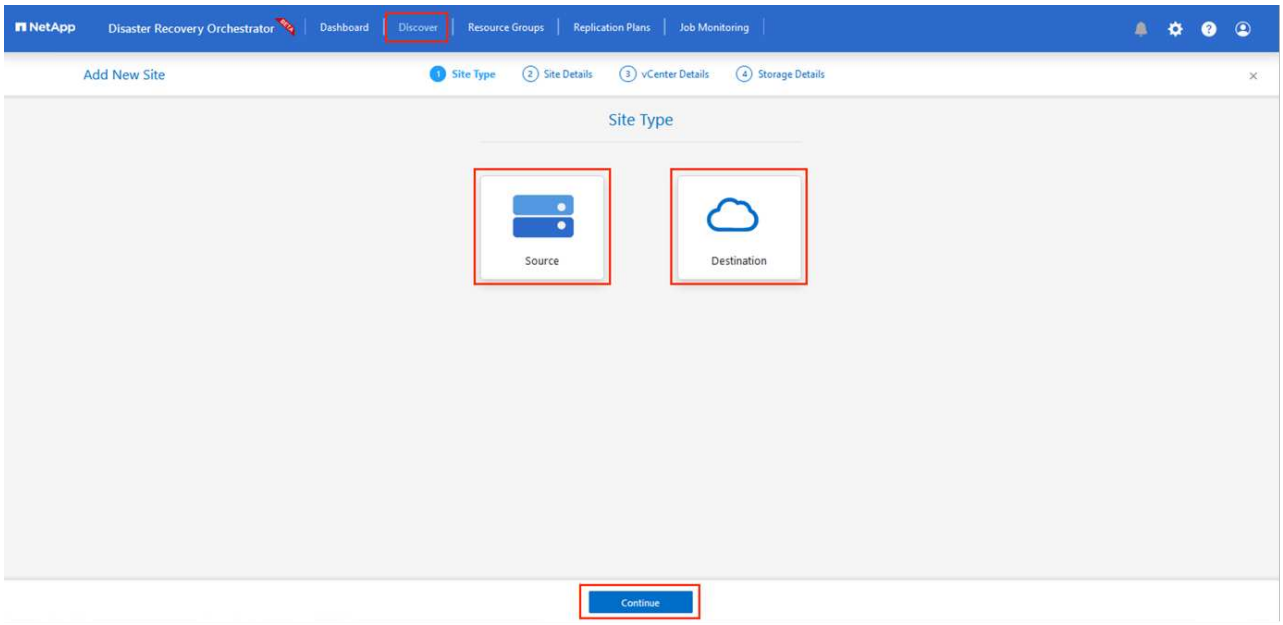


자격 증명을 추가한 후에는 운영 및 보조 AVS 사이트(vCenter 및 Azure NetApp Files 스토리지 계정 모두)를 검색하고 DRO에 추가해야 합니다. 소스 및 대상 사이트를 추가하려면 다음 단계를 수행하십시오.

6. 검색 * 탭으로 이동합니다.
7. 새 사이트 추가 * 를 클릭합니다.
8. 다음 기본 AVS 사이트(콘솔에서 * 소스 * 로 지정됨)를 추가합니다.
   - SDDC vCenter

- Azure NetApp Files 스토리지 계정입니다

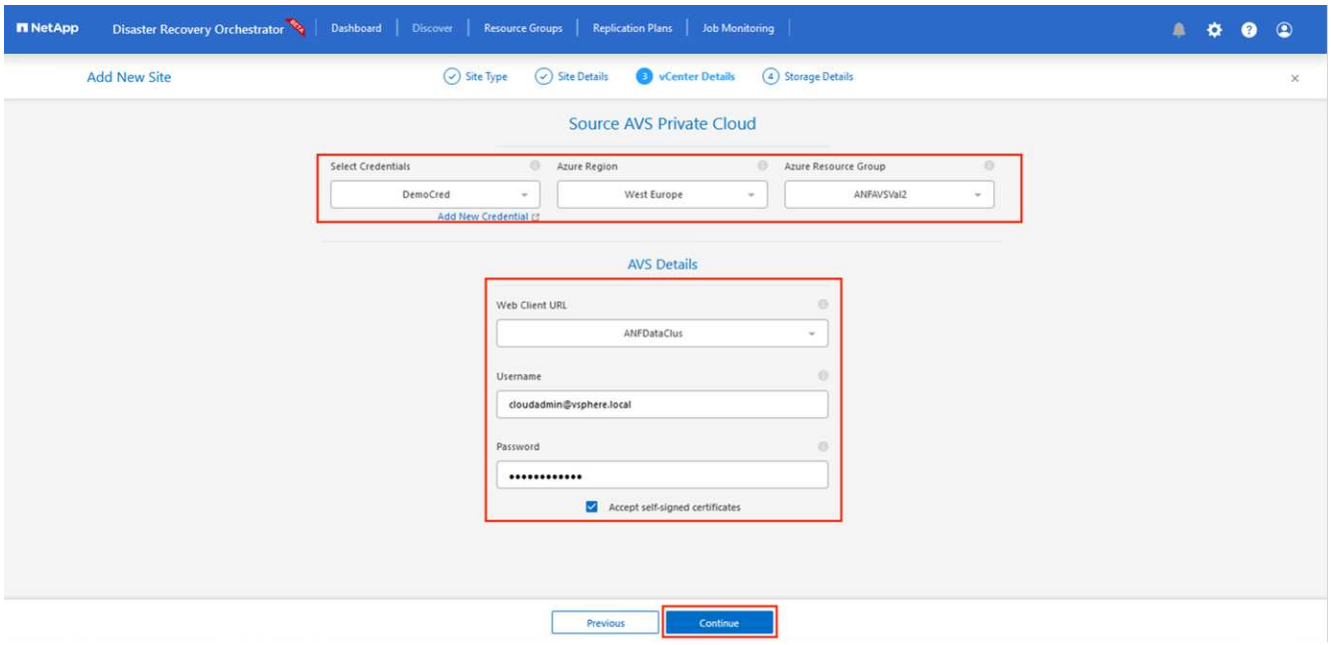
9. 다음 보조 AVS 사이트(* 콘솔에서 * 대상 * 으로 지정됨)를 추가합니다.
   - SDDC vCenter
   - Azure NetApp Files 스토리지 계정입니다



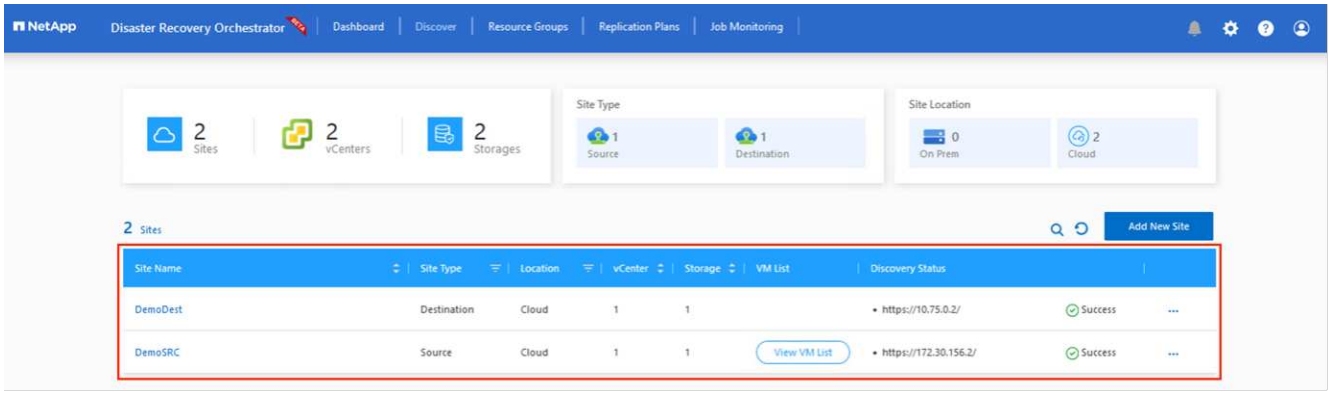
10. Source, * 를 차례로 클릭하여 사이트 세부 정보를 추가하고 친숙한 사이트 이름을 입력한 다음 커넥터를 선택합니다. 그런 다음 * 계속 * 을 클릭합니다.

   데모용으로 소스 사이트 추가는 이 문서에서 다룹니다.

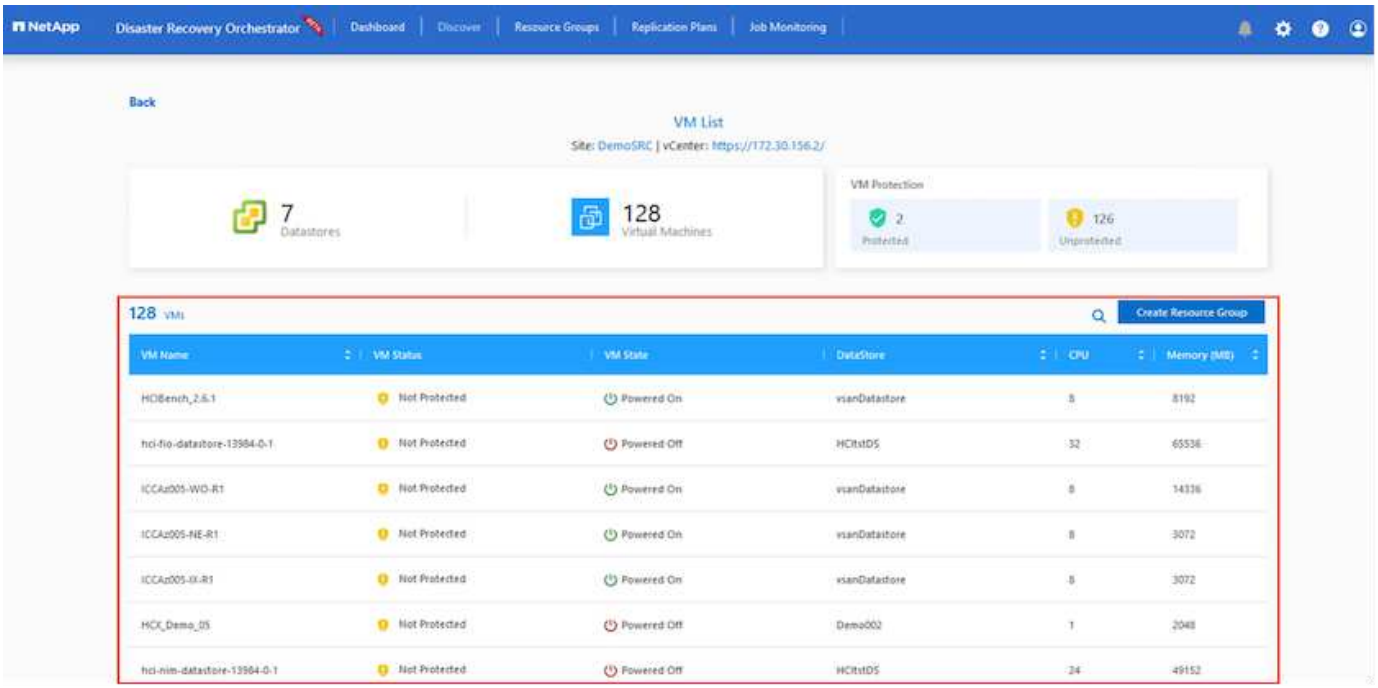
11. vCenter 세부 정보를 업데이트합니다. 이렇게 하려면 기본 AVS SDDC 드롭다운에서 자격 증명, Azure 지역 및 리소스 그룹을 선택합니다.
12. DRO는 해당 지역 내에서 사용 가능한 모든 DC를 나열합니다. 드롭다운에서 지정된 사설 클라우드 URL을 선택합니다.
13. 를 입력합니다 `cloudadmin@vsphere.local` 사용자 자격 증명. 이 기능은 Azure Portal에서 액세스할 수 있습니다. 여기에 설명된 단계를 따릅니다 "링크". 완료되면 * Continue * 를 클릭합니다.



14. Azure Resource 그룹과 NetApp 계정을 선택하여 Source Storge 세부 정보(ANF)를 선택합니다.
15. Create Site * 를 클릭합니다.



DRO가 추가되면 자동 검색을 수행하고 소스 사이트에서 대상 사이트로 해당 지역 간 복제본이 있는 VM을 표시합니다. DRO는 VM에서 사용하는 네트워크와 세그먼트를 자동으로 감지하여 채웁니다.



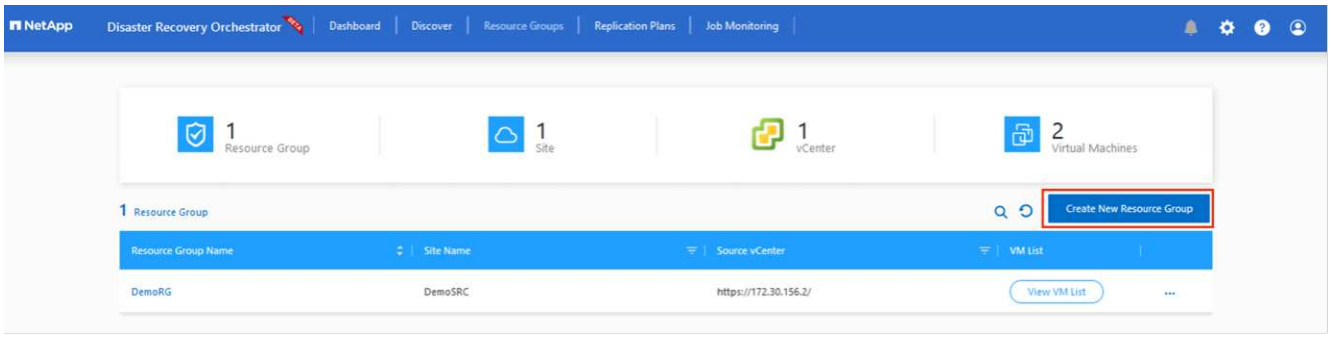
다음 단계는 필요한 VM을 자원 그룹으로 그룹화하는 것입니다.

리소스 그룹화

플랫폼을 추가한 후 복구하려는 VM을 리소스 그룹으로 그룹화합니다. DRO 리소스 그룹을 사용하면 종속 VM 집합을 부팅 순서, 부팅 지연 및 복구 시 실행할 수 있는 선택적 응용 프로그램 유효성 검사가 포함된 논리 그룹으로 그룹화할 수 있습니다.

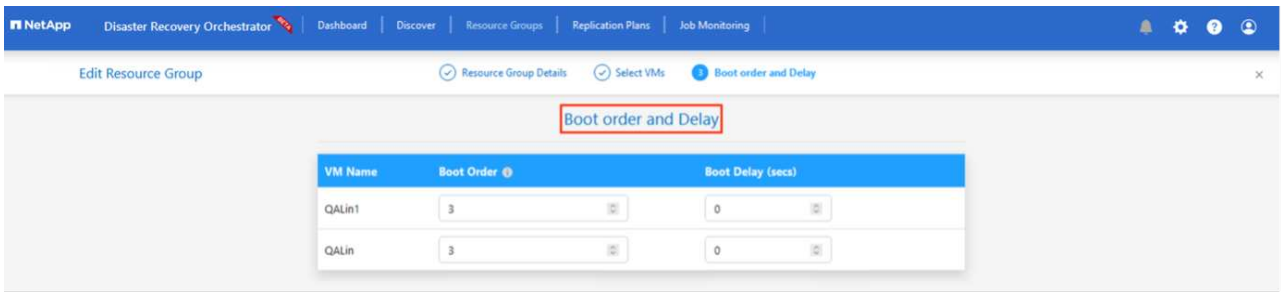
자원 그룹 만들기를 시작하려면 * 새 자원 그룹 만들기 * 메뉴 항목을 클릭합니다.

1. Resource 그룹 * PS에 액세스하고 * Create New Resource Group * 을 클릭합니다.

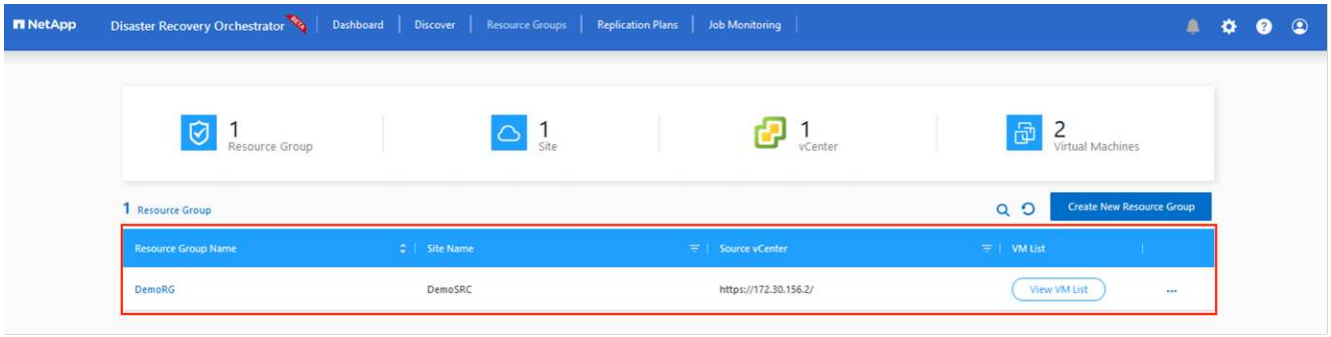


2. 새 리소스 그룹 아래의 드롭다운에서 소스 사이트를 선택하고 * 만들기 * 를 클릭합니다.
3. 리소스 그룹 세부 정보를 입력하고 * Continue * 를 클릭합니다.
4. 검색 옵션을 사용하여 적절한 VM을 선택합니다.
5. 선택한 모든 VM에 대해 * 부트 순서 * 및 * 부트 지연 * (초)을 선택합니다. 각 가상 머신을 선택하고 우선 순위를 설정하여 전원 켜기 순서의 순서를 설정합니다. 모든 가상 머신의 기본값은 3입니다. 옵션은 다음과 같습니다.
   - 전원을 켤 첫 번째 가상 시스템
   - 기본값

◦ 전원을 켤 마지막 가상 컴퓨터



6. 리소스 그룹 만들기 * 를 클릭합니다.

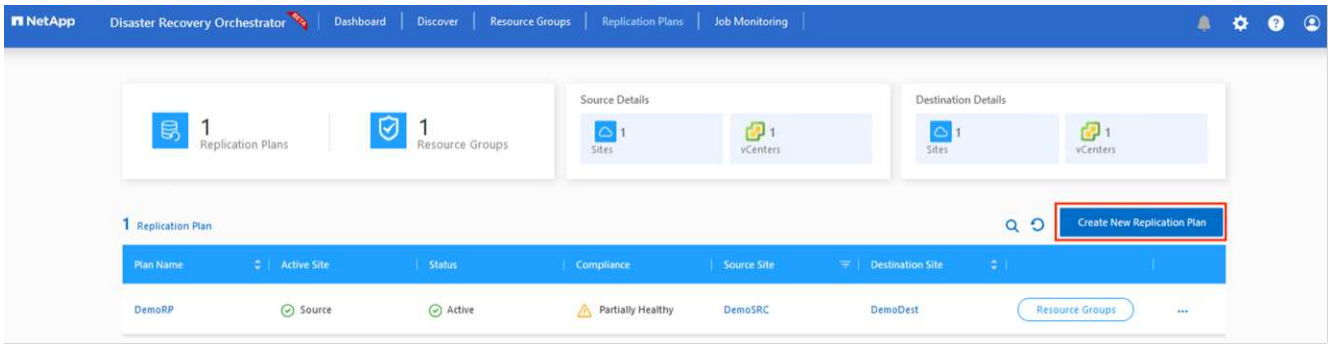


복제 계획

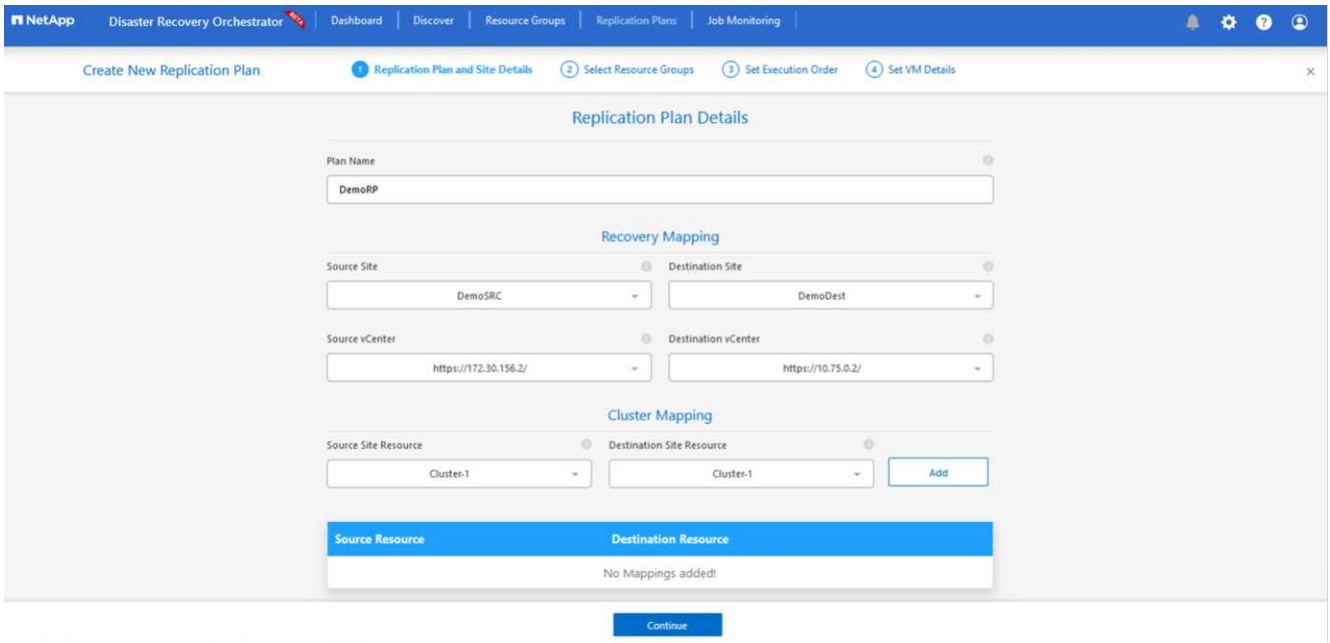
재해가 발생할 경우 애플리케이션을 복구할 계획이 있어야 합니다. 드롭다운에서 소스 및 대상 vCenter 플랫폼을 선택하고, 이 계획에 포함할 리소스 그룹을 선택하고, 애플리케이션 복구 및 전원 켜기 방식(예: 도메인 컨트롤러, 계층 1, 계층 2 등)의 그룹도 포함합니다. 계획도 종종 청사진이라고 부릅니다. 복구 계획을 정의하려면 Replication Plan 탭으로 이동하여 * New Replication Plan * 을 클릭합니다.

복제 계획 생성을 시작하려면 다음 단계를 수행하십시오.

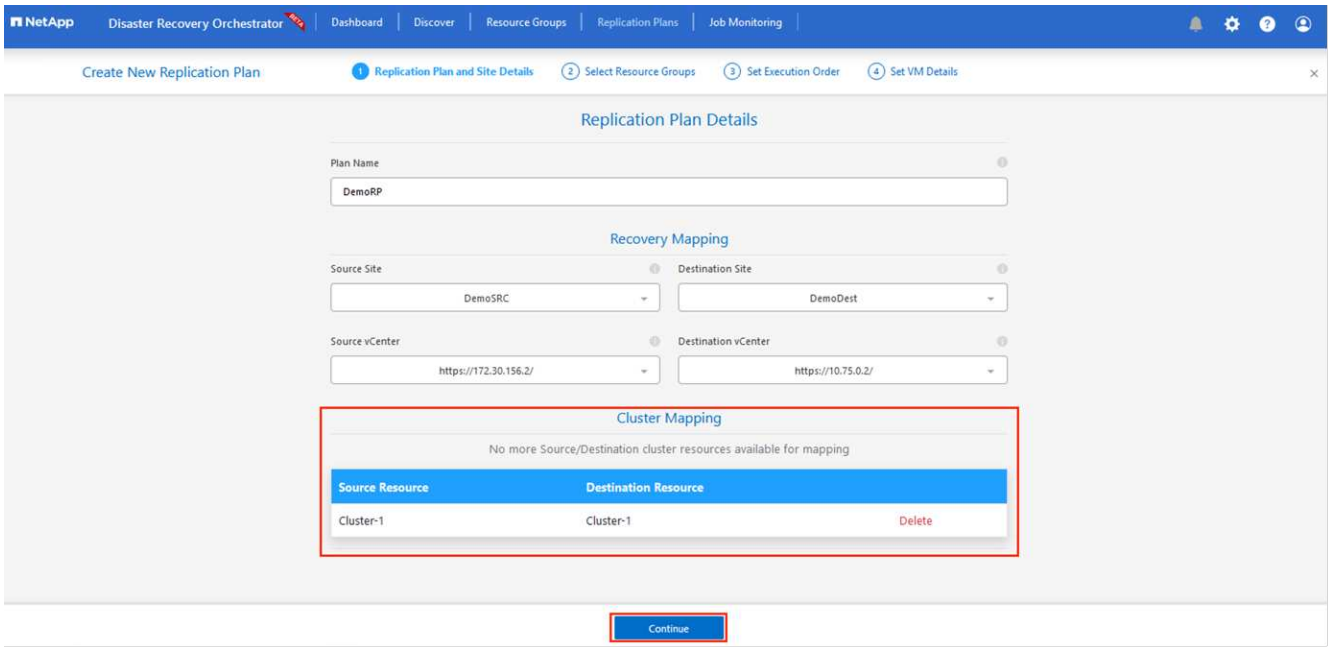
1. Replication Plans * 로 이동하고 * Create New Replication Plan * 을 클릭합니다.



2. 새 복제 계획 * 에서 소스 사이트, 연결된 vCenter, 대상 사이트 및 연결된 vCenter를 선택하여 계획의 이름을 제공하고 복구 매핑을 추가합니다.

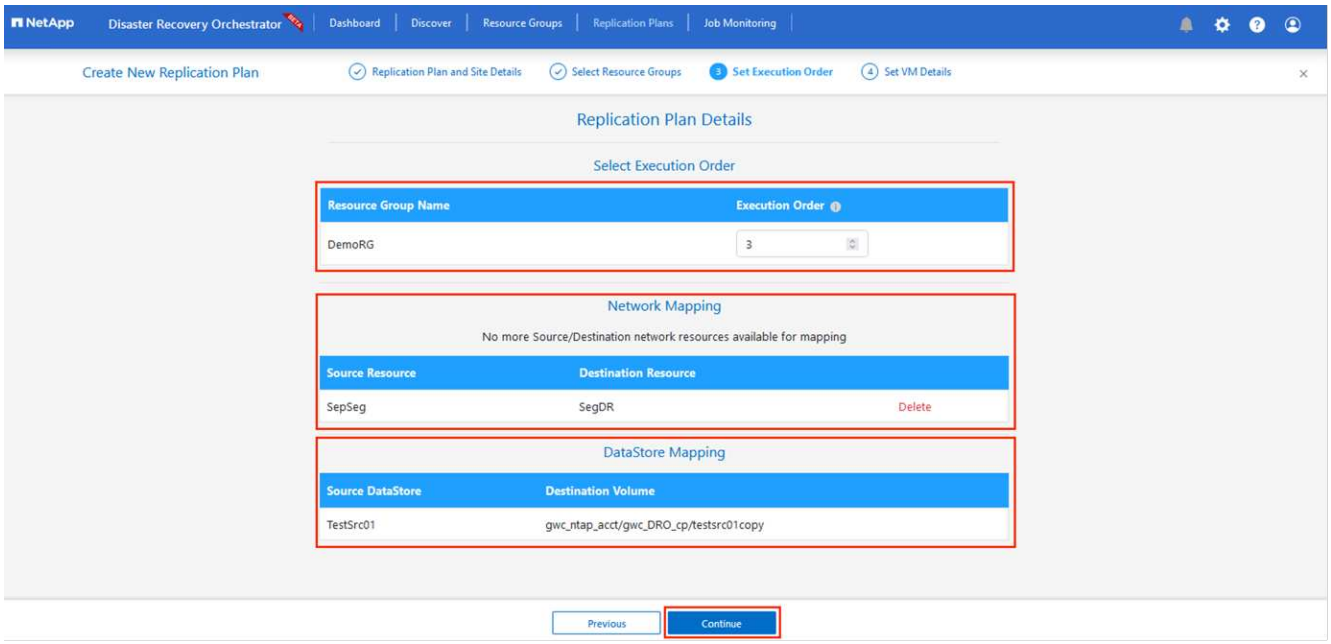


3. 복구 매핑이 완료되면 * 클러스터 매핑 * 을 선택합니다.

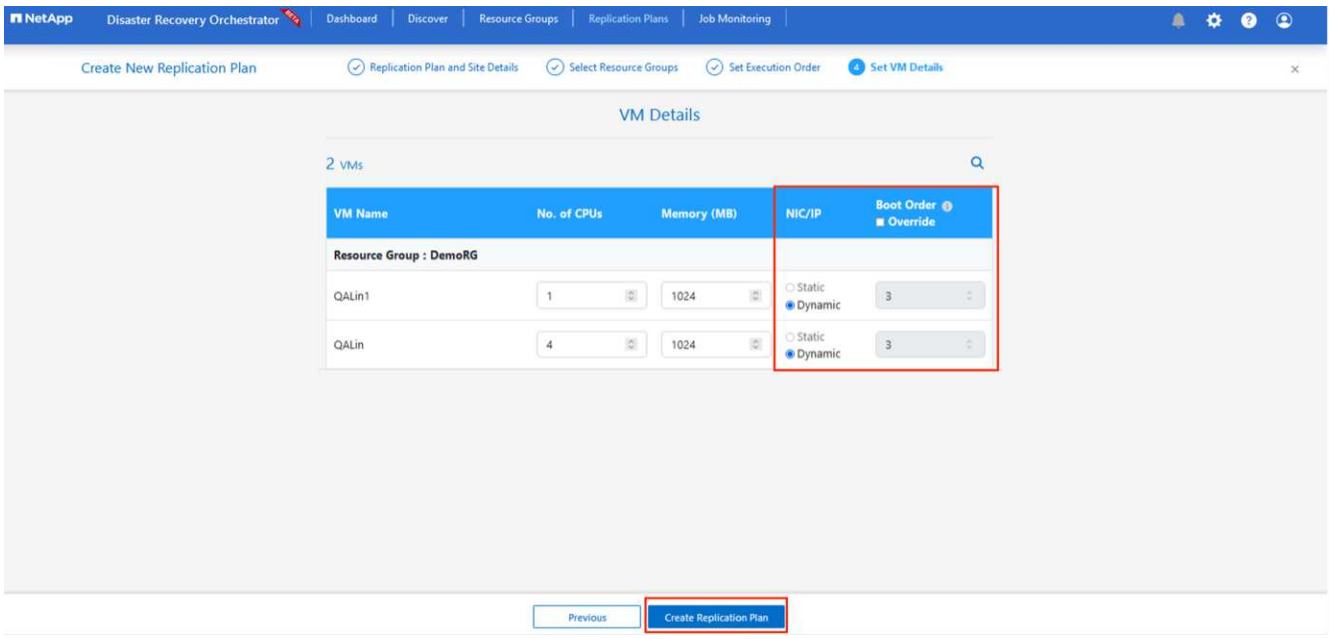


4. 리소스 그룹 세부 정보 * 를 선택하고 * 계속 * 을 클릭합니다.
5. 리소스 그룹의 실행 순서를 설정합니다. 이 옵션을 사용하면 여러 리소스 그룹이 있을 때 작업 순서를 선택할 수 있습니다.
6. 완료되면 네트워크 매핑을 해당 세그먼트에 설정합니다. 세그먼트는 이미 보조 AVS 클러스터에서 프로비저닝되어야 하며, VM을 이러한 세그먼트로 매핑하려면 적절한 세그먼트를 선택하십시오.
7. 데이터 저장소 매핑은 선택한 VM에 따라 자동으로 선택됩니다.

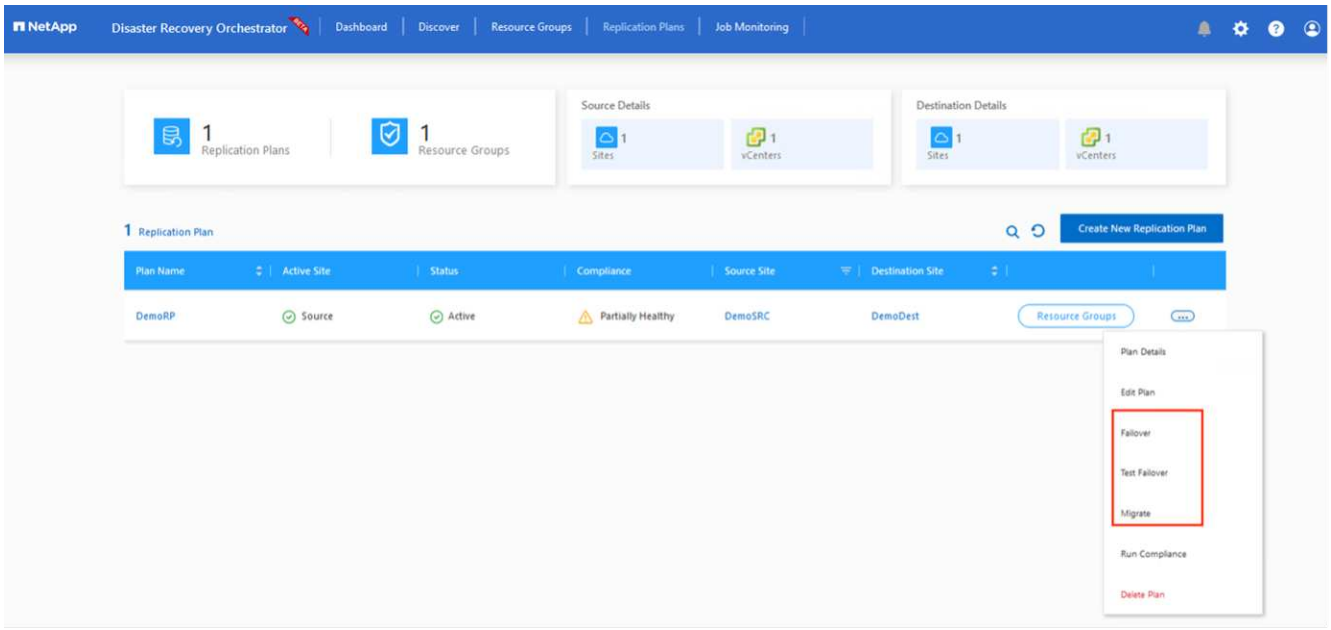
CRR(교차 지역 복제)이 볼륨 레벨에 있습니다. 따라서 해당 볼륨에 상주하는 모든 VM이 CRR 대상에 복제됩니다. 복제 계획에 포함된 가상 머신만 처리되므로 데이터 저장소의 일부인 모든 VM을 선택해야 합니다.



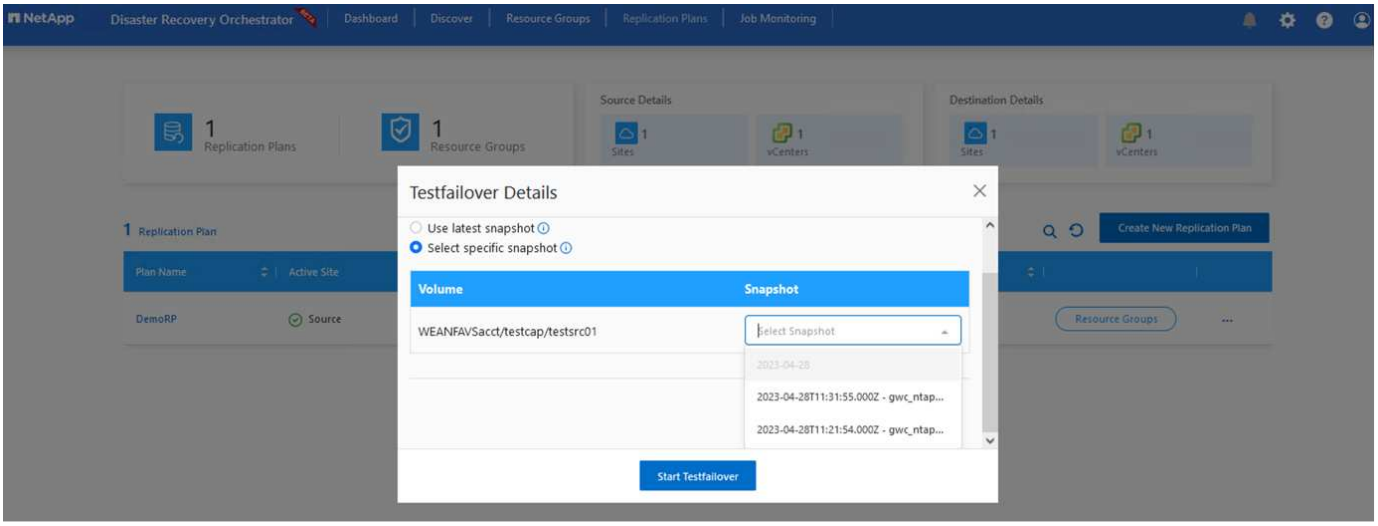
8. VM 세부 정보 아래에서 VM CPU 및 RAM 매개 변수의 크기를 선택적으로 조정할 수 있습니다. 이 기능은 대규모 환경을 소규모 타겟 클러스터로 복구하거나 일대일 물리적 VMware 인프라를 프로비저닝하지 않고 DR 테스트를 수행할 때 매우 유용합니다. 또한 리소스 그룹에서 선택한 모든 VM에 대한 부팅 순서 및 부팅 지연(초)을 수정합니다. 리소스 그룹 부팅 순서를 선택하는 동안 선택한 항목에서 변경이 필요한 경우 부팅 순서를 수정하는 추가 옵션이 있습니다. 기본적으로 리소스 그룹을 선택하는 동안 선택한 부팅 순서가 사용되지만 이 단계에서는 모든 수정 작업을 수행할 수 있습니다.



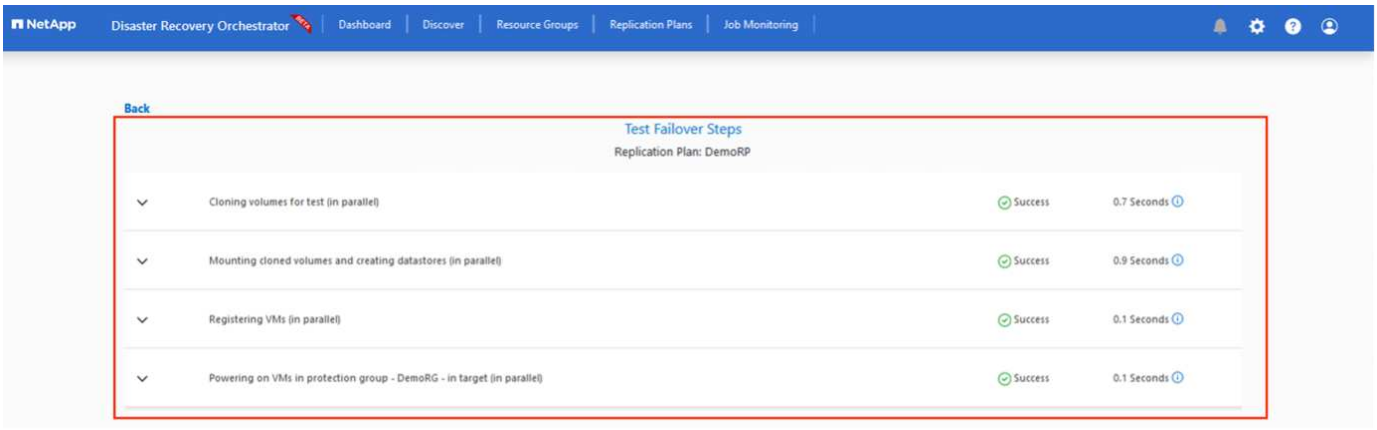
9. Create Replication Plan * 을 클릭합니다. 복제 계획이 생성되면 요구 사항에 따라 장애 조치, 테스트 대체 작동 또는 마이그레이션 옵션을 실행할 수 있습니다.



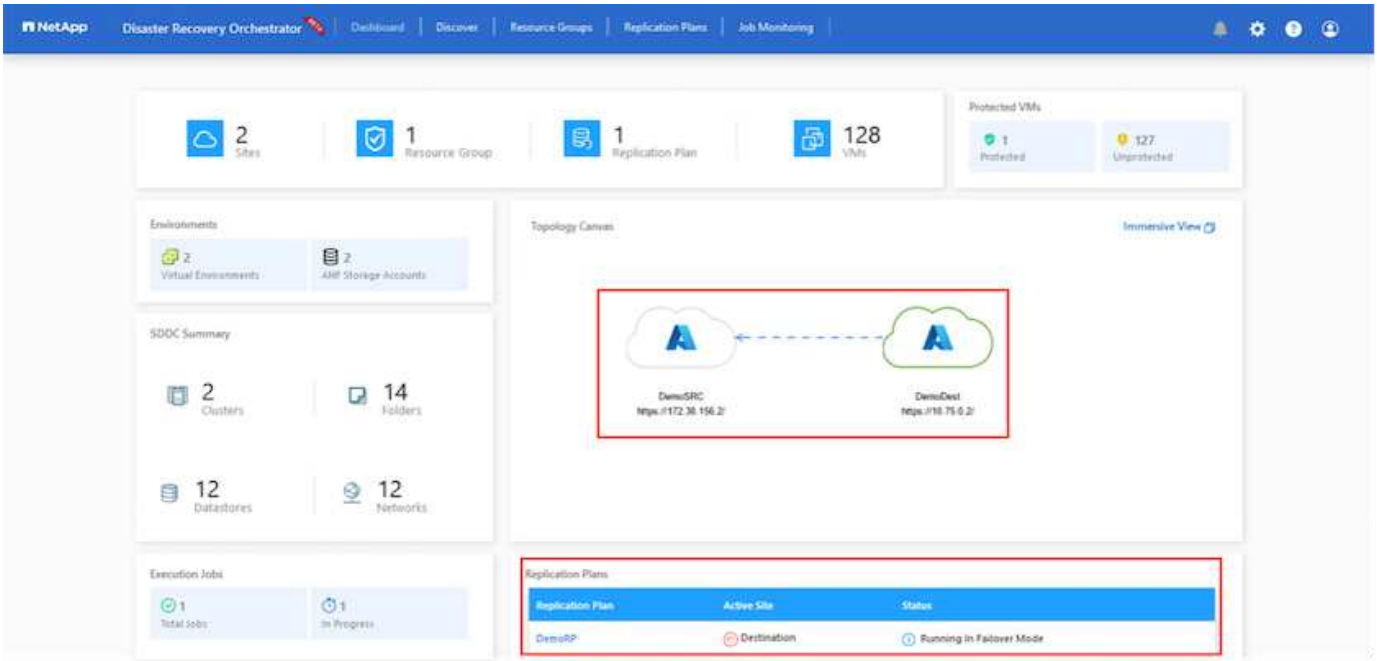
페일오버 및 테스트 페일오버 옵션 중에 최신 스냅샷이 사용되거나 특정 시점 스냅샷에서 특정 스냅샷을 선택할 수 있습니다. 가장 최근의 복제본이 이미 손상 또는 암호화된 상태에서 랜섬웨어와 같은 손상 이벤트가 발생할 경우 시점 옵션이 매우 유용할 수 있습니다. DRO는 사용 가능한 모든 시점을 표시합니다.



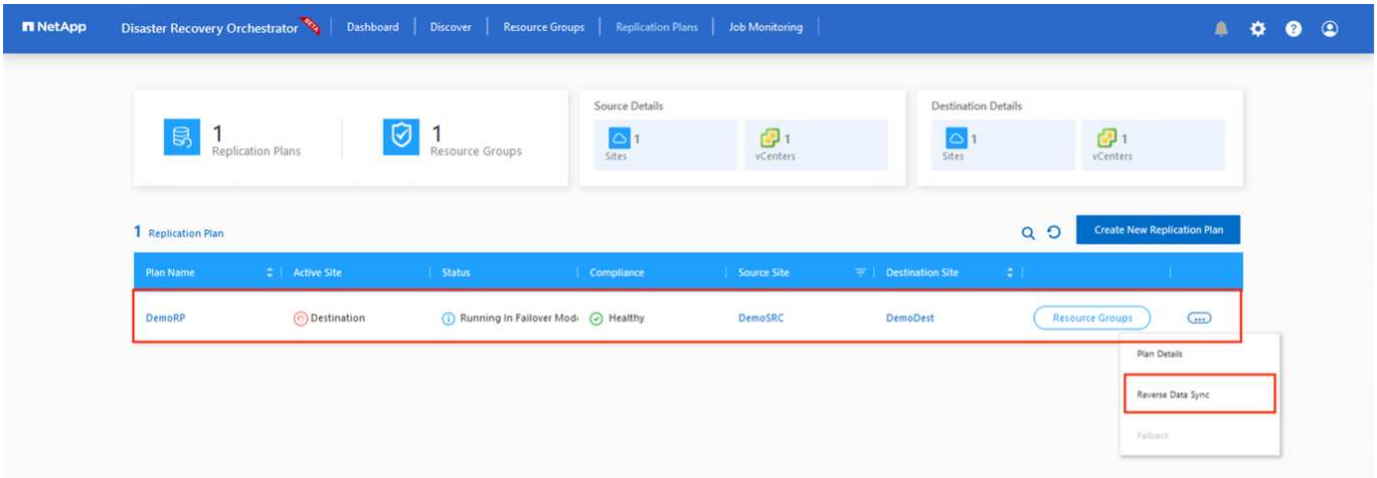
복제 계획에 지정된 구성으로 대체 작동을 트리거하거나 테스트 대체 작동을 트리거하려면 * 장애 조치 * 또는 * 테스트 장애 조치 * 를 클릭합니다. 작업 메뉴에서 복제 계획을 모니터링할 수 있습니다.



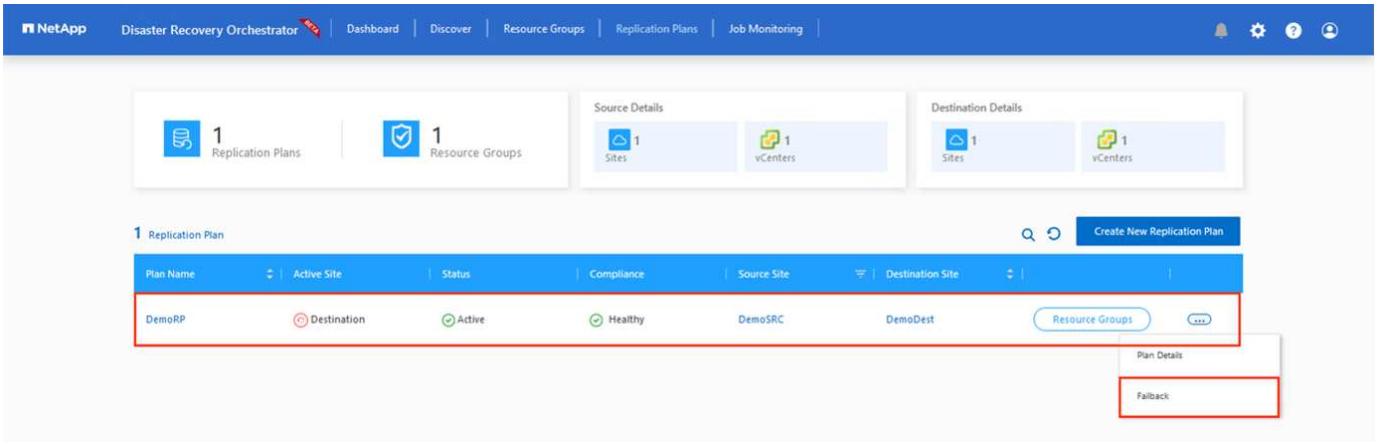
페일오버가 트리거된 후 보조 사이트 AVS SDDC vCenter(VM, 네트워크 및 데이터 저장소)에서 복구된 항목을 볼 수 있습니다. 기본적으로 VM은 Workload 폴더로 복구됩니다.

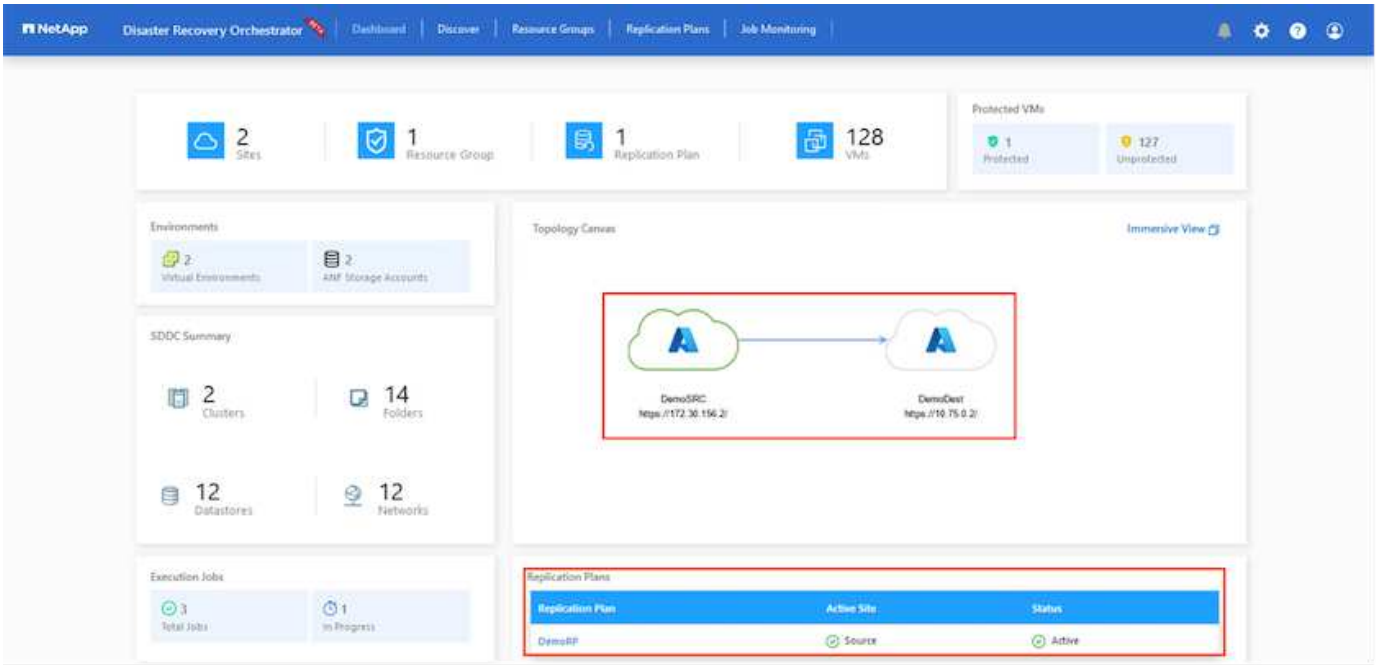


페일백은 복제 계획 레벨에서 트리거될 수 있습니다. 테스트 대체 작동의 경우, tear down 옵션을 사용하여 변경 사항을 롤백하고 새로 생성된 볼륨을 제거할 수 있습니다. 장애 조치와 관련된 장애 복구는 2단계 프로세스입니다. 복제 계획을 선택하고 * Reverse Data sync * 를 선택합니다.



이 단계가 완료된 후 페일백을 트리거하여 기본 AVS 사이트로 다시 이동합니다.





Azure 포털에서 보조 사이트 AVS SDDC에 읽기/쓰기 볼륨으로 매핑된 적절한 볼륨에 대한 복제 상태가 끊어진 것을 확인할 수 있습니다. 테스트 페일오버 중에 DRO는 대상 또는 복제본 볼륨을 매핑하지 않습니다. 대신 필요한 교차 지역 복제 스냅샷의 새 볼륨을 생성하고 볼륨을 데이터 저장소로 노출합니다. 그러면 용량 풀의 추가 물리적 용량을 사용하고 소스 볼륨이 수정되지 않습니다. 특히, DR 테스트 또는 선별적 워크플로우 중에도 복제 작업을 계속할 수 있습니다. 또한 이 프로세스를 통해 오류가 발생하거나 손상된 데이터가 복구되면 복제본이 손상될 위험 없이 복구를 정리할 수 있습니다.

랜섬웨어 복구

랜섬웨어에서 복구하는 것은 매우 힘든 작업이 될 수 있습니다. 특히, IT 조직은 안전한 반환 지점이 무엇인지 정확히 파악하기가 어려울 수 있으며, 일단 결정된 후에는 복구된 워크로드가 재발생하는 공격으로부터 보호하는 방법(예: 휴면 맬웨어로부터 또는 취약한 응용 프로그램을 통해)을 찾기가 어려울 수 있습니다.

DRO는 조직이 사용 가능한 모든 시점에서 복구할 수 있도록 함으로써 이러한 문제를 해결합니다. 그런 다음, 워크로드가 기능적/고립된 네트워크로 복구되어 애플리케이션이 서로 작동하고 통신할 수 있지만 남북 트래픽에 노출되지 않도록 합니다. 이 프로세스를 통해 보안 팀은 법의학 조사를 수행하고 숨겨진 맬웨어 또는 침낭된 맬웨어를 식별할 수 있는 안전한 장소를 확보할 수 있습니다.

결론

Azure NetApp Files 및 Azure VMware 재해 복구 솔루션은 다음과 같은 이점을 제공합니다.

- 효율적이고 탄력적인 Azure NetApp Files 교차 지역 복제 활용
- 스냅샷 보존을 통해 사용 가능한 모든 시점으로 복구합니다.
- 스토리지, 컴퓨팅, 네트워크 및 애플리케이션 검증 단계에서 수백, 수천 개의 VM을 복구하는 데 필요한 모든 단계를 완전히 자동화합니다.
- 워크로드 복구에서는 복제된 볼륨을 조작하지 않는 "최신 스냅샷에서 새 볼륨 생성" 프로세스를 활용합니다.
- 볼륨 또는 스냅샷의 데이터 손상 위험을 방지합니다.
- DR 테스트 워크플로우 중에 복제 중단을 방지합니다.
- DR 이외의 작업에 개발/테스트, 보안 테스트, 패치 및 업그레이드 테스트, 문제 해결 테스트 등 DR 데이터와 클라우드 컴퓨팅 리소스를 활용할 수 있습니다.
- CPU 및 RAM 최적화를 통해 보다 작은 컴퓨팅 클러스터로 복구할 수 있으므로 클라우드 비용을 절감할 수 있습니다.

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹 사이트를 검토하십시오.

- Azure NetApp Files에 대한 볼륨 복제를 생성합니다

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Azure NetApp Files 볼륨의 교차 지역 복제

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"

- "Azure VMware 솔루션"

  "https://learn.microsoft.com/en-us/azure/azure-vmware/introduction"

- Azure에서 가상화 환경을 구축하고 구성합니다

  "Azure에서 AVS 설정"

- Azure VMware 솔루션을 구축 및 구성합니다

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Azure VMware Solution으로 재해 복구를 위해 **Veeam Replication** 및 **Azure NetApp Files** 데이터 저장소를 사용합니다

저자: Niyaz Mohamed-NetApp Solutions Engineering

개요

Azure NetApp Files(ANF) 데이터 저장소는 스토리지를 컴퓨팅에서 분리하여 모든 조직에 워크로드를 클라우드로 전환하는 데 필요한 유연성을 제공합니다. 컴퓨팅 리소스와 독립적으로 확장이 가능한 유연한 고성능 스토리지 인프라를

고객에게 제공합니다. Azure NetApp Files 데이터 저장소는 Azure VMware Solution(AVS)과 함께 온프레미스 VMware 환경을 위한 재해 복구 사이트인 구축을 간소화하고 최적화합니다.

Azure NetApp Files(ANF) 볼륨 기반 NFS 데이터 저장소를 사용하여 VM 복제 기능을 제공하는 검증된 타사 솔루션을 사용하여 사내에서 데이터를 복제할 수 있습니다. Azure NetApp Files 데이터 저장소를 추가하면 스토리지를 수용할 수 있는 엄청난 양의 ESXi 호스트를 포함하는 Azure VMware Solution SDDC를 구축하는 것보다 비용 최적화된 배포를 실현할 수 있습니다. 이러한 접근 방식을 "파일럿 라이트 클러스터"라고 합니다. 파일럿 라이트 클러스터는 Azure NetApp Files 데이터 저장소 용량과 함께 최소 AVS 호스트 구성(AVS 노드 3개)입니다.

목표는 페일오버를 처리하기 위해 모든 핵심 구성 요소를 사용하여 저렴한 인프라를 유지하는 것입니다. 페일오버가 발생하는 경우 파일럿 라이트 클러스터가 스케일아웃되고 더 많은 AVS 호스트를 프로비저닝할 수 있습니다. 그리고 페일오버가 완료되고 정상 작동이 복원되면 파일럿 라이트 클러스터를 저비용 운영 모드로 확장할 수 있습니다.

이 문서의 목적

이 기사에서는 Veeam 백업 및 복제와 함께 Azure NetApp Files 데이터 저장소를 사용하여 Veeam VM 복제 소프트웨어 기능을 사용하여 온프레미스 VMware VM용 재해 복구를 AVS(으)로 설정하는 방법을 설명합니다.

Veeam Backup & Replication은 가상 환경을 위한 백업 및 복제 애플리케이션입니다. 가상 머신이 복제되면 Veeam Backup & Replication이 AVS에서 복제되며 소프트웨어는 타겟 AVS SDDC 클러스터에 네이티브 VMware vSphere 형식으로 VM의 정확한 복제본을 생성합니다. Veeam Backup & Replication은 복제본을 원래 VM과 동기화된 상태로 유지합니다. 재해 복구 사이트에 시작 준비 상태의 VM 복제본이 마운트되어 있기 때문에 복제는 최상의 RTO(복구 시간 목표)를 제공합니다.

이 복제 메커니즘은 재해 발생 시 AVS SDDC에서 워크로드를 신속하게 시작할 수 있도록 합니다. Veeam Backup & Replication 소프트웨어는 또한 WAN을 통한 복제 및 느린 연결을 위해 트래픽 전송을 최적화합니다. 또한 중복 데이터 블록, 제로 데이터 블록, 스왑 파일 및 "제외된 VM 게스트 OS 파일"도 필터링합니다. 소프트웨어는 복제본 트래픽도 압축합니다. 복제 작업이 전체 네트워크 대역폭을 소비하는 것을 방지하기 위해 WAN 가속기 및 네트워크 조절 규칙을 활용할 수 있습니다.

Veeam Backup & Replication의 복제 프로세스는 작업 중심으로 수행되므로 복제 작업을 구성하여 복제가 수행됩니다. 재해 이벤트의 경우 해당 복제본 복제본으로 장애 조치를 수행하여 VM을 복구하기 위해 페일오버를 트리거할 수 있습니다. 페일오버가 수행되면 복제된 VM이 원래 VM의 역할을 대신합니다. 페일오버는 복제본의 최신 상태 또는 알려진 정상 복구 지점으로 수행할 수 있습니다. 따라서 필요에 따라 랜섬웨어 복구 또는 격리된 테스트가 가능합니다. Veeam Backup & Replication은 다양한 재해 복구 시나리오를 처리할 수 있는 다양한 옵션을 제공합니다.

[]

솔루션 구축

고급 단계

1. Veeam Backup and Replication 소프트웨어는 적절한 네트워크 연결을 갖춘 사내 환경에서 실행됩니다.
2. "Azure VMware Solution(AVS) 배포" 프라이빗 클라우드 및 "Azure NetApp Files 데이터 저장소를 연결합니다" Azure VMware Solution 호스트에 연결할 수 있습니다.

   최소 구성으로 설정된 파일럿 라이트 환경을 DR 목적으로 사용할 수 있습니다. 장애 발생 시 VM이 이 클러스터로 페일오버되고 추가 노드를 추가할 수 있습니다.)

3. Veeam Backup and Replication을 사용하여 VM 복제본을 생성하도록 복제 작업을 설정합니다.
4. 페일오버 계획을 만들고 페일오버를 수행합니다.

5. 재해 이벤트가 완료되고 운영 사이트가 가동되면 운영 VM으로 다시 전환합니다.

AVS 및 **ANF** 데이터 저장소로의 **Veeam VM** 복제를 위한 사전 요구 사항

1. Veeam Backup & Replication 백업 VM이 소스 및 타겟 AVS SDDC 클러스터에 연결되어 있는지 확인합니다.
2. 백업 서버는 짧은 이름을 확인하고 소스 및 타겟 vCenter에 연결할 수 있어야 합니다.
3. 타겟 Azure NetApp Files 데이터 저장소에 복제된 VM의 VMDK를 저장할 수 있는 충분한 여유 공간이 있어야 합니다.

자세한 내용은 "고려 사항 및 제한 사항"을 참조하십시오 "여기".

배포 세부 정보

1단계**: VM** 복제

Veeam Backup & Replication은 VMware vSphere 스냅샷 기능을 활용하며/ 복제 중에 Veeam Backup & Replication은 VMware vSphere에 VM 스냅샷을 생성하도록 요청합니다. VM 스냅샷은 가상 디스크, 시스템 상태, 구성 및 메타데이터를 포함하는 VM의 시점 복제본입니다. Veeam Backup & Replication은 이 스냅샷을 복제용 데이터 소스로 사용합니다.

VM을 복제하려면 다음 단계를 수행하십시오.

1. Veeam Backup & Replication Console을 엽니다.
2. 홈 보기에서. 작업 노드를 마우스 오른쪽 버튼으로 클릭하고 복제 작업 > 가상 머신 을 선택합니다.
3. 작업 이름을 지정하고 해당 고급 제어 확인란을 선택합니다. 다음 을 클릭합니다.
   - 온-프레미스와 Azure 간의 연결에 대역폭이 제한된 경우 복제 시드 확인란을 선택합니다.
     - Azure VMware Solution SDDC의 세그먼트가 온프레미스 사이트 네트워크의 세그먼트와 일치하지 않는 경우 네트워크 재매핑(네트워크가 다른 AVS SDDC 사이트의 경우) 확인란을 선택합니다.
   - 온프레미스 운영 사이트의 IP 주소 지정 체계가 타겟 AVS 사이트의 체계와 다른 경우 복제 Re-IP(IP 주소 지정 체계가 다른 DR 사이트의 경우) 확인란을 선택합니다.

     []
4. 가상 * 머신 * 단계에서 Azure VMware Solution SDDC에 연결된 Azure NetApp Files 데이터 저장소에 복제할 VM을 선택합니다. vSAN에 가상 머신을 배치하여 사용 가능한 vSAN 데이터스토어 용량을 채울 수 있습니다. 파일럿 라이트 클러스터에서는 3노드 클러스터의 가용 용량이 제한됩니다. 나머지 데이터는 Azure NetApp Files 데이터 저장소에 쉽게 배치하여 VM을 복구할 수 있으며, 클러스터를 확장하여 CPU/메모리 요구 사항을 충족할 수 있습니다. Add * 를 클릭한 다음 * Add Object * 창에서 필요한 VM 또는 VM 컨테이너를 선택하고 * Add * 를 클릭합니다. 다음 * 을 클릭합니다.

   []
5. 그런 다음 대상을 Azure VMware Solution SDDC 클러스터/호스트와 적절한 리소스 풀, VM 폴더 및 VM 복제본용 FSx for ONTAP 데이터 저장소로 선택합니다. 그런 다음 * 다음 * 을 클릭합니다.

   []
6. 다음 단계에서는 필요에 따라 소스 및 대상 가상 네트워크 간의 매핑을 생성합니다.

   []
7. 작업 설정 * 단계에서 VM 복제본, 보존 정책 등에 대한 메타데이터를 저장할 백업 리포지토리를 지정합니다.
8. 데이터 전송 * 단계에서 * 원본 * 및 * 대상 * 프록시 서버를 업데이트하고 * 자동 * 선택(기본값)을 그대로 두고 * 직접 * 옵션을 선택한 후 * 다음 * 을 클릭합니다.
9. Guest Processing * 단계에서 필요에 따라 * Enable application-aware processing * 옵션을 선택합니다. 다음 * 을 클릭합니다.

   []
10. 정기적으로 실행할 복제 작업을 실행할 복제 스케줄을 선택합니다.

    []

11. 마법사의 * Summary * 단계에서 복제 작업의 세부 정보를 검토합니다. 마법사를 닫은 후 바로 작업을 시작하려면 * 마침을 클릭하면 작업 실행 * 확인란을 선택하고, 그렇지 않으면 확인란을 선택하지 않은 상태로 둡니다. 그런 다음 * 마침 * 을 클릭하여 마법사를 닫습니다.

    []

복제 작업이 시작되면 지정된 접미사의 VM이 대상 AVS SDDC 클러스터/호스트에 채워집니다.

[]

Veeam 복제에 대한 자세한 내용은 을 참조하십시오 "복제 작동 방법"

2단계**:** 장애 조치 계획을 만듭니다

초기 복제 또는 시드가 완료되면 페일오버 계획을 생성합니다. 페일오버 계획은 종속 VM에 대해 하나씩 또는 그룹으로 자동 페일오버를 수행하는 데 도움이 됩니다. 페일오버 계획은 부팅 지연을 포함하여 VM이 처리되는 순서에 대한 청사진입니다. 또한 페일오버 계획은 중요한 종속 VM이 이미 실행 중인지 확인하는 데 도움이 됩니다.

계획을 생성하려면 * Replicas * 라는 새 하위 섹션으로 이동하여 * Failover Plan * 을 선택합니다. 적절한 VM을 선택합니다. Veeam Backup & Replication은 이 시점에 가장 가까운 복원 지점을 찾아 VM 복제를 시작하는 데 사용합니다.

ⓘ 초기 복제가 완료되고 VM 복제본이 준비 상태가 된 후에만 페일오버 계획을 추가할 수 있습니다.

ⓘ 페일오버 계획을 실행할 때 동시에 시작할 수 있는 최대 VM 수는 10개입니다

ⓘ 페일오버 프로세스 중에는 소스 VM의 전원이 꺼지지 않습니다

장애 조치 계획 * 을 만들려면 다음을 수행합니다.

1. 홈 보기에서. 복제본 노드를 마우스 오른쪽 버튼으로 클릭하고 페일오버 계획 > 페일오버 계획 > VMware vSphere를 선택합니다.

    []

2. 그런 다음 계획에 대한 이름과 설명을 입력합니다. 필요에 따라 사전 및 사후 페일오버 스크립트를 추가할 수 있습니다. 예를 들어 복제된 VM을 시작하기 전에 VM을 종료하는 스크립트를 실행합니다.

    []

3. VM을 계획에 추가하고 애플리케이션 종속성을 충족하도록 VM 부팅 순서 및 부팅 지연을 수정합니다.

    []

복제 작업 생성에 대한 자세한 내용은 을 참조하십시오 "복제 작업을 생성하는 중입니다".

3단계**:** 페일오버 계획을 실행합니다

페일오버 중에 프로덕션 사이트의 소스 VM이 재해 복구 사이트의 해당 복제본으로 전환됩니다. 페일오버 프로세스의 일부로 Veeam Backup & Replication은 VM 복제본을 필요한 복구 지점으로 복구하고 소스 VM의 모든 입출력 작업을 해당 복제본으로 이동합니다. 복제본은 재해 발생 시에만 사용할 수 있으며 DR 드릴을 시뮬레이션하는 데도 사용할 수 있습니다. 페일오버 시뮬레이션 중에는 소스 VM이 계속 실행 중입니다. 필요한 모든 테스트가 수행되면 페일오버를 취소하고 정상 작업으로 돌아갈 수 있습니다.

페일오버 중에 IP 충돌을 피하기 위해 네트워크 분할이 제대로 수행되었는지 확인하십시오.

장애 조치 계획을 시작하려면 * 장애 조치 계획 * 탭을 클릭하고 장애 조치 계획을 마우스 오른쪽 버튼으로 클릭합니다. 시작 * 을 선택합니다. 이렇게 하면 VM 복제본의 최신 복구 지점을 사용하여 장애 조치가 수행됩니다. VM 복제본의 특정 복원 지점으로 페일오버하려면 * 시작 * 을 선택합니다.

[]

[]

VM 복제본의 상태가 Ready에서 Failover로 변경되고 VM은 대상 AVS(Azure VMware Solution) SDDC 클러스터/호스트에서 시작됩니다.

[]

페일오버가 완료되면 VM의 상태가 "페일오버"로 변경됩니다.

[]

Veeam Backup & Replication은 소스 VM의 복제본이 준비 상태로 돌아갈 때까지 소스 VM에 대한 모든 복제 작업을 중지합니다.

페일오버 계획에 대한 자세한 내용은 을 참조하십시오 "페일오버 계획".

4단계**:** 프로덕션 사이트로 페일백합니다

장애 조치 계획이 실행 중인 경우 중간 단계로 간주되며 요구 사항에 따라 확정되어야 합니다. 다음과 같은 옵션이 있습니다.

- * Failback to Production * - 원래 VM으로 다시 전환하고 VM 복제본이 실행되는 동안 발생한 모든 변경 사항을 원래 VM으로 전송합니다.

> ⓘ 페일백을 수행하면 변경 내용이 전송되지만 게시되지는 않습니다. 원래 VM이 예상대로 작동하지 않는 경우 * 페일백 커밋 * (원래 VM이 예상대로 작동하는 것으로 확인된 경우) 또는 페일백 실행 취소 를 선택하여 VM 복제본으로 돌아갑니다.

- * 장애 조치 실행 취소 * - 원래 VM으로 다시 전환하고 실행 중에 VM 복제본의 모든 변경 사항을 취소합니다.
- * 영구 장애 조치 * - 원래 VM에서 VM 복제본으로 영구적으로 전환하고 이 복제본을 원래 VM으로 사용합니다.

이 데모에서는 Failback to Production을 선택했습니다. 마법사의 대상 단계에서 원래 VM으로 페일백이 선택되었고 "복원 후 VM 전원 켜기" 확인란이 활성화되었습니다.

[]

[]

[]

[]

페일백 커밋은 페일백 작업을 완료하는 방법 중 하나입니다. 페일백이 커밋되면 장애가 발생한 VM(운영 VM)에 전송된 변경 사항이 예상대로 작동하는지 확인합니다. 커밋 작업 후에 Veeam Backup & Replication은 운영 VM에 대한 복제 작업을 재개합니다.

페일백 프로세스에 대한 자세한 내용은 의 Veeam 문서를 참조하십시오 "복제를 위한 페일오버 및 페일백".

[]

운영 환경으로 페일백이 성공한 후 VM이 모두 원래 운영 사이트로 복구됩니다.

[]

결론

Azure NetApp Files 데이터 저장소 기능을 사용하면 Veeam 또는 검증된 타사 툴에서 VM 복제만 수용하기 위해 대규모 클러스터를 구성하는 대신 파일럿 라이트 클러스터를 활용하는 방법으로 저렴한 DR 솔루션을 제공할 수 있습니다. 이렇게 하면 맞춤형 재해 복구 계획을 효과적으로 처리하고 DR에 기존 백업 제품을 재사용할 수 있어, 온프레미스 DR 데이터 센터에서 클라우드 기반 재해 복구가 가능합니다. 재해가 발생한 경우 단추를 클릭하여 장애 조치를 수행하거나 재해가 발생한 경우 자동으로 장애 조치를 수행할 수 있습니다.

이 프로세스에 대해 자세히 알아보려면 자세한 단계별 안내 비디오를 참조하십시오.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278

Azure/AVS에서 워크로드 마이그레이션

TR-4940: VMware HCX-Quickstart 가이드를 사용하여 워크로드를 **Azure NetApp Files** 데이터 저장소로 마이그레이션합니다

저자: NetApp 솔루션 엔지니어링

개요**: VMware HCX, Azure NetApp Files** 데이터 저장소 및 **Azure VMware** 솔루션을 사용하여 가상 시스템 마이그레이션

Azure VMware 솔루션 및 Azure NetApp Files 데이터 저장소의 가장 일반적인 사용 사례 중 하나는 VMware 워크로드 마이그레이션입니다. VMware HCX가 선호되는 옵션이며, 온프레미스 VM(가상 머신)과 데이터를 Azure NetApp Files 데이터 저장소로 이동하는 다양한 마이그레이션 메커니즘을 제공합니다.

VMware HCX는 주로 클라우드 전반에서 애플리케이션 마이그레이션, 워크로드 재조정 및 비즈니스 연속성을 간소화하도록 설계된 마이그레이션 플랫폼입니다. Azure VMware Solution 프라이빗 클라우드의 일부로 포함되어 있으며 다양한 방법으로 워크로드를 마이그레이션하여 DR(재해 복구) 작업에 사용할 수 있습니다.

이 문서에서는 Azure NetApp Files 데이터 저장소를 프로비저닝한 후 VMware HCX를 다운로드, 구축 및 구성하기 위한 단계별 지침을 제공하며, 여기에는 다양한 VM 마이그레이션 메커니즘을 지원하는 상호 연결, 네트워크 확장, WAN 최적화를 비롯한 온프레미스 및 Azure VMware 솔루션 측의 모든 주요 구성 요소가 포함됩니다.

VMware HCX는 마이그레이션이 VM 레벨에 있으므로 모든 데이터 저장소 유형과 함께 작동합니다. 따라서 이 문서는 비용 효율적인 VMware 클라우드 구축을 위해 Azure VMware 솔루션을 포함한 Azure NetApp Files를 구축하려는 기존 NetApp 고객 및 타사 고객에게 적용됩니다.

높은 수준의 단계

이 목록은 Azure 클라우드 측에서 HCX Cloud Manager를 설치 및 구성하고 HCX Connector를 온프레미스에 설치하는 데 필요한 높은 수준의 단계를 제공합니다.

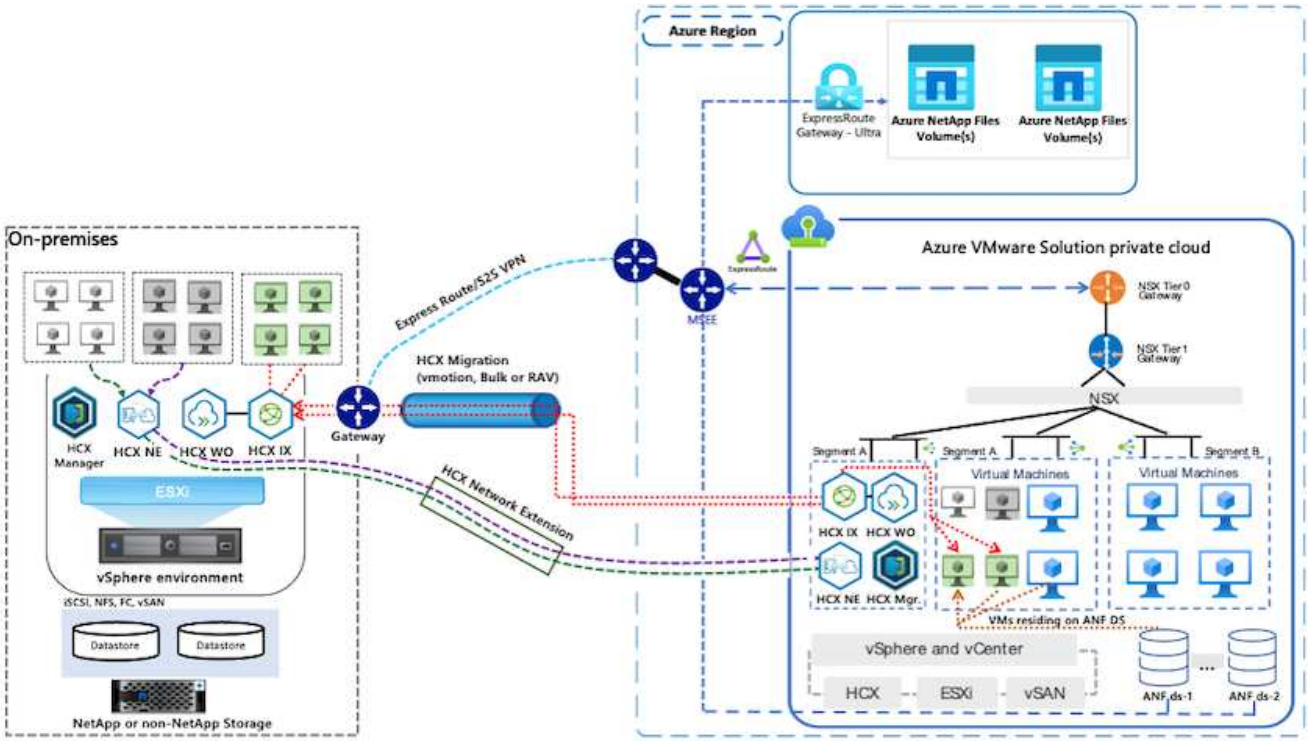
1. Azure 포털을 통해 HCX를 설치합니다.
2. 사내 VMware vCenter Server에서 HCX Connector OVA(Open Virtualization Appliance) 설치 프로그램을 다운로드하여 구축합니다.
3. 라이센스 키를 사용하여 HCX를 활성화합니다.
4. 온프레미스 VMware HCX Connector를 Azure VMware Solution HCX Cloud Manager와 페어링합니다.
5. 네트워크 프로파일, 컴퓨팅 프로파일 및 서비스 메시를 구성합니다.
6. (선택 사항) 마이그레이션 중에 재IP를 방지하기 위해 네트워크 확장을 수행합니다.
7. 어플라이언스 상태를 확인하고 마이그레이션이 가능한지 확인합니다.
8. VM 워크로드를 마이그레이션합니다.

시작하기 전에 다음 필수 구성 요소가 충족되었는지 확인하십시오. 자세한 내용은 다음을 참조하십시오 "링크". 연결을 포함한 필수 구성 요소가 구축된 후에는 Azure VMware Solution 포털에서 라이센스 키를 생성하여 HCX를 구성하고 활성화합니다. OVA 설치 프로그램을 다운로드한 후 아래 설명된 대로 설치 프로세스를 진행합니다.

HCX Advanced가 기본 옵션이며 VMware HCX Enterprise Edition도 지원 티켓을 통해 제공되며 추가 비용 없이 지원됩니다.

- 기존 Azure VMware 솔루션 SDDC(소프트웨어 정의 데이터 센터)를 사용하거나 이를 사용하여 프라이빗 클라우드를 생성합니다 "NetApp 링크" 또는 이 "Microsoft 링크".
- 사내 VMware vSphere 지원 데이터 센터에서 VM 및 관련 데이터를 마이그레이션하려면 데이터 센터에서 SDDC 환경으로 네트워크를 연결해야 합니다. 워크로드를 마이그레이션하기 전에 "사이트 간 VPN 또는 Express 라우트 전역 연결 연결을 설정합니다" 데이터 관리 및 보호
- 사내 VMware vCenter Server 환경에서 Azure VMware Solution 프라이빗 클라우드로 가는 네트워크 경로는 vMotion을 사용하여 VM 마이그레이션을 지원해야 합니다.
- 필수 를 확인하십시오 "방화벽 규칙 및 포트" 온-프레미스 vCenter Server와 SDDC vCenter 간에 vMotion 트래픽이 허용됩니다. 프라이빗 클라우드에서 vMotion 네트워크의 라우팅은 기본적으로 구성됩니다.
- Azure NetApp Files NFS 볼륨은 Azure VMware 솔루션에서 데이터 저장소로 마운트되어야 합니다. 이에 설명된 단계를 따릅니다 "링크" Azure NetApp Files 데이터 저장소를 Azure VMware 솔루션 호스트에 연결합니다.

테스트 목적으로, 이 검증에 사용된 온프레미스 랩 환경은 Azure VMware 솔루션에 대한 온프레미스 연결을 허용하는 사이트 간 VPN을 통해 연결되었습니다.



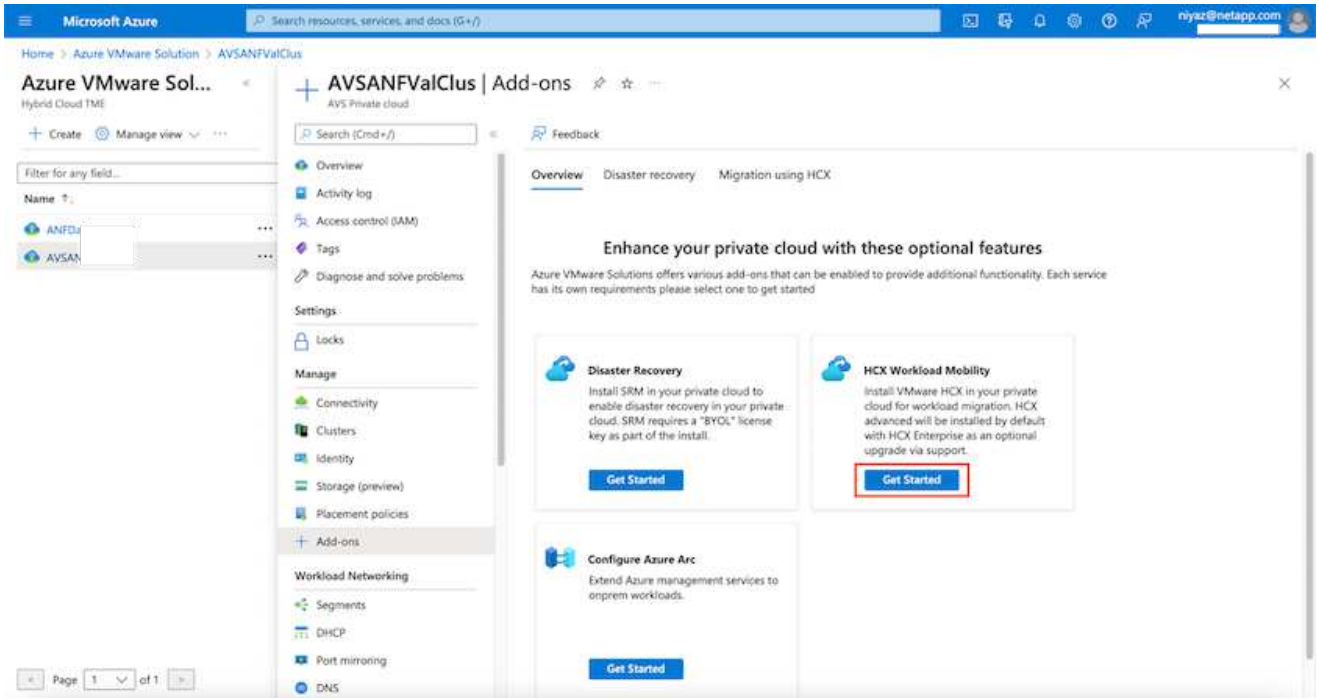
솔루션 구축

이 솔루션의 배포를 완료하려면 다음 단계를 따르십시오.

1단계**:** 추가 기능 옵션을 사용하여 **Azure Portal**을 통해 **HCX**를 설치합니다

설치를 수행하려면 다음 단계를 수행하십시오.

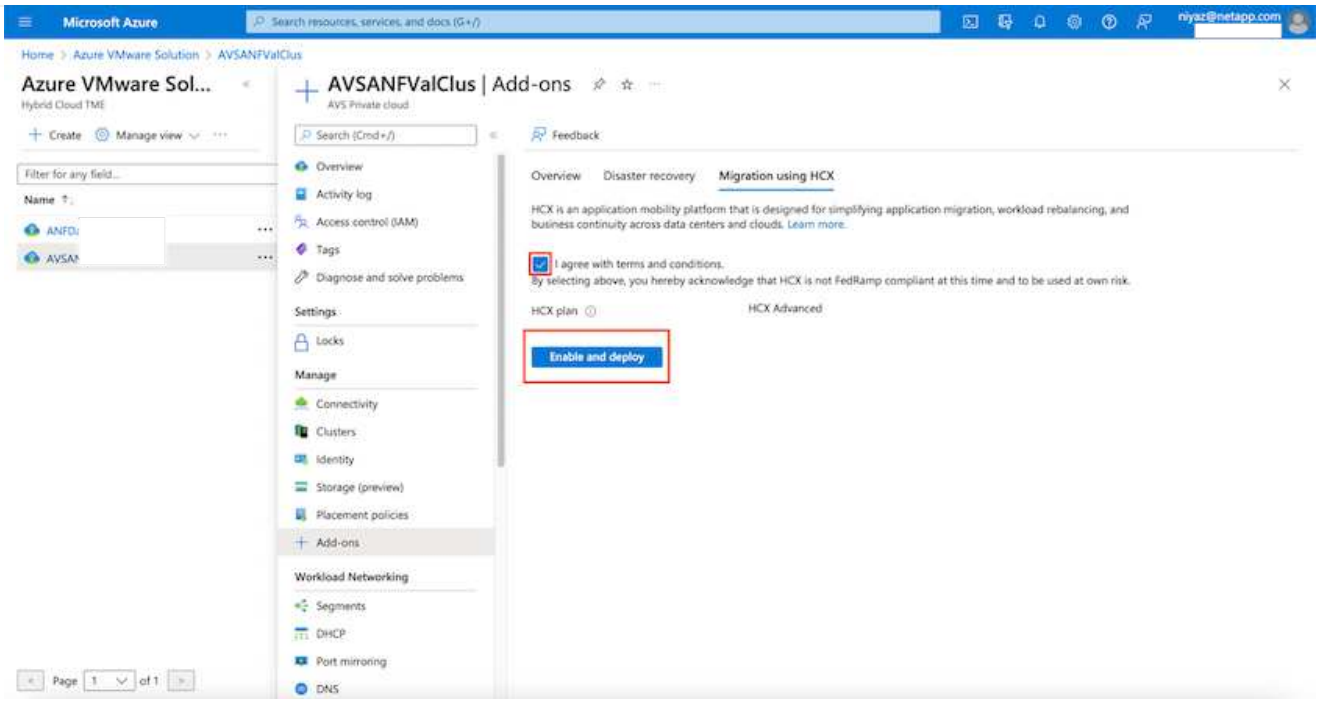
1. Azure Portal에 로그인하여 Azure VMware Solution 프라이빗 클라우드에 액세스합니다.
2. 적절한 프라이빗 클라우드를 선택하고 애드온 에 액세스합니다. 이 작업은 * 관리 > 추가 기능 * 으로 이동하여 수행할 수 있습니다.
3. HCX 워크로드 이동성 섹션에서 * 시작하기 * 를 클릭합니다.



1. 이용 약관에 동의함 * 옵션을 선택하고 * 사용 및 배포 * 를 클릭합니다.

기본 배포는 HCX Advanced입니다. Enterprise 버전을 사용하도록 지원 요청을 엽니다.

배포에는 약 25~30분이 소요됩니다.


Microsoft Azure
Search resources, services, and docs (G+/)
niyaz@netapp.com
Home > Azure VMware Solution > AVSANFValClus
Azure VMware Sol...
Hybrid Cloud TME
Create
Manage view
Filter for any field...
Name
ANFDi
AVSAN
Page 1 of 1
AVSANFValClus | Add-ons
AVS Private cloud
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
Manage
Connectivity
Clusters
Identity
Storage (preview)
Placement policies
Add-ons
Workload Networking
Segments
DHCP
Port mirroring
DNS
Feedback
Overview
Disaster recovery
Migration using HCX
HCX is an application mobility platform that is designed for simplifying application migration, workload rebalancing, and business continuity across data centers and clouds. Learn more.
I agree with terms and conditions.
By selecting above, you hereby acknowledge that HCX is not FedRamp compliant at this time and to be used at own risk.
HCX plan
HCX Advanced
Enable and deploy

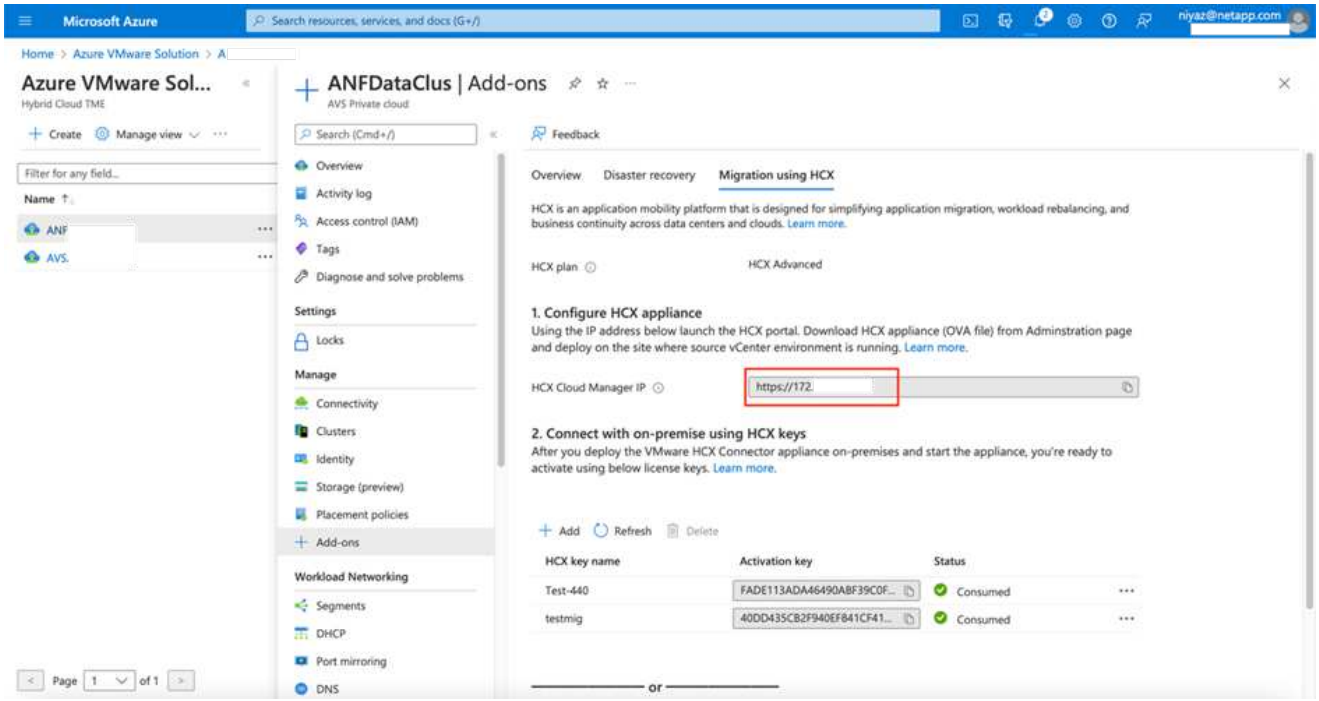
2단계**:** 온**-**프레미스 **vCenter Server**에 설치 관리자 **OVA**를 구축합니다

온프레미스 커넥터가 Azure VMware 솔루션의 HCX Manager에 연결하려면 적절한 방화벽 포트가 온-프레미스 환경에서 열려 있어야 합니다.

온-프레미스 vCenter Server에서 HCX Connector를 다운로드하여 설치하려면 다음 단계를 수행하십시오.

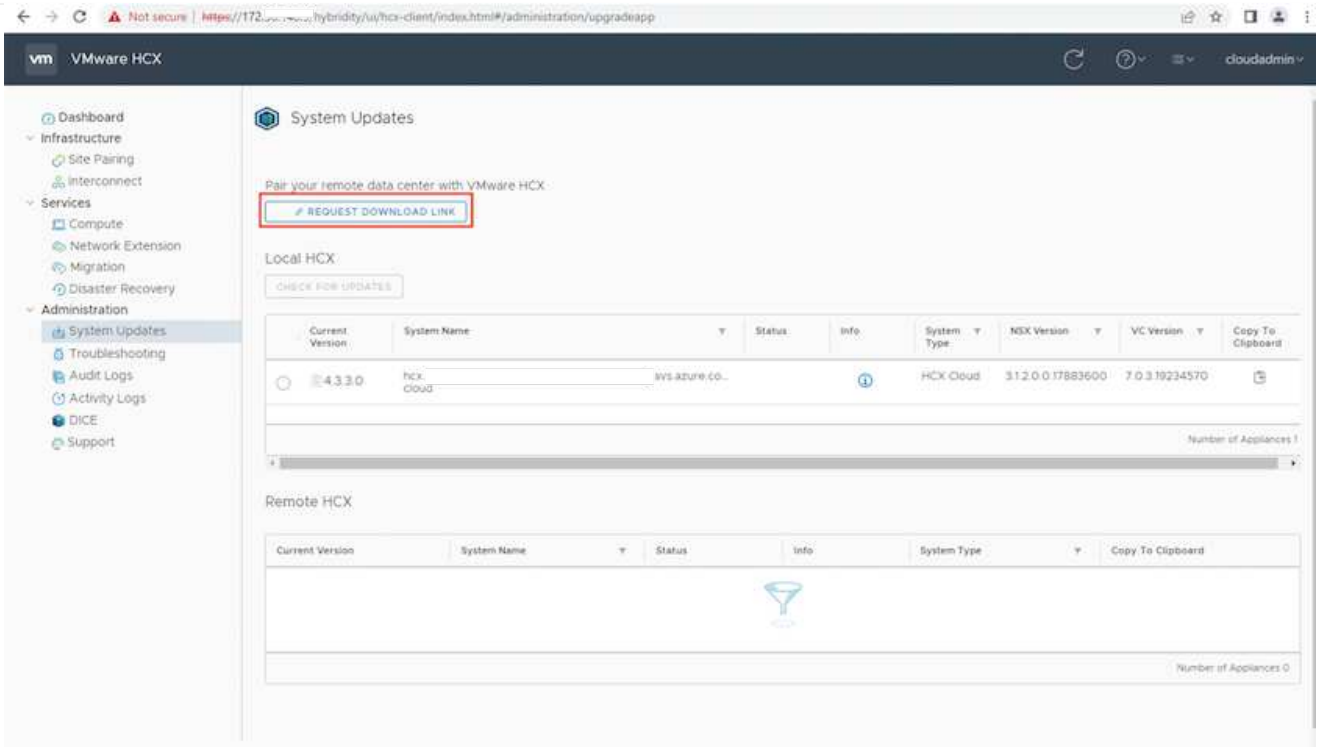
1. Azure 포털에서 Azure VMware 솔루션으로 이동하여 프라이빗 클라우드를 선택한 다음 * 관리 > 추가 기능 > HCX를 사용한 마이그레이션 * 을 선택하고 HCX Cloud Manager 포털을 복사하여 OVA 파일을 다운로드합니다.

기본 CloudAdmin 사용자 자격 증명을 사용하여 HCX 포털에 액세스합니다.

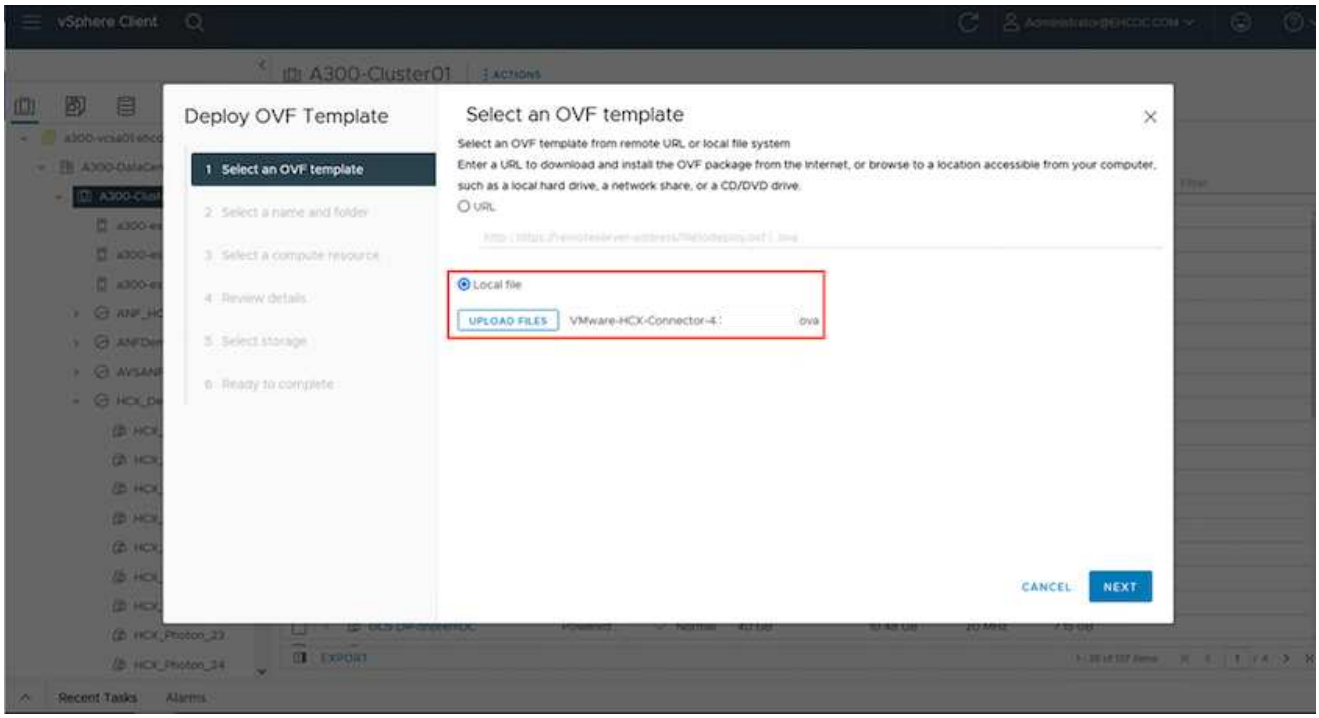


1. jumphost를 사용하여 mailto:cloudadmin@vsphere.loca l[cloudadmin@vsphere.loca l^]으로 HCX 포털에 액세스한 후 * 관리 > 시스템 업데이트 * 로 이동하여 * 다운로드 링크 요청 * 을 클릭합니다.

OVA에 대한 링크를 다운로드하거나 복사하여 브라우저에 붙여 넣으면 온-프레미스 vCenter Server에 구축할 VMware HCX Connector OVA 파일의 다운로드 프로세스가 시작됩니다.



1. OVA를 다운로드한 후 * Deploy OVF Template * 옵션을 사용하여 온프레미스 VMware vSphere 환경에 구축합니다.



1. OVA 배포에 필요한 모든 정보를 입력하고 * Next * 를 클릭한 다음 * Finish * 를 클릭하여 VMware HCX 커넥터 OVA를 배포합니다.

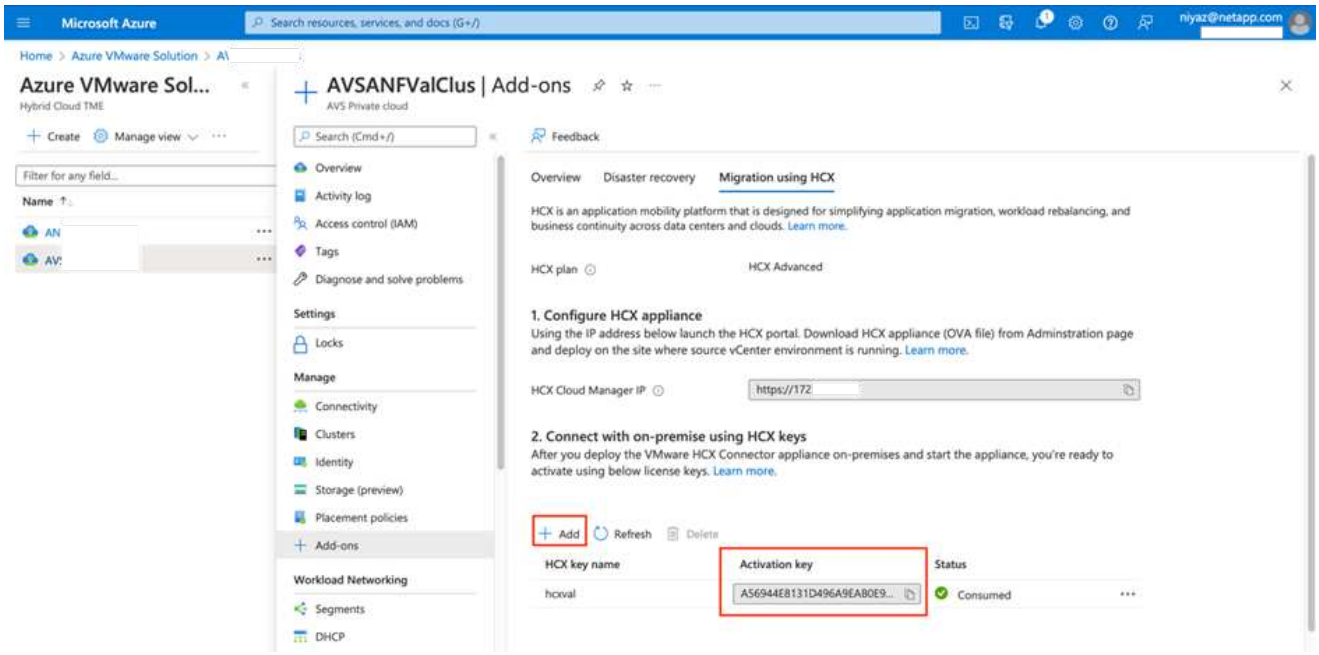
가상 어플라이언스의 전원을 수동으로 켭니다.

단계별 지침은 를 참조하십시오 "VMware HCX 사용자 가이드".

3단계**:** 라이센스 키로 **HCX** 커넥터를 활성화합니다

VMware HCX 커넥터 OVA를 온-프레미스로 배포하고 어플라이언스를 시작한 후 다음 단계를 수행하여 HCX 커넥터를 활성화하십시오. Azure VMware Solution 포털에서 라이센스 키를 생성하고 VMware HCX Manager에서 활성화합니다.

1. Azure 포털에서 Azure VMware 솔루션으로 이동하여 프라이빗 클라우드를 선택하고 * 관리 > 추가 기능 > HCX * 를 사용한 마이그레이션 을 선택합니다.
2. HCX 키를 사용하여 온-프레미스로 연결 * 에서 * 추가 * 를 클릭하고 활성화 키를 복사합니다.



배포된 각 온프레미스 HCX Connector에는 별도의 키가 필요합니다.

1. 사내 VMware HCX Manager()에 로그인합니다 "https://hcxmanagerIP:9443" 관리자 자격 증명을 사용합니다.

OVA 배포 중에 정의된 암호를 사용합니다.

1. 라이센스에서 3단계에서 복사한 키를 입력하고 * Activate * 를 클릭합니다.

온프레미스 HCX 커넥터는 인터넷에 연결되어 있어야 합니다.

1. 데이터 센터 위치 * 에서 VMware HCX Manager를 사내에 설치할 수 있는 가장 가까운 위치를 제공합니다. 계속 * 을 클릭합니다.
2. 시스템 이름 * 에서 이름을 업데이트하고 * 계속 * 을 클릭합니다.
3. 예, 계속 * 을 클릭합니다.
4. vCenter * 연결 아래에서 vCenter Server의 FQDN(정규화된 도메인 이름) 또는 IP 주소와 해당 자격 증명을 입력하고 * 계속 * 을 클릭합니다.

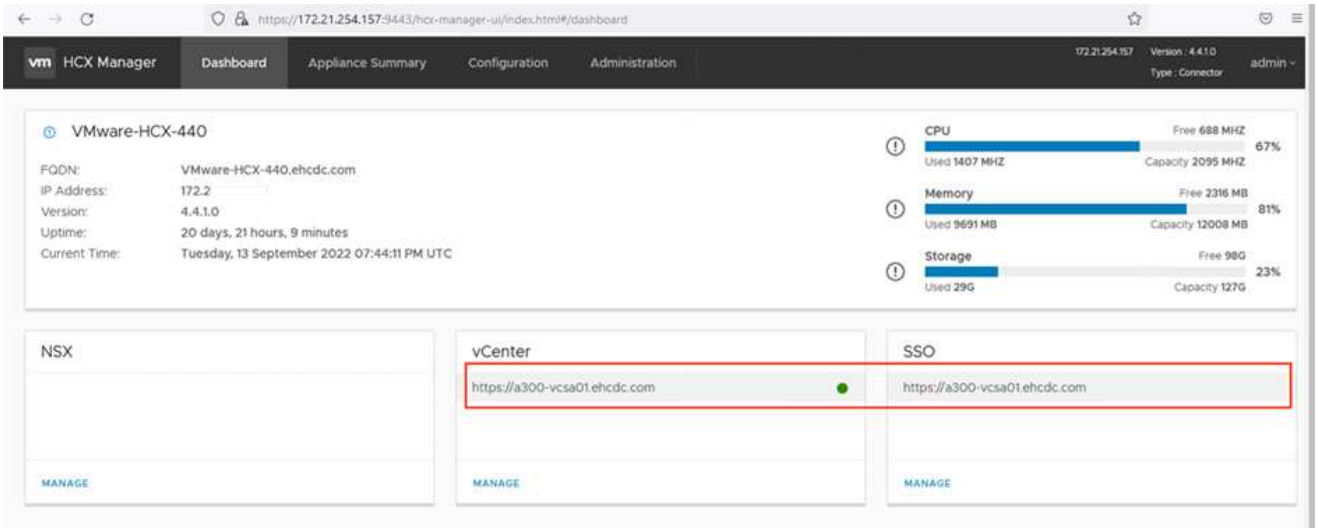
나중에 연결 문제를 방지하려면 FQDN을 사용합니다.

1. SSO/PSC * 구성 아래에서 플랫폼 서비스 컨트롤러의 FQDN 또는 IP 주소를 입력하고 * 계속 * 을 클릭합니다.

VMware vCenter Server FQDN 또는 IP 주소를 입력합니다.

1. 입력한 정보가 올바른지 확인하고 * Restart * (재시작 *)를 클릭합니다.
2. 서비스를 다시 시작하면 표시되는 페이지에 vCenter Server가 녹색으로 표시됩니다. vCenter Server와 SSO 모두 적절한 구성 매개 변수를 가져야 하며, 이는 이전 페이지와 동일해야 합니다.

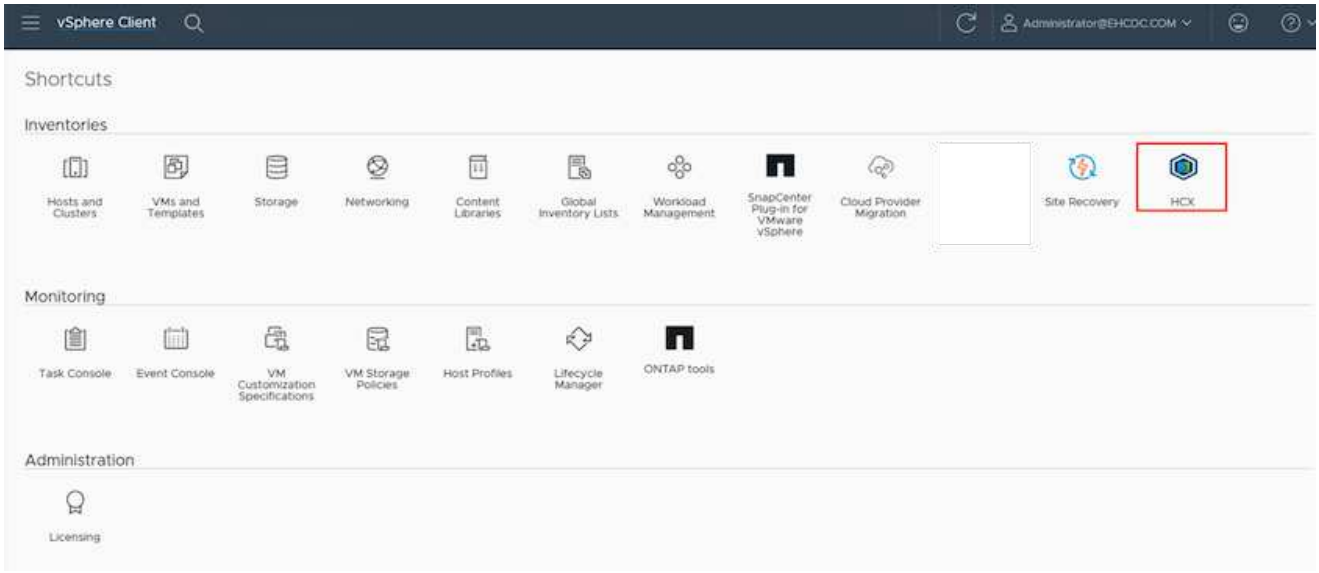
이 프로세스는 약 10~20분 정도 소요되며 플러그인이 vCenter Server에 추가되어야 합니다.



4단계: 온프레미스 **VMware HCX Connector**를 **Azure VMware Solution HCX Cloud Manager**와 페어링합니다

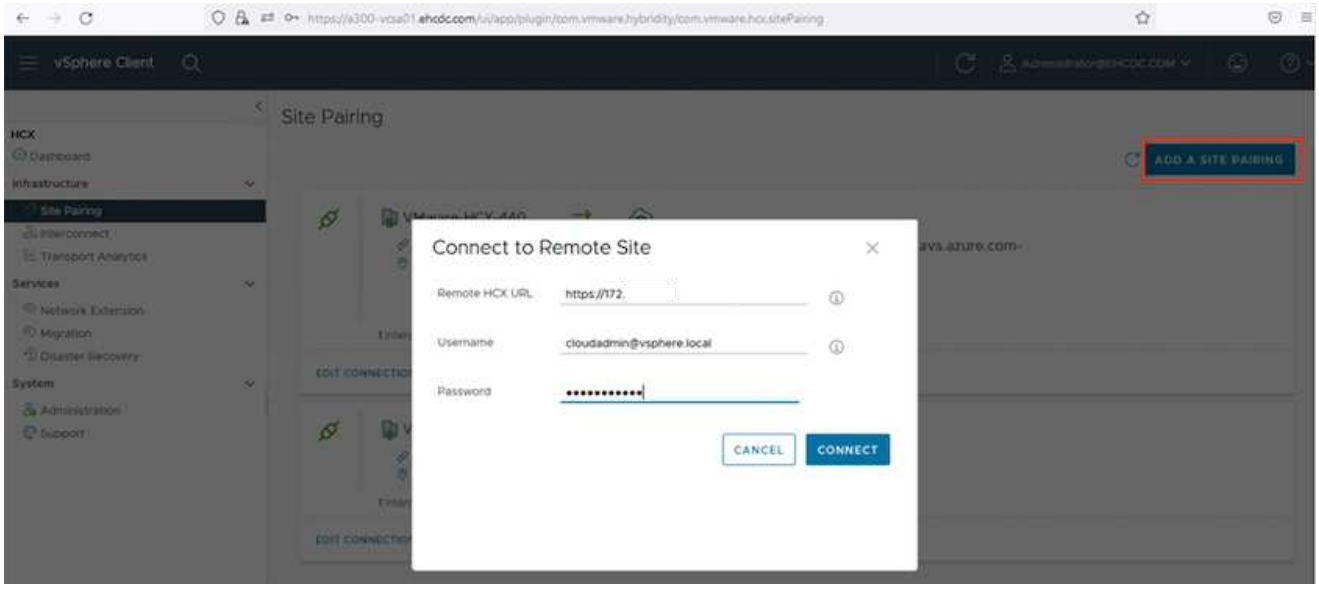
HCX Connector를 온프레미스 및 Azure VMware 솔루션에 설치한 후 페어링을 추가하여 온프레미스 VMware HCX Connector for Azure VMware Solution 프라이빗 클라우드를 구성합니다. 사이트 페어링을 구성하려면 다음 단계를 수행하십시오.

1. 온-프레미스 vCenter 환경과 Azure VMware Solution SDDC 간에 사이트 쌍을 생성하려면 온-프레미스 vCenter Server에 로그인하고 새 HCX vSphere Web Client 플러그인에 액세스합니다.



1. 인프라 에서 * 사이트 페어링 추가 * 를 클릭합니다.

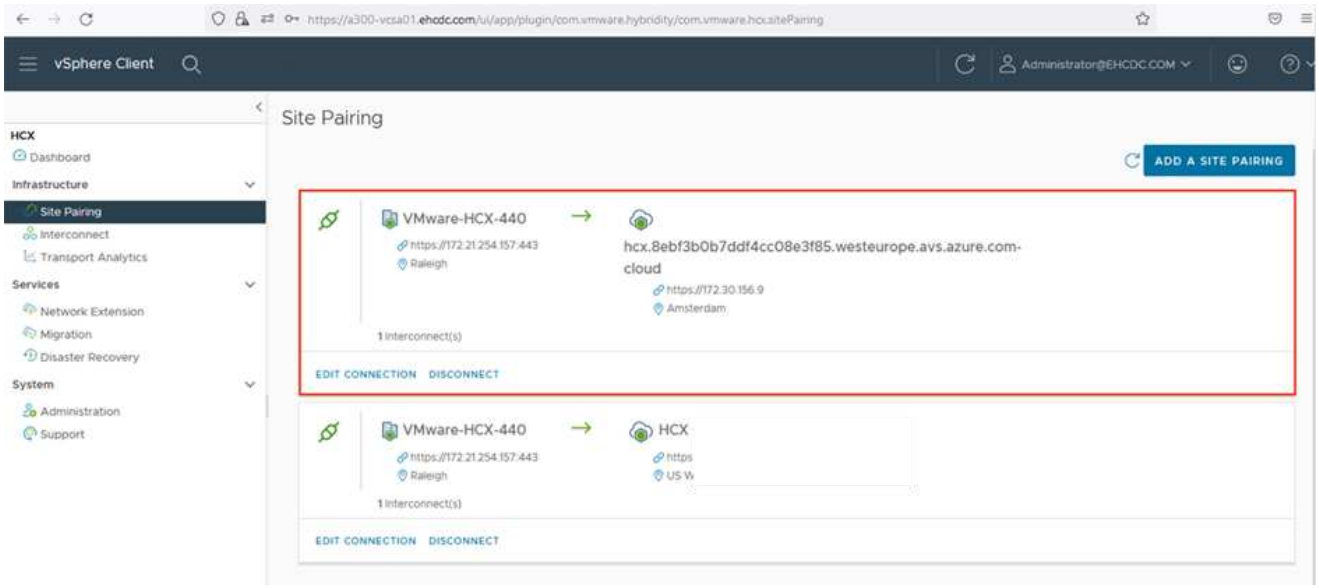
Azure VMware 솔루션 HCX Cloud Manager URL 또는 IP 주소와 프라이빗 클라우드에 액세스하기 위한 CloudAdmin 역할의 자격 증명을 입력합니다.



1. 연결 * 을 클릭합니다.

VMware HCX Connector는 포트 443을 통해 HCX Cloud Manager IP로 라우팅할 수 있어야 합니다.

1. 페어링이 생성된 후에는 새로 구성된 사이트 페어링을 HCX 대시보드에서 사용할 수 있습니다.

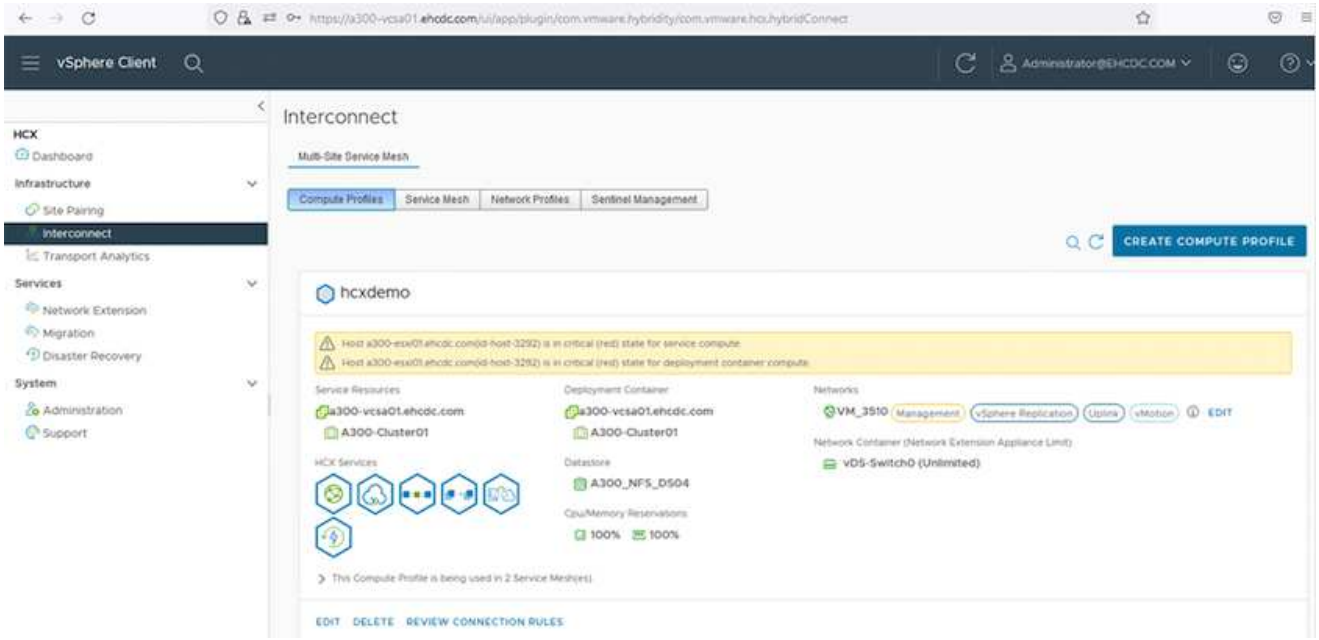


5단계**:** 네트워크 프로파일**,** 컴퓨팅 프로파일 및 서비스 메시를 구성합니다

VMware HCX Interconnect 서비스 어플라이언스는 인터넷을 통해 복제 및 vMotion 기반 마이그레이션 기능과 타겟 사이트에 대한 프라이빗 연결을 제공합니다. 상호 연결은 암호화, 트래픽 엔지니어링 및 VM 이동성을 제공합니다. 상호 연결 서비스 어플라이언스를 생성하려면 다음 단계를 수행하십시오.

1. 인프라 아래에서 * 상호 연결 > 멀티 사이트 서비스 메시 > 컴퓨팅 프로파일 > 컴퓨팅 프로파일 생성 * 을 선택합니다.

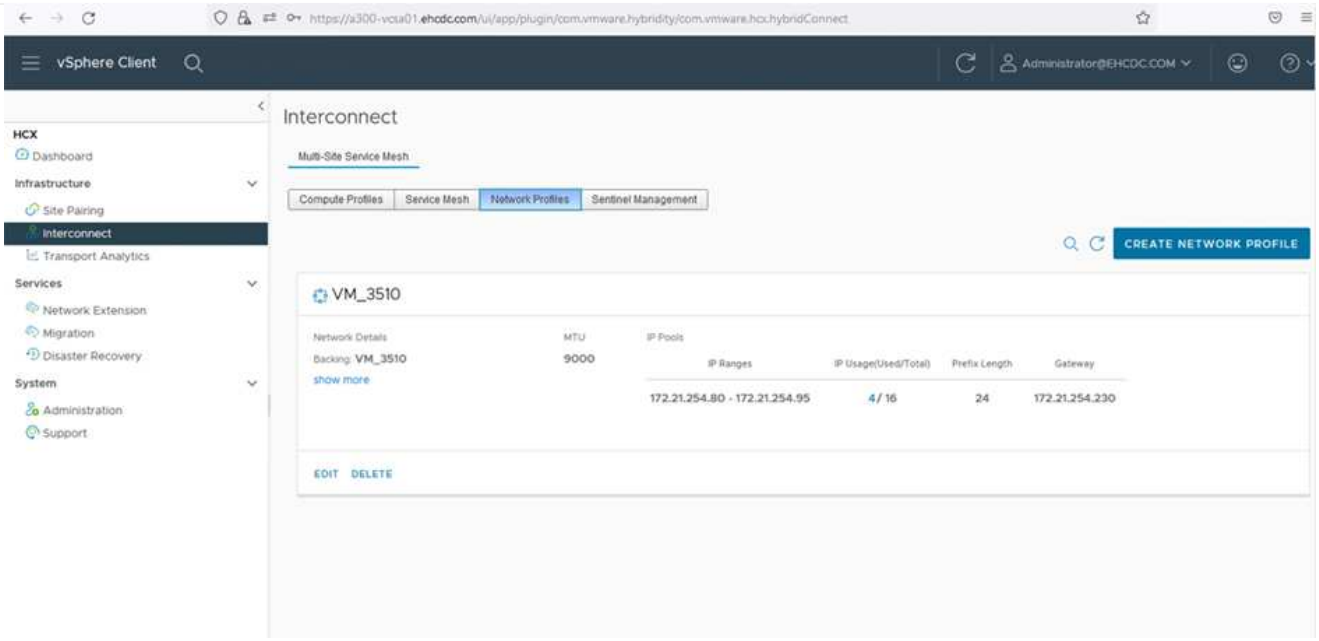
컴퓨팅 프로필은 구축된 어플라이언스와 HCX 서비스에서 액세스할 수 있는 VMware 데이터 센터 부분을 포함하여 구축 매개 변수를 정의합니다.



1. 컴퓨팅 프로파일을 만든 후 * 다중 사이트 서비스 메시 > 네트워크 프로파일 > 네트워크 프로파일 만들기 * 를 선택하여 네트워크 프로파일을 만듭니다.

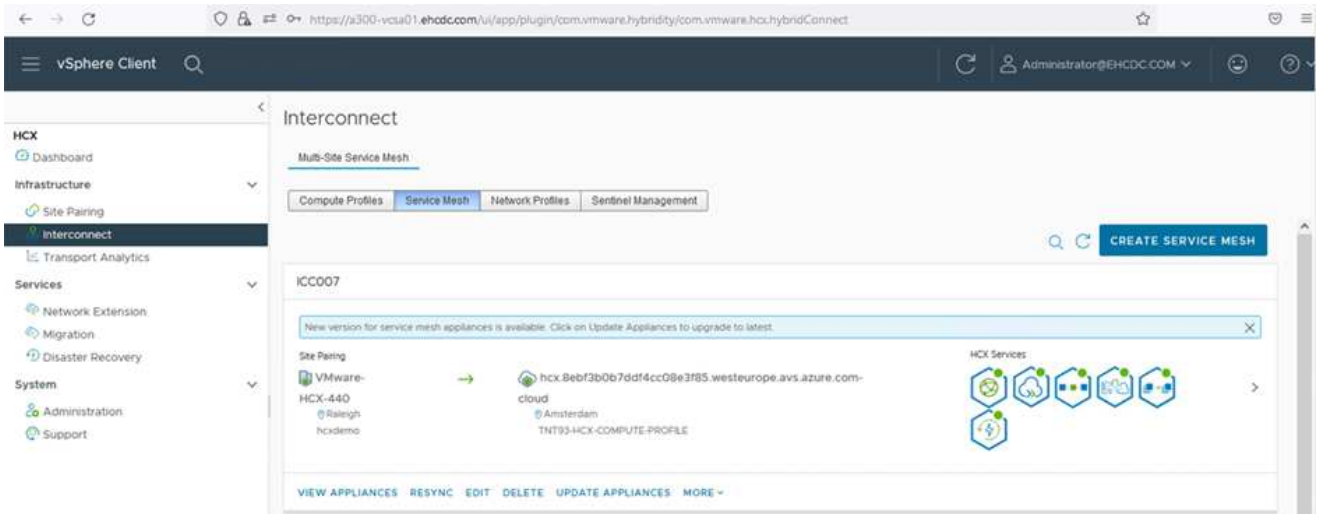
네트워크 프로파일은 HCX가 가상 어플라이언스에 사용하는 IP 주소 및 네트워크의 범위를 정의합니다.

이 단계에서는 두 개 이상의 IP 주소가 필요합니다. 이러한 IP 주소는 관리 네트워크에서 상호 연결 어플라이언스로 할당됩니다.

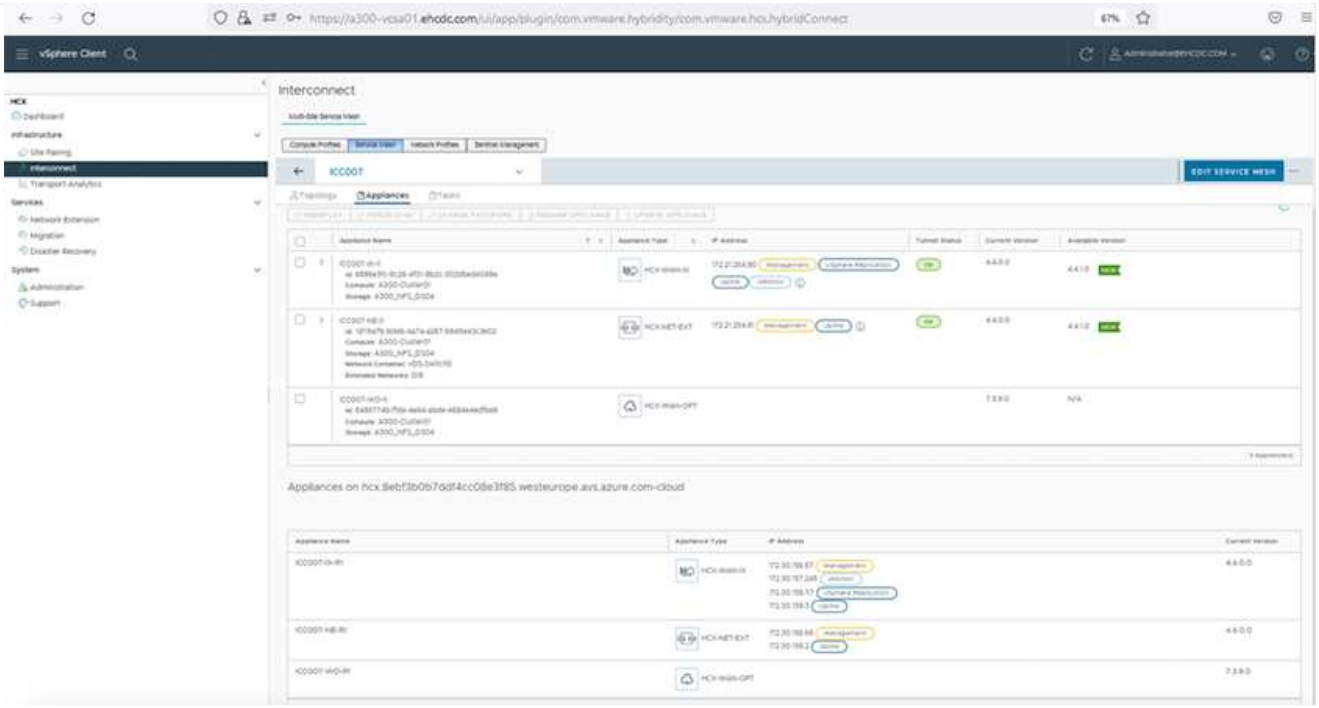


1. 현재 컴퓨팅 및 네트워크 프로파일이 성공적으로 생성되었습니다.
2. Interconnect * 옵션 내에서 * Service Mesh * 탭을 선택하고 온프레미스 및 Azure SDDC 사이트를 선택하여 Service Mesh를 생성합니다.
3. 서비스 메시는 로컬 및 원격 계산 및 네트워크 프로파일 쌍을 지정합니다.

이 프로세스의 일환으로 안전한 전송 패브릭을 생성하기 위해 소스 사이트와 타겟 사이트 모두에 HCX 어플라이언스를 구축하고 자동으로 구성합니다.



1. 이 단계는 구성의 마지막 단계입니다. 구축을 완료하는 데 약 30분이 소요됩니다. 서비스 메시가 구성된 후 작업 부하 VM을 마이그레이션하도록 IPsec 터널이 성공적으로 생성된 환경이 준비됩니다.


vSphere Client
Interconnect
EDIT SERVICE MESH
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

6단계**:** 워크로드 마이그레이션

다양한 VMware HCX 마이그레이션 기술을 사용하여 온프레미스 및 Azure SDDC 간에 워크로드를 양방향으로 마이그레이션할 수 있습니다. VM은 HCX 대량 마이그레이션, HCX vMotion, HCX 콜드 마이그레이션, HCX Replication Assisted vMotion(HCX Enterprise Edition에서 사용 가능) 및 HCX OS 지원 마이그레이션(HCX Enterprise Edition에서 사용 가능)과 같은 여러 마이그레이션 기술을 사용하여 VMware HCX 활성 엔터티로 또는 VMware에서 이동할 수 있습니다.

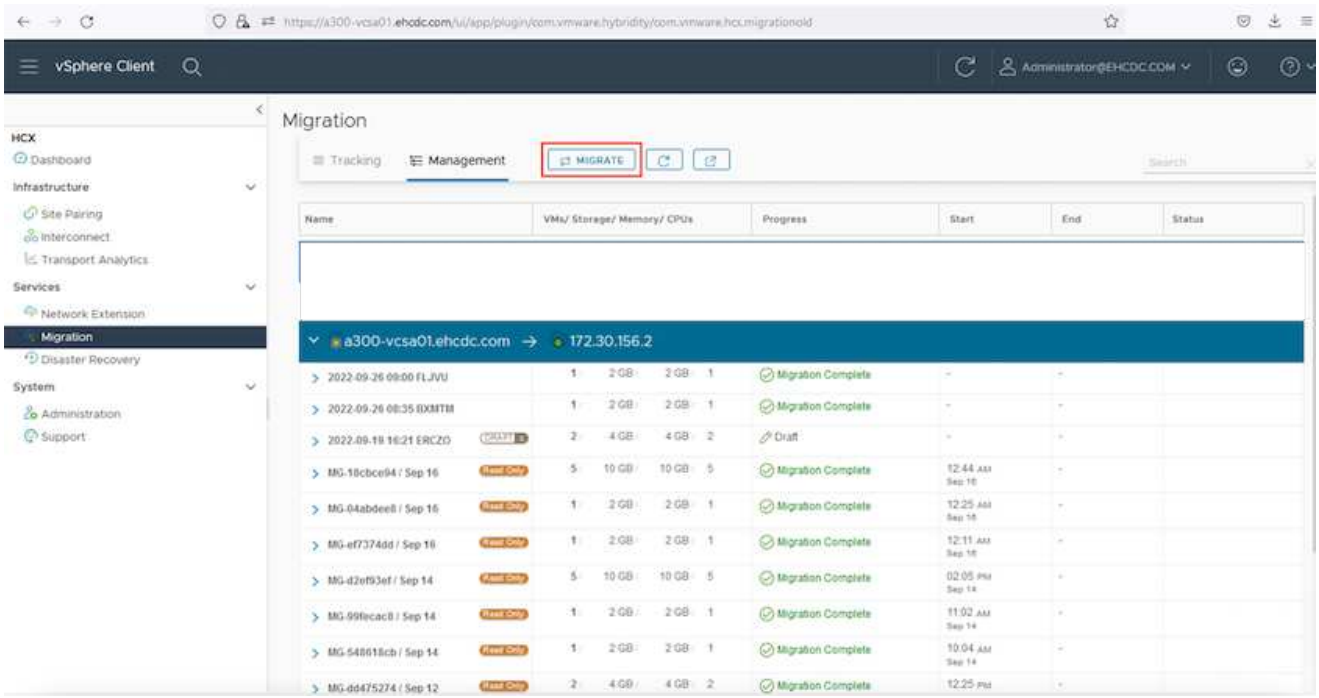
다양한 HCX 마이그레이션 메커니즘에 대한 자세한 내용은 을 참조하십시오 "VMware HCX 마이그레이션 유형".

- 대량 마이그레이션 *

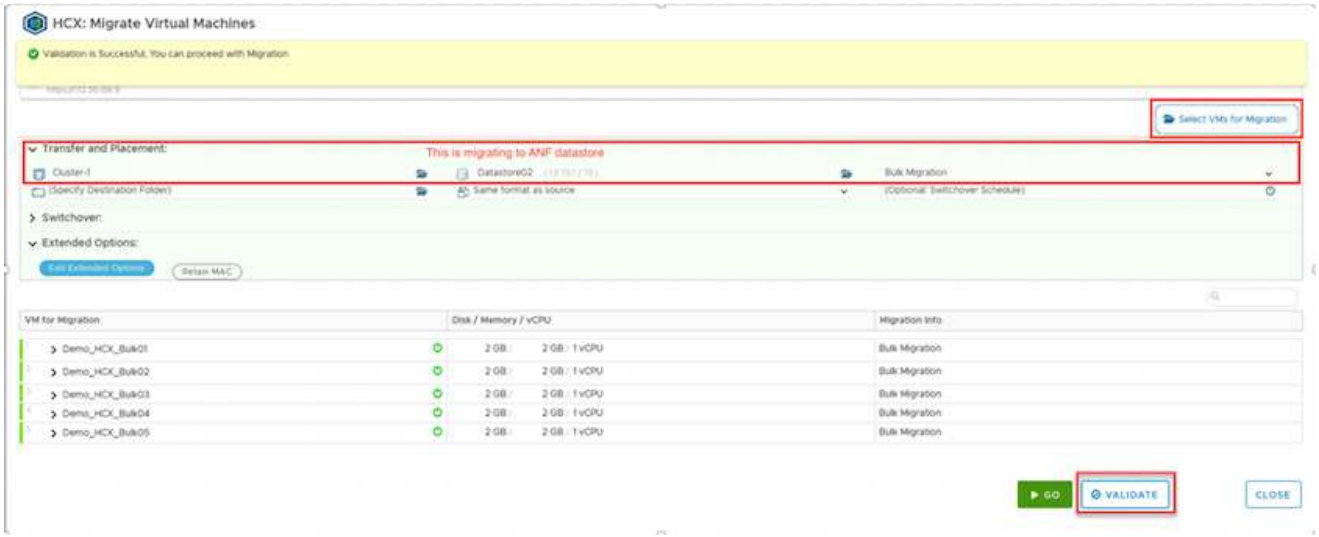
이 섹션에서는 대량 마이그레이션 메커니즘에 대해 자세히 설명합니다. 대량 마이그레이션 중에 HCX의 대량 마이그레이션 기능은 vSphere Replication을 사용하여 디스크 파일을 마이그레이션하는 동시에 대상 vSphere HCX 인스턴스에서 VM을 다시 생성합니다.

대량 VM 마이그레이션을 시작하려면 다음 단계를 수행하십시오.

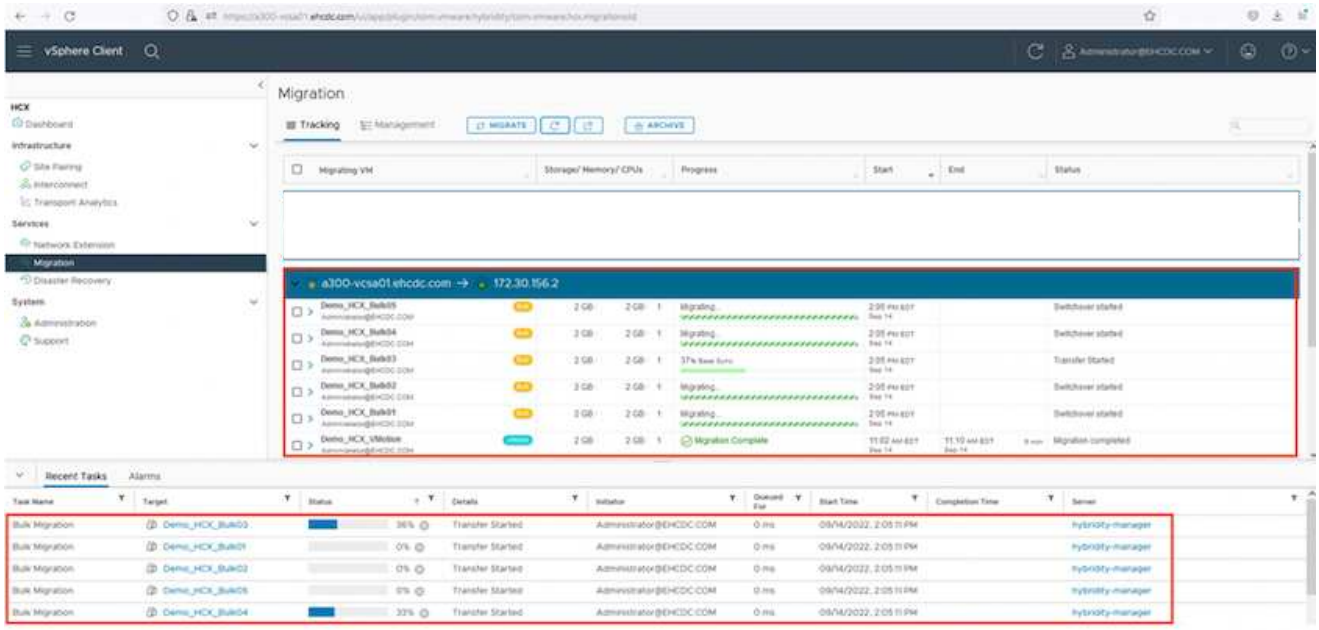
1. 서비스 > 마이그레이션 * 에서 * 마이그레이션 * 탭에 액세스합니다.



1. 원격 사이트 연결 * 에서 원격 사이트 연결을 선택하고 소스 및 대상을 선택합니다. 이 예에서 대상은 Azure VMware Solution SDDC HCX 엔드포인트입니다.
2. 마이그레이션을 위한 VM 선택 * 을 클릭합니다. 이 목록에는 모든 온-프레미스 VM 목록이 표시됩니다. match:value 식을 기준으로 VM을 선택하고 * Add * 를 클릭합니다.
3. Transfer and Placement * 섹션에서 마이그레이션 프로파일을 포함하여 필수 필드(* Cluster *, * Storage *, * Destination * 및 * Network *)를 업데이트하고 * Validate * 를 클릭합니다.

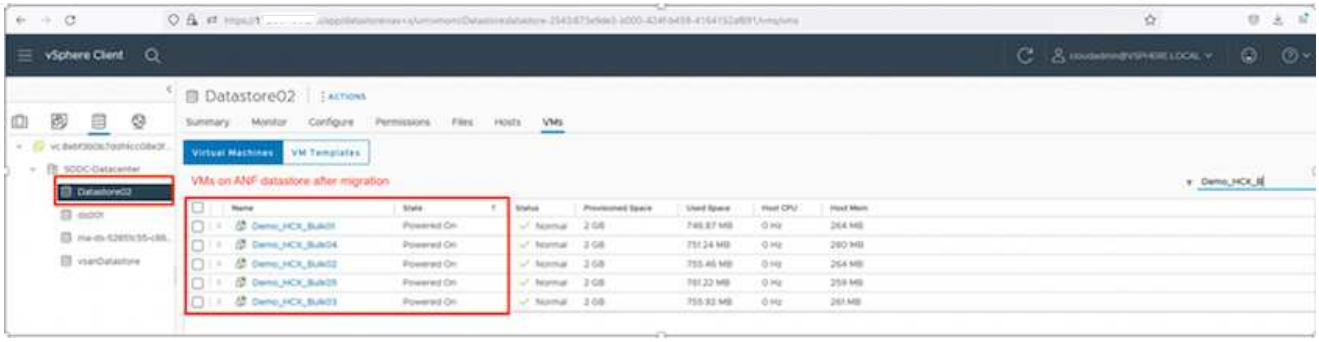


1. 유효성 검사가 완료된 후 * GO * 를 클릭하여 마이그레이션을 시작합니다.



이 마이그레이션 중에 소스 VM 디스크의 데이터를 자리 표시자 디스크로 복제할 수 있도록 대상 vCenter 내의 지정된 Azure NetApp Files 데이터 저장소에 자리 표시자 디스크가 생성됩니다. HBR은 타겟에 대한 전체 동기화를 위해 트리거되며, 기준선이 완료되면 RPO(복구 시점 목표) 주기에 따라 증가분 동기화가 수행됩니다. 전체/증분 동기화가 완료되면 특정 일정이 설정되지 않으면 전환이 자동으로 트리거됩니다.

1. 마이그레이션이 완료된 후 대상 SDDC vCenter에 액세스하여 동일한 검증을 수행합니다.

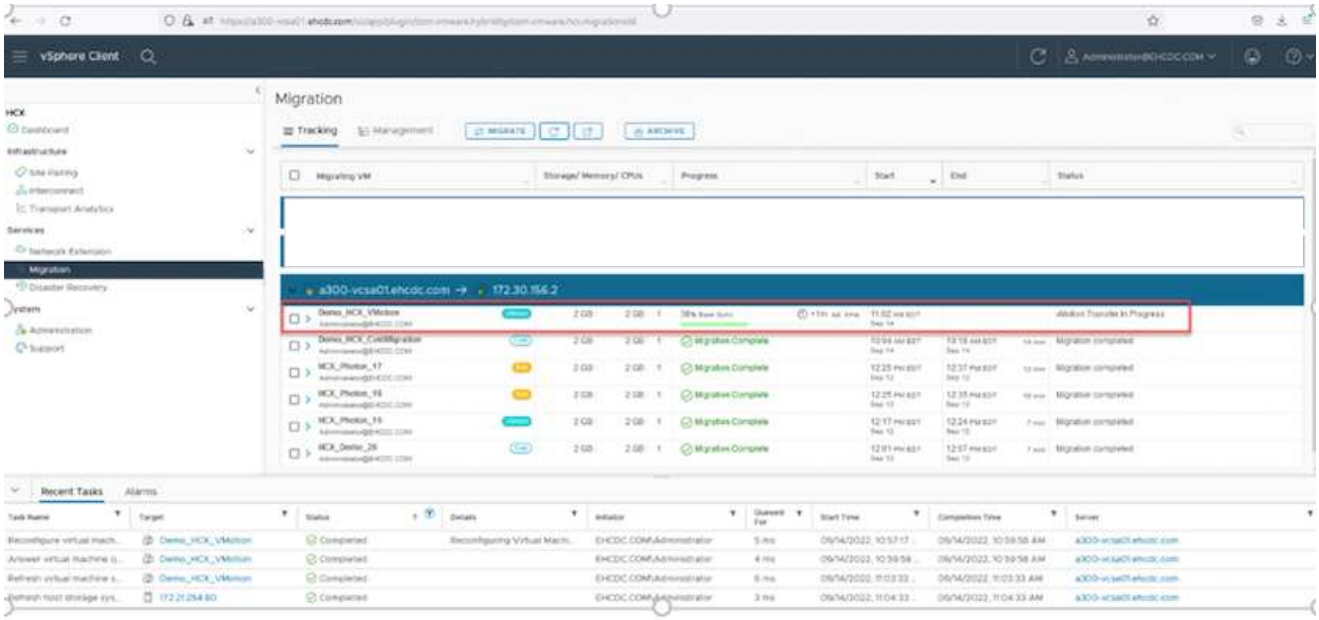


다양한 마이그레이션 옵션과 HCX를 사용하여 워크로드를 온프레미스에서 Azure VMware 솔루션으로 마이그레이션하는 방법에 대한 자세한 내용은 을 참조하십시오 "VMware HCX 사용자 가이드".

이 프로세스에 대해 자세히 알아보려면 다음 비디오를 시청하십시오.

HCX를 사용한 워크로드 마이그레이션

다음은 HCX vMotion 옵션의 스크린샷입니다.



이 프로세스에 대해 자세히 알아보려면 다음 비디오를 시청하십시오.

HCX 마이그레이션

ⓘ 마이그레이션을 처리할 수 있는 대역폭이 충분한지 확인합니다.

ⓘ 타겟 ANF 데이터 저장소에 마이그레이션을 처리할 충분한 공간이 있어야 합니다.

결론

Azure NetApp Files와 HCX는 사내 모든 유형/공급업체 스토리지에 상주하는 모든 클라우드 또는 하이브리드 클라우드 및 데이터를 대상으로 애플리케이션 워크로드에 대한 데이터 요구 사항을 애플리케이션 계층에 원활하게 제공함으로써

TCO를 절감하는 동시에 애플리케이션 워크로드를 배포 및 마이그레이션할 수 있는 탁월한 옵션을 제공합니다. 어떤 사용 사례에서든 Azure NetApp Files와 함께 Azure VMware 솔루션을 선택하면 클라우드의 이점, 일관된 인프라, 사내 및 멀티 클라우드 전반의 운영, 워크로드의 양방향 이동성, 엔터프라이즈급 용량 및 성능을 빠르게 실현할 수 있습니다. VMware vSphere Replication, VMware vMotion 또는 NFC(네트워크 파일 복사)를 사용하여 스토리지를 연결하고 VM을 마이그레이션하는 데 사용되는 익숙한 프로세스와 절차가 동일합니다.

이점

이 문서의 핵심 사항은 다음과 같습니다.

- 이제 Azure NetApp Files를 Azure VMware 솔루션 SDDC에서 데이터 저장소로 사용할 수 있습니다.
- 사내의 데이터를 Azure NetApp Files 데이터 저장소로 손쉽게 마이그레이션할 수 있습니다.
- 마이그레이션 작업 중에 용량 및 성능 요구 사항을 충족하도록 Azure NetApp Files 데이터 저장소를 쉽게 확장 및 축소할 수 있습니다.

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 웹 사이트 링크를 참조하십시오.

- Azure VMware 솔루션 설명서

"https://docs.microsoft.com/en-us/azure/azure-vmware/"

- Azure NetApp Files 설명서

"https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- VMware HCX 사용자 가이드

"https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

지역 가용성 **– ANF**용 보조 **NFS** 데이터 저장소

Azure/AVS에서 보조 NFS 데이터 저장소의 가용성은 Microsoft에서 정의합니다. 먼저 AVS와 ANF를 특정 지역에서 모두 사용할 수 있는지 확인해야 합니다. 그런 다음 해당 지역에서 ANF 보조 NFS 데이터 저장소가 지원되는지 여부를 확인해야 합니다.

- AVS 및 ANF의 가용성을 확인하십시오 "여기".
- ANF 보조 NFS 데이터 저장소의 가용성을 확인합니다 "여기".

Google Cloud Platform GCVE를 위한 NetApp의 기능

NetApp이 GCP(Google Cloud Platform) Google Cloud VMware Engine(GCVE)에 제공하는 기능에 대해 자세히 알아보십시오. NetApp(게스트 연결 스토리지 장치 또는 보조 NFS 데이터 저장소부터 마이그레이션, 클라우드로 확장/버스트, 재해 복구까지.

다음 옵션 중 하나를 선택하여 원하는 콘텐츠의 섹션으로 이동합니다.

- "GCP에서 GCVE 구성"

- "GCVE용 NetApp 스토리지 옵션"
- "NetApp/VMware 클라우드 솔루션"

GCP에서 GCVE 구성

온프레미스에서와 마찬가지로 클라우드 기반 가상화 환경을 계획하는 것은 VM 및 마이그레이션을 생성할 수 있는 성공적인 프로덕션 준비 환경에 매우 중요합니다.

이 섹션에서는 GCVE를 설정 및 관리하고 NetApp 스토리지를 연결하는 데 사용할 수 있는 옵션과 함께 사용하는 방법을 설명합니다.

> 게스트 내 저장소는 Cloud Volumes ONTAP 및 Cloud Volumes Services를 GCVE에 연결하는 유일한 지원 방법입니다.

설치 프로세스는 다음 단계로 나눌 수 있습니다.

- GCVE 배포 및 구성
- GCVE에 대한 개인 액세스를 활성화합니다

자세한 내용을 확인하십시오 "GCVE에 대한 구성 단계".

GCVE용 NetApp 스토리지 옵션

NetApp 스토리지는 GCP GCVE 내에서 guess Connected 또는 보충 NFS 데이터 저장소로 여러 가지 방법으로 활용할 수 있습니다.

를 방문하십시오 "지원되는 NetApp 스토리지 옵션" 를 참조하십시오.

Google Cloud는 다음과 같은 구성에서 NetApp 스토리지를 지원합니다.

- CVO(Cloud Volumes ONTAP)를 게스트 연결 스토리지로 사용합니다
- CVS(Cloud Volumes Service)를 게스트 연결 스토리지로 사용합니다
- CVS(Cloud Volumes Service)를 보조 NFS 데이터 저장소로 사용

자세한 내용을 확인하십시오 "GCVE에 대한 게스트 연결 저장소 옵션".

에 대해 자세히 알아보십시오 "Google Cloud VMware Engine에 대한 NetApp Cloud Volumes Service 데이터 저장소 지원(NetApp 블로그)" 또는 "NetApp CVS를 Google Cloud VMware Engine용 데이터 저장소로 사용하는 방법(Google 블로그)"

솔루션 사용 사례

NetApp 및 VMware 클라우드 솔루션을 사용하면 많은 사용 사례를 Azure AVS에서 간단하게 구축할 수 있습니다. SE 사례는 VMware에서 정의한 각 클라우드 영역에 대해 정의됩니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 확장
- 마이그레이션

"Google Cloud GCVE용 NetApp 솔루션을 찾아보십시오"

GCP/GCVE에서 워크로드 보호

NetApp SnapCenter 및 Veeam 복제를 통해 애플리케이션 정합성이 보장되는 재해 복구

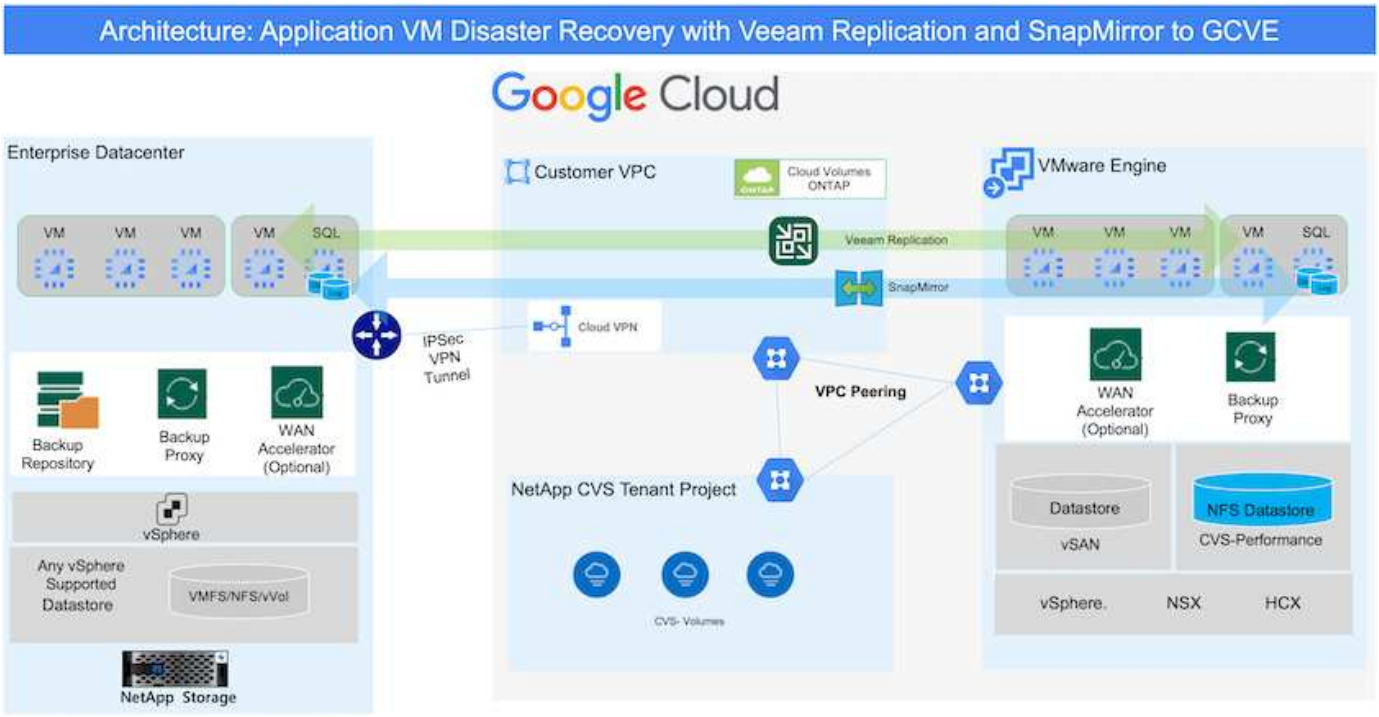
저자: NetApp Suesh Thoppay

개요

많은 고객이 VMware vSphere에서 호스팅되는 애플리케이션 VM을 위한 효율적인 재해 복구 솔루션을 찾고 있습니다. 이 중 다수는 기존 백업 솔루션을 사용하여 DIaster를 실행하는 동안 복구를 수행합니다.
이러한 솔루션은 RTO를 높여주고 기대에 미치지 못합니다. RPO 및 RTO를 줄이기 위해 적절한 권한이 있는 네트워크 연결 및 환경을 사용할 수 있는 한 Veeam VM 복제를 사내에서 GCVE로 활용할 수 있습니다.
참고: Veeam VM 복제는 게스트 VM 내부의 iSCSI 또는 NFS 마운트와 같은 VM 게스트에 연결된 스토리지 디바이스를 보호하지 않습니다. 별도로 보호해야 합니다.

SQL VM의 애플리케이션 정합성이 보장되는 복제 및 RTO를 줄이기 위해 SnapCenter을 사용하여 SQL 데이터베이스 및 로그 볼륨의 SnapMirror 작업을 오케스트레이션했습니다.

이 문서에서는 NetApp SnapMirror, Veeam 및 Google Cloud VMware Engine(GCVE)을 사용하는 재해 복구를 설정하고 수행하기 위한 단계별 접근 방식을 제공합니다.



가정

이 문서에서는 애플리케이션 데이터(게스트 연결)를 위한 게스트 내 스토리지에 초점을 두고 사내 환경에서 애플리케이션 정합성 보장 백업을 위해 SnapCenter를 사용하고 있다고 가정합니다.

> 이 문서는 타사 백업 또는 복구 솔루션에 적용됩니다. 환경에 사용된 솔루션에 따라 Best Practice를 따라 조직 SLA를 충족하는 백업 정책을 생성합니다.

온프레미스 환경과 Google Cloud 네트워크 간의 연결을 위해 전용 상호 연결 또는 Cloud VPN과 같은 연결 옵션을 사용합니다. 세그먼트는 사내 VLAN 설계를 기반으로 생성해야 합니다.

> 온프레미스 데이터 센터를 Google Cloud에 연결하는 옵션에는 여러 가지가 있으며, 이로 인해 NetApp에서 이 문서의 특정 워크플로우를 개괄적으로 설명하지 못하게 됩니다. 적절한 온프레미스 -Google 연결 방법은 Google Cloud 설명서를 참조하십시오.

DR 솔루션 구축

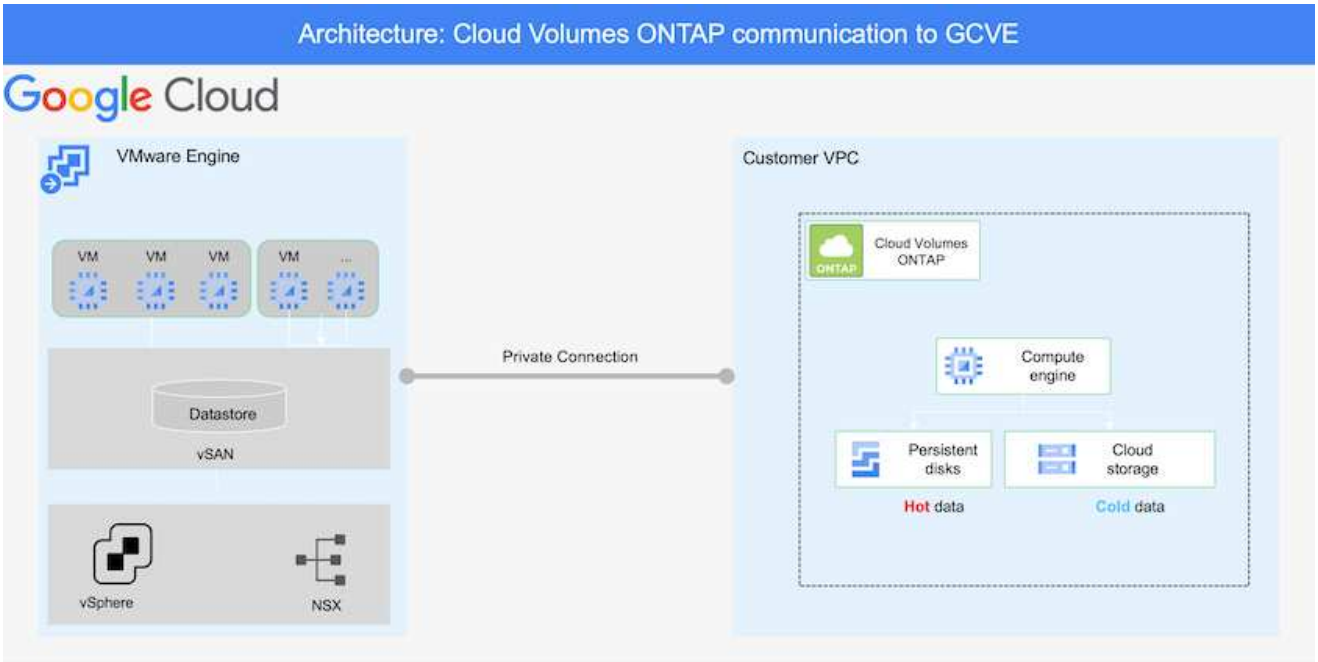
솔루션 구축 개요

1. 필요한 RPO 요구 사항에 따라 SnapCenter를 사용하여 애플리케이션 데이터를 백업했는지 확인합니다.
2. 적절한 가입 및 가상 네트워크 내에서 BlueXP를 사용하여 Cloud Volumes ONTAP의 인스턴스 크기를 올바르게 프로비저닝합니다.
    a. 관련 애플리케이션 볼륨에 대해 SnapMirror를 구성합니다.
    b. 예약된 작업 후 SnapMirror 업데이트를 트리거하도록 SnapCenter의 백업 정책을 업데이트합니다.
3. Veeam 소프트웨어를 설치하고 Google Cloud VMware Engine 인스턴스에 가상 머신 복제를 시작합니다.
4. 재해 발생 시 BlueXP를 사용하여 SnapMirror 관계를 중단시키고 Veeam으로 가상 시스템의 페일오버를 트리거하십시오.
    a. 애플리케이션 VM에 대한 iSCSI LUN 및 NFS 마운트를 다시 연결합니다.
    b. 애플리케이션을 온라인으로 전환합니다.
5. 운영 사이트가 복구된 후 SnapMirror를 다시 동기화하여 보호 사이트에 대한 페일백을 호출합니다.

배포 세부 정보

Google Cloud에서 **CVO**를 구성하고 볼륨을 **CVO**로 복제합니다

첫 번째 단계는 Cloud Volumes ONTAP Google Cloud("CVO")를 사용하여 원하는 볼륨을 Cloud Volumes ONTAP에 복제하고 원하는 빈도와 스냅샷 보존 기능을 사용할 수 있습니다.



SnapCenter 설정 및 데이터 복제에 대한 단계별 지침은 을 참조하십시오 "SnapCenter를 사용하여 복제를 설정합니다"

SnapCenter를 사용한 SQL VM 보호 검토

GCVE 호스트 및 **CVO** 데이터 액세스를 구성합니다

SDDC를 배포할 때 고려해야 할 두 가지 중요한 요소는 GCVE 솔루션의 SDDC 클러스터의 크기와 SDDC를 사용할 수 있는 기간 입니다. 재해 복구 솔루션의 두 가지 주요 고려 사항은 전체 운영 비용을 절감하는 데 도움이 됩니다. SDDC는 최대 3개의 호스트까지 구성할 수 있으며, 전체 구축 환경에서 다중 호스트 클러스터까지 가능합니다.

NFS 데이터 저장소용 NetApp Cloud Volume Service와 SQL 데이터베이스 및 로그용 Cloud Volumes ONTAP를 모든 VPC 및 GCVE에 구축할 수 있습니다. NFS 데이터 저장소를 마운트하고 VM을 iSCSI LUN에 연결하려면 해당 VPC에 대한 전용 연결이 있어야 합니다.

GCVE SDDC를 구성하려면 를 참조하십시오 "Google Cloud Platform(GCP)에서 가상화 환경 구축 및 구성". 먼저 GCVE 호스트에 상주하는 게스트 VM이 연결이 설정된 후 Cloud Volumes ONTAP의 데이터를 사용할 수 있는지 확인합니다.

Cloud Volumes ONTAP 및 GCVE가 올바르게 구성된 후에는 Veeam 복제 기능을 사용하고 Cloud Volumes ONTAP에 애플리케이션 볼륨 복사본에 SnapMirror를 활용하여 사내 워크로드(게스트 내 스토리지가 있는 애플리케이션 VMDK 및 VM이 있는 VM)를 GCVE로 자동 복구하도록 Veeam 구성을 시작하십시오.

Veeam 구성 요소를 설치합니다

Veeam 백업 서버, 백업 저장소 및 구축해야 하는 백업 프록시가 구축 시나리오에 기반을 두고 있습니다. 이 경우 Veeam 및 스케일아웃 저장소에도 오브젝트 저장소를 구축할 필요가 없습니다.
"설치 절차는 Veeam 설명서를 참조하십시오"
자세한 내용은 을 참조하십시오 "Veeam 복제를 사용한 마이그레이션"

Veeam으로 **VM** 복제를 설정합니다

사내 vCenter와 GCVE vCenter를 모두 Veeam에 등록해야 합니다. "vSphere VM 복제 작업을 설정합니다"
마법사의 게스트 처리 단계에서 애플리케이션 인식 백업 및 복구를 위해 SnapCenter를 활용할 예정이므로 애플리케이션 처리 비활성화 를 선택합니다.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

Microsoft SQL Server VM의 페일오버

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

이 솔루션의 이점

- SnapMirror의 효율적이고 복원력이 뛰어난 복제를 사용합니다.
- ONTAP 스냅샷 보존을 사용하여 사용 가능한 모든 시점 복구
- 스토리지, 컴퓨팅, 네트워크 및 애플리케이션 검증 단계에서 수백 또는 수천 개의 VM을 복구하는 데 필요한 모든 단계에서 완전한 자동화가 가능합니다.
- SnapCenter는 복제된 볼륨을 변경하지 않는 클론 생성 메커니즘을 사용합니다.
  - 이렇게 하면 볼륨 및 스냅숏에 대한 데이터 손상 위험이 방지됩니다.
  - DR 테스트 워크플로우 중에 복제 중단 방지
  - 개발/테스트, 보안 테스트, 패치 및 업그레이드 테스트, 수정 테스트 등 DR 이외의 워크플로우에 DR 데이터를 활용합니다.
- Veeam Replication을 사용하면 DR 사이트에서 VM IP 주소를 변경할 수 있습니다.

SnapCenter, Cloud Volumes ONTAP, Veeam 복제를 통한 애플리케이션 재해 복구

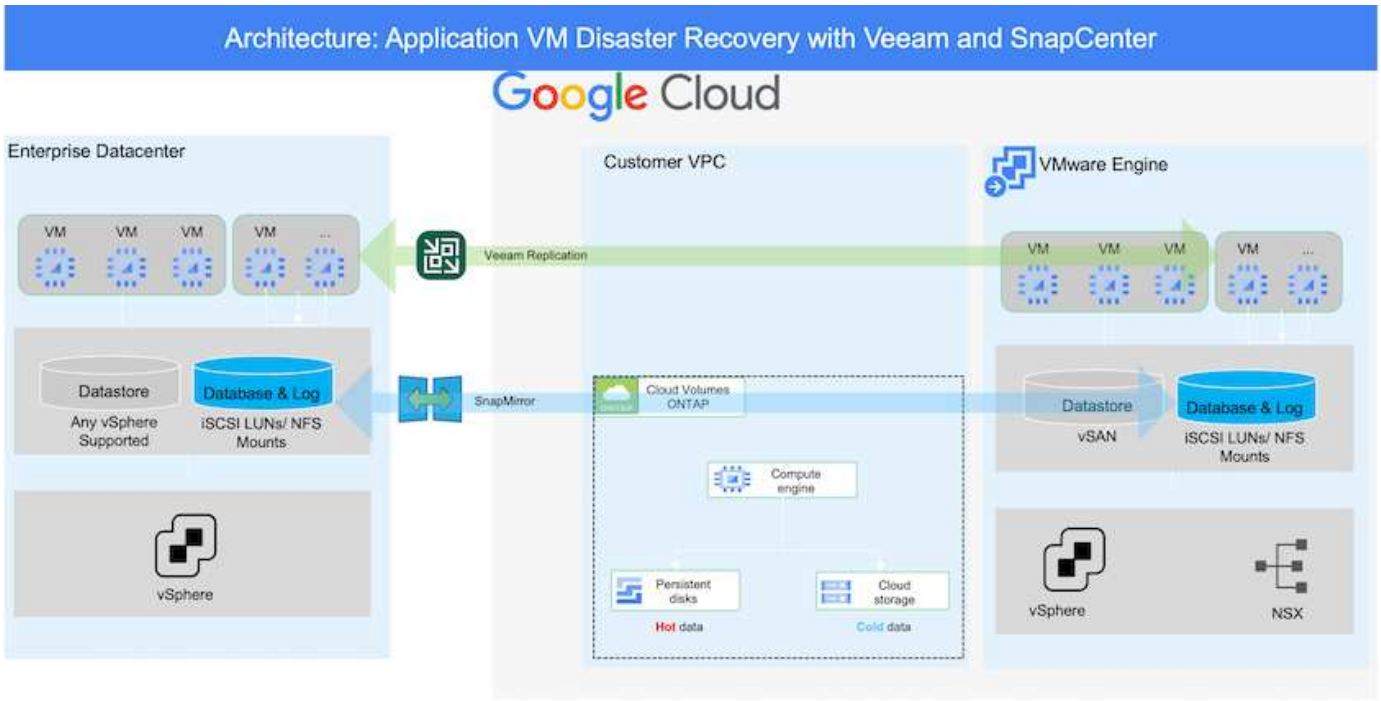
저자: NetApp Suesh Thoppay

개요

클라우드로 재해 복구는 랜섬웨어 등 사이트 운영 중단 및 데이터 손상 이벤트로부터 워크로드를 보호하는 복원력이 있는 비용 효율적인 방법입니다. NetApp SnapMirror를 사용하면 게스트 연결 스토리지를 사용하는 사내 VMware 워크로드를 Google Cloud에서 실행 중인 NetApp Cloud Volumes ONTAP로 복제할 수 있습니다. 여기에는 애플리케이션 데이터가 포함됩니다. 하지만 실제 VM 자체는 어떻습니까? 재해 복구는 가상 머신, VMDK, 애플리케이션 데이터 등을 비롯한 모든 종속 구성 요소를 포함해야 합니다. 이를 위해 Veeam과 함께 SnapMirror를 사용하여 VM VMDK에 vSAN 스토리지를 사용하면서 사내에서 Cloud Volumes ONTAP로 복제된 워크로드를 원활하게 복구할 수

있습니다.

이 문서에서는 NetApp SnapMirror, Veeam 및 Google Cloud VMware Engine(GCVE)을 사용하는 재해 복구를 설정하고 수행하기 위한 단계별 접근 방식을 제공합니다.



가정

이 문서에서는 애플리케이션 데이터(게스트 연결)를 위한 게스트 내 스토리지에 초점을 두고 사내 환경에서 애플리케이션 정합성 보장 백업을 위해 SnapCenter를 사용하고 있다고 가정합니다.

> 이 문서는 타사 백업 또는 복구 솔루션에 적용됩니다. 환경에 사용된 솔루션에 따라 Best Practice를 따라 조직 SLA를 충족하는 백업 정책을 생성합니다.

온프레미스 환경과 Google Cloud 네트워크 간의 연결을 위해 전용 상호 연결 또는 Cloud VPN과 같은 연결 옵션을 사용합니다. 세그먼트는 사내 VLAN 설계를 기반으로 생성해야 합니다.

> 온프레미스 데이터 센터를 Google Cloud에 연결하는 옵션에는 여러 가지가 있으며, 이로 인해 NetApp에서 이 문서의 특정 워크플로우를 개괄적으로 설명하지 못하게 됩니다. 적절한 온프레미스 -Google 연결 방법은 Google Cloud 설명서를 참조하십시오.

DR 솔루션 구축

솔루션 구축 개요

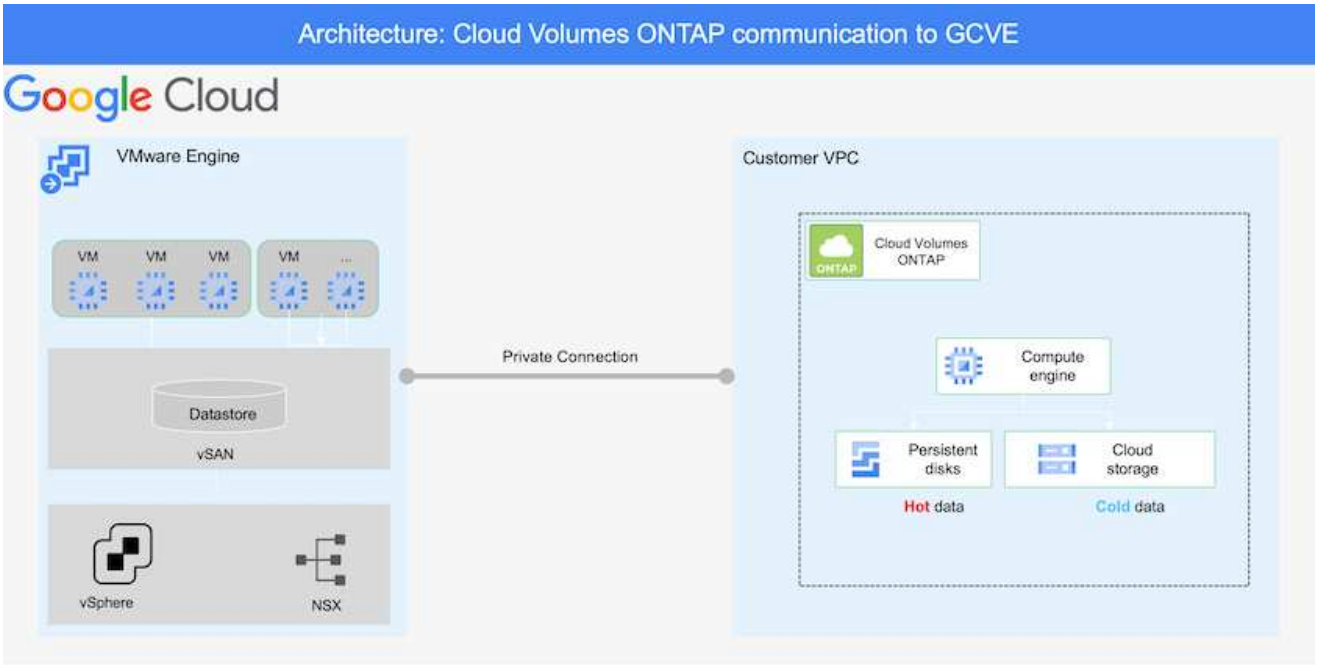
1. 필요한 RPO 요구 사항에 따라 SnapCenter를 사용하여 애플리케이션 데이터를 백업했는지 확인합니다.
2. 적절한 서브스크립션 및 가상 네트워크 내에서 Cloud Manager를 사용하여 올바른 인스턴스 크기로 Cloud Volumes ONTAP를 프로비저닝합니다.
   a. 관련 애플리케이션 볼륨에 대해 SnapMirror를 구성합니다.
   b. 예약된 작업 후 SnapMirror 업데이트를 트리거하도록 SnapCenter의 백업 정책을 업데이트합니다.

3. Veeam 소프트웨어를 설치하고 Google Cloud VMware Engine 인스턴스에 가상 머신 복제를 시작합니다.
4. 재해 발생 시 Cloud Manager를 사용하여 SnapMirror 관계를 맺고 Veeam으로 가상 시스템의 페일오버를 트리거하십시오.
    a. 애플리케이션 VM에 대한 iSCSI LUN 및 NFS 마운트를 다시 연결합니다.
    b. 애플리케이션을 온라인으로 전환합니다.
5. 운영 사이트가 복구된 후 SnapMirror를 다시 동기화하여 보호 사이트에 대한 페일백을 호출합니다.

배포 세부 정보

Google Cloud에서 **CVO**를 구성하고 볼륨을 **CVO**로 복제합니다

첫 번째 단계는 Cloud Volumes ONTAP Google Cloud("CVO")를 사용하여 원하는 볼륨을 Cloud Volumes ONTAP에 복제하고 원하는 빈도와 스냅샷 보존 기능을 사용할 수 있습니다.



SnapCenter 설정 및 데이터 복제에 대한 단계별 지침은 을 참조하십시오 "SnapCenter를 사용하여 복제를 설정합니다"

SnapCenter를 사용하여 복제를 설정합니다

GCVE 호스트 및 **CVO** 데이터 액세스를 구성합니다

SDDC를 배포할 때 고려해야 할 두 가지 중요한 요소는 GCVE 솔루션의 SDDC 클러스터의 크기와 SDDC를 사용할 수 있는 기간 입니다. 재해 복구 솔루션의 두 가지 주요 고려 사항은 전체 운영 비용을 절감하는 데 도움이 됩니다. SDDC는 최대 3개의 호스트까지 구성할 수 있으며, 전체 구축 환경에서 다중 호스트 클러스터까지 가능합니다.

모든 VPC 및 GCVE에 Cloud Volumes ONTAP를 구축할 수 있습니다. VM이 iSCSI LUN에 접속하려면 해당 VPC에 대한 전용 연결이 있어야 합니다.

GCVE SDDC를 구성하려면 를 참조하십시오 "Google Cloud Platform(GCP)에서 가상화 환경 구축 및 구성". 먼저 GCVE 호스트에 상주하는 게스트 VM이 연결이 설정된 후 Cloud Volumes ONTAP의 데이터를 사용할 수 있는지 확인합니다.

Cloud Volumes ONTAP 및 GCVE가 올바르게 구성된 후에는 Veeam 복제 기능을 사용하고 Cloud Volumes ONTAP에 애플리케이션 볼륨 복사본에 SnapMirror를 활용하여 사내 워크로드(게스트 내 스토리지가 있는 애플리케이션 VMDK 및 VM이 있는 VM)를 GCVE로 자동 복구하도록 Veeam 구성을 시작하십시오.

Veeam 구성 요소를 설치합니다

Veeam 백업 서버, 백업 저장소 및 구축해야 하는 백업 프록시가 구축 시나리오에 기반을 두고 있습니다. 이 경우 Veeam 및 스케일아웃 저장소에도 오브젝트 저장소를 구축할 필요가 없습니다.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["설치 절차는 Veeam 설명서를 참조하십시오"]

Veeam으로 **VM** 복제를 설정합니다

사내 vCenter와 GCVE vCenter를 모두 Veeam에 등록해야 합니다. "vSphere VM 복제 작업을 설정합니다" 마법사의 게스트 처리 단계에서 애플리케이션 인식 백업 및 복구를 위해 SnapCenter를 활용할 예정이므로 애플리케이션 처리 비활성화 를 선택합니다.

vSphere VM 복제 작업을 설정합니다

Microsoft SQL Server VM의 페일오버

Microsoft SQL Server VM의 페일오버

이 솔루션의 이점

- SnapMirror의 효율적이고 복원력이 뛰어난 복제를 사용합니다.
- ONTAP 스냅샷 보존을 사용하여 사용 가능한 모든 시점 복구
- 스토리지, 컴퓨팅, 네트워크 및 애플리케이션 검증 단계에서 수백 또는 수천 개의 VM을 복구하는 데 필요한 모든 단계에서 완전한 자동화가 가능합니다.
- SnapCenter는 복제된 볼륨을 변경하지 않는 클론 생성 메커니즘을 사용합니다.
  - 이렇게 하면 볼륨 및 스냅숏에 대한 데이터 손상 위험이 방지됩니다.
  - DR 테스트 워크플로우 중에 복제 중단 방지

◦ 개발/테스트, 보안 테스트, 패치 및 업그레이드 테스트, 수정 테스트 등 DR 이외의 워크플로우에 DR 데이터를 활용합니다.

- Veeam Replication을 사용하면 DR 사이트에서 VM IP 주소를 변경할 수 있습니다.

GCP/GCVE에서 워크로드를 마이그레이션하는 중입니다

VMware HCX-Quickstart 가이드를 사용하여 Google Cloud VMware Engine에서 NetApp Cloud Volume Service 데이터 저장소로 워크로드를 마이그레이션합니다

저자: NetApp 솔루션 엔지니어링

개요: VMware HCX, NetApp Cloud Volume Service 데이터 저장소 및 Google Cloud VMware Engine(GCVE)을 사용하여 가상 머신 마이그레이션

Google Cloud VMware Engine 및 Cloud Volume Service 데이터 저장소의 가장 일반적인 사용 사례 중 하나는 VMware 워크로드 마이그레이션입니다. VMware HCX는 선호되는 옵션이며 사내 VM(가상 머신)과 데이터를 Cloud Volume Service NFS 데이터 저장소로 이동하는 다양한 마이그레이션 메커니즘을 제공합니다.

VMware HCX는 주로 클라우드 전반에서 애플리케이션 마이그레이션, 워크로드 재조정 및 비즈니스 연속성을 간소화하도록 설계된 마이그레이션 플랫폼입니다. 이 제품은 Google Cloud VMware Engine 프라이빗 클라우드의 일부로 포함되어 있으며 워크로드를 마이그레이션할 수 있는 다양한 방법을 제공하므로 재해 복구(DR) 작업에 사용할 수 있습니다.

이 문서에서는 Cloud Volume Service 데이터 저장소를 프로비저닝하기 위한 단계별 지침을 제공하고, 온프레미스 및 Google Cloud VMware Engine 측에 있는 모든 주요 구성 요소(상호 연결, 네트워크 확장, 다양한 VM 마이그레이션 메커니즘을 지원하기 위한 WAN 최적화 포함)를 포함하여 VMware HCX를 다운로드, 구축 및 구성하는 방법을 설명합니다.

VMware HCX는 마이그레이션이 VM 레벨에 있으므로 모든 데이터 저장소 유형과 함께 작동합니다. 따라서 이 문서는 비용 효율적인 VMware 클라우드 구축을 위해 Google Cloud VMware Engine과 함께 Cloud Volume Service를 구축하려는 기존 NetApp 고객 및 타사 고객에게 적용됩니다.

높은 수준의 단계

이 목록은 HCX Connector On-Premises에서 Google Cloud VMware Engine의 HCX Cloud Manager로 VM을 페어링 및 마이그레이션하는 데 필요한 고급 단계를 제공합니다.

1. Google VMware Engine 포털을 통해 HCX를 준비합니다.
2. 사내 VMware vCenter Server에서 HCX Connector OVA(Open Virtualization Appliance) 설치 프로그램을 다운로드하여 구축합니다.
3. 라이센스 키를 사용하여 HCX를 활성화합니다.
4. 온프레미스 VMware HCX Connector를 Google Cloud VMware Engine HCX Cloud Manager와 페어링합니다.
5. 네트워크 프로파일, 컴퓨팅 프로파일 및 서비스 메시를 구성합니다.
6. (선택 사항) 마이그레이션 중에 재IP를 방지하기 위해 네트워크 확장을 수행합니다.
7. 어플라이언스 상태를 확인하고 마이그레이션이 가능한지 확인합니다.
8. VM 워크로드를 마이그레이션합니다.

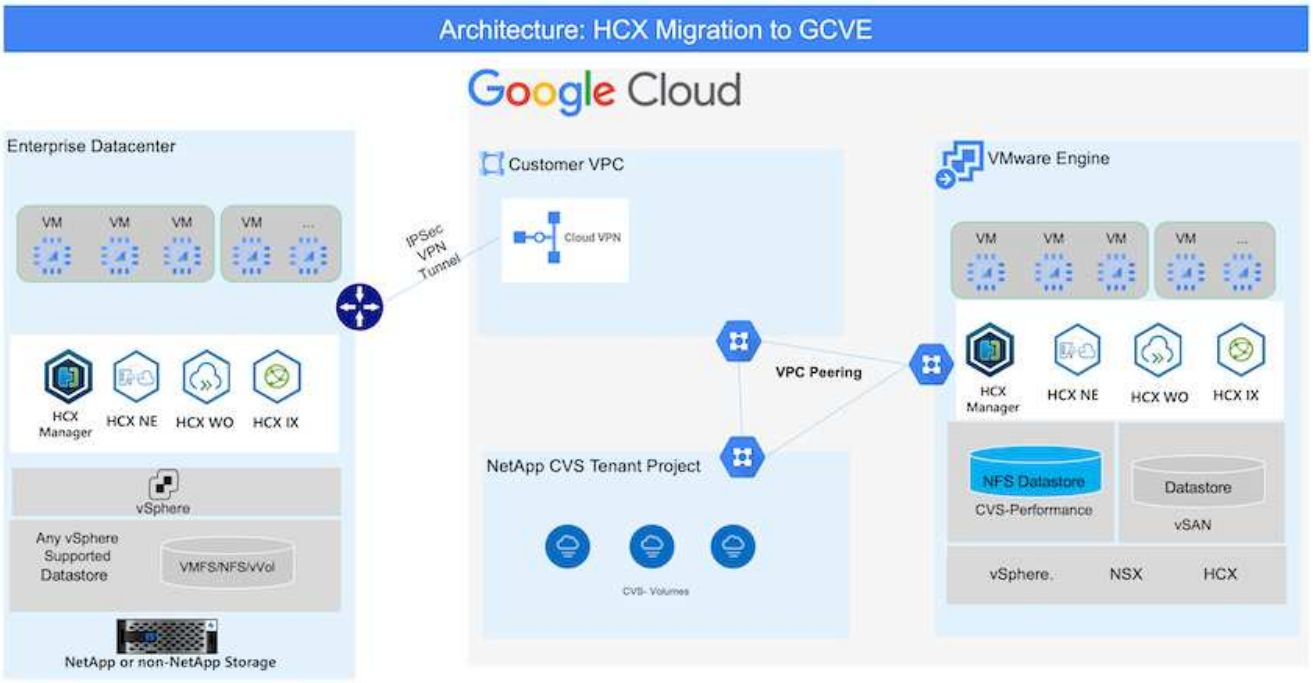
시작하기 전에 다음 필수 구성 요소가 충족되었는지 확인하십시오. 자세한 내용은 다음을 참조하십시오 "링크". 연결을 포함한 필수 구성 요소가 구축된 후에는 Google Cloud VMware Engine 포털에서 HCX 라이센스 키를 다운로드하십시오. OVA 설치 프로그램을 다운로드한 후 아래 설명된 대로 설치 프로세스를 진행합니다.

HCX Advanced가 기본 옵션이며 VMware HCX Enterprise Edition도 지원 티켓을 통해 제공되며 추가 비용 없이 지원됩니다. 을 참조하십시오 "이 링크"

- 기존 Google Cloud VMware Engine SDDC(소프트웨어 정의 데이터 센터)를 사용하거나 이를 사용하여 프라이빗 클라우드를 생성합니다 "NetApp 링크" 또는 이 "Google 링크".
- 사내 VMware vSphere 지원 데이터 센터에서 VM 및 관련 데이터를 마이그레이션하려면 데이터 센터에서 SDDC 환경으로 네트워크를 연결해야 합니다. 워크로드를 마이그레이션하기 전에 "Cloud VPN 또는 Cloud Interconnect 연결을 설정합니다" 데이터 관리 및 보호
- 사내 VMware vCenter Server 환경에서 Google Cloud로 연결되는 네트워크 경로 VMware Engine 프라이빗 클라우드는 vMotion을 사용하여 VM 마이그레이션을 지원해야 합니다.
- 필수 를 확인하십시오 "방화벽 규칙 및 포트" 온-프레미스 vCenter Server와 SDDC vCenter 간에 vMotion 트래픽이 허용됩니다.
- Cloud Volume Service NFS 볼륨은 Google Cloud VMware Engine에서 데이터 저장소로 마운트되어야 합니다. 이에 설명된 단계를 따릅니다 "링크" Google Cloud VMware Engine 호스트에 Cloud Volume Service 데이터 저장소를 연결하려면 다음을 수행합니다.

고급 아키텍처

테스트 목적으로, 이 검증에 사용된 온프레미스 연구소 환경이 Cloud VPN을 통해 연결되어 Google Cloud VPC에 사내 연결을 가능하게 했습니다.



HCX에 대한 자세한 다이어그램은 을 참조하십시오 "VMware 링크"

솔루션 구축

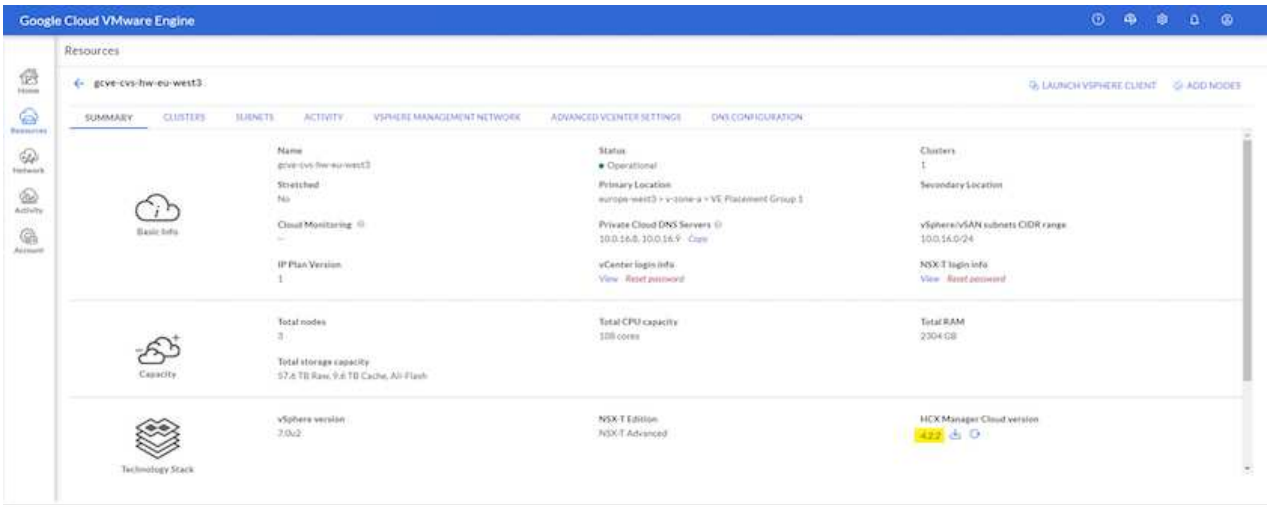
이 솔루션의 배포를 완료하려면 다음 단계를 따르십시오.

1단계**: Google VMware Engine Portal**을 통해 **HCX**를 준비합니다

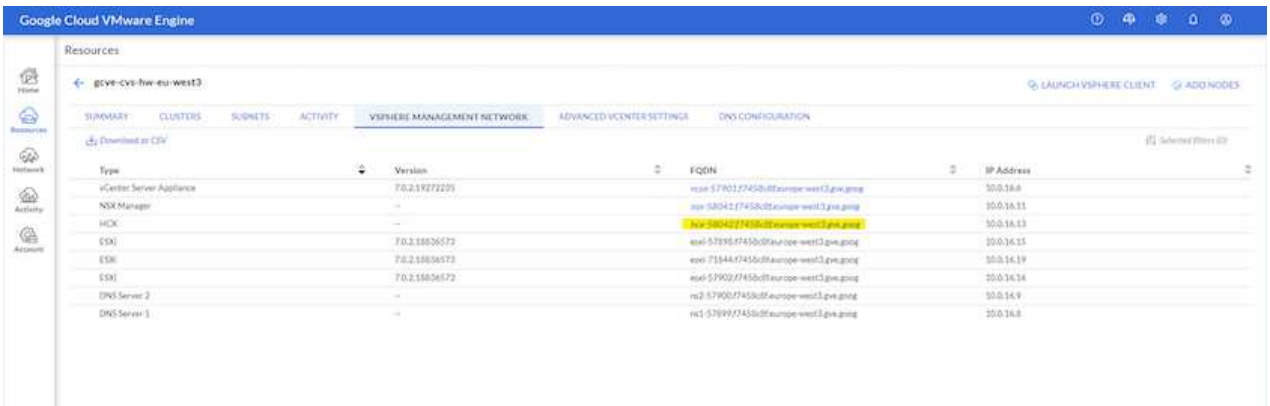
VMware Engine을 사용하여 프라이빗 클라우드를 프로비저닝할 때 HCX Cloud Manager 구성 요소가 자동으로 설치됩니다. 사이트 페어링을 준비하려면 다음 단계를 완료하십시오.

1. Google VMware Engine Portal에 로그인하고 HCX Cloud Manager에 로그인합니다.

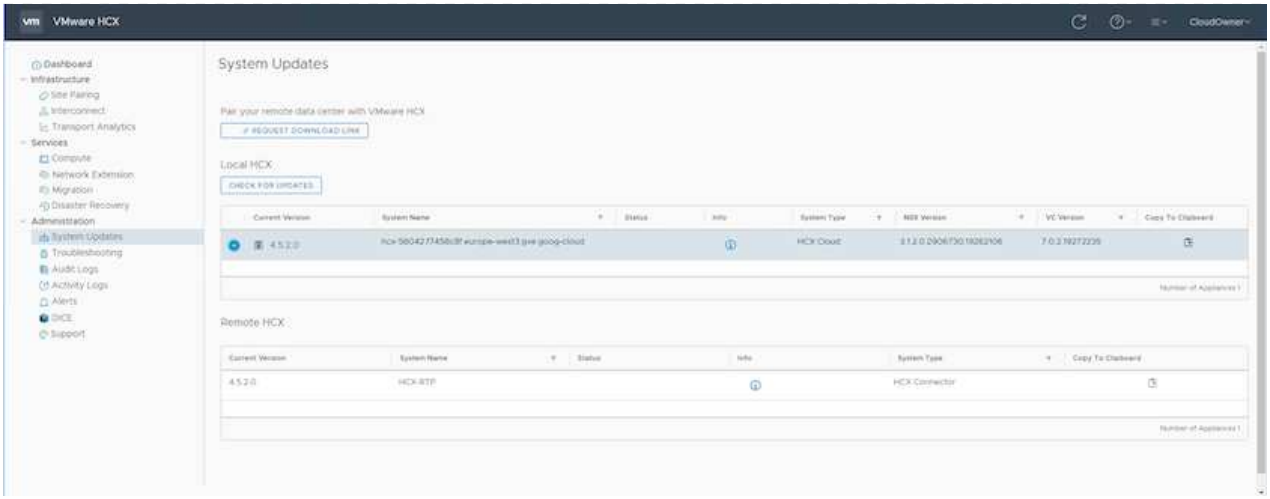
   HCX 버전 링크를 클릭하여 HCX 콘솔에 로그인할 수 있습니다



   또는 vSphere Management Network 탭에서 HCX FQDN을 클릭합니다
   .



2. HCX Cloud Manager에서 * 관리 > 시스템 업데이트 * 로 이동합니다.
3. 다운로드 요청 링크 * 를 클릭하고 OVA 파일을 다운로드합니다
   .



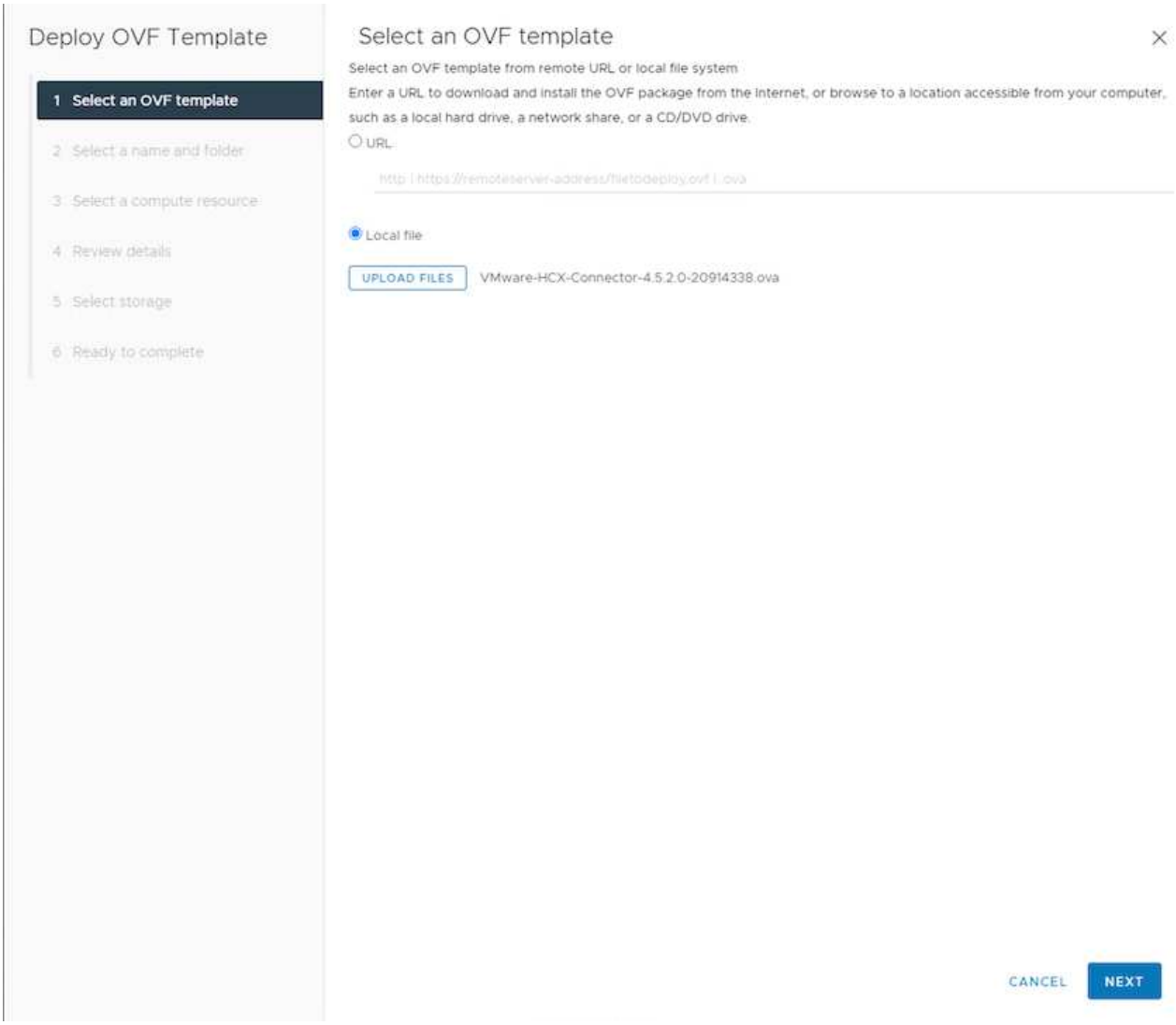
4. HCX Cloud Manager를 HCX Cloud Manager UI에서 사용 가능한 최신 버전으로 업데이트합니다.

2단계**:** 온**-**프레미스 **vCenter Server**에 설치 관리자 **OVA**를 구축합니다

온프레미스 커넥터가 Google Cloud VMware Engine의 HCX Manager에 연결하려면 적절한 방화벽 포트가 사내 환경에서 열려 있는지 확인합니다.

온-프레미스 vCenter Server에서 HCX Connector를 다운로드하여 설치하려면 다음 단계를 수행하십시오.

1. 이전 단계에서 설명한 대로 Google Cloud VMware Engine의 HCX 콘솔에서 OVA를 다운로드하도록 합니다.
2. OVA를 다운로드한 후 * Deploy OVF Template * 옵션을 사용하여 온프레미스 VMware vSphere 환경에 구축합니다.



3. OVA 배포에 필요한 모든 정보를 입력하고 * Next * 를 클릭한 다음 * Finish * 를 클릭하여 VMware HCX 커넥터 OVA를 배포합니다.

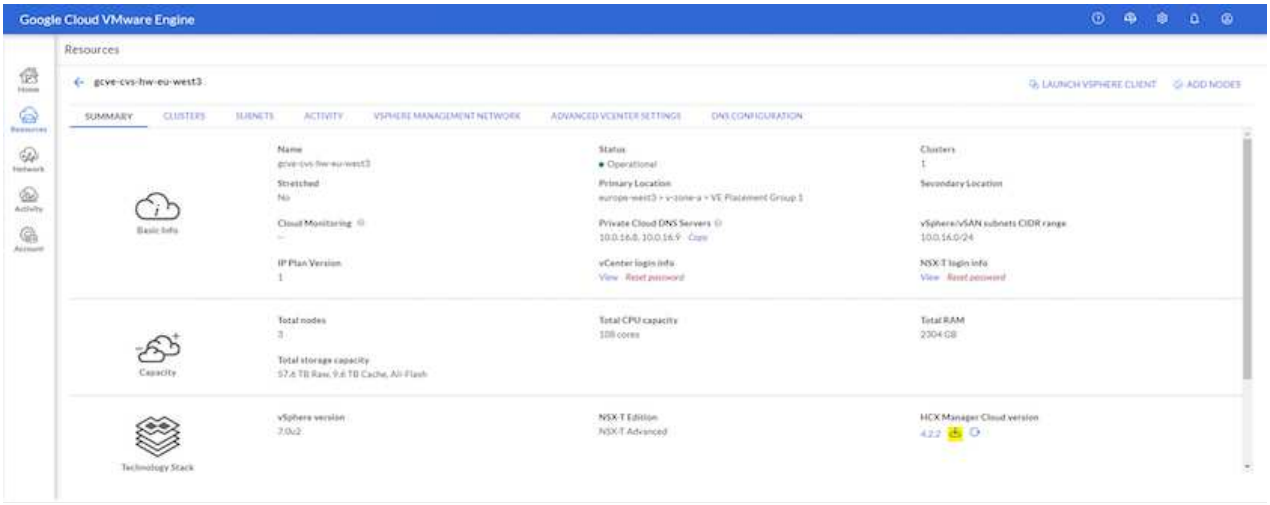
가상 어플라이언스의 전원을 수동으로 켭니다.

단계별 지침은 를 참조하십시오 "VMware HCX 사용자 가이드".

3단계**:** 라이센스 키로 **HCX** 커넥터를 활성화합니다

VMware HCX 커넥터 OVA를 온-프레미스로 배포하고 어플라이언스를 시작한 후 다음 단계를 수행하여 HCX 커넥터를 활성화하십시오. Google Cloud VMware Engine 포털에서 라이센스 키를 생성하고 VMware HCX Manager에서 활성화합니다.

1. VMware Engine 포털에서 리소스를 클릭하고 프라이빗 클라우드를 선택한 다음 * HCX Manager Cloud Version * 에서 다운로드 아이콘을 클릭합니다
.



다운로드한 파일을 열고 라이센스 키 문자열을 복사합니다.

2. 사내 VMware HCX Manager()에 로그인합니다 "https://hcxmanagerIP:9443" 관리자 자격 증명을 사용합니다.

   OVA 배포 중에 정의된 hcxmanageIP 및 암호를 사용합니다.

3. 라이센스에서 3단계에서 복사한 키를 입력하고 * Activate * 를 클릭합니다.

   온프레미스 HCX 커넥터는 인터넷에 연결되어 있어야 합니다.

4. 데이터 센터 위치 * 에서 VMware HCX Manager를 사내에 설치할 수 있는 가장 가까운 위치를 제공합니다. 계속 * 을 클릭합니다.
5. 시스템 이름 * 에서 이름을 업데이트하고 * 계속 * 을 클릭합니다.
6. 예, 계속 * 을 클릭합니다.
7. vCenter * 연결 아래에서 vCenter Server의 FQDN(정규화된 도메인 이름) 또는 IP 주소와 해당 자격 증명을 입력하고 * 계속 * 을 클릭합니다.

   나중에 연결 문제를 방지하려면 FQDN을 사용합니다.

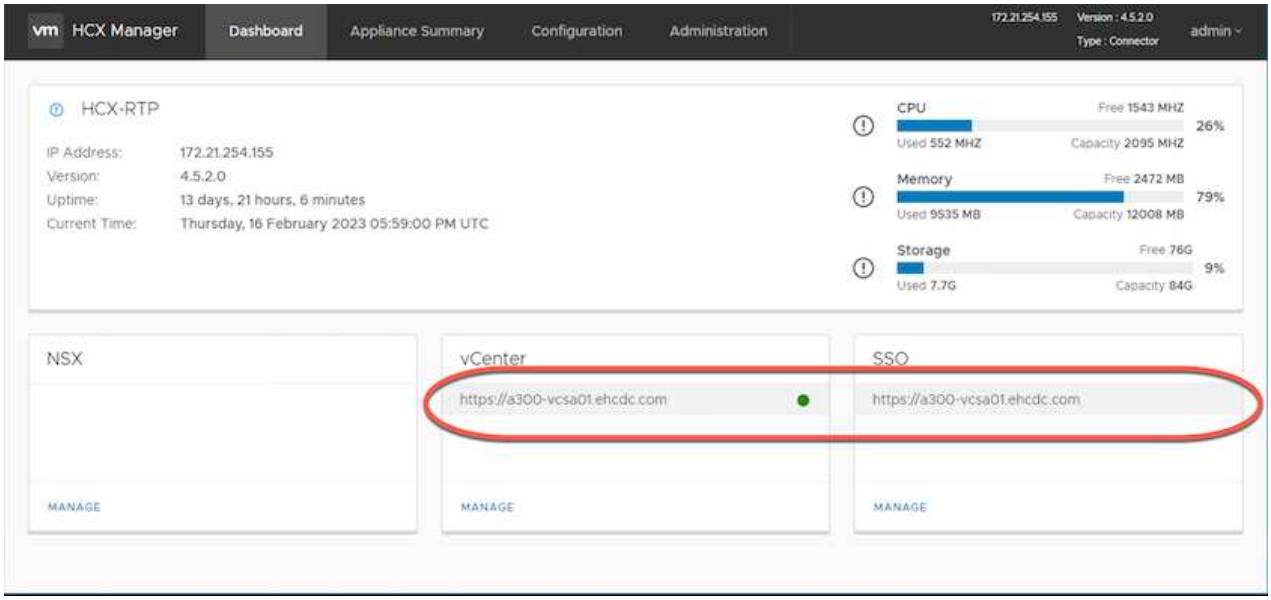
8. SSO/PSC * 구성 아래에서 플랫폼 서비스 컨트롤러(PSC) FQDN 또는 IP 주소를 제공하고 * 계속 * 을 클릭합니다.

   Embedded PSC의 경우 VMware vCenter Server FQDN 또는 IP 주소를 입력합니다.

9. 입력한 정보가 올바른지 확인하고 * Restart * (재시작 *)를 클릭합니다.

10. 서비스를 다시 시작하면 표시되는 페이지에 vCenter Server가 녹색으로 표시됩니다. vCenter Server와 SSO 모두 적절한 구성 매개 변수를 가져야 하며, 이는 이전 페이지와 동일해야 합니다.

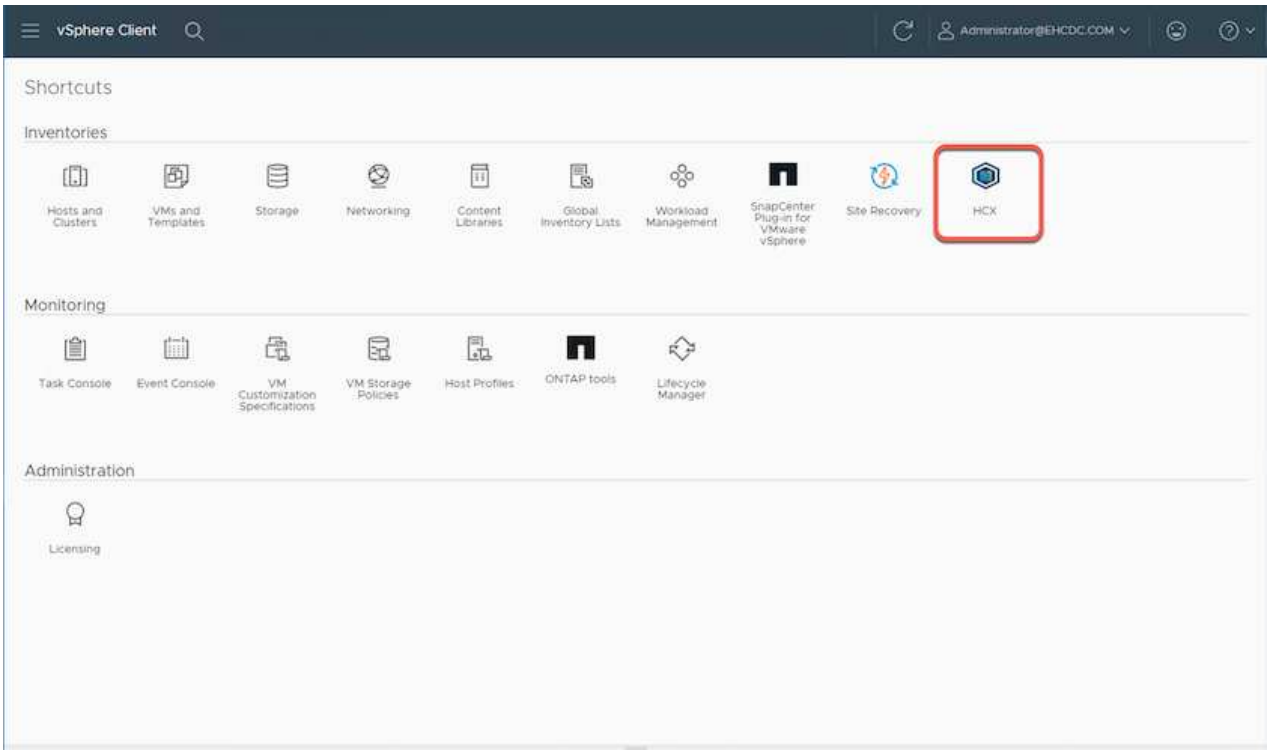
   이 프로세스는 약 10~20분 정도 소요되며 플러그인이 vCenter Server에 추가되어야 합니다.



4단계: 온프레미스 **VMware HCX Connector**를 **Google Cloud VMware Engine HCX Cloud Manager**와 페어링합니다

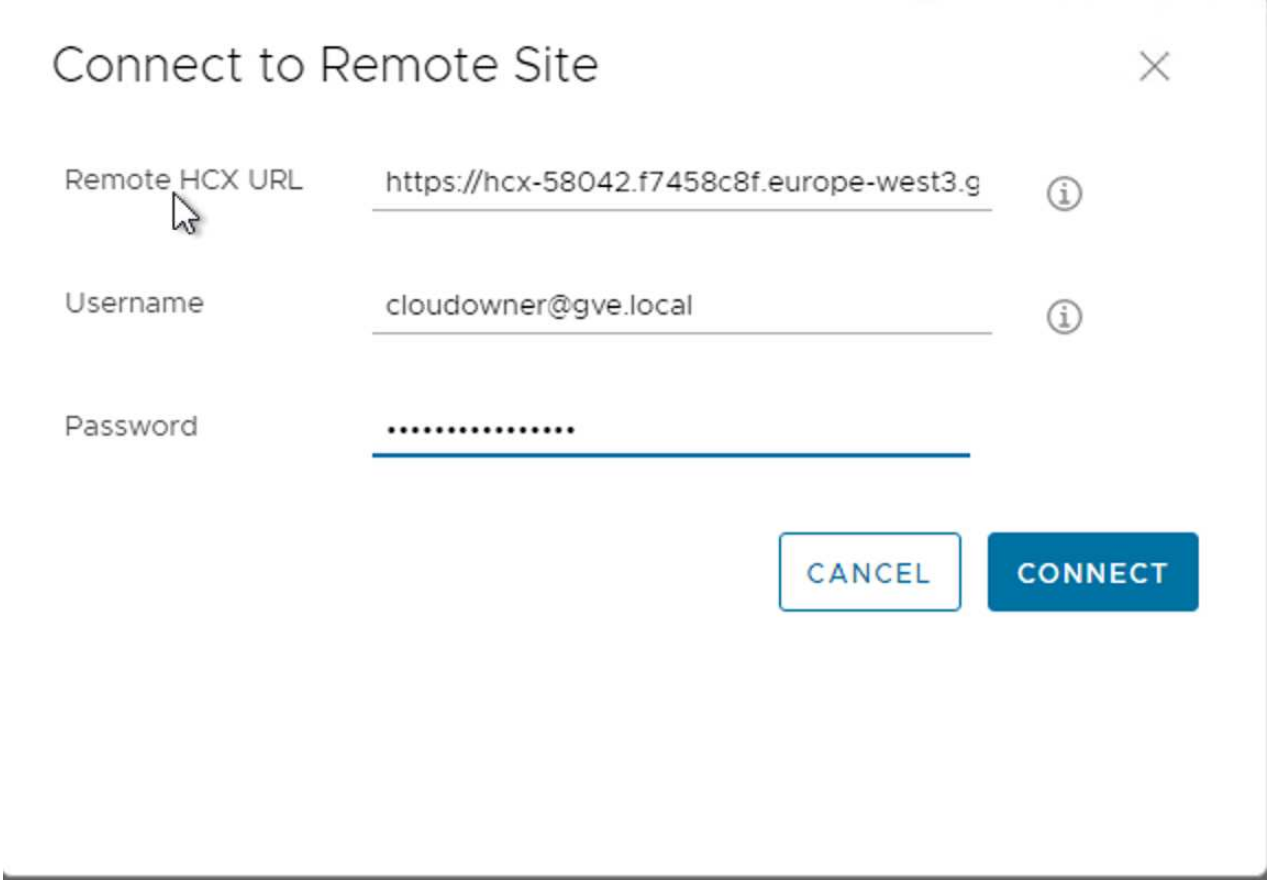
HCX Connector를 사내 vCenter에 구축 및 구성한 후 페어링을 추가하여 Cloud Manager에 연결합니다. 사이트 페어링을 구성하려면 다음 단계를 수행하십시오.

1. 온-프레미스 vCenter 환경과 Google Cloud VMware Engine SDDC 간에 사이트 쌍을 생성하려면 온-프레미스 vCenter Server에 로그인하고 새 HCX vSphere Web Client 플러그인에 액세스합니다.



2. 인프라 에서 * 사이트 페어링 추가 * 를 클릭합니다.

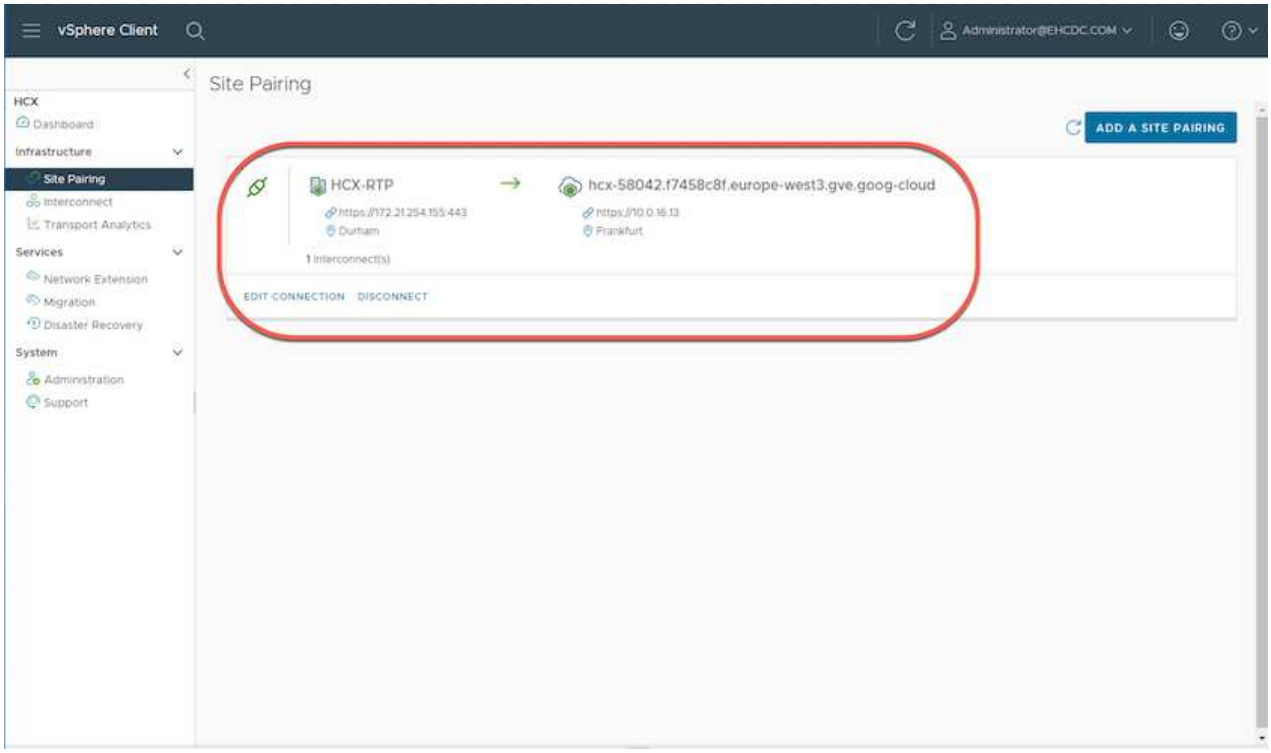
Google Cloud VMware Engine HCX Cloud Manager URL 또는 IP 주소와 Cloud-Owner-Role 권한이 있는 사용자의 자격 증명을 입력하여 프라이빗 클라우드에 액세스합니다.



3. 연결 * 을 클릭합니다.

VMware HCX Connector는 포트 443을 통해 HCX Cloud Manager IP로 라우팅할 수 있어야 합니다.

4. 페어링이 생성된 후에는 새로 구성된 사이트 페어링을 HCX 대시보드에서 사용할 수 있습니다.

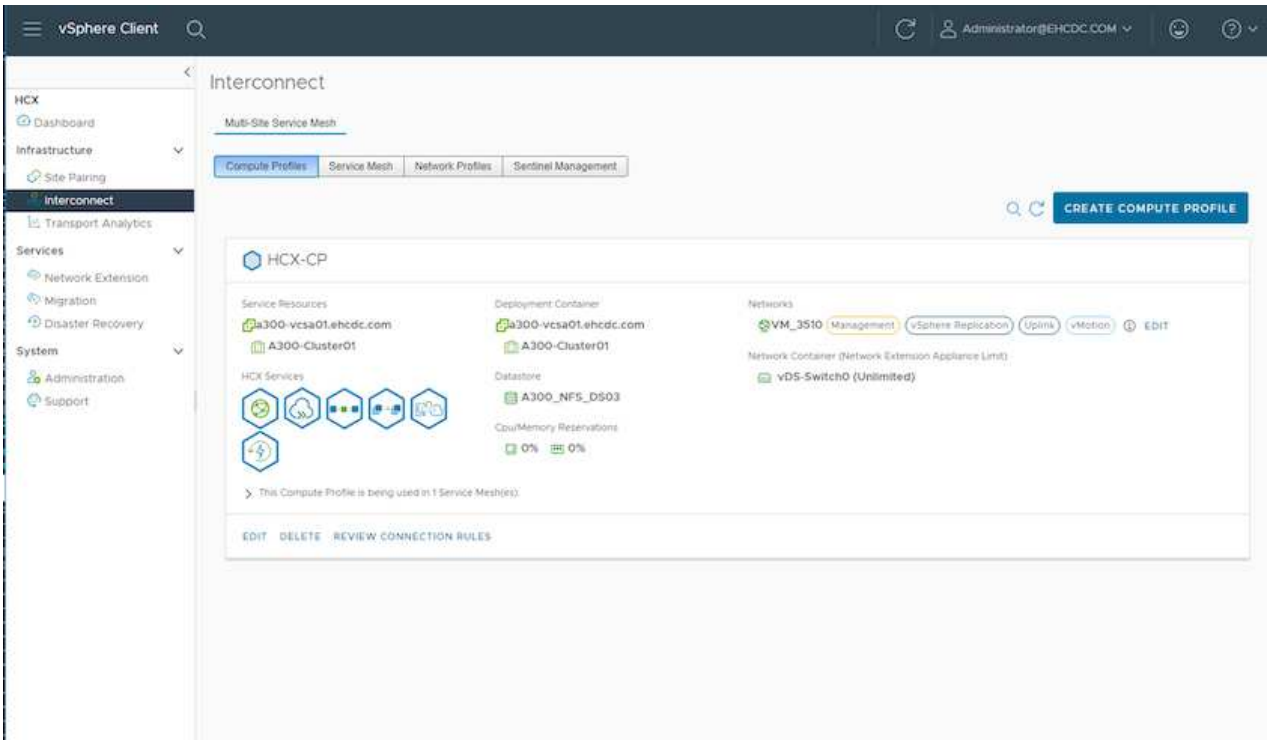

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud
https://10.0.16.13
Frankfurt
1 Interconnect(s)
EDIT CONNECTION
DISCONNECT

5단계**:** 네트워크 프로파일**,** 컴퓨팅 프로파일 및 서비스 메시를 구성합니다

VMware HCX Interconnect 서비스 어플라이언스는 인터넷을 통해 복제 및 vMotion 기반 마이그레이션 기능과 타겟 사이트에 대한 프라이빗 연결을 제공합니다. 상호 연결은 암호화, 트래픽 엔지니어링 및 VM 이동성을 제공합니다. 상호 연결 서비스 어플라이언스를 생성하려면 다음 단계를 수행하십시오.

1. 인프라 아래에서 * 상호 연결 > 멀티 사이트 서비스 메시 > 컴퓨팅 프로파일 > 컴퓨팅 프로파일 생성 * 을 선택합니다.

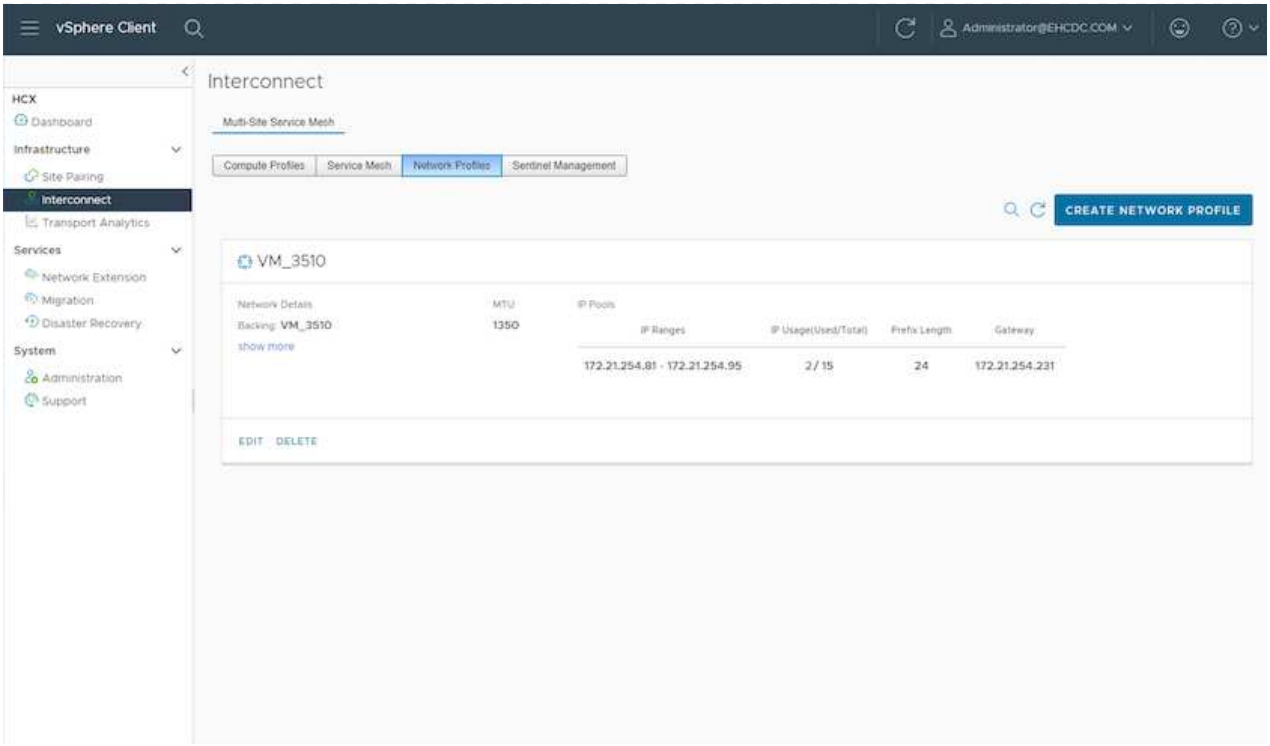
   컴퓨팅 프로필은 구축된 어플라이언스와 HCX 서비스에서 액세스할 수 있는 VMware 데이터 센터 부분을 포함하여 구축 매개 변수를 정의합니다.



2. 컴퓨팅 프로파일을 만든 후 * 다중 사이트 서비스 메시 > 네트워크 프로파일 > 네트워크 프로파일 만들기 * 를 선택하여 네트워크 프로파일을 만듭니다.

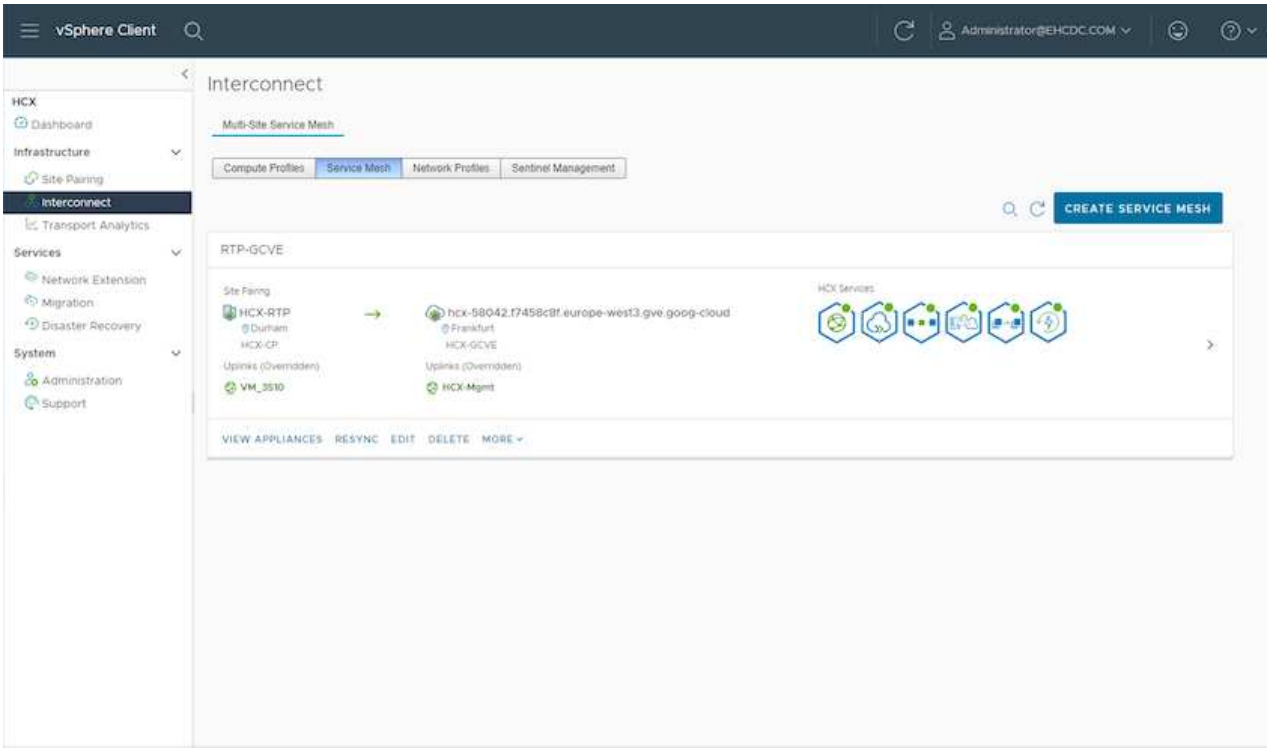
   네트워크 프로파일은 HCX가 가상 어플라이언스에 사용하는 IP 주소 및 네트워크의 범위를 정의합니다.

   이 단계에서는 두 개 이상의 IP 주소가 필요합니다. 이러한 IP 주소는 관리 네트워크에서 상호 연결 어플라이언스로 할당됩니다.

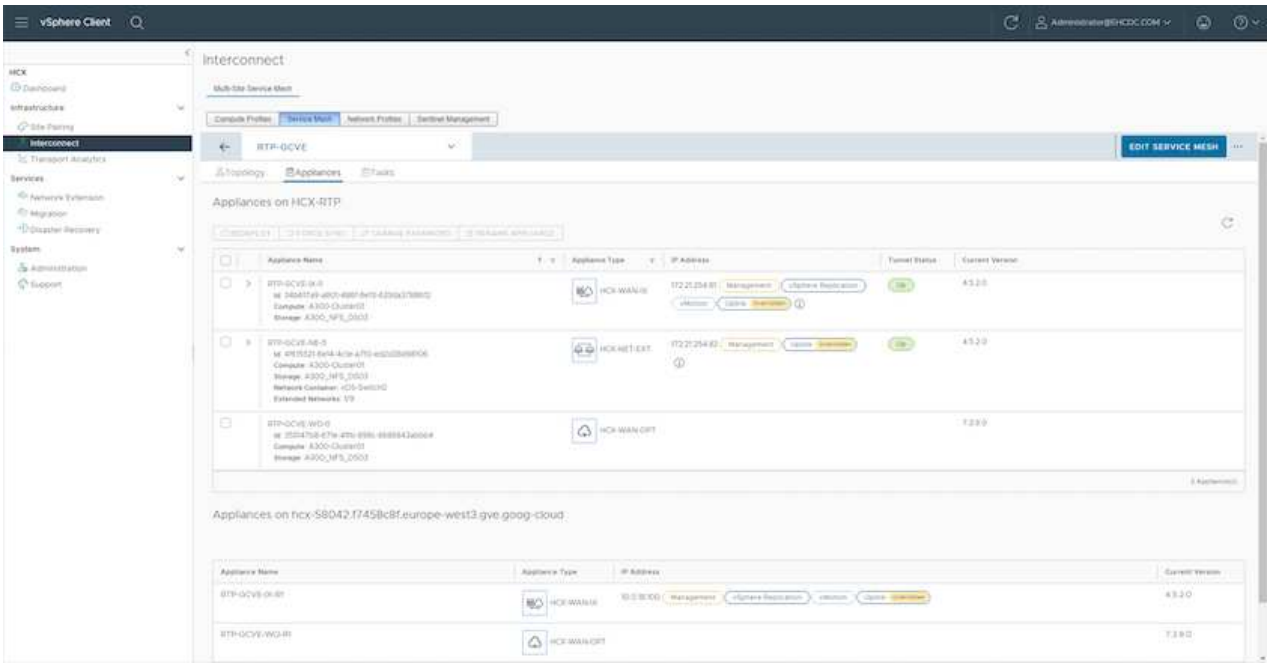


3. 현재 컴퓨팅 및 네트워크 프로파일이 성공적으로 생성되었습니다.
4. 상호 연결 * 옵션 내에서 * 서비스 메시 * 탭을 선택하고 온-프레미스 및 GCVE SDDC 사이트를 선택하여 서비스 메시를 생성합니다.
5. 서비스 메시는 로컬 및 원격 계산 및 네트워크 프로파일 쌍을 지정합니다.

이 프로세스의 일환으로 안전한 전송 패브릭을 생성하기 위해 소스 사이트와 타겟 사이트 모두에 HCX 어플라이언스를 구축하고 자동으로 구성합니다.



6. 이 단계는 구성의 마지막 단계입니다. 구축을 완료하는 데 약 30분이 소요됩니다. 서비스 메시가 구성된 후 작업 부하 VM을 마이그레이션하도록 IPsec 터널이 성공적으로 생성된 환경이 준비됩니다.



6단계**:** 워크로드 마이그레이션

다양한 VMware HCX 마이그레이션 기술을 사용하여 온프레미스 및 GCVE SDDC 간에 워크로드를 양방향으로 마이그레이션할 수 있습니다. VM은 HCX 대량 마이그레이션, HCX vMotion, HCX 콜드 마이그레이션, HCX Replication Assisted vMotion(HCX Enterprise Edition에서 사용 가능) 및 HCX OS 지원 마이그레이션(HCX Enterprise Edition에서 사용 가능)과 같은 여러 마이그레이션 기술을 사용하여 VMware HCX 활성 엔터티로 또는 VMware에서 이동할 수 있습니다.

다양한 HCX 마이그레이션 메커니즘에 대한 자세한 내용은 을 참조하십시오 "VMware HCX 마이그레이션 유형".

HCX-IX 어플라이언스는 Mobility Agent 서비스를 사용하여 vMotion, Cold 및 RAV(Replication Assisted vMotion) 마이그레이션을 수행합니다.

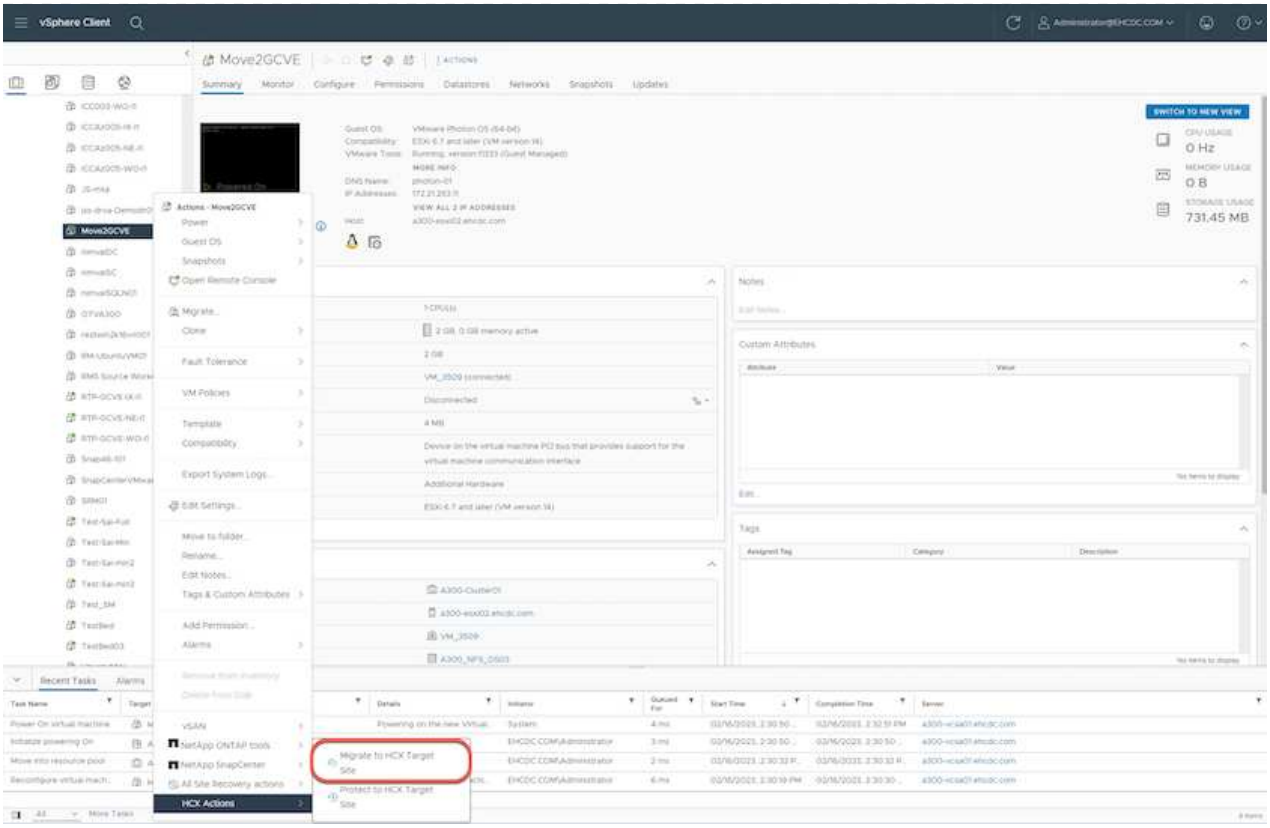
HCX-IX 어플라이언스는 vCenter Server에서 Mobility Agent 서비스를 호스트 개체로 추가합니다. 이 개체에 표시되는 프로세서, 메모리, 스토리지 및 네트워킹 리소스는 IX 어플라이언스를 호스팅하는 물리적 하이퍼바이저의 실제 소비량을 나타내지 않습니다.

- HCX vMotion *

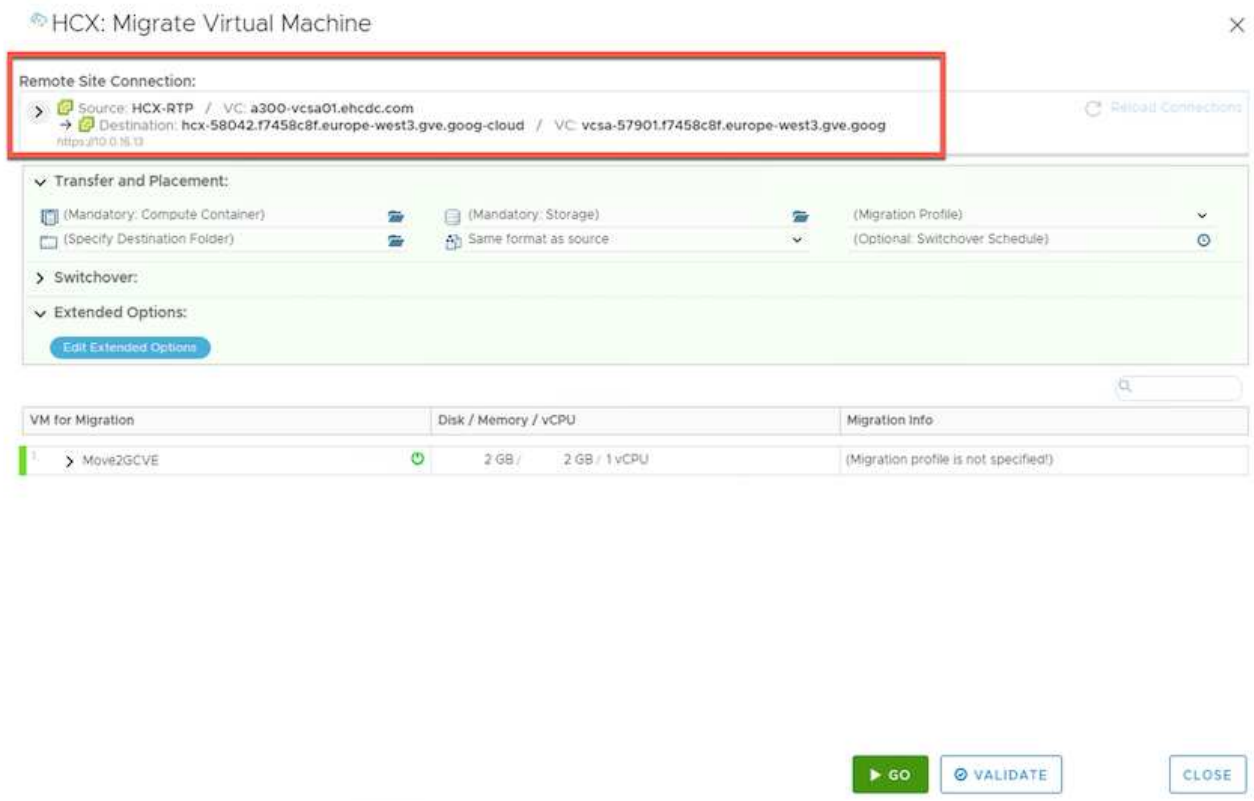
이 섹션에서는 HCX vMotion 메커니즘을 설명합니다. 이 마이그레이션 기술은 VMware vMotion 프로토콜을 사용하여 VM을 GCVE로 마이그레이션합니다. vMotion 마이그레이션 옵션은 한 번에 하나의 VM의 VM 상태를 마이그레이션하는 데 사용됩니다. 이 마이그레이션 방법 중에는 서비스가 중단되지 않습니다.

IP 주소를 변경할 필요 없이 VM을 마이그레이션하려면 네트워크 확장이 있어야 합니다(VM이 연결된 포트 그룹의 경우).

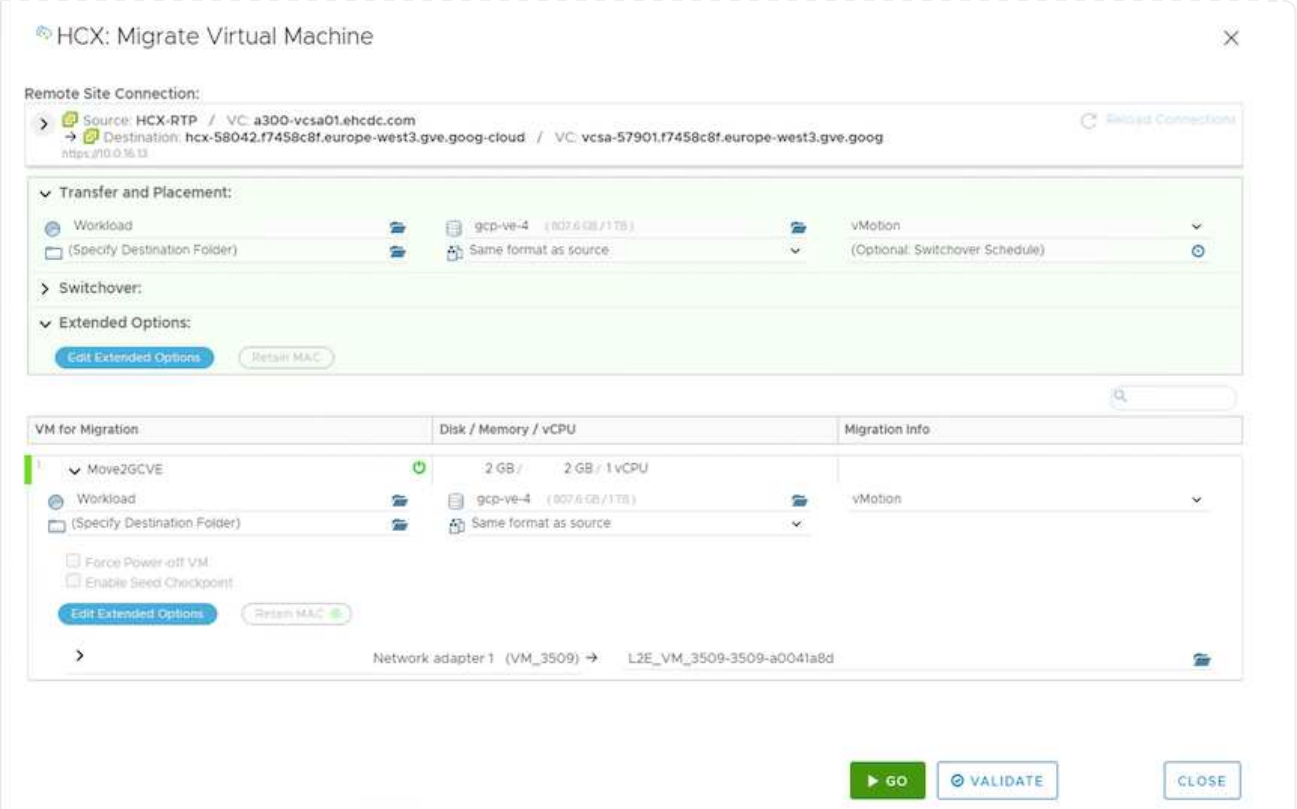
1. 온-프레미스 vSphere Client에서 Inventory로 이동하여 마이그레이션할 VM을 마우스 오른쪽 버튼으로 클릭하고 HCX Actions > Migrate to HCX Target Site를 선택합니다.



2. 가상 컴퓨터 마이그레이션 마법사에서 원격 사이트 연결(대상 GCVE)을 선택합니다.



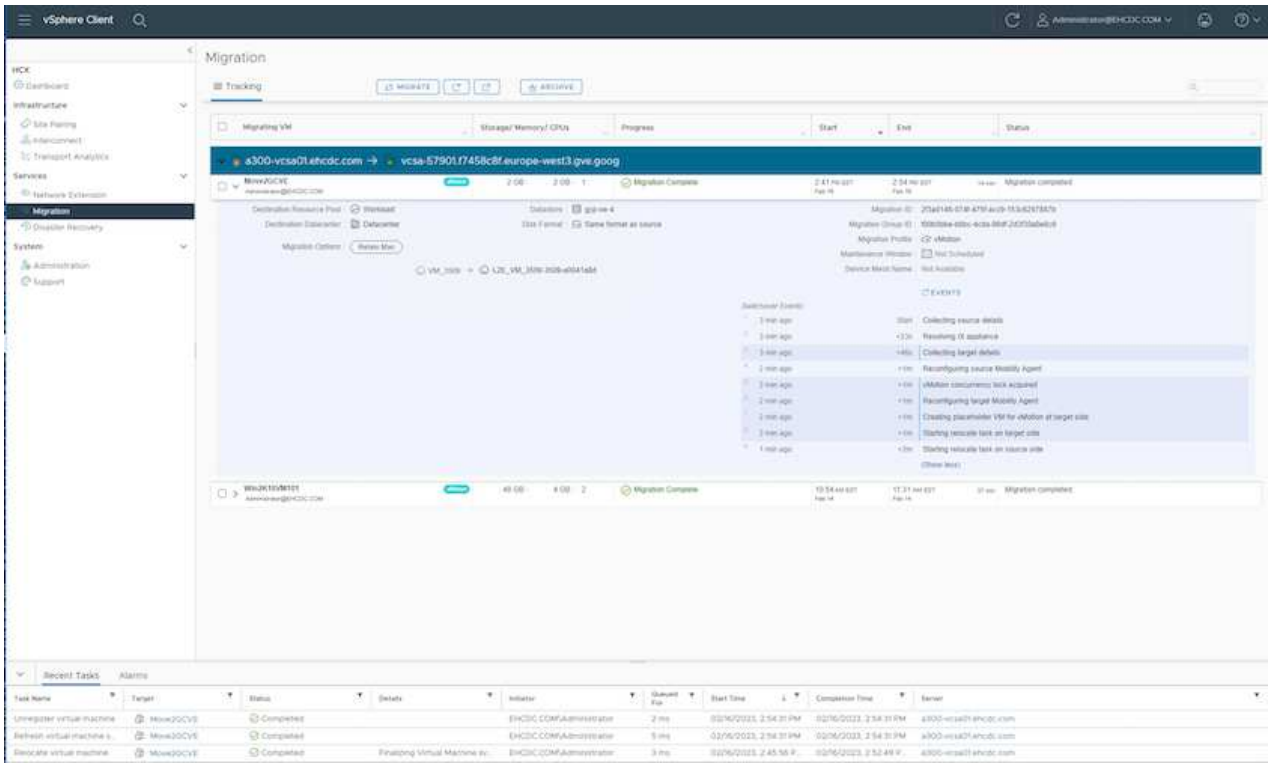
3. 필수 필드(클러스터, 스토리지 및 대상 네트워크)를 업데이트하고 검증 을 클릭합니다.



4. 유효성 검사가 완료된 후 이동을 클릭하여 마이그레이션을 시작합니다.

> vMotion 전송은 VM 활성 메모리, 실행 상태, IP 주소 및 MAC 주소를 캡처합니다. HCX vMotion의 요구 사항 및 제한 사항에 대한 자세한 내용은 을 참조하십시오 "VMware HCX vMotion 및 콜드 마이그레이션 이해".

5. HCX > 마이그레이션 대시보드에서 vMotion의 진행 상황과 완료 상태를 모니터링할 수 있습니다.



타겟 CVS NFS 데이터 저장소에 마이그레이션을 처리할 충분한 공간이 있어야 합니다.

결론

클라우드 볼륨 서비스 및 HCX는 온프레미스(On-Premises)의 모든 유형/공급업체 스토리지에 있는 모든 클라우드 또는 하이브리드 클라우드 및 데이터를 대상으로 하는 모든 환경에서 애플리케이션 워크로드를 배포 및 마이그레이션하는 동시에 데이터 요구 사항을 애플리케이션 계층으로 원활하게 만들어 TCO를 절감하는 탁월한 옵션을 제공합니다. 어떤 사용 사례에서든 Cloud Volume Service와 함께 Google Cloud VMware Engine을 사용하면 사내 및 멀티 클라우드 전체의 클라우드 이점, 일관된 인프라 및 운영을 신속하게 실현하고, 워크로드의 양방향 이동성을 제공하며, 엔터프라이즈급 용량과 성능을 실현할 수 있습니다. VMware vSphere Replication, VMware vMotion 또는 NFC(네트워크 파일 복사)를 사용하여 스토리지를 연결하고 VM을 마이그레이션하는 데 사용되는 익숙한 프로세스와 절차가 동일합니다.

이점

이 문서의 핵심 사항은 다음과 같습니다.

- 이제 Cloud Volume Service를 Google Cloud VMware Engine SDDC에서 데이터 저장소로 사용할 수 있습니다.
- 온프레미스에서 Cloud Volume Service 데이터 저장소로 데이터를 쉽게 마이그레이션할 수 있습니다.
- 마이그레이션 작업 중에 용량 및 성능 요구사항을 충족하기 위해 Cloud Volume Service 데이터 저장소를 쉽게 확장 및 축소할 수 있습니다.

Google 및 **VMware**의 비디오를 참조하십시오

Google에서

- "GCVE를 사용하여 HCX Connector를 배포합니다"
- "GCVE로 HCX ServiceMesh를 구성합니다"
- "HCX를 사용하는 VM을 GCVE로 마이그레이션합니다"

수 있습니다

- "GCVE에 대한 HCX Connector 배포"
- "GCVE에 대한 HCX ServiceMesh 구성"
- "GCVE로 HCX 워크로드 마이그레이션"

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 웹 사이트 링크를 참조하십시오.

- Google Cloud VMware Engine 설명서

  "https://cloud.google.com/vmware-engine/docs/overview"

- Cloud Volume Service 설명서

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes"

- VMware HCX 사용자 가이드

  "https://docs.vmware.com/en/VMware-HCX/index.html"

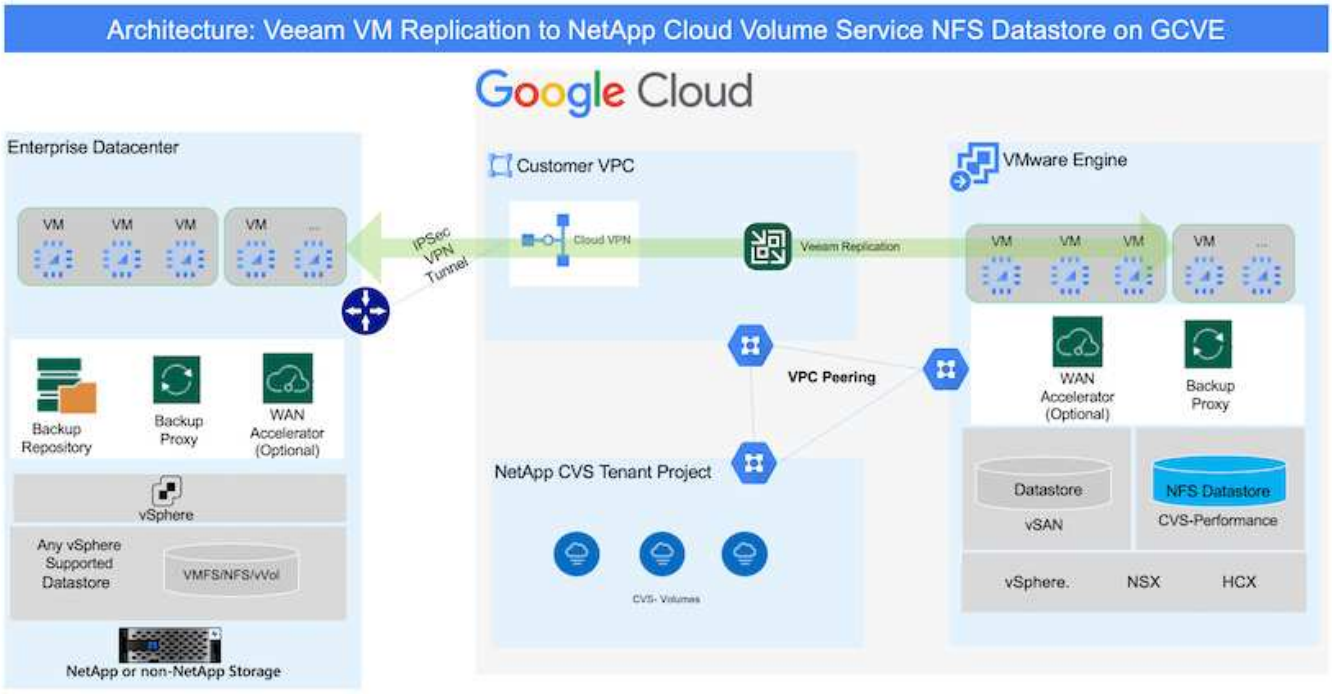
Veeam 복제 기능을 사용하여 **Google Cloud VMware Engine**에서 **NetApp Cloud Volume Service NFS** 데이터 저장소로 **VM** 마이그레이션

개요

저자: NetApp Suesh Thoppay

VMware vSphere에서 실행되는 VM 워크로드는 Veeam Replication 기능을 활용하여 Google Cloud VMware Engine(GCVE)으로 마이그레이션할 수 있습니다.

이 문서에서는 NetApp Cloud Volume Service, Veeam 및 Google Cloud VMware Engine(GCVE)을 사용하는 VM 마이그레이션을 설정하고 수행하기 위한 단계별 접근 방식을 제공합니다.



가정

이 문서에서는 기존 vSphere 서버에서 Google Cloud VMware Engine으로의 네트워크 연결을 설정할 수 있는 Google Cloud VPN 또는 Cloud Interconnect 또는 기타 네트워킹 옵션이 있다고 가정합니다.

온프레미스 데이터 센터를 Google Cloud에 연결하는 옵션에는 여러 가지가 있으며, 이로 인해 NetApp에서 이 문서의 특정 워크플로우를 개괄적으로 설명하지 못하게 됩니다.
을 참조하십시오 "Google Cloud 설명서" 을 참조하십시오.

마이그레이션 솔루션 배포

솔루션 구축 개요

1. NetApp 클라우드 볼륨 서비스의 NFS 데이터 저장소가 GCVE vCenter에 마운트되어 있는지 확인합니다.
2. Veeam Backup Recovery를 기존 VMware vSphere 환경에 구축했는지 확인합니다
3. 복제 작업을 생성하여 가상 시스템을 Google Cloud VMware Engine 인스턴스로 복제를 시작합니다.
4. Veeam 복제 작업의 페일오버를 수행합니다.
5. Veeam에서 영구 페일오버를 수행합니다.

배포 세부 정보

NetApp 클라우드 볼륨 서비스의 **NFS** 데이터 저장소가 **GCVE vCenter**에 마운트되어 있는지 확인합니다

GCVE vCenter에 로그인하고 공간이 충분한 NFS 데이터 저장소를 사용할 수 있는지 확인합니다.
그렇지 않은 경우 을 참조하십시오 "GCVE에서 NetApp CVS를 NFS 데이터 저장소로 마운트합니다"

Veeam Backup Recovery를 기존 **VMware vSphere** 환경에 구축했는지 확인합니다

을 참조하십시오 "Veeam 복제 구성 요소" 필요한 구성 요소 설치 설명서

복제 작업을 생성하여 가상 시스템을 **Google Cloud VMware Engine** 인스턴스로 복제를 시작합니다**.**

사내 vCenter와 GCVE vCenter를 모두 Veeam에 등록해야 합니다. "vSphere VM 복제 작업을 설정합니다"
다음은 방법을 설명하는 비디오입니다
"복제 작업을 구성합니다".

> 복제 VM은 소스 VM과 다른 IP를 가질 수 있으며 다른 포트 그룹에 연결할 수도 있습니다. 자세한 내용은 위의 동영상을 확인하십시오.

Veeam 복제 작업의 페일오버를 수행합니다

VM을 마이그레이션하려면 를 수행합니다 "페일오버를 수행합니다"

Veeam에서 영구 페일오버를 수행합니다**.**

GCVE를 새 소스 환경으로 처리하려면 를 수행합니다 "영구 페일오버"

이 솔루션의 이점

- 기존 Veeam 백업 인프라를 마이그레이션에 활용할 수 있습니다.
- Veeam Replication을 사용하면 타겟 사이트에서 VM IP 주소를 변경할 수 있습니다.
- Veeam 외부에서 복제된 기존 데이터를 재매핑할 수 있습니다(예: BlueXP의 복제된 데이터).
- 대상 사이트에 다른 네트워크 포트 그룹을 지정할 수 있습니다.
- VM의 전원 켜기 순서를 지정할 수 있습니다.
- VMware Change Block Tracking을 활용하여 WAN을 통해 전송할 데이터 양을 최소화합니다.
- 복제를 위해 사전/사후 스크립트를 실행할 수 있는 기능
- 스냅샷에 대한 사전/사후 스크립트를 실행할 수 있습니다.

지역 가용성 **– Google Cloud Platform(GCP)**용 보조 **NFS** 데이터 저장소

GCVE용 보조 NFS 데이터 저장소는 NetApp 클라우드 볼륨 서비스에서 지원됩니다.

> CVS 전용 - GCVE NFS 데이터 저장소에는 성능 볼륨을 사용할 수 있습니다.
> 사용 가능한 위치는 을 참조하십시오 "글로벌 지역 지도"

Google Cloud VMware Engine은 다음 위치에서 사용할 수 있습니다

지연 시간을 최소화하려면 볼륨을 마운트하려는 NetApp CVS 볼륨 및 GCVE가 동일한 가용성 영역에 있어야 합니다.
Google 및 NetApp 솔루션 설계자와 협력하여 가용성 및 TCO 최적화

보안 개요 - Google Cloud의 NetApp CVS(Cloud Volumes Service

TR-4918: 보안 개요 **- Google Cloud**의 **NetApp Cloud Volumes Service**

Oliver Krause, Justin Parisi, NetApp

문서 범위

특히, 인프라가 스토리지 관리자의 제어 범위를 벗어난 클라우드의 경우 보안은 데이터를 클라우드 공급자가 제공하는 서비스 제공에 맡기는 것이 무엇보다 중요합니다. 이 문서는 NetApp의 보안 제품에 대한 개요입니다 "Cloud Volumes Service는 Google Cloud에서 제공합니다".

대상

이 문서의 대상 고객은 다음과 같은 역할을 포함하지만 이에 국한되지 않습니다.

- 설명합니다
- 스토리지 관리자
- 스토리지 설계자
- 현장 리소스
- 비즈니스 의사 결정자

이 기술 보고서의 내용에 대해 궁금한 점이 있으면 섹션을 참조하십시오 ""문의하기""

약어	정의
CVS-SW	Cloud Volumes Service, 서비스 유형 CVS
CVS - 성능	클라우드 볼륨 서비스, 서비스 유형 CVS - 성능
PSA	

Google Cloud의 **Cloud Volumes Service**로 데이터를 보호하는 방법

Google Cloud의 Cloud Volumes Service는 기본적으로 데이터를 보호할 수 있는 다양한 방법을 제공합니다.

안전한 아키텍처 및 테넌시 모델

Cloud Volumes Service는 서로 다른 엔드포인트에 걸쳐 서비스 관리(컨트롤 플레인)와 데이터 액세스(데이터 플레인)를 세분화하여 Google Cloud의 보안 아키텍처를 제공하므로 다른 엔드포인트에 영향을 미치지 않습니다(섹션 참조) ""Cloud Volumes Service 아키텍처"")를 클릭합니다. Google을 사용합니다 "프라이빗 서비스 액세스" (PSA) 프레임워크를 사용하여 서비스를 제공합니다. 이 프레임워크는 NetApp에서 제공하고 운영하는 서비스 생산자와 고객 프로젝트에서 VPC(가상 프라이빗 클라우드)인 서비스 소비자 간의 차이를 구별하며, Cloud Volumes Service 파일 공유에 액세스할 클라이언트를 호스팅합니다.

이 아키텍처에서 테넌트는 섹션을 참조하십시오 ""임차 모델"")는 사용자가 명시적으로 연결하지 않는 한 서로 완전히 격리된 Google Cloud 프로젝트로 정의됩니다. 테넌트를 통해 Cloud Volumes Service 볼륨 플랫폼을 사용하는 다른 테넌트에서 데이터 볼륨, 외부 이름 서비스 및 기타 필수 요소를 완벽하게 격리할 수 있습니다. Cloud Volumes Service 플랫폼은 VPC 피어링을 통해 연결되므로 이러한 격리가 적용됩니다. 공유 VPC를 사용하여 여러 프로젝트 간에 Cloud Volumes Service 볼륨을 공유할 수 있습니다(섹션 참조) ""공유 VPC"")를 클릭합니다. SMB 공유 및 NFS 내보내기에

액세스 제어를 적용하여 데이터 세트를 보거나 수정할 수 있는 사용자 또는 항목을 제한할 수 있습니다.

컨트롤 플레인을 위한 강력한 **ID** 관리

Cloud Volumes Service 구성이 수행되는 컨트롤 플레인에서 을 사용하여 ID 관리를 관리합니다 "IAM(Identity Access Management)". IAM은 Google Cloud 프로젝트 인스턴스에 대한 인증(로그인) 및 권한 부여(권한)를 제어할 수 있는 표준 서비스입니다. 모든 구성은 TLS 1.2 암호화를 사용하는 보안 HTTPS 전송을 통해 Cloud Volumes Service API로 수행되며, 보안을 강화하기 위해 JWT 토큰을 사용하여 인증이 수행됩니다. Cloud Volumes Service용 Google 콘솔 UI는 사용자 입력을 Cloud Volumes Service API 호출로 변환합니다.

보안 강화 - 공격 표면 제한

효과적인 보안 기능 중 일부는 서비스에서 사용할 수 있는 공격 표면의 수를 제한하고 있습니다. 공격 표면에는 유휴 데이터, 전송 중 데이터 전송, 로그인 및 데이터 세트 자체를 비롯한 다양한 사항이 포함될 수 있습니다.

관리되는 서비스는 기본적으로 설계의 일부 공격 표면을 제거합니다. 섹션에 설명된 대로 인프라스트럭처 관리 ""서비스 운영,"" 전담 팀에 의해 처리되고, 사람이 실제로 구성에 접촉하는 횟수를 줄이기 위해 자동화되어 의도적이거나 의도하지 않은 오류의 수를 줄입니다. 필요한 서비스만 서로 액세스할 수 있도록 네트워킹이 차단되었습니다. 암호화는 데이터 저장소에 저장되며 데이터 플레인에 대해서만 Cloud Volumes Service 관리자의 보안 주의가 필요합니다. API 인터페이스 뒤에 대부분의 관리 기능을 숨기면 공격 표면을 제한하여 보안을 달성할 수 있습니다.

제로 트러스트 모델

역사적으로 IT 보안 철학은 위협을 완화하기 위해 외부 메커니즘(예: 방화벽 및 침입 탐지 시스템)에만 의존하는 것으로 확인되고 검증해야 했습니다. 그러나 피싱, 사회 공학, 내부자 위협 및 네트워크에 침입하고 파괴를 초래할 수 있는 확인 기능을 제공하는 기타 방법을 통해 환경의 확인을 우회하기 위해 공격과 침해가 진화했습니다.

제로 트러스트는 "모든 것을 검증하면서 아무것도 신뢰하지 않는다"라는 현재의 원칙을 바탕으로 보안 측면에서 새로운 방식이 되었습니다. 따라서 기본적으로 액세스가 허용되지 않습니다. 표준 방화벽, 침입 탐지 시스템(IDS)을 비롯한 다양한 방법과 다음과 같은 방법을 바탕으로 이러한 원칙을 적용합니다.

- 강력한 인증 방법(예: AES 암호화 Kerberos 또는 JWT 토큰)
- 강력한 단일 ID 소스(예: Windows Active Directory, LDAP(Lightweight Directory Access Protocol) 및 Google IAM)
- 네트워크 세분화 및 보안 멀티 테넌시(테넌트만 기본적으로 액세스 허용)
- 최소 권한 액세스 정책을 통한 세분화된 액세스 제어
- 디지털 감사 및 종이 추적을 지원하는 신뢰할 수 있는 전담 관리자의 소규모 독점 목록

Google Cloud에서 실행되는 Cloud Volumes Service는 "신뢰, 모든 것을 확인"하는 입장을 구현하여 제로 트러스트 모델을 고수합니다.

암호화

유휴 데이터 암호화(섹션 참조 ""저장된 데이터 암호화"") XTS-AES-256 암호를 NetApp Volume Encryption(NVE)과 함께 사용하고 를 사용하여 전송 중입니다 ""SMB 암호화"" 또는 NFS Kerberos 5p를 지원합니다. TLS 1.2 암호화로 지역 간 복제 전송이 보호되므로 안심하십시오(섹션 참조) ""지역 간 복제"")를 클릭합니다. 또한 Google 네트워킹은 암호화된 통신도 제공합니다(섹션 참조) ""전송 중인 데이터 암호화"")를 사용하여 공격에 대한 보호 계층을 추가합니다. 전송 암호화에 대한 자세한 내용은 섹션을 참조하십시오 ""Google Cloud 네트워크"".

데이터 보호 및 백업

보안은 단순한 공격 방지에 관한 것이 아닙니다. 또한 공격이 발생할 경우 또는 발생할 때 공격을 어떻게 복구하는지도 다룹니다. 이 전략에는 데이터 보호 및 백업이 포함됩니다. Cloud Volumes Service는 정전 발생 시 다른 지역으로 복제할 수 있는 방법을 제공합니다(섹션 참조) ""지역 간 복제"") 또는 데이터 세트가 랜섬웨어 공격의 영향을 받는 경우 또한 을 사용하여 Cloud Volumes Service 인스턴스 외부의 위치에 데이터를 비동기식으로 백업할 수도 있습니다 "Cloud Volumes Service 백업". 정기적인 백업을 사용하면 보안 이벤트를 완화하는데 소요되는 시간을 줄이고 비용을 절감하고 관리자에게 불안감을 줄 수 있습니다.

업계 최고 수준의 **Snapshot** 복사본으로 랜섬웨어에 신속하게 대응

Cloud Volumes Service은 데이터 보호 및 백업 외에도 변경 불가능한 스냅샷 복사본에 대한 지원을 제공합니다(섹션 참조) ""변경 불가능한 Snapshot 복사본""랜섬웨어 공격으로부터 복구할 수 있는 볼륨(섹션 참조 ""서비스 운영"") 문제를 발견하는 후 몇 초 이내에 운영 중단을 최소화하십시오. 복구 시간과 효과는 스냅샷 일정에 따라 다르지만 랜섬웨어 공격의 경우 한 시간 차이만큼 작은 스냅샷 복사본을 생성할 수 있습니다. 스냅샷 복사본은 성능 및 용량 사용에 거의 영향을 주지 않고, 데이터 세트를 보호하는 데 있어 위험이 낮은 하이 보상 접근 방식입니다.

보안 고려 사항 및 공격 대상

데이터를 보호하는 방법을 이해하기 위한 첫 번째 단계는 위험 및 잠재적 공격 경로를 식별하는 것입니다.

여기에는 다음이 포함됩니다(이에 국한되지 않음).

- 관리 및 로그인
- 사용되지 않는 데이터
- 전송 중인 데이터
- 네트워크 및 방화벽
- 랜섬웨어, 맬웨어 및 바이러스

공격 경로를 이해하면 환경을 보다 안전하게 보호할 수 있습니다. Google Cloud의 Cloud Volumes Service는 이미 이러한 많은 항목을 고려하고 있으며 관리 개입 없이 기본적으로 보안 기능을 구현합니다.

보안 로그인 보장

중요 인프라 구성 요소를 보호할 때는 승인된 사용자만 환경에 로그인하여 관리할 수 있도록 해야 합니다. 공격자들이 관리 자격 증명을 위반하는 경우, 성을 위한 키가 있으며 구성 변경, 볼륨 및 백업 삭제, 백도어 생성, 스냅샷 스케줄 비활성화 등 원하는 모든 작업을 수행할 수 있습니다.

Cloud Volumes Service for Google Cloud는 StaaS(Storage as a Service)의 난독화 기능을 통해 무단 관리 로그인으로부터 보호합니다. Cloud Volumes Service은 외부에서 로그인할 수 없는 상태에서 클라우드 공급자가 완벽하게 유지합니다. 모든 설정 및 구성 작업이 완전히 자동화되므로 매우 드문 경우를 제외하고, 사용자 관리자는 시스템과 상호 작용할 필요가 없습니다.

로그인이 필요한 경우, Google Cloud의 Cloud Volumes Service는 시스템에 로그인할 수 있는 매우 간단한 신뢰할 수 있는 관리자 목록을 유지하여 로그인을 보호합니다. 이 가문부수는 액세스 권한이 있는 잠재적 불량 행위자의 수를 줄이는 데 도움이 됩니다. 또한 Google Cloud 네트워킹은 네트워크 보안 계층 뒤에서 시스템을 숨기고 외부 환경에 필요한 것만 노출합니다. Google Cloud, Cloud Volumes Service 아키텍처에 대한 자세한 내용은 섹션을 참조하십시오 ""Cloud Volumes Service 아키텍처.""

클러스터 관리 및 업그레이드

잠재적 보안 위험이 있는 두 가지 영역에는 클러스터 관리(잘못된 행위자가 관리자 액세스 권한을 가지고 있는 경우 발생하는 현상) 및 업그레이드(소프트웨어 이미지가 손상된 경우 발생하는 현상)가 포함됩니다.

스토리지 관리 보호

서비스형 스토리지를 사용하면 클라우드 데이터 센터 외부의 최종 사용자에 대한 액세스를 제거하여 관리자가 노출될 가능성을 최소화할 수 있습니다. 대신 고객이 데이터 액세스 플레인을 위해 설정하는 것이 유일한 구성입니다. 각 테넌트는 자체 볼륨을 관리하며 테넌트가 다른 Cloud Volumes Service 인스턴스에 연결할 수 없습니다. 이 서비스는 자동화를 통해 관리되며, 이 섹션에서 설명하는 프로세스를 통해 시스템에 액세스할 수 있는 신뢰할 수 있는 관리자의 목록은 매우 적습니다 ""서비스 운영""

CVS - 성능 서비스 유형은 지역 간 복제를 옵션으로 제공하여 지역 장애가 발생할 경우 다른 지역에 데이터를 보호합니다. 이 경우 Cloud Volumes Service를 영향을 받지 않는 영역으로 페일오버하여 데이터 액세스를 유지할 수 있습니다.

서비스 업그레이드

업데이트는 취약한 시스템을 보호하는 데 도움이 됩니다. 각 업데이트는 공격 경로를 최소화하는 보안 향상 기능 및 버그 수정을 제공합니다. 소프트웨어 업데이트는 중앙 저장소에서 다운로드되고 업데이트가 공식 이미지가 사용되고 잘못된 행위자에 의해 업그레이드에 영향을 받지 않는지 확인하기 전에 검증됩니다.

Cloud Volumes Service를 사용하면 클라우드 제공업체 팀이 업데이트를 처리하므로 관리자가 프로세스를 자동화하고 완벽하게 테스트한 구성 및 업그레이드에 정통하여 위험에 노출될 가능성을 줄일 수 있습니다. 업그레이드는 무중단으로 수행할 수 있으며 Cloud Volumes Service는 최신 업데이트를 유지하여 전체적인 결과를 최대한 제공합니다.

이러한 서비스 업그레이드를 수행하는 관리자 팀에 대한 자세한 내용은 섹션을 참조하십시오 ""서비스 운영""

사용되지 않는 데이터의 보안

유휴 데이터 암호화는 디스크 도난, 반환 또는 용도 변경이 발생할 경우 중요한 데이터를 보호하는 데 중요합니다. Cloud Volumes Service의 데이터는 소프트웨어 기반 암호화를 사용하여 유휴 상태에서 보호됩니다.

- Google에서 생성한 키는 CVS-SW에 사용됩니다.
- CVS - 성능의 경우 볼륨별 키는 Cloud Volumes Service에 내장된 키 관리자에 저장되며, NetApp ONTAP CryptoMod를 사용하여 AES-256 암호화 키를 생성합니다. CryptoMod는 CMVP FIPS 140-2 검증 모듈 목록에 나열되어 있습니다. 을 참조하십시오 "FIPS 140-2 인증 번호 4144".

2021년 11월부터 CVS-Performance에 CMEK(Customer-managed Encryption) 기능을 미리 볼 수 있습니다. 이 기능을 사용하면 Google KMS(Key Management Service)에서 호스팅되는 프로젝트별, 지역별 마스터 키를 사용하여 볼륨별 키를 암호화할 수 있습니다. KMS를 사용하면 외부 키 관리자를 연결할 수 있습니다.

CVS용 KMS 구성 방법에 대한 자세한 내용은 "Cloud Volumes Service 설명서를 참조하십시오".

아키텍처에 대한 자세한 내용은 섹션을 참조하십시오 ""Cloud Volumes Service 아키텍처.""

전송 중인 데이터 보안

유휴 데이터의 보안 외에도 Cloud Volumes Service 인스턴스와 클라이언트 또는 복제 타겟 간에 전송 중인 데이터를 안전하게 보호할 수 있어야 합니다. Cloud Volumes Service는 Kerberos를 사용한 SMB 암호화, 패킷의 서명/봉인 및 데이터 전송의 엔드 투 엔드 암호화를 위한 NFS Kerberos 5p 등의 암호화 방법을 사용하여 NAS 프로토콜을 통해 전송

중인 데이터에 대한 암호화를 제공합니다.

Cloud Volumes Service 볼륨의 복제는 TLS-GCM 암호화 방법을 활용하는 TLS 1.2를 사용합니다.

텔넷, NDMP 등과 같이 안전하지 않은 전송 중 프로토콜은 기본적으로 비활성화되어 있습니다. 그러나 DNS는 Cloud Volumes Service에 의해 암호화되지 않으며(DNS 초 지원 없음) 가능하면 외부 네트워크 암호화를 사용하여 암호화해야 합니다. 섹션을 참조하십시오 ""전송 중인 데이터 암호화"" 전송 중인 데이터 보안에 대한 자세한 내용은 를 참조하십시오.

NAS 프로토콜 암호화에 대한 자세한 내용은 섹션을 참조하십시오 ""NAS 프로토콜."""

NAS 권한에 대한 사용자 및 그룹

클라우드에서 데이터를 보호하기 위해서는 적절한 사용자 및 그룹 인증이 필요합니다. 여기서 데이터에 액세스하는 사용자는 해당 환경의 실제 사용자로서 확인되고 그룹에는 유효한 사용자가 포함됩니다. 이러한 사용자 및 그룹은 스토리지 시스템의 파일 및 폴더에 대한 권한 검증뿐만 아니라 초기 공유 및 내보내기 액세스를 제공합니다.

Cloud Volumes Service는 SMB 공유 및 Windows 스타일 권한에 표준 Active Directory 기반 Windows 사용자 및 그룹 인증을 사용합니다. 또한 UNIX용 LDAP 사용자 및 NFS 내보내기, NFSv4 ID 검증, Kerberos 인증 및 NFSv4 ACL을 위한 그룹 등의 UNIX ID 공급자를 활용할 수 있습니다.

현재 Active Directory LDAP만 Cloud Volumes Service for LDAP 기능에서 지원됩니다.

랜섬웨어, 맬웨어 및 바이러스의 감지, 방지 및 완화

랜섬웨어, 맬웨어 및 바이러스는 관리자에게 지속적인 위협이며 이러한 위협을 탐지, 예방 및 완화하는 것은 엔터프라이즈 조직의 최우선 고려입니다. 중요 데이터 세트에서 랜섬웨어 이벤트를 한 번 수행해도 수백만 달러의 비용이 발생할 수 있으므로 위험을 최소화하는 것이 좋습니다.

Cloud Volumes Service에는 현재 바이러스 백신 보호 또는 같은 기본 감지 또는 방지 조치가 포함되어 있지 않습니다 "자동 랜섬웨어 탐지"정기적인 Snapshot 일정을 활성화하여 랜섬웨어 이벤트에서 신속하게 복구할 수 있는 방법이 있습니다. 스냅샷 복사본은 변경할 수 없으며 파일 시스템의 변경된 블록에 대한 읽기 전용 포인터만 사용할 수 있으며, 거의 즉각적으로 성능에 미치는 영향이 최소화되고, 데이터가 변경 또는 삭제될 때만 공간을 사용합니다. 원하는 RPO(복구 시점 목표)/RTO(복구 시간 목표)에 맞게 Snapshot 복사본의 일정을 설정할 수 있으며 볼륨당 최대 1,024개의 Snapshot 복사본을 유지할 수 있습니다.

스냅샷 지원은 Cloud Volumes Service에서 추가 비용 없이(스냅샷 복사본에 의해 유지되는 변경된 블록/데이터에 대한 데이터 스토리지 비용 제외) 포함되며, 랜섬웨어 공격의 경우 공격이 발생하기 전에 스냅샷 복사본으로 롤백하는 데 사용할 수 있습니다. 스냅샷 복원을 완료하는 데 몇 초 밖에 걸리지 않습니다. 그런 다음 정상 데이터 상태로 되돌릴 수 있습니다. 자세한 내용은 을 참조하십시오 "랜섬웨어용 NetApp 솔루션".

랜섬웨어가 비즈니스에 영향을 주지 않도록 하려면 다음 중 하나 이상이 포함된 다계층 접근 방식이 필요합니다.

- 엔드포인트 보호
- 네트워크 방화벽을 통한 외부 위협으로부터 보호
- 데이터 이상 감지
- 중요 데이터 세트에 대한 다중 백업(온사이트 및 오프사이트
- 백업의 정기적인 복원 테스트
- 변경 불가능한 읽기 전용 NetApp Snapshot 복사본

- 중요 인프라를 위한 다단계 인증
- 시스템 로그인에 대한 보안 감사

이 목록은 전체적인 것으로부터 멀리 떨어져 있지만 랜섬웨어 공격의 가능성을 해결할 때 따라야 할 좋은 청사진입니다. Google Cloud의 Cloud Volumes Service는 랜섬웨어 이벤트를 방지하고 효과를 줄일 수 있는 여러 방법을 제공합니다.

변경 불가능한 스냅샷 복사본

Cloud Volumes Service은 데이터를 삭제하거나 랜섬웨어 공격으로 인해 전체 볼륨이 희생된 경우 사용자 지정이 가능한 일정에 따라 진행되는 변경 불가능한 읽기 전용 스냅샷 복사본을 기본적으로 제공합니다. 스냅샷 스케줄 및 RTO/RPO의 보존 기간을 기준으로 Snapshot을 이전 Snapshot 복제본으로 빠르게 복구하고 데이터 손실을 최소화합니다. 스냅샷 기술을 사용할 경우 성능 영향은 미미합니다.

Cloud Volumes Service의 스냅샷 복사본은 읽기 전용이므로 랜섬웨어가 데이터 세트에 확산되지 않고 Snapshot 복사본이 랜섬웨어에 의해 감염된 데이터를 가져가지 않는 한 랜섬웨어에 감염될 수 없습니다. 따라서 데이터 이상을 기반으로 랜섬웨어 탐지를 고려해야 하는 이유가 됩니다. Cloud Volumes Service는 현재 탐지 기능을 기본적으로 제공하지 않지만 외부 모니터링 소프트웨어를 사용할 수 있습니다.

백업 및 복원

Cloud Volumes Service는 표준 NAS 클라이언트 백업 기능(예: NFS 또는 SMB를 통한 백업)을 제공합니다.

- CVS - 성능은 다른 CVS - 성능 볼륨에 대한 교차 지역 볼륨 복제를 제공합니다. 자세한 내용은 을 참조하십시오 "볼륨 복제" Cloud Volumes Service 설명서를 참조하십시오.
- CVS-SW는 서비스 네이티브 볼륨 백업/복원 기능을 제공합니다. 자세한 내용은 을 참조하십시오 "클라우드 백업" Cloud Volumes Service 설명서를 참조하십시오.

볼륨 복제는 랜섬웨어 이벤트를 포함하여 재해 발생 시 신속한 페일오버를 위해 소스 볼륨의 정확한 복사본을 제공합니다.

지역 간 복제

CVS - 성능은 Google 네트워크에서 실행되는 복제에 사용되는 특정 인터페이스를 사용하여 NetApp이 제어하는 백엔드 서비스 네트워크에서 TLS1.2 AES 256 GCM 암호화를 사용하여 데이터 보호 및 아카이브 사용 사례를 위해 Google Cloud 지역 전반에 걸쳐 볼륨을 안전하게 복제할 수 있게 해줍니다. 운영(소스) 볼륨에는 활성 운영 데이터가 포함되어 있으며 보조(대상) 볼륨에 복제하여 운영 데이터 세트의 정확한 복제본을 제공합니다.

초기 복제는 모든 블록을 전송하지만 업데이트는 변경된 블록만 운영 볼륨에서 전송합니다. 예를 들어, 기본 볼륨에 상주하는 1TB 데이터베이스가 보조 볼륨으로 복제되면 1TB 공간이 초기 복제 시 전송됩니다. 해당 데이터베이스에 초기화와 다음 업데이트 간에 변경되는 수백 개의 행(몇 MB)이 있는 경우 변경된 행이 있는 블록만 보조 블록(몇 MB)으로 복제됩니다. 이렇게 하면 전송 시간이 낮게 유지되고 복제 비용이 계속 감소되도록 할 수 있습니다.

파일 및 폴더에 대한 모든 권한은 보조 볼륨으로 복제되지만 내보내기 정책 및 규칙, SMB 공유 및 ACL 공유 등의 공유 액세스 권한은 별도로 처리해야 합니다. 사이트 장애 조치의 경우 대상 사이트는 동일한 이름 서비스와 Active Directory 도메인 연결을 활용하여 사용자 및 그룹 ID와 사용 권한을 일관된 방식으로 처리해야 합니다. 재해 발생 시 보조 볼륨을 페일오버 타겟으로 사용할 수 있습니다. 즉, 2차 볼륨을 읽기-쓰기로 변환하는 복제 관계를 끊으면 됩니다.

볼륨 복사본은 읽기 전용이며, 바이러스가 감염된 데이터를 가지고 있거나 랜섬웨어가 기본 데이터 세트를 암호화한 경우 데이터를 빠르게 복구하기 위해 변경 불가능한 데이터 사본을 오프사이트에 제공합니다. 읽기 전용 데이터는 암호화되지 않지만 운영 볼륨이 영향을 받고 복제가 발생하는 경우 감염된 블록도 복제됩니다. 오래되고 영향을 받지 않는 Snapshot 복사본을 사용하여 복구할 수 있지만, 공격이 탐지되는 속도에 따라 SLA가 약속된 RTO/RPO의 범위를

벗어날 수 있습니다.

또한 Google Cloud에서 CRR(Cross-Region Replication) 관리를 통해 볼륨 삭제, 스냅샷 삭제 또는 스냅샷 스케줄 변경과 같은 악의적인 관리 작업을 방지할 수 있습니다. 이 작업은 볼륨 관리자를 분리하는 사용자 지정 역할을 생성하여 수행합니다. 볼륨 관리자는 소스 볼륨을 삭제할 수는 있지만 미러를 중단할 수는 없으므로 볼륨 작업을 수행할 수 없는 CRR 관리자로부터 대상 볼륨을 삭제할 수 없습니다. 을 참조하십시오 "보안 고려 사항" 각 관리자 그룹이 허용하는 권한에 대한 Cloud Volumes Service 문서

Cloud Volumes Service 백업

Cloud Volumes Service는 높은 데이터 내구성을 제공하지만 외부 이벤트는 데이터 손실을 일으킬 수 있습니다. 바이러스 또는 랜섬웨어와 같은 보안 이벤트가 발생할 경우, 백업 및 복원이 시기적절하게 데이터 액세스를 재개하는 데 중요한 역할을 합니다. 관리자가 실수로 Cloud Volumes Service 볼륨을 삭제할 수 있습니다. 또는 사용자가 단순히 데이터 백업 버전을 몇 개월 동안 유지하고 볼륨 내에 추가 Snapshot 복사본 공간을 유지하는 것은 비용 문제가 됩니다. Snapshot 복사본이 최근 몇 주 동안 손실된 데이터를 복원하는 백업 버전을 보관하는 기본 방법이어야 하지만, 볼륨 내에 있으며 볼륨이 없어지면 손실됩니다.

이러한 모든 이유로 NetApp Cloud Volumes Service은 를 통해 백업 서비스를 제공합니다 "Cloud Volumes Service 백업".

Cloud Volumes Service 백업은 GCS(Google Cloud Storage)에서 볼륨의 복사본을 생성합니다. 사용 가능한 공간이 아닌 볼륨 내에 저장된 실제 데이터만 백업합니다. 영구 증분 방식으로 작동하므로 볼륨 콘텐츠를 한 번 전송하고 변경된 데이터만 계속 백업합니다. 여러 개의 전체 백업을 사용하는 기존 백업 개념에 비해 많은 양의 백업 스토리지를 절약하여 비용을 절감합니다. 백업 공간의 월별 가격이 볼륨에 비해 낮기 때문에 백업 버전을 더 오래 유지하는 것이 좋습니다.

사용자는 Cloud Volumes Service 백업을 사용하여 모든 백업 버전을 동일한 지역 내의 동일한 볼륨 또는 다른 볼륨으로 복원할 수 있습니다. 소스 볼륨이 삭제되면 백업 데이터가 보존되므로 독립적으로 관리(예: 삭제)해야 합니다.

Cloud Volumes Service 백업은 Cloud Volumes Service에 옵션으로 내장되어 있습니다. 사용자는 볼륨별로 Cloud Volumes Service 백업을 활성화하여 보호할 볼륨을 결정할 수 있습니다. 를 참조하십시오 "Cloud Volumes Service 백업 설명서" 백업에 대한 자세한 내용은 를 참조하십시오 "지원되는 최대 백업 버전 수입니다", 스케줄링 및 을 참조하십시오 "가격".

프로젝트의 모든 백업 데이터는 GCS 버킷 내에 저장되며, 이 버킷은 서비스에서 관리되며 사용자에게 표시되지 않습니다. 프로젝트마다 다른 버킷을 사용합니다. 현재 버킷은 Cloud Volumes Service 볼륨과 동일한 영역에 있지만 더 많은 옵션에 대해 논의 중입니다. 최신 상태는 설명서를 참조하십시오.

Cloud Volumes Service 버킷에서 GCS로 데이터를 전송하는 경우 HTTPS 및 TLS1.2가 포함된 서비스 내부 Google 네트워크를 사용합니다. 데이터는 Google에서 관리하는 키로 유휴 상태로 암호화됩니다.

Cloud Volumes Service 백업(백업 생성, 삭제 및 복원)을 관리하려면 사용자에게 이 있어야 합니다 " 역할/netappcloudvolumes.admin" 역할.

있습니다

개요

클라우드 솔루션을 신뢰하는 것은 아키텍처와 보안 방식을 이해하는 것입니다. 이 섹션에서는 Google의 Cloud Volumes Service 아키텍처의 다양한 측면을 다루어 데이터 보안 방식에 대한 잠재적 우려를 완화하고 가장 안전한 배포를 위해 추가 구성 단계가 필요할 수 있는 영역을 설명합니다.

Cloud Volumes Service의 일반 아키텍처는 컨트롤 플레인과 데이터 플레인의 두 가지 주요 구성 요소로 나눌 수 있습니다.

컨트롤 플레인

Cloud Volumes Service의 제어 플레인은 Cloud Volumes Service 관리자와 NetApp 기본 자동화 소프트웨어가 관리하는 백엔드 인프라입니다. 이 방식은 최종 사용자에게 전혀 영향을 미치지 않으며 네트워킹, 스토리지 하드웨어, 소프트웨어 업데이트 등을 포함하여 Cloud Volumes Service와 같은 클라우드 상주 솔루션에 가치를 제공하는 데 도움을 줍니다.

데이터 플레인

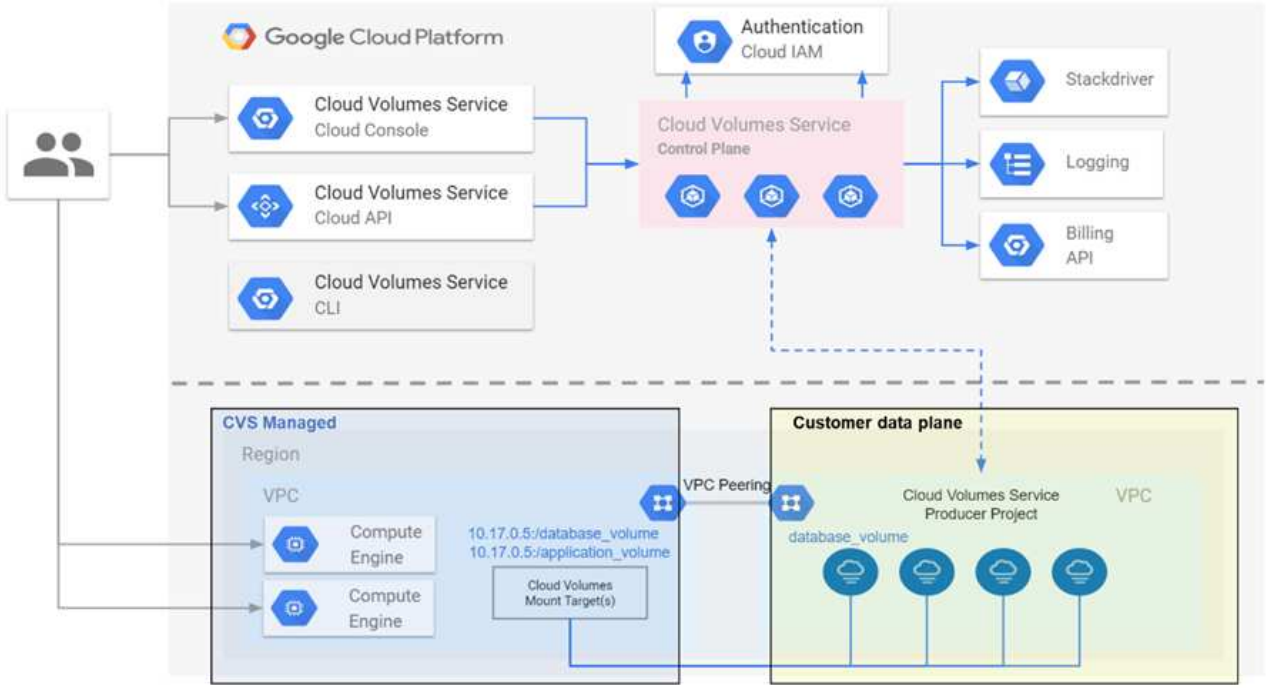
Cloud Volumes Service의 데이터 계층에는 실제 데이터 볼륨과 전체 Cloud Volumes Service 구성(액세스 제어, Kerberos 인증 등)이 포함됩니다. 데이터 플레인은 전적으로 최종 사용자와 Cloud Volumes Service 플랫폼 소비자를 제어하는 것입니다.

각 평면의 보안 및 관리 방법은 서로 다릅니다. 다음 섹션에서는 Cloud Volumes Service 아키텍처 개요부터 이러한 차이점에 대해 설명합니다.

Cloud Volumes Service 아키텍처

CloudSQL, GCVE(Google Cloud VMware Engine) 및 파일 저장소와 같은 다른 Google Cloud 네이티브 서비스와 유사한 방식으로 Cloud Volumes Service는 을 사용합니다 "Google PSA" 서비스를 제공합니다. PSA에서는 서비스를 사용하는 서비스 프로듀서 프로젝트에 내장하고 있습니다 "VPC 네트워크 피어링" 서비스 소비자에 연결합니다. 서비스 생산자는 NetApp에서 제공 및 운영하고, 서비스 소비자는 고객 프로젝트에서 VPC로, Cloud Volumes Service 파일 공유에 액세스하려는 클라이언트를 호스팅합니다.

에서 참조하는 다음 그림 "아키텍처 섹션을 참조하십시오" 에서는 Cloud Volumes Service 설명서의 개략적인 보기를 보여 줍니다.



점선 위의 파트는 볼륨 수명 주기를 제어하는 서비스의 컨트롤 평면을 보여줍니다. 점선 아래의 부분은 데이터 평면을 나타냅니다. 왼쪽 파란색 상자는 사용자 VPC(서비스 소비자)를 나타내고 오른쪽 파란색 상자는 NetApp에서 제공하는 서비스 생산업체입니다. 둘 다 VPC 피어링을 통해 연결됩니다.

테넌시 모델

Cloud Volumes Service에서 개별 프로젝트는 고유한 테넌트로 간주됩니다. 즉, 볼륨, 스냅샷 복사본 등을 프로젝트 단위로 조작할 수 있습니다. 즉, 모든 볼륨은 자신이 만든 프로젝트의 소유이며 해당 프로젝트에서만 기본적으로 해당 볼륨 내의 데이터를 관리하고 액세스할 수 있습니다. 이는 서비스의 컨트롤 플레인 뷰로 간주됩니다.

공유 **VPC**

데이터 평면 보기에서 Cloud Volumes Service는 공유 VPC에 연결할 수 있습니다. 호스팅 프로젝트 또는 공유 VPC에 연결된 서비스 프로젝트 중 하나에서 볼륨을 생성할 수 있습니다. 공유 VPC에 연결된 모든 프로젝트(호스트 또는 서비스)는 네트워크 계층(TCP/IP)에서 볼륨에 연결할 수 있습니다. 공유 VPC에서 네트워크 연결을 사용하는 모든 클라이언트는 NAS 프로토콜을 통해 데이터에 액세스할 수 있으므로 개별 볼륨의 액세스 제어(예: 사용자/그룹 ACL(액세스 제어 목록) 및 NFS 내보내기의 호스트 이름/IP 주소)를 사용하여 데이터에 액세스할 수 있는 사용자를 제어해야 합니다.

고객 프로젝트당 최대 5대의 VPC에 Cloud Volumes Service를 연결할 수 있습니다. 제어 플레인에서 프로젝트를 사용하면 연결된 VPC에 관계없이 생성된 모든 볼륨을 관리할 수 있습니다. 데이터 플레인에서 VPC는 서로 격리되며 각 볼륨은 하나의 VPC에만 연결할 수 있습니다.

개별 볼륨에 대한 액세스는 프로토콜별(NFS/SMB) 액세스 제어 메커니즘에 의해 제어됩니다.

즉, 네트워크 계층에서 공유 VPC에 연결된 모든 프로젝트가 볼륨을 볼 수 있는 반면 관리 측면에서는 소유자 프로젝트만 볼륨을 볼 수 있습니다.

VPC 서비스 제어

VPC 서비스 제어는 인터넷에 연결되어 있고 전 세계적으로 액세스할 수 있는 Google Cloud 서비스에 대한 액세스 제어 경계를 설정합니다. 이러한 서비스는 사용자 ID를 통해 액세스 제어를 제공하지만 어떤 네트워크 위치 요청이 시작되기까지의 지 제한할 수 없습니다. VPC 서비스는 정의된 네트워크에 대한 액세스를 제한하는 기능을 도입하여 이러한 격차를 해소합니다.

Cloud Volumes Service 데이터 플레인은 외부 인터넷에 연결되지 않고 잘 정의된 네트워크 경계(경계)가 있는 전용 VPC에 연결됩니다. 해당 네트워크 내에서 각 볼륨은 프로토콜별 액세스 제어를 사용합니다. 외부 네트워크 연결은 Google Cloud 프로젝트 관리자가 명시적으로 만듭니다. 그러나 컨트롤 플레인은 데이터 플레인과 동일한 보호 기능을 제공하지 않으며 모든 곳에서 유효한 자격 증명( )을 사용하여 액세스할 수 있습니다 "JWT 토큰")를 클릭합니다.

즉, Cloud Volumes Service 데이터 플레인은 VPC 서비스 제어를 지원할 필요 없이 VPC 서비스 제어를 명시적으로 사용하지 않고 네트워크 액세스 제어 기능을 제공합니다.

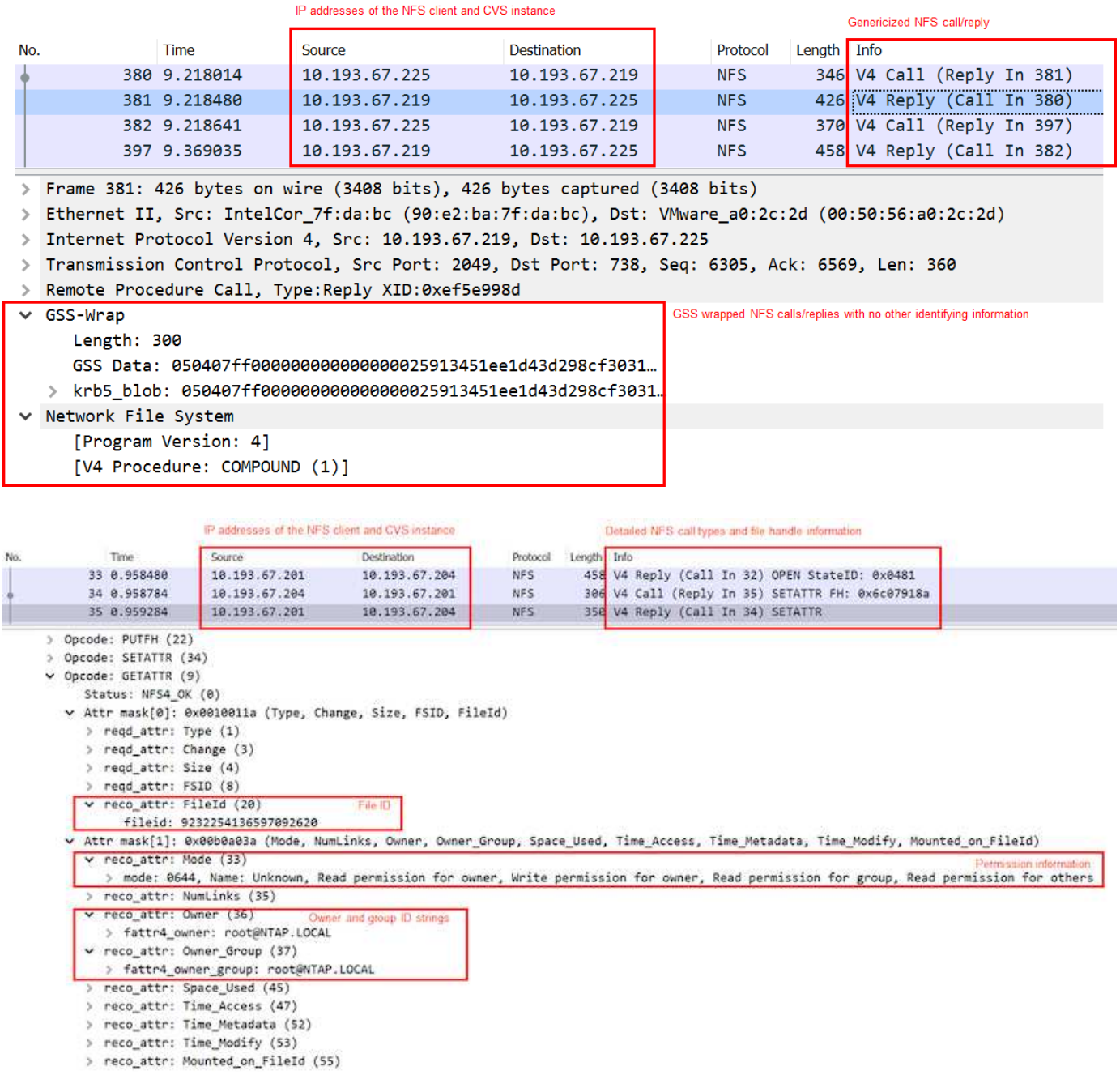
패킷 스니핑/추적 고려 사항

패킷 캡처는 네트워크 문제 또는 기타 문제(예: NAS 권한, LDAP 연결 등)를 해결하는 데 유용할 수 있지만 네트워크 IP 주소, MAC 주소, 사용자 및 그룹 이름 및 엔드포인트에서 사용되는 보안 수준에 대한 정보를 얻기 위해 악의적으로 사용할 수도 있습니다. Google Cloud 네트워킹, VPC 및 방화벽 규칙이 구성된 방식 때문에 사용자 로그인 자격 증명 또는 없이 네트워크 패킷에 대한 원치 않는 액세스를 얻기가 어렵습니다 "JWT 토큰" 클라우드로 인스턴스. 공유 VPC 및/또는 외부 네트워크 터널/IP 전달을 사용하여 엔드포인트에 대한 외부 트래픽을 명시적으로 허용하지 않는 한 패킷 캡처는 엔드포인트(예: 가상 머신(VM))에서만 가능하며 VPC 내부 엔드포인트에서만 가능합니다. 클라이언트 외부의 트래픽을 스니핑할 수 있는 방법은 없습니다.

공유 VPC를 사용하는 경우 NFS Kerberos 및/또는 를 사용하여 전송 중 암호화 "SMB 암호화" 트레이스에서 얻은 정보의 대부분을 가릴 수 있습니다. 그러나 일부 트래픽은 과 같은 일반 텍스트로 계속 전송됩니다 "DNS" 및 "LDAP 쿼리입니다". 다음 그림에서는 Cloud Volumes Service에서 생성된 일반 텍스트 LDAP 쿼리 및 노출된 잠재적 식별 정보의 패킷 캡처를 보여 줍니다. Cloud Volumes Service의 LDAP 쿼리는 현재 SSL을 통한 암호화 또는 LDAP를 지원하지 않습니다. Active Directory에서 요청하는 경우 CVS - 성능은 LDAP 서명을 지원합니다. CVS-SW는 LDAP 서명을 지원하지 않습니다.

unixUserPassword는 LDAP에 의해 쿼리되며 일반 텍스트로 전송되지 않고 소염 해시로 보내집니다. 기본적으로 Windows LDAP는 unixUserPassword 필드를 채우지 않습니다. 이 필드는 LDAP를 통해 클라이언트에 대화형 로그인을 위해 Windows LDAP를 활용해야 하는 경우에만 필요합니다. Cloud Volumes Service는 인스턴스에 대한 대화형 LDAP 로그인을 지원하지 않습니다.

다음 그림에서는 AUTH_SYS를 통한 NFS 캡처 옆에 있는 NFS Kerberos 대화의 패킷 캡처를 보여 줍니다. 추적에서 사용할 수 있는 정보가 두 가지 간에 어떻게 다른지, 그리고 전송 중 암호화를 사용하여 NAS 트래픽에 대한 전반적인 보안을 강화하는 방법을 확인하십시오.



VM 네트워크 인터페이스

공격자는 의 VM에 새 NIC(네트워크 인터페이스 카드)를 추가하려고 시도할 수 있습니다 "무차별 모드" 모든 트래픽을 스니핑하기 위해 기존 NIC에서 Promiscuous 모드를 활성화(포트 미러링)하거나 활성화합니다. Google Cloud에서 새 NIC를 추가하려면 VM을 완전히 종료해야 하므로 경고가 생성되므로 공격자가 이를 놓치지 않고 확인할 수 없습니다.

또한 NIC를 무차별 모드로 설정할 수 없으며 Google Cloud에서 경고를 트리거합니다.

컨트롤 플레인 아키텍처

Cloud Volumes Service에 대한 모든 관리 작업은 API를 통해 수행됩니다. GCP 클라우드 콘솔에 통합된 Cloud Volumes Service 관리도 Cloud Volumes Service API를 사용합니다.

ID 및 액세스 관리

ID 및 액세스 관리 ("IAM")는 Google Cloud 프로젝트 인스턴스에 대한 인증(로그인) 및 권한 부여(권한)를 제어할 수 있는 표준 서비스입니다. Google IAM은 권한 승인 및 제거에 대한 전체 감사 추적을 제공합니다. 현재 Cloud Volumes Service는 제어 평면 감사를 제공하지 않습니다.

인증/권한 개요

IAM은 Cloud Volumes Service에 대한 세분화된 기본 권한을 제공합니다. 를 찾을 수 있습니다 "여기에서 세분화된 사용 권한의 전체 목록을 확인할 수 있습니다".

IAM은 또한 netapcloudvolumes.admin과 netapcloudvolumes.viewer라는 두 가지 사전 정의된 역할을 제공합니다. 이러한 역할은 특정 사용자 또는 서비스 계정에 할당할 수 있습니다.

IAM 사용자가 Cloud Volumes Service를 관리할 수 있도록 적절한 역할 및 권한을 할당합니다.

세분화된 사용 권한을 사용하는 예는 다음과 같습니다.

- 사용자가 볼륨을 삭제할 수 없도록 get/list/create/update 권한만 가진 사용자 지정 역할을 만듭니다.
- '스냅샷 *' 권한으로만 사용자 지정 역할을 사용하여 애플리케이션 정합성 보장 스냅샷 통합을 구축하는 데 사용되는 서비스 계정을 생성합니다.
- 특정 사용자에게 '볼륨 증가 *'를 위임하는 사용자 지정 역할을 만듭니다.

서비스 계정

또는 스크립트를 통해 Cloud Volumes Service API 호출을 수행하는 방법 "Terraform(Terraform" 역할/netapcloudvolumes.admin의 역할을 사용하여 서비스 계정을 생성해야 합니다. 이 서비스 계정을 사용하여 Cloud Volumes Service API 요청을 인증하는 데 필요한 JWT 토큰을 다음 두 가지 방법으로 생성할 수 있습니다.

- JSON 키를 생성하고 Google API를 사용하여 JWT 토큰을 파생시킵니다. 이 방법이 가장 간단한 방법이지만 수동 비밀(JSON 키) 관리와 관련이 있습니다.
- 사용 "서비스 계정 가장" 역할/iam.serviceAccountTokenCreator` 포함. 이 코드(스크립트, Terraform 등)는 에서 실행됩니다 "애플리케이션 기본 자격 증명" 서비스 계정을 가장하여 권한을 얻습니다. 이 접근 방식은 Google 보안 모범 사례를 반영합니다.

을 참조하십시오 "서비스 계정 및 개인 키 생성" 자세한 내용은 Google 클라우드 설명서를 참조하십시오.

Cloud Volumes Service API를 참조하십시오

Cloud Volumes Service API는 HTTPS(TLSv1.2)를 기본 네트워크 전송으로 사용하여 REST 기반 API를 사용합니다. 최신 API 정의를 찾을 수 있습니다 "여기" 및 에서 API 사용 방법에 대한 정보를 참조하십시오 "Google Cloud 설명서에서 Cloud Volumes API를 참조하십시오".

API 엔드포인트는 표준 HTTPS(TLSv1.2) 기능을 사용하여 NetApp에서 작동 및 보안됩니다.

JWT 토큰

API에 대한 인증은 JWT 베어러 토큰을 사용하여 수행됩니다 ("RFC-7519")를 클릭합니다. Google Cloud IAM 인증을 사용하여 유효한 JWT 토큰을 얻어야 합니다. 서비스 계정 JSON 키를 제공하여 IAM에서 토큰을 가져와 수행해야 합니다.

로깅 감사

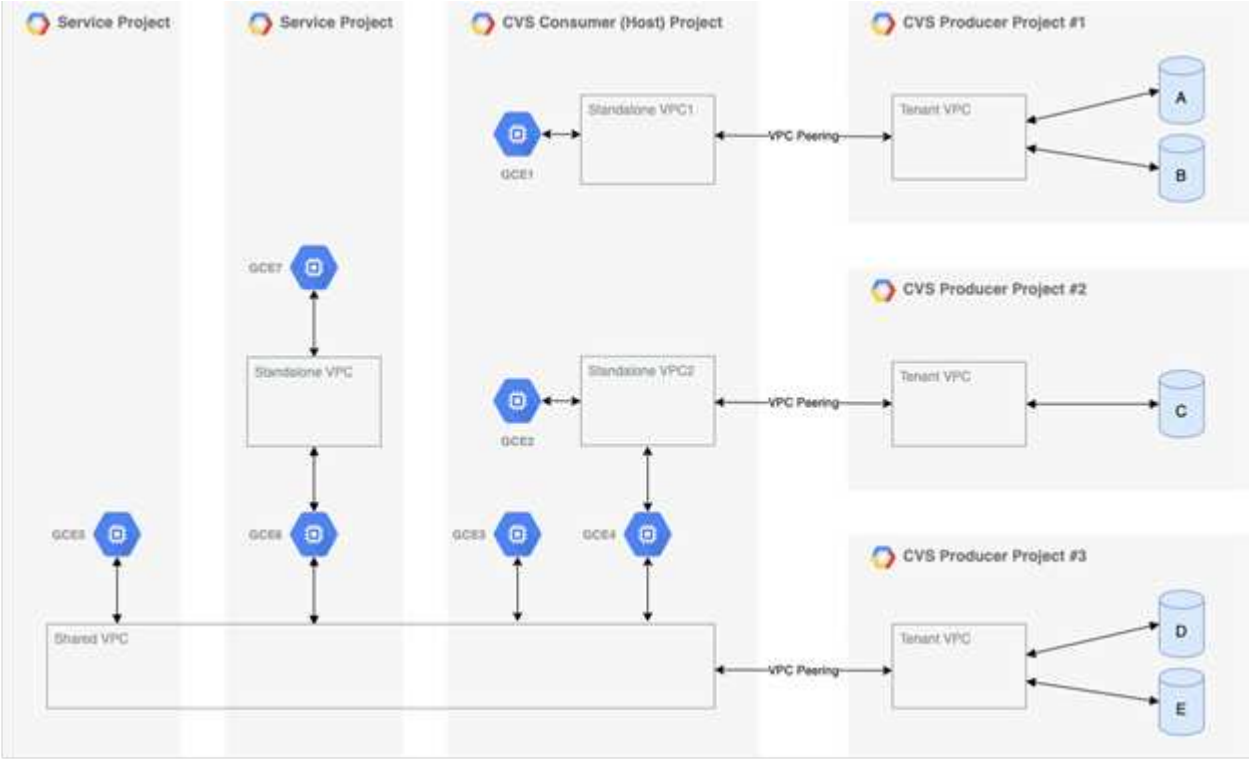
현재 사용자가 액세스할 수 있는 컨트롤 플레인 감사 로그를 사용할 수 없습니다.

데이터 플레인 아키텍처

Cloud Volumes Service for Google Cloud는 Google Cloud를 활용합니다 "프라이빗 서비스 액세스" 프레임워크: 이 프레임워크에서는 사용자가 Cloud Volumes Service에 연결할 수 있습니다. 이 프레임워크는 다른 Google Cloud 서비스와 같은 서비스 네트워킹 및 VPC 피어링 구조를 사용하여 테넌트 간의 완전한 격리를 보장합니다.

Google Cloud용 Cloud Volumes Service의 아키텍처 개요는 를 참조하십시오 "Cloud Volumes Service용 아키텍처".

사용자 VPC(독립 실행형 또는 공유)는 볼륨을 호스팅하는 Cloud Volumes Service 관리 테넌트 프로젝트 내의 VPC에 대해 자세히 살펴봅니다.



위 그림에서는 Cloud Volumes Service에 연결된 VPC 네트워크 3개와 볼륨을 공유하는 GCE1-7(다중 컴퓨팅 엔진 VM)이 포함된 프로젝트(중간 CVS 소비자 프로젝트)를 보여 줍니다.

- VPC1을 사용하면 GCE1이 볼륨 A와 B에 액세스할 수 있습니다

- VPC2는 GCE2와 GCE4가 볼륨 C에 액세스할 수 있도록 합니다
- 세 번째 VPC 네트워크는 공유 VPC로, 두 개의 서비스 프로젝트와 공유됩니다. GCE3, GCE4, GCE5 및 GCE6에서 D 및 E 볼륨에 액세스할 수 있습니다 공유 VPC 네트워크는 CVS 성능 서비스 유형의 볼륨에만 지원됩니다.

GCE7은 어떤 볼륨에도 액세스할 수 없습니다.

데이터는 전송 중(Kerberos 및/또는 SMB 암호화 사용) 및 Cloud Volumes Service에 저장된 데이터를 모두 암호화할 수 있습니다.

전송 중인 데이터 암호화

전송 중인 데이터는 NAS 프로토콜 계층에서 암호화할 수 있으며, Google Cloud 네트워크 자체는 다음 섹션에 설명된 대로 암호화됩니다.

Google Cloud 네트워크

Google Cloud는 에 설명된 대로 네트워크 수준의 트래픽을 암호화합니다 "전송 중인 암호화" Google 문서. “Cloud Volumes Services 아키텍처” 섹션에서 언급한 것처럼 Cloud Volumes Service는 NetApp이 제어하는 PSA 생산자 프로젝트를 통해 제공됩니다.

CVS-SW의 경우 프로듀서 테넌트는 Google VM을 실행하여 서비스를 제공합니다. 사용자 VM과 Cloud Volumes Service VM 간의 트래픽은 Google에서 자동으로 암호화됩니다.

CVS의 데이터 경로 - 성능은 네트워크 계층에서 완전히 암호화되지 않지만, NetApp과 Google은 이 조합을 사용합니다 "IEEE 802.1AE 암호화(MACSec)", "캡슐화" (데이터 암호화) 및 물리적으로 제한된 네트워크를 통해 Cloud Volumes Service CVS - 성능 서비스 유형과 Google 클라우드 간에 전송 중인 데이터를 보호합니다.

NAS 프로토콜

NFS 및 SMB NAS 프로토콜은 프로토콜 계층에서 선택적 전송 암호화를 제공합니다.

SMB 암호화

"SMB 암호화" SMB 데이터의 엔드 투 엔드 암호화를 제공하고 신뢰할 수 없는 네트워크에서 데이터를 도청하지 못하도록 보호합니다. 클라이언트/서버 데이터 연결(SMB3.x 가능 클라이언트에만 사용 가능)과 서버/도메인 컨트롤러 인증에 대해 암호화를 설정할 수 있습니다.

SMB 암호화가 활성화된 경우 암호화를 지원하지 않는 클라이언트는 공유에 액세스할 수 없습니다.

Cloud Volumes Service는 SMB 암호화를 위한 RC4-HMAC, AES-128-CTS-HMAC-SHA1 및 AES-256-CTS-HMAC-SHA1 보안 암호를 지원합니다. SMB는 서버에서 지원되는 가장 높은 암호화 유형으로 협상합니다.

NFSv4.1 Kerberos

NFSv4.1의 경우 CVS - 성능은 에서 설명한 대로 Kerberos 인증을 제공합니다 "RFC7530". 볼륨별로 Kerberos를 활성화할 수 있습니다.

Kerberos에서 현재 가장 강력한 암호화 유형은 AES-256-CTS-HMAC-SHA1입니다. NetApp Cloud Volumes Service는 NFS용 AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 및 DES를 지원합니다. 또한 CIFS/SMB 트래픽에 대해 ARCFOUR-HMAC(RC4)를 지원하지만 NFS에는 지원하지 않습니다.

Kerberos는 Kerberos 보안의 강화 방법을 선택할 수 있는 NFS 마운트에 대해 세 가지 서로 다른 보안 수준을 제공합니다.

RedHat에 따름 "일반 마운트 옵션" 설명서:

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

일반적으로 Kerberos 보안 수준이 많을수록 클라이언트와 서버가 전송된 각 패킷의 NFS 작업을 암호화하고 해독하는 데 시간을 소비하므로 성능이 저하됩니다. 많은 클라이언트와 NFS 서버가 AES-NI 오프로딩을 CPU에 지원하므로 전반적인 환경이 개선되지만 Kerberos 5p(전체 엔드 투 엔드 암호화)의 성능 영향은 Kerberos 5(사용자 인증)의 영향보다 훨씬 큽니다.

다음 표에서는 보안 및 성능에 대한 각 수준의 차이점을 보여 줍니다.

보안 수준	보안	성능
NFSv3 - 시스템	• 최소 보안, 숫자 사용자 ID/그룹 ID가 있는 일반 텍스트 • UID, GID, 클라이언트 IP 주소, 내보내기 경로, 파일 이름, 패킷 캡처의 권한	• 대부분의 경우에 적합합니다
NFSv4.x - 시스템	• NFSv3(클라이언트 ID, 이름 문자열/도메인 문자열 일치)보다 더 안전하지만 여전히 일반 텍스트입니다 • UID, GID, 클라이언트 IP 주소, 이름 문자열, 도메인 ID를 볼 수 있습니다. 패킷 캡처의 내보내기 경로, 파일 이름, 권한	• 순차적 워크로드(예: VM, 데이터베이스, 대용량 파일)에 적합 • 파일 개수가 많음/메타데이터 많음(30~50% 악화)

보안 수준	보안	성능
NFS — krb5	• 모든 NFS 패킷의 자격 증명에 대한 Kerberos 암호화 - GSS 래퍼의 RPC 호출에서 사용자 /그룹의 UID/GID를 래핑합니다 • 마운트 액세스를 요청하는 사용자는 유효한 Kerberos 티켓(사용자 이름/암호 또는 수동 키 탭 교환)이 필요합니다. 티켓은 지정된 기간 후에 만료되며 사용자는 액세스를 위해 다시 인증해야 합니다 • 마운트/portmapper/NLM 같은 NFS 작업 또는 보조 프로토콜에 대한 암호화 없음(내보내기 경로, IP 주소, 파일 핸들, 권한, 파일 이름 패킷 캡처의 atime/mtime)	• Kerberos의 경우 대부분 최상, AUTH_SYS보다 나쁨
NFS — krb5i	• 모든 NFS 패킷의 자격 증명에 대한 Kerberos 암호화 - GSS 래퍼의 RPC 호출에서 사용자 /그룹의 UID/GID를 래핑합니다 • 마운트 액세스를 요청하는 사용자는 유효한 Kerberos 티켓(사용자 이름/암호 또는 수동 키 탭 교환)이 필요합니다. 티켓은 지정된 기간 후에 만료되며 사용자는 액세스를 위해 다시 인증해야 합니다 • 마운트/portmapper/NLM 같은 NFS 작업 또는 보조 프로토콜에 대한 암호화 없음(내보내기 경로, IP 주소, 파일 핸들, 권한, 파일 이름 패킷 캡처의 atime/mtime) • Kerberos GSS 체크섬은 패킷을 가로챌 수 없도록 모든 패킷에 추가됩니다. 체크섬이 일치하면 대화가 허용됩니다.	• NFS 페이로드가 암호화되지 않기 때문에 krb5p보다 낫습니다. krb5와 비교하여 추가된 오버헤드만 무결성 체크섬입니다. krb5i의 성능은 krb5보다 훨씬 나쁘지는 않지만 약간의 성능 저하가 발생할 수 있습니다.

보안 수준	보안	성능
NFS – krb5p	• 모든 NFS 패킷의 자격 증명에 대한 Kerberos 암호화 - GSS 래퍼의 RPC 호출에서 사용자 /그룹의 UID/GID를 래핑합니다 • 마운트 액세스를 요청하는 사용자는 유효한 Kerberos 티켓(사용자 이름/암호 또는 수동 키 탭 교환)이 필요합니다. 티켓은 지정된 기간 이후에 만료되며 사용자는 액세스를 위해 다시 인증해야 합니다 • 모든 NFS 패킷 페이로드는 GSS 래퍼로 암호화됩니다(패킷 캡처에서 파일 핸들, 권한, 파일 이름, atime/mtime을 볼 수 없음). • 무결성 검사를 포함합니다. • NFS 작업 유형이 표시됩니다(FSINFO, ACCESS, GETATTR 등). • 보조 프로토콜(마운트, 포트 맵, NLM 등)이 암호화되지 않음 - (내보내기 경로, IP 주소 확인 가능)	• 보안 수준의 최악의 성능: krb5p는 더 많은 암호화/암호 해독을 해야 합니다. • 파일 개수가 많은 워크로드에 대해 NFSv4.x를 사용할 경우 krb5p보다 성능이 더 우수합니다.

Cloud Volumes Service에서 구성된 Active Directory 서버는 Kerberos 서버 및 LDAP 서버로 사용됩니다(RFC2307 호환 스키마에서 사용자 ID를 조회하기 위해). 다른 Kerberos 또는 LDAP 서버는 지원되지 않습니다. Cloud Volumes Service에서 ID 관리를 위해 LDAP를 사용하는 것이 좋습니다. NFS Kerberos가 패킷 캡처에 표시되는 방법에 대한 자세한 내용은 섹션을 참조하십시오 ""패킷 감지/추적 고려 사항""

유휴 데이터 암호화

Cloud Volumes Service의 모든 볼륨은 AES-256 암호화를 사용하여 유휴 상태로 암호화되므로 미디어에 기록된 모든 사용자 데이터가 암호화되며 볼륨당 키를 통해서만 해독할 수 있습니다.

- CVS-SW의 경우 Google에서 생성한 키가 사용됩니다.
- CVS - 성능의 경우 볼륨별 키는 Cloud Volumes Service에 내장된 키 관리자에 저장됩니다.

2021년 11월부터 CMEK(고객 관리 암호화 키) 기능을 미리 볼 수 있습니다. 이렇게 하면 에서 호스팅되는 프로젝트별, 지역별 마스터 키를 사용하여 볼륨별 키를 암호화할 수 있습니다 "Google KMS(키 관리 서비스)." KMS를 사용하면 외부 키 관리자를 연결할 수 있습니다.

CVS용 KMS 구성 - 성능에 대한 자세한 내용은 을 참조하십시오 "고객이 관리하는 암호화 키 설정".

방화벽

Cloud Volumes Service는 NFS 및 SMB 공유를 지원하기 위해 여러 TCP 포트를 노출합니다.

- "NFS 액세스에 필요한 포트 수"
- "SMB 액세스에 필요한 포트"

또한 Kerberos를 비롯한 LDAP를 지원하는 SMB, NFS 및 이중 프로토콜 구성을 사용하려면 Windows Active Directory 도메인에 대한 액세스가 필요합니다. Active Directory 연결은 이어야 합니다 "구성됨" 지역별로 제공됩니다. Active Directory 도메인 컨트롤러(DC)는 를 사용하여 식별합니다 "DNS 기반 DC 검색" 지정된 DNS 서버를 사용합니다. 반환된 DC 중 하나가 사용됩니다. Active Directory 사이트를 지정하면 자격 있는 DC 목록을 제한할 수 있습니다.

Cloud Volumes Service는 와 함께 할당된 CIDR 범위의 IP 주소를 사용하여 에 도달합니다 `gcloud compute address` 명령을 실행하는 동안 "Cloud Volumes Service에 대한 온보딩". 이 CIDR을 소스 주소로 사용하여 Active Directory 도메인 컨트롤러에 대한 인바운드 방화벽을 구성할 수 있습니다.

Active Directory 도메인 컨트롤러가 필요합니다 "여기에 설명된 대로 Cloud Volumes Service CIDR에 포트를 노출합니다".

NAS 프로토콜

NAS 프로토콜 개요

NAS 프로토콜에는 NFS(v3 및 v4.1) 및 SMB/CIFS(2.x 및 3.x)가 포함됩니다. 이러한 프로토콜은 CVS에서 여러 NAS 클라이언트 간에 데이터에 대한 공유 액세스를 허용하는 방법입니다. 또한 Cloud Volumes Service는 NFS 및 SMB/CIFS 클라이언트(이중 프로토콜)에 대한 액세스를 동시에 제공하는 동시에 NAS 공유의 파일 및 폴더에 대한 모든 ID 및 권한 설정을 존중할 수 있습니다. Cloud Volumes Service는 가장 높은 데이터 전송 보안을 유지하기 위해 SMB 암호화 및 NFS Kerberos 5p를 사용하여 전송 중인 프로토콜 암호화를 지원합니다.

ⓘ 이중 프로토콜은 CVS에서 사용할 수 있습니다. - 성능만 지원됩니다.

NAS 프로토콜의 기본 사항

NAS 프로토콜은 여러 클라이언트의 네트워크 상에서 Cloud Volumes Service on GCP와 같은 스토리지 시스템의 동일한 데이터에 액세스하는 방법입니다. NFS 및 SMB는 정의된 NAS 프로토콜로, Cloud Volumes Service이 서버 역할을 하는 클라이언트/서버 단위로 작동합니다. 클라이언트는 서버에 액세스, 읽기 및 쓰기 요청을 보내고, 서버는 파일에 대한 잠금 메커니즘을 조정하고, 사용 권한을 저장하고, ID 및 인증 요청을 처리할 책임이 있습니다.

예를 들어, NAS 클라이언트가 폴더에 새 파일을 생성하려는 경우 다음과 같은 일반 프로세스가 적용됩니다.

1. 클라이언트가 서버에 디렉터리(권한, 소유자, 그룹, 파일 ID, 사용 가능한 공간, 등). 서버는 요청한 클라이언트 및 사용자에게 상위 폴더에 대한 필요한 권한이 있는 경우 해당 정보로 응답합니다.
2. 디렉토리의 사용 권한이 액세스를 허용할 경우 클라이언트는 생성 중인 파일 이름이 파일 시스템에 이미 있는지 서버에 묻습니다. 파일 이름이 이미 사용 중인 경우 생성이 실패합니다. 파일 이름이 없는 경우 서버는 클라이언트가 계속 진행할 수 있음을 알려 줍니다.
3. 클라이언트는 디렉토리 핸들 및 파일 이름으로 파일을 만들기 위해 서버에 대한 호출을 수행하고 액세스 및 수정 시간을 설정합니다. 서버에서 파일에 고유한 파일 ID를 발급하여 동일한 파일 ID로 다른 파일이 생성되지 않도록 합니다.

4. 클라이언트는 쓰기 작업 전에 파일 특성을 확인하는 호출을 전송합니다. 권한이 허용하는 경우 클라이언트는 새 파일을 씁니다. 프로토콜/응용 프로그램에서 잠금을 사용하는 경우 클라이언트는 다른 클라이언트가 잠금 상태에서 파일에 액세스하지 못하도록 서버에 잠금을 요청합니다. 잠금 상태에서는 데이터 손상을 방지할 수 있습니다.

NFS 를 참조하십시오

NFS는 RFC(Request for Comments)에 정의된 공개 IETF 표준인 분산 파일 시스템 프로토콜로, 누구나 프로토콜을 구현할 수 있도록 합니다.

Cloud Volumes Service의 볼륨은 클라이언트 또는 클라이언트 세트에 액세스할 수 있는 경로를 내보내 NFS 클라이언트에 공유됩니다. 이러한 내보내기를 마운트할 수 있는 권한은 Cloud Volumes Service 관리자가 구성할 수 있는 내보내기 정책 및 규칙에 의해 정의됩니다.

NetApp NFS 구현은 프로토콜의 골드 표준으로 간주되며 수많은 엔터프라이즈 NAS 환경에서 사용됩니다. 다음 섹션에서는 NFS와 Cloud Volumes Service에서 사용할 수 있는 특정 보안 기능 및 구현 방법에 대해 설명합니다.

기본 로컬 **UNIX** 사용자 및 그룹

Cloud Volumes Service에는 다양한 기본 기능을 위한 여러 기본 UNIX 사용자 및 그룹이 포함되어 있습니다. 이러한 사용자 및 그룹은 현재 수정 또는 삭제할 수 없습니다. 현재 새 로컬 사용자 및 그룹을 Cloud Volumes Service에 추가할 수 없습니다. 기본 사용자 및 그룹 외부의 UNIX 사용자 및 그룹은 외부 LDAP 이름 서비스에서 제공해야 합니다.

다음 표에서는 기본 사용자 및 그룹과 해당 숫자 ID를 보여 줍니다. LDAP 또는 이러한 숫자 ID를 다시 사용하는 로컬 클라이언트에서는 새 사용자 또는 그룹을 생성하지 않는 것이 좋습니다.

기본 사용자**:** 숫자 **ID**	기본 그룹**:** 숫자 **ID**
• 루트: 0 • pcuser: 65534 • 아무도 없다: 65535	• 루트: 0 • 데몬: 1 • pcuser: 65534 • 아무도 없다: 65535

NFSv4.1을 사용하는 경우 NFS 클라이언트에서 디렉토리 목록 명령을 실행할 때 루트 사용자가 아무도 표시되지 않을 수 있습니다. 이는 클라이언트의 ID 도메인 매핑 구성 때문입니다. 의 섹션을 참조하십시오 NFSv4.1 및 그 누구도 사용자/그룹을 대상으로 하지 않습니다 이 문제에 대한 자세한 내용 및 해결 방법을 확인하십시오.

루트 사용자입니다

Linux에서 루트 계정은 Linux 기반 파일 시스템의 모든 명령, 파일 및 폴더에 액세스할 수 있습니다. 이 계정의 강력한 기능 때문에 보안 모범 사례에 따라 루트 사용자를 비활성화하거나 제한해야 하는 경우가 많습니다. NFS 내보내기에서 루트 사용자가 파일과 폴더에 가지고 있는 파워는 내보내기 정책과 규칙, 루트 스쿼시(root squash)라는 개념을 통해 Cloud Volumes Service에서 제어할 수 있습니다.

루트 스쿼싱 기능을 사용하면 NFS 마운트에 액세스하는 루트 사용자가 익명 숫자 사용자 65534에 스쿼트됩니다(“ 섹션 참조)익명 사용자") 및 은(는) 현재 CVS - Performance를 사용하는 경우에만 사용할 수 있습니다. 이 경우 내보내기 정책 규칙 생성 중 루트 액세스에 대해 Off를 선택합니다. 루트 사용자가 익명 사용자에게 스쿼트되면 chown 또는 을 실행할 수 있는 액세스 권한이 더 이상 없습니다 "setuid/setgid 명령(고정 비트)" NFS 마운트의 파일 또는 폴더와 루트 사용자가 생성한 파일 또는 폴더에 anon UID가 소유자/그룹으로 표시됩니다. 또한 루트 사용자가 NFSv4 ACL을

수정할 수 없습니다. 그러나 루트 사용자는 chmod 및 삭제된 파일에 대한 명시적 권한이 없는 액세스 권한을 계속 가집니다. 루트 사용자의 파일 및 폴더 권한에 대한 액세스를 제한하려면 NTFS ACL을 사용하여 볼륨을 사용하고, "root"라는 Windows 사용자를 생성하고, 파일 또는 폴더에 원하는 권한을 적용하는 것이 좋습니다.

익명 사용자

익명(anon) 사용자 ID는 유효한 NFS 자격 증명 없이 도착하는 클라이언트 요청에 매핑된 UNIX 사용자 ID 또는 사용자 이름을 지정합니다. 여기에는 루트 스쿼싱 사용 시 루트 사용자가 포함될 수 있습니다. Cloud Volumes Service의 anon 사용자는 65534입니다.

이 UID는 일반적으로 Linux 환경의 사용자 이름 'nobody' 또는 'nfsnobody'와 관련이 있습니다. Cloud Volumes Service는 로컬 UNIX 사용자 ' pcuser ' 로 65534도 사용합니다(" 절 참조)기본 로컬 UNIX 사용자 및 그룹"). LDAP에서 일치하는 유효한 UNIX 사용자를 찾을 수 없는 경우 Windows에서 UNIX로의 이름 매핑의 기본 대체 사용자입니다.

Linux의 사용자 이름과 UID 65534의 Cloud Volumes Service 간 사용자 이름 차이로 인해 65534에 매핑된 사용자의 이름 문자열이 NFSv4.1을 사용할 때 일치하지 않을 수 있습니다. 따라서 일부 파일 및 폴더에 대해 사용자로 'nobody'가 표시될 수 있습니다. 자세한 내용은 " 단원을 참조하십시오NFSv4.1 및 그 누구도 사용자/그룹을 대상으로 하지 않습니다"를 참조하십시오.

액세스 제어/내보내기

NFS 마운트에 대한 초기 엑스포트/공유 액세스는 엑스포트 정책 내에 포함된 호스트 기반 엑스포트 정책 규칙을 통해 제어됩니다. 호스트 IP, 호스트 이름, 서브넷, 넷그룹 또는 도메인이 정의되어 NFS 공유를 마운트하는 액세스 권한과 호스트에 허용되는 액세스 수준을 허용합니다. 엑스포트 정책 규칙 구성 옵션은 Cloud Volumes Service 레벨에 따라 다릅니다.

CVS-SW의 경우 내보내기 정책 구성에 다음 옵션을 사용할 수 있습니다.

- * 클라이언트 일치. * 쉼표로 구분된 IP 주소 목록, 쉼표로 구분된 호스트 이름, 서브넷, 넷그룹, 도메인 이름 목록.
- * RO/RW 액세스 규칙 * 내보내기에 대한 액세스 수준을 제어하려면 읽기/쓰기 또는 읽기 전용 을 선택합니다. CVS - 성능은 다음 옵션을 제공합니다.
- * 클라이언트 일치. * 쉼표로 구분된 IP 주소 목록, 쉼표로 구분된 호스트 이름, 서브넷, 넷그룹, 도메인 이름 목록.
- * RO/RW 액세스 규칙. * 읽기/쓰기 또는 읽기 전용 을 선택하여 내보내기에 대한 액세스 수준을 제어합니다.
- * 루트 액세스(켜기/끄기). * 루트 스쿼시를 구성합니다(" 절 참조)루트 사용자입니다"를 참조하십시오.)
- * Protocol type. * 이 옵션은 NFS 마운트에 대한 액세스를 특정 프로토콜 버전으로 제한합니다. 볼륨에 대해 NFSv3과 NFSv4.1을 모두 지정할 때 두 확인란을 모두 비워 두거나 두 확인란을 모두 선택합니다.
- * Kerberos 보안 수준(Kerberos 활성화 가 선택된 경우). * 읽기 전용 또는 읽기-쓰기 액세스에 대해 krb5, krb5i 및/또는 krb5p의 옵션을 제공합니다.

변경 소유권**(chown)** 및 변경 그룹**(chgrp)**

Cloud Volumes Service의 NFS에서는 루트 사용자만 파일 및 폴더에 대해 chown/chgrp를 실행할 수 있습니다. 다른 사용자는 자신이 소유한 파일에서도 'Operation not mitted(작업이 허용되지 않음)' 오류를 볼 수 있습니다. 루트 스쿼시를 사용하는 경우(" 섹션에서 다룹니다루트 사용자입니다"), 루트가 비루트 사용자에게 스쿼트되고 chown 및 chgrp에 대한 액세스가 허용되지 않습니다. 현재 Cloud Volumes Service에는 루트 이외의 사용자에 대한 chown 및 chgrp를 허용하는 대안이 없습니다. 소유권을 변경해야 하는 경우 이중 프로토콜 볼륨을 사용하고 보안 스타일을 NTFS로 설정하여 Windows 측의 권한을 제어할 수 있습니다.

권한 관리

Cloud Volumes Service는 모드 비트(예: rwx의 경우 644, 777 등)와 NFSv4.1 ACL을 모두 지원하여 UNIX 보안 스타일을 사용하는 볼륨의 NFS 클라이언트에 대한 사용 권한을 제어합니다. 이러한 사용자(chmod, chown 또는 nfs4_setfacl 등)에 대해 표준 권한 관리가 사용되며 이를 지원하는 모든 Linux 클라이언트와 함께 작동합니다.

또한 NTFS로 설정된 이중 프로토콜 볼륨을 사용하는 경우 NFS 클라이언트는 Windows 사용자에 대한 Cloud Volumes Service 이름 매핑을 활용할 수 있으며, 이 이름 매핑은 NTFS 권한을 확인하는 데 사용됩니다. Cloud Volumes Service를 Windows 사용자 이름에 올바르게 매핑하려면 유효한 UNIX 사용자 이름이 필요하기 때문에 이를 위해서는 Cloud Volumes Service에 대한 LDAP 연결이 필요합니다.

NFSv3에 대한 세부적인 **ACL** 제공

모드 비트 사용 권한은 소유자, 그룹 및 다른 모든 관련자만 사용할 수 있습니다. 즉, 기본 NFSv3에 대해 세부적인 사용자 액세스 제어를 사용할 수 없습니다. Cloud Volumes Service는 POSIX ACL 또는 확장된 특성(예: chattr)을 지원하지 않으므로 NFSv3을 사용하는 다음 시나리오에서만 세분화된 ACL을 사용할 수 있습니다.

- 유효한 UNIX와 Windows 사용자 간 매핑을 사용하는 NTFS 보안 스타일 볼륨(CIFS 서버 필요)
- NFSv4.1 ACL은 관리 클라이언트 마운트 NFSv4.1을 사용하여 ACL을 적용하여 적용됩니다.

두 방법 모두 UNIX ID 관리를 위한 LDAP 연결과 유효한 UNIX 사용자 및 그룹 정보를 채워야 합니다(섹션 참조) ""LDAP"") 및 은 CVS - 성능 인스턴스에서만 사용할 수 있습니다. NFS에서 NTFS 보안 스타일 볼륨을 사용하려면 SMB 연결이 구성되어 있지 않더라도 이중 프로토콜(SMB 및 NFSv3) 또는 이중 프로토콜(SMB 및 NFSv4.1)을 사용해야 합니다. NFSv3 마운트에서 NFSv4.1 ACL을 사용하려면 프로토콜 유형으로 'both(NFSv3/NFSv4.1)'를 선택해야 합니다.

일반 UNIX 모드 비트는 NTFS 또는 NFSv4.x ACL이 제공하는 사용 권한과 동일한 수준의 세분성을 제공하지 않습니다. 다음 표에서는 NFSv3 모드 비트와 NFSv4.1 ACL 간의 사용 권한 세분화를 비교합니다. NFSv4.1 ACL에 대한 자세한 내용은 을 참조하십시오 "NFS4_ACL-NFSv4 액세스 제어 목록".

NFSv3 모드 비트	NFSv4.1 ACL
• 실행 시 사용자 ID를 설정합니다 • 실행 시 그룹 ID를 설정합니다 • 바꾼 텍스트 저장(POSIX에 정의되지 않음) • 소유자에 대한 읽기 권한 • 소유자의 쓰기 권한 • 파일의 소유자에 대한 권한을 실행하거나 디렉터리에서 소유자를 찾기(검색) 권한을 실행합니다 • 그룹에 대한 읽기 권한 • 그룹에 대한 쓰기 권한 • 파일의 그룹에 대한 권한을 실행하거나 디렉터리의 그룹에 대한 검색 권한을 찾습니다 • 다른 사람의 읽기 권한 • 다른 사람에 대한 권한을 작성합니다 • 파일의 다른 사람에 대한 권한을 실행하거나 디렉터리에서 다른 사람에 대한 검색 권한을 찾습니다	ACE(액세스 제어 항목) 형식(허용/거부/감사) * 상속 플래그 * directory-inherit * file-inherit * no-propagate-inherit * inherit-only 권한 * 읽기-데이터(파일)/목록-디렉토리(디렉토리) * 쓰기-데이터(파일)/생성-파일(디렉토리) * 추가-데이터(파일)/생성-하위 디렉토리(디렉토리) * 실행(파일)/변경-디렉토리(디렉토리) * 삭제 * delete-child * read-attributes * write-named-attributes * write-named-acner-write-write-acl-write-write-write-write-acl-write-write-write-write-acl-write-write-write-write-

마지막으로, RPC 패킷 제한에 따라 NFS 그룹 멤버 자격(NFSv3 및 NFSv4.x에서 모두)은 AUTH_SYS에 대한 기본값 최대 16으로 제한됩니다. NFS Kerberos는 최대 32개의 그룹과 NFSv4 ACL을 제공하므로 사용자 및 그룹 ACL(ACE당 최대 1024개 항목)을 세부적으로 적용하여 제한을 제거할 수 있습니다.

또한 Cloud Volumes Service는 지원되는 최대 그룹을 32개까지 확장할 수 있도록 확장된 그룹 지원을 제공합니다. 이를 위해서는 유효한 UNIX 사용자 및 그룹 ID가 포함된 LDAP 서버에 대한 LDAP 연결이 필요합니다. 이 구성을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오 "NFS 볼륨 생성 및 관리" Google 문서.

NFSv3 사용자 및 그룹 ID

NFSv3 사용자 및 그룹 ID는 이름이 아닌 숫자 ID로 와이어를 통해 제공됩니다. Cloud Volumes Service는 NFSv3을 사용하는 이러한 숫자 ID에 대해 사용자 이름 확인을 수행하지 않으며 UNIX 보안 스타일 볼륨에서는 모드 비트만 사용합니다. NFSv4.1 ACL이 있으면 NFSv3을 사용하더라도 ACL을 제대로 해결하려면 숫자 ID 조회 및/또는 이름 문자열 조회가 필요합니다. NTFS 보안 스타일 볼륨에서 Cloud Volumes Service는 유효한 UNIX 사용자로 숫자 ID를 확인한 다음 유효한 Windows 사용자에게 매핑하여 액세스 권한을 협상해야 합니다.

NFSv3 사용자 및 그룹 ID의 보안 제한

NFSv3에서는 클라이언트와 서버가 숫자 ID로 읽기 또는 쓰기를 시도하는 사용자가 유효한 사용자인지 확인할 필요가 없으며 암시적으로 신뢰됩니다. 이렇게 하면 숫자 ID를 스푸핑하여 파일 시스템이 잠재적 위반으로 열립니다. 이와 같은 보안 문제를 방지하기 위해 Cloud Volumes Service에서 몇 가지 옵션을 사용할 수 있습니다.

- NFS용 Kerberos를 구현하면 사용자가 사용자 이름 및 암호 또는 keytab 파일로 인증하여 Kerberos 티켓을 받아 마운트에 액세스할 수 있도록 합니다. Kerberos는 CVS에서 사용 가능 - 성능 인스턴스와 NFSv4.1에서만 지원됩니다.
- 엑스포트 정책 규칙에 따라 호스트 목록을 제한하면 NFSv3 클라이언트가 Cloud Volumes Service 볼륨에 액세스할 수 있는 범위가 제한됩니다.

- 이중 프로토콜 볼륨을 사용하고 NTFS ACL을 볼륨에 적용하면 NFSv3 클라이언트가 숫자 ID를 유효한 UNIX 사용자 이름으로 확인하게 되어 액세스 마운트에 대한 올바른 인증이 필요합니다. 이를 위해서는 LDAP를 설정하고 UNIX 사용자 및 그룹 ID를 구성해야 합니다.
- 루트 사용자를 스쿼팅하면 루트 사용자가 NFS 마운트에 수행할 수 있는 손상을 제한하지만 위험을 완전히 제거할 수는 없습니다. 자세한 내용은 " 단원을 참조하십시오루트 사용자입니다."

궁극적으로 NFS 보안은 고객이 제공하는 프로토콜 버전으로 제한됩니다. NFSv3은 일반적으로 NFSv4.1보다 더 우수한 성능을 제공하지만, 같은 수준의 보안을 제공하지 않습니다.

NFSv4.1

NFSv4.1은 NFSv3과 비교할 때 다음과 같은 이유로 더욱 뛰어난 보안 및 안정성을 제공합니다.

- 임대 기반 메커니즘을 통한 통합 잠금
- 상태 저장 세션
- 단일 포트에서 모든 NFS 기능 지원(2049)
- TCP 전용
- ID 도메인 매핑
- Kerberos 통합(NFSv3은 Kerberos 사용 가능, NFS에만 해당, NLM 같은 보조 프로토콜에는 사용할 수 없음)

NFSv4.1 종속성

NFSv4.1의 추가 보안 기능 덕분에 NFSv3을 사용할 필요가 없는 몇 가지 외부 의존성이 발생했습니다(Active Directory와 같은 SMB의 의존도 필요 방식과 유사).

NFSv4.1 ACL

Cloud Volumes Service는 NFSv4.x ACL을 지원하므로 다음과 같은 일반적인 POSIX 스타일 사용 권한에 비해 뚜렷한 이점을 제공합니다.

- 파일 및 디렉토리에 대한 사용자 액세스를 세부적으로 제어
- NFS 보안 강화
- CIFS/SMB와의 상호 운용성 향상
- AUTH_SYS 보안을 사용하여 사용자당 16개 그룹의 NFS 제한을 제거합니다
- ACL은 GID(Group ID) 확인이 필요하지 않으므로 GID 리무진을 효과적으로 제거할 수 있습니다. 따라서 Cloud Volumes Service가 아닌 NFS 클라이언트에서 ACL을 제어할 수 있습니다. NFSv4.1 ACL을 사용하려면 클라이언트의 소프트웨어 버전이 이를 지원하고 적절한 NFS 유틸리티가 설치되어 있어야 합니다.

NFSv4.1 ACL과 **SMB** 클라이언트 간의 호환성

NFSv4 ACL은 Windows 파일 레벨 ACL(NTFS ACL)과 다르지만 유사한 기능을 제공합니다. 그러나 멀티 프로토콜 NAS 환경에서 NFSv4.1 ACL이 있고 동일한 데이터 세트의 NFS 및 SMB(이중 프로토콜 액세스)를 사용 중인 경우에는 SMB2.0 이상을 사용하는 클라이언트에서 Windows 보안 탭의 ACL을 보거나 관리할 수 없습니다.

NFSv4.1 ACL의 작동 방식

참고로 다음 용어가 정의되어 있습니다.

- * 액세스 제어 목록(ACL). * 권한 항목의 목록입니다.
- * ACE(액세스 제어 항목).* 목록에 있는 권한 항목.

SetAttr 작업 중에 클라이언트가 파일에서 NFSv4.1 ACL을 설정하면 Cloud Volumes Service는 개체에 해당 ACL을 설정하여 기존 ACL을 대체합니다. 파일에 ACL이 없으면 파일에 대한 모드 권한은 owner@, group@ 및 everyone@에서 계산됩니다. 파일에 기존 SUID/SGID/고정 비트가 있으면 영향을 받지 않습니다.

GETATTR 작업 중에 클라이언트가 파일에서 NFSv4.1 ACL을 받으면 Cloud Volumes Service는 오브젝트와 연결된 NFSv4.1 ACL을 읽고 ACE 목록을 생성하고 목록을 클라이언트에 반환합니다. 파일에 NT ACL 또는 모드 비트가 있는 경우 ACL은 모드 비트에서 구성되며 클라이언트로 반환됩니다.

ACL에 거부 ACE가 있는 경우 액세스가 거부되고 ACE 허용 이 있는 경우 액세스가 부여됩니다. 그러나 ACL에 ACE가 없는 경우에도 액세스가 거부됩니다.

보안 설명자는 SACL(보안 ACL) 및 DACL(임의 ACL)으로 구성됩니다. NFSv4.1이 CIFS/SMB와 상호 운용될 경우 DACL은 NFSv4와 CIFS에 매핑된 일대일 매핑입니다. DACL은 allow 및 deny ACE로 구성됩니다.

NFSv4.1 ACL이 설정된 파일 또는 폴더에서 기본적인 "chmod"를 실행하면 기존 사용자 및 그룹 ACL이 유지되지만 기본 소유자 @, group@, everyone@acls는 수정됩니다.

NFSv4.1 ACL을 사용하는 클라이언트는 시스템의 파일 및 디렉토리에 대한 ACL을 설정하고 볼 수 있습니다. ACL이 있는 디렉터리에 새 파일이나 하위 디렉터리가 만들어지면 해당 개체는 해당 ACL로 태그가 지정된 ACL의 모든 ACE를 상속합니다 "상속 플래그".

파일 또는 디렉토리에 NFSv4.1 ACL이 있으면 해당 ACL을 사용하여 파일 또는 디렉토리에 액세스하는 데 사용되는 프로토콜에 관계없이 액세스를 제어할 수 있습니다.

파일 및 디렉토리는 ACE에 올바른 상속 플래그가 지정된 경우 상위 디렉토리의 NFSv4 ACL에서 ACE를 상속합니다(적절한 수정 사항이 있을 수 있음).

NFSv4 요청의 결과로 파일 또는 디렉토리가 생성되면 결과 파일 또는 디렉토리의 ACL은 파일 생성 요청에 ACL이 포함되어 있는지 또는 표준 UNIX 파일 액세스 권한만 포함되는지에 따라 달라집니다. ACL은 상위 디렉토리에 ACL이 있는지 여부에도 따라 달라집니다.

- 요청에 ACL이 포함된 경우 해당 ACL이 사용됩니다.
- 요청에 표준 UNIX 파일 액세스 권한만 있고 상위 디렉토리에 ACL이 없는 경우 클라이언트 파일 모드를 사용하여 표준 UNIX 파일 액세스 권한을 설정합니다.
- 요청에 표준 UNIX 파일 액세스 권한만 있고 상위 디렉토리에 상속할 수 없는 ACL이 있는 경우, 요청에 전달된 모드 비트를 기반으로 하는 기본 ACL이 새 개체에 설정됩니다.
- 요청에 표준 UNIX 파일 액세스 권한만 포함되어 있지만 상위 디렉토리에 ACL이 있는 경우 ACE에 적절한 상속 플래그가 지정된 경우 상위 디렉토리의 ACL에 있는 ACE는 새 파일 또는 디렉토리에 의해 상속됩니다.

ACE 권한

NFSv4.1 ACL 사용 권한은 일련의 대문자 및 소문자 값('rxtncy' 등)을 사용하여 액세스를 제어합니다. 이러한 문자 값에 대한 자세한 내용은 을 참조하십시오 "방법: NFSv4 ACL 사용".

umask 및 **ACL** 상속을 사용하는 **NFSv4.1 ACL** 동작

"NFSv4 ACL을 사용하면 ACL 상속을 제공할 수 있습니다". ACL 상속은 NFSv4.1 ACL이 설정된 개체 아래에 생성된 파일 또는 폴더가 의 구성에 따라 ACL을 상속할 수 있음을 의미합니다 "ACL 상속 플래그입니다".

"umask(umask" 관리자 개입 없이 디렉터리에서 파일과 폴더를 만들 수 있는 권한 수준을 제어하는 데 사용됩니다. 기본적으로 Cloud Volumes Service에서는 umask 가 에 따라 예상되는 동작을 나타내는 상속된 ACL을 재정의할 수 있도록 합니다 "RFC 5661".

ACL 형식 지정

NFSv4.1 ACL에는 특정한 형식이 있습니다. 다음은 파일에 설정된 ACE 예제입니다.

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

앞의 예제는 의 ACL 형식 지침을 따릅니다.

```
type:flags:principal:permissions
```

A의 유형은 "허용"을 의미합니다. 이 경우 보안 주체가 그룹이 아니며 상속을 포함하지 않으므로 상속 플래그가 설정되지 않습니다. 또한 ACE는 감사 항목이 아니므로 감사 플래그를 설정할 필요가 없습니다. NFSv4.1 ACL에 대한 자세한 내용은 을 참조하십시오 "http://linux.die.net/man/5/nfs4_acl".

NFSv4.1 ACL이 제대로 설정되지 않았거나 클라이언트 및 서버에서 이름 문자열을 확인할 수 없는 경우 ACL이 예상대로 작동하지 않거나 ACL 변경이 적용되지 않고 오류가 발생할 수 있습니다.

샘플 오류에는 다음이 포함됩니다.

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

명시적 거부

NFSv4.1 권한에는 소유자, 그룹 및 모든 사용자에 대한 명시적 거부 특성이 포함될 수 있습니다. 따라서 NFSv4.1 ACL은 기본적으로 -deny를 사용하기 때문에 ACL이 명시적으로 ACE에 의해 부여되지 않으면 거부됩니다. 명시적 거부 특성은 액세스 ACE를 명시적 또는 명시적으로 재정의합니다.

거부 ACE는 Ddes 특성 태그로 설정됩니다.

아래 예에서 group@은 모든 읽기 및 실행 권한을 허용하지만 모든 쓰기 액세스는 거부됩니다.

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

거부 ACE는 혼란스럽고 복잡할 수 있으므로 가능하면 피해야 합니다. 명시적으로 정의되지 않은 ACL 허용 은 암시적으로 거부됩니다. 거부 ACE가 설정되면 사용자에게 액세스 권한이 부여될 것으로 예상되는 경우 액세스가 거부될 수 있습니다.

앞의 ACE 집합은 모드 비트에서 755와 동일하며, 이는 다음을 의미합니다.

- 소유자에게는 모든 권한이 있습니다.
- 그룹은 읽기 전용입니다.
- 다른 사람들은 읽기 전용입니다.

그러나 사용 권한이 775 상응 권한으로 조정되더라도 모든 사용자에 대해 명시적 거부 설정이 설정되어 있으므로 액세스가 거부될 수 있습니다.

NFSv4.1 ID 도메인 매핑 종속성

NFSv4.1은 ID 도메인 매핑 논리를 보안 계층으로 활용하여 NFSv4.1 마운트에 액세스하려는 사용자가 실제로 자신들이 주장하는 사용자인지 확인합니다. 이 경우 NFSv4.1 클라이언트에서 들어오는 사용자 이름 및 그룹 이름에 이름 문자열이 추가되고 Cloud Volumes Service 인스턴스로 보내집니다. 사용자 이름/그룹 이름 및 ID 문자열 조합이 일치하지 않으면 사용자 및/또는 그룹이 클라이언트의 '/etc/idmapd.conf' 파일에 지정된 기본 nobody 사용자로 충돌합니다.

이 ID 문자열은 특히 NFSv4.1 ACL 및/또는 Kerberos를 사용하는 경우 적절한 권한 준수를 위한 요구 사항입니다. 따라서 적절한 사용자 및 그룹 이름 ID 확인을 위해 클라이언트와 Cloud Volumes Service 간에 일관성을 유지하기 위해 LDAP 서버와 같은 이름 서비스 서버 종속성이 필요합니다.

Cloud Volumes Service는 정적 기본 ID 도메인 이름 값인 ddefaultv4iddomain.com 를 사용합니다. NFS 클라이언트는 ID 도메인 이름 설정에 대해 DNS 도메인 이름으로 기본 설정되지만, '/etc/idmapd.conf'에서 ID 도메인 이름을 수동으로 조정할 수 있습니다.

Cloud Volumes Service에서 LDAP가 활성화된 경우 Cloud Volumes Service는 NFS ID 도메인을 자동화하여 DNS에서 검색 도메인에 대해 구성된 대로 변경할 수 있으며, 다른 DNS 도메인 검색 이름을 사용하지 않는 한 클라이언트를 수정할 필요가 없습니다.

Cloud Volumes Service가 로컬 파일 또는 LDAP에서 사용자 이름 또는 그룹 이름을 확인할 수 있는 경우 도메인 문자열이 사용되고 일치하지 않는 도메인 ID는 아무도 입력할 수 없습니다. Cloud Volumes Service가 로컬 파일 또는 LDAP에서 사용자 이름 또는 그룹 이름을 찾을 수 없는 경우 숫자 ID 값이 사용되며 NFS 클라이언트가 이름을 제대로 확인합니다(NFSv3 동작과 유사).

클라이언트의 NFSv4.1 ID 도메인을 Cloud Volumes Service 볼륨에서 사용 중인 도메인과 일치하도록 변경하지 않고도 다음과 같은 동작이 발생합니다.

- 로컬 UNIX 사용자 및 그룹에 정의된 루트와 같이 Cloud Volumes Service에 로컬 항목이 있는 UNIX 사용자 및 그룹이 nobody 값으로 스쿼트됩니다.
- LDAP에 항목이 있는 UNIX 사용자 및 그룹(Cloud Volumes Service가 LDAP를 사용하도록 구성된 경우)은 DNS 도메인이 NFS 클라이언트와 Cloud Volumes Service 간에 서로 다른 경우 아무도 사용하지 않습니다.
- 로컬 항목이나 LDAP 항목이 없는 UNIX 사용자 및 그룹은 숫자 ID 값을 사용하고 NFS 클라이언트에 지정된 이름으로 확인합니다. 클라이언트에 이름이 없으면 숫자 ID만 표시됩니다.

다음은 이전 시나리오의 결과입니다.

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

클라이언트 및 서버 ID 도메인이 일치하면 동일한 파일 목록이 표시됩니다.

```
# ls -la
total 8
drwxr-xr-x 2 root   root          4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root          4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835          9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

이 문제와 해결 방법에 대한 자세한 내용은 " 절을 참조하십시오NFSv4.1 및 그 누구도 사용자/그룹을 대상으로 하지 않습니다."

Kerberos 종속성

NFS에서 Kerberos를 사용하려면 Cloud Volumes Service에서 다음 권한이 있어야 합니다.

- Kerberos KDC(메일 센터 서비스)용 Active Directory 도메인
- LDAP 기능에 대한 UNIX 정보로 채워진 사용자 및 그룹 속성이 있는 Active Directory 도메인(Cloud Volumes Service의 NFS Kerberos에는 적절한 기능을 위해 사용자 SPN-UNIX 사용자 매핑이 필요합니다.)
- Cloud Volumes Service 인스턴스에 대해 LDAP가 설정되었습니다
- DNS 서비스에 대한 Active Directory 도메인입니다

NFSv4.1 및 그 누구도 사용자/그룹을 대상으로 하지 않습니다

NFSv4.1 구성에서 가장 흔히 발생하는 문제 중 하나는 'user:group'의 'nobody:nobody'의 조합으로 'ls'를 사용하여 파일 또는 폴더가 목록에 표시되는 것입니다.

예를 들면 다음과 같습니다.

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

숫자 ID는 99입니다.

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

경우에 따라 파일의 소유자가 올바르지만 '아무도'가 그룹에 표시되지 않을 수 있습니다.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

아무도 없나요?

NFSv4.1의 'nobody' 사용자는 nfsnobody 사용자와 다릅니다. "id" 명령을 실행하여 NFS 클라이언트가 각 사용자를 보는 방법을 볼 수 있습니다.

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

NFSv4.1에서는 'nobody' 사용자가 'idmapd.conf' 파일에 정의된 기본 사용자이며 사용할 모든 사용자로 정의할 수 있습니다.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

이 문제가 발생하는 이유는 무엇입니까?

이름 문자열 매핑을 통한 보안은 NFSv4.1 작업의 핵심 요소이므로 이름 문자열이 제대로 일치하지 않을 때 기본 동작은 일반적으로 사용자와 그룹이 소유한 파일 및 폴더에 액세스할 수 없는 사용자에게 스쿼시를 하는 것입니다.

파일 목록에서 사용자 및/또는 그룹에 대해 'nobody'가 표시되는 경우 이는 일반적으로 NFSv4.1에서 잘못 구성된 항목이 있음을 의미합니다. 케이스 민감도는 여기에서 확인할 수 있습니다.

예를 들어 user1@CVSDEMO.LOCA L(uid 1234, gid 1234)이 내보내기에 액세스하는 경우 Cloud Volumes Service에서 user1@CVSDEMO.LOCA L(uid 1234, gid 1234)을 찾을 수 있어야 합니다. Cloud Volumes Service의 사용자가 USER1@CVSDEMO.LOCA L인 경우 일치하지 않습니다(대문자 user1과 소문자 user1 비교). 대부분의 경우 클라이언트의 메시지 파일에서 다음을 볼 수 있습니다.

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

클라이언트와 서버는 모두 사용자가 실제로 자신이 주장하는 사람이라는 데 동의해야 합니다. 따라서 클라이언트가 보는 사용자에게 Cloud Volumes Service가 보는 사용자와 동일한 정보가 있는지 확인하려면 다음을 확인해야 합니다.

- * NFSv4.x ID domain. * Client:'idmapd.conf' file; Cloud Volumes Service는 defaultv4iddomain.com 파일을 사용하며 수동으로 변경할 수 없습니다. NFSv4.1과 함께 LDAP를 사용하는 경우 Cloud Volumes Service는 ID 도메인을 AD 도메인과 동일한 DNS 검색 도메인이 사용 중인 것으로 변경합니다.
- * 사용자 이름 및 숫자 ID. * 이 옵션은 클라이언트가 사용자 이름을 찾는 위치를 결정하고 이름 서비스 스위치 구성(client: ' nsswitch.conf' 및/또는 로컬 passwd 및 group 파일)을 활용합니다. Cloud Volumes Service는 이를 수정할 수 없지만 활성화된 경우 구성에 LDAP를 자동으로 추가합니다.
- * 그룹 이름 및 숫자 ID. * 이 옵션은 클라이언트가 그룹 이름을 찾는 위치를 결정하고 이름 서비스 스위치 구성(client: ' nsswitch.conf' 및/또는 로컬 passwd 및 group 파일)을 활용합니다. Cloud Volumes Service는 이를 수정할 수 없지만 활성화된 경우 구성에 LDAP를 자동으로 추가합니다.

거의 모든 경우에 클라이언트의 사용자 및 그룹 목록에 'nobody'가 표시되면 Cloud Volumes Service와 NFS 클라이언트 간의 사용자 또는 그룹 이름 도메인 ID 변환입니다. 이 시나리오를 방지하려면 LDAP를 사용하여 클라이언트와 Cloud Volumes Service 간의 사용자 및 그룹 정보를 확인합니다.

클라이언트의 **NFSv4.1**에 대한 이름 **ID** 문자열을 보는 중입니다

NFSv4.1을 사용하는 경우 앞서 설명한 대로 NFS 작업 중에 이름 문자열 매핑이 발생합니다.

NFSv4 ID에 대한 문제를 찾기 위해 '/var/log/messages'를 사용하는 것 외에도 을 사용할 수 있습니다 "nfsidmap -l" NFSv4 도메인에 올바르게 매핑된 사용자 이름을 보려면 NFS 클라이언트에서 명령을 실행하십시오.

예를 들어, 이 명령은 클라이언트에서 찾을 수 있는 사용자 및 Cloud Volumes Service가 NFSv4.x 마운트에 액세스하는 이후의 명령 출력입니다.

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

NFSv4.1 ID 도메인(이 경우, 즉 NetApp-user)에 제대로 매핑되지 않는 사용자가 동일한 마운트에 액세스하여 파일을 만지려고 하면 'nobody:nobody'가 예상한 대로 할당됩니다.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

nfsidmap-l 출력에서는 디스플레이에 사용자 pcuser가 표시되지만 NetApp-user는 표시되지 않습니다. 이는 엑스포트 정책 규칙('65534')의 익명 사용자입니다.

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

중소기업

"중소기업" 는 이더넷 네트워크를 통해 여러 SMB 클라이언트에 중앙 집중식 사용자/그룹 인증, 권한, 잠금 및 파일 공유를 제공하는 Microsoft에서 개발한 네트워크 파일 공유 프로토콜입니다. 파일 및 폴더는 다양한 공유 속성으로 구성할 수 있고 공유 수준 권한을 통해 액세스 제어를 제공하는 공유를 통해 클라이언트에 제공됩니다. SMB는 Windows, Apple 및 Linux 클라이언트를 비롯하여 프로토콜을 지원하는 모든 클라이언트에 제공될 수 있습니다.

Cloud Volumes Service는 SMB 2.1 및 3.x 버전의 프로토콜을 지원합니다.

액세스 제어/**SMB** 공유

- Windows 사용자 이름이 Cloud Volumes Service 볼륨에 대한 액세스를 요청하면 Cloud Volumes Service는 Cloud Volumes Service 관리자가 구성한 방법을 사용하여 UNIX 사용자 이름을 찾습니다.
- 외부 UNIX ID 공급자(LDAP)가 구성되어 있고 Windows/UNIX 사용자 이름이 동일한 경우 Windows 사용자 이름은 추가 구성 없이 1:1을 UNIX 사용자 이름으로 매핑합니다. LDAP가 설정되면 Active Directory를 사용하여 사용자 및 그룹 객체에 대한 UNIX 속성을 호스팅합니다.
- Windows 이름과 UNIX 이름이 동일하게 일치하지 않으면 Cloud Volumes Service에서 LDAP 이름 매핑 구성을

사용할 수 있도록 LDAP를 구성해야 합니다(섹션 참조) ""비대칭 이름 매핑에 LDAP 사용"")를 클릭합니다.

- LDAP를 사용하지 않는 경우 Windows SMB 사용자는 Cloud Volumes Service의 기본 로컬 UNIX 사용자 "pcuser"로 매핑됩니다. 즉, 멀티프로토콜 NAS 환경에서 pcuser로 매핑되는 사용자가 Windows에서 작성한 파일이 UNIX 소유권을 pcuser로 표시합니다. 여기에 있는 'pcuser'는 사실상 리눅스 환경(UID 65534)의 'nobody' 사용자입니다.

SMB만 사용하는 배포에서는 "pcuser" 매핑이 계속 발생하지만 Windows 사용자 및 그룹 소유권이 올바르게 표시되고 SMB 전용 볼륨에 대한 NFS 액세스가 허용되지 않으므로 문제가 되지 않습니다. 또한 SMB 전용 볼륨은 생성된 후 NFS 또는 이중 프로토콜 볼륨으로의 전환을 지원하지 않습니다.

Windows는 Active Directory 도메인 컨트롤러에서 사용자 이름 인증에 Kerberos를 사용합니다. 이 경우 AD DC와 사용자 이름/암호 교환이 필요하며 이는 Cloud Volumes Service 인스턴스 외부에 있습니다. Kerberos 인증은 SMB 클라이언트가 '\\서버 이름' UNC 경로를 사용하는 경우 사용되며 다음 조건이 적용됩니다.

- 서버 이름 에 대한 DNS A/AAAA 항목이 있습니다
- SMB/CIFS 액세스에 유효한 SPN이 SERVERNAME에 존재합니다

Cloud Volumes Service SMB 볼륨이 생성되면 섹션에 정의된 대로 시스템 계정 이름이 생성됩니다 ""Cloud Volumes Service가 Active Directory에 표시되는 방식"" Cloud Volumes Service는 DDNS(동적 DNS)를 활용하여 DNS에 필요한 A/AAAA 및 PTR 항목을 생성하고 시스템 계정 보안 주체에 필요한 SPN 항목을 생성하기 때문에 해당 시스템 계정 이름도 SMB 공유 액세스 경로가 됩니다.

PTR 항목을 작성하려면 Cloud Volumes Service 인스턴스 IP 주소에 대한 역방향 조회 영역이 DNS 서버에 있어야 합니다.

예를 들어, 이 Cloud Volumes Service 볼륨은 '\\cvs-east-433d.cvsdemo.local' UNC 공유 경로를 사용합니다.

Active Directory에서는 Cloud Volumes Service에서 생성한 SPN 항목이 다음과 같습니다.

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

DNS 정방향/역방향 조회 결과입니다.

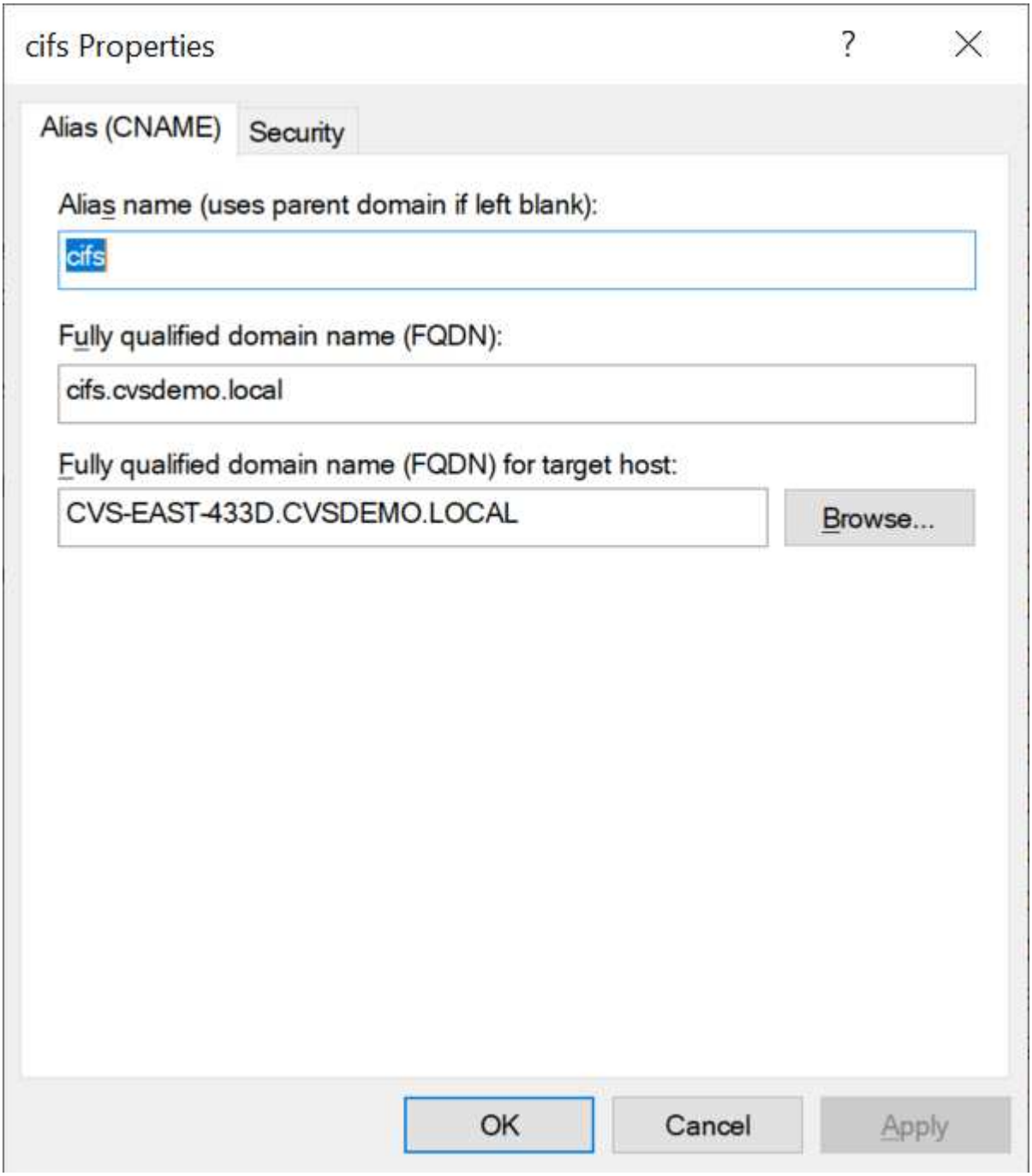
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

선택적으로 Cloud Volumes Service에서 SMB 공유에 대한 SMB 암호화를 설정/요구하여 더 많은 액세스 제어를 적용할 수 있습니다. 엔드포인트 중 하나가 SMB 암호화를 지원하지 않는 경우 액세스가 허용되지 않습니다.

SMB 이름 별칭 사용

경우에 따라 최종 사용자가 Cloud Volumes Service에 사용 중인 컴퓨터 계정 이름을 알아야 하는 보안 문제가 발생할 수 있습니다. 또는 최종 사용자에게 더 간단한 액세스 경로를 제공하려는 경우도 있습니다. 이 경우 SMB 별칭을 생성할 수 있습니다.

SMB 공유 경로에 대한 별칭을 만들려는 경우 DNS에서 CNAME 레코드로 알려진 별칭을 활용할 수 있습니다. 예를 들어 이름이 \\cvs-east-433d.cvssdemo.local이 아닌 공유에 액세스하기 위해 \\cifs"를 사용하되 Kerberos 인증을 계속 사용하려면 기존 A/AAAA 레코드를 가리키는 DNS의 CNAME과 기존 컴퓨터 계정에 추가된 추가 SPN이 Kerberos 액세스를 제공합니다.



CNAME을 추가한 후 생성되는 DNS 정방향 조회 결과입니다.

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

새 SPN을 추가한 후 생성되는 SPN 쿼리입니다.

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

패킷 캡처에서는 CNAME에 연결된 SPN을 사용하여 세션 설정 요청을 볼 수 있습니다.

```
431 4.156722                                    SMB2     308 Negotiate Protocol Response
432 4.156785                                    SMB2     232 Negotiate Protocol Request
434 4.158108                                    SMB2     374 Negotiate Protocol Response
435 4.160977                                    SMB2    1978 Session Setup Request
437 4.166224                                    SMB2     322 Session Setup Response
438 4.166891                                    SMB2     152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2     138 Tree Connect Response
```

```
realm: CVSDEMO.LOCAL
sname
    name-type: kRB5-NT-SRV-INST (2)
    sname-string: 2 items
        SNameString: cifs
        SNameString: cifs
enc-part
    etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

SMB 인증 방언

Cloud Volumes Service는 다음을 지원합니다 "방언" SMB 인증의 경우:

- LM
- NTLM
- NTLMv2
- Kerberos

SMB 공유 액세스를 위한 Kerberos 인증은 사용할 수 있는 가장 안전한 인증 수준입니다. AES 및 SMB 암호화를 활성화하면 보안 수준이 더욱 높아집니다.

또한 Cloud Volumes Service는 LM 및 NTLM 인증에 대한 이전 버전과의 호환성을 지원합니다. Kerberos가 잘못 구성된 경우(예: SMB 별칭 생성 시), 공유 액세스는 NTLMv2와 같은 취약한 인증 방법으로 되돌아갑니다. 이러한 메커니즘은 보안성이 떨어지기 때문에 일부 Active Directory 환경에서는 비활성화됩니다. 취약한 인증 방법을 사용하지 않도록 설정하고 Kerberos를 제대로 구성하지 않으면 다시 사용할 유효한 인증 방법이 없기 때문에 공유 액세스가 실패합니다.

Active Directory에서 지원되는 인증 수준을 구성/보는 방법에 대한 자세한 내용은 을 참조하십시오 "네트워크 보안: LAN Manager 인증 레벨".

권한 모델

NTFS/파일 권한

NTFS 권한은 NTFS 로직을 따르는 파일 시스템의 파일 및 폴더에 적용되는 권한입니다. 기본 또는 고급 에서 NTFS 권한을 적용할 수 있으며 액세스 제어를 위해 허용 또는 거부 로 설정할 수 있습니다.

기본 사용 권한은 다음과 같습니다.

- 모든 권한
- 수정
- 읽기 및 실행
- 읽기
- 쓰기

ACE라고 하는 사용자 또는 그룹에 대한 사용 권한을 설정하면 ACL에 상주합니다. NTFS 권한은 UNIX 모드 비트와 동일한 읽기/쓰기/실행 기본 사항을 사용하지만 소유권 가져오기, 폴더 만들기/데이터 추가, 속성 쓰기 등과 같은 보다 세분화된 확장 액세스 제어(특수 권한이라고도 함)로 확장할 수도 있습니다.

표준 UNIX 모드 비트는 NTFS 권한과 동일한 수준의 세분화 수준을 제공하지 않습니다(예: ACL에서 개별 사용자 및 그룹 개체에 대한 권한을 설정하거나 확장 속성을 설정할 수 있음). 그러나 NFSv4.1 ACL은 NTFS ACL과 동일한 기능을 제공합니다.

NTFS 권한은 공유 권한보다 더 구체적이며 공유 권한과 함께 사용할 수 있습니다. NTFS 권한 구조에서는 가장 제한적인 권한이 적용됩니다. 따라서 사용자 또는 그룹에 대한 명시적 변명의 경우 액세스 권한을 정의할 때 전체 제어보다 우선합니다.

NTFS 권한은 Windows SMB 클라이언트에서 제어됩니다.

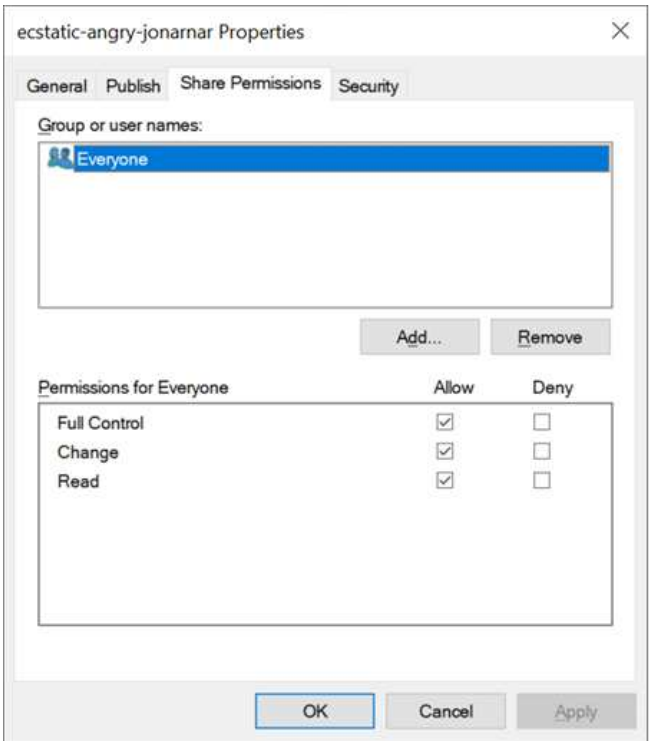
공유 권한

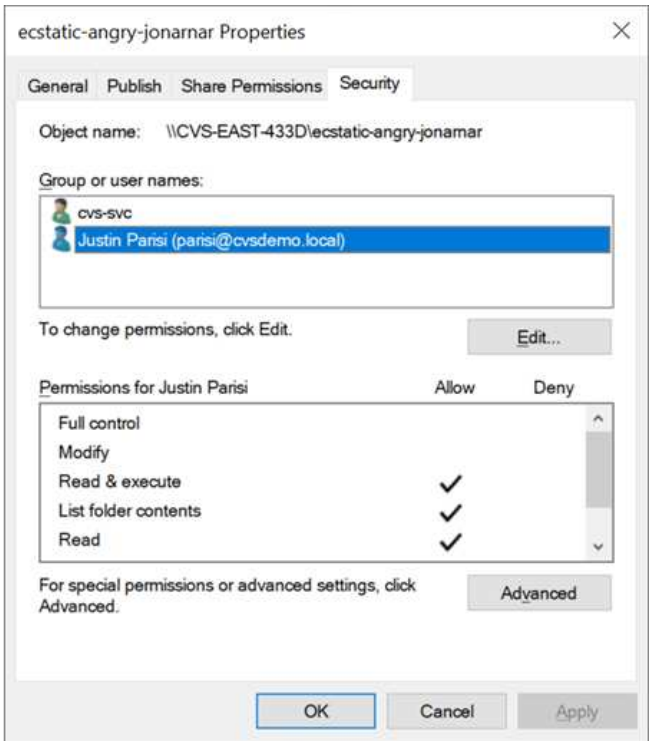
공유 권한은 NTFS 권한(읽기/변경/모든 제어만 해당)보다 더 일반적이며, SMB 공유의 초기 항목을 제어합니다. 이는 NFS 내보내기 정책 규칙의 작동 방식과 유사합니다.

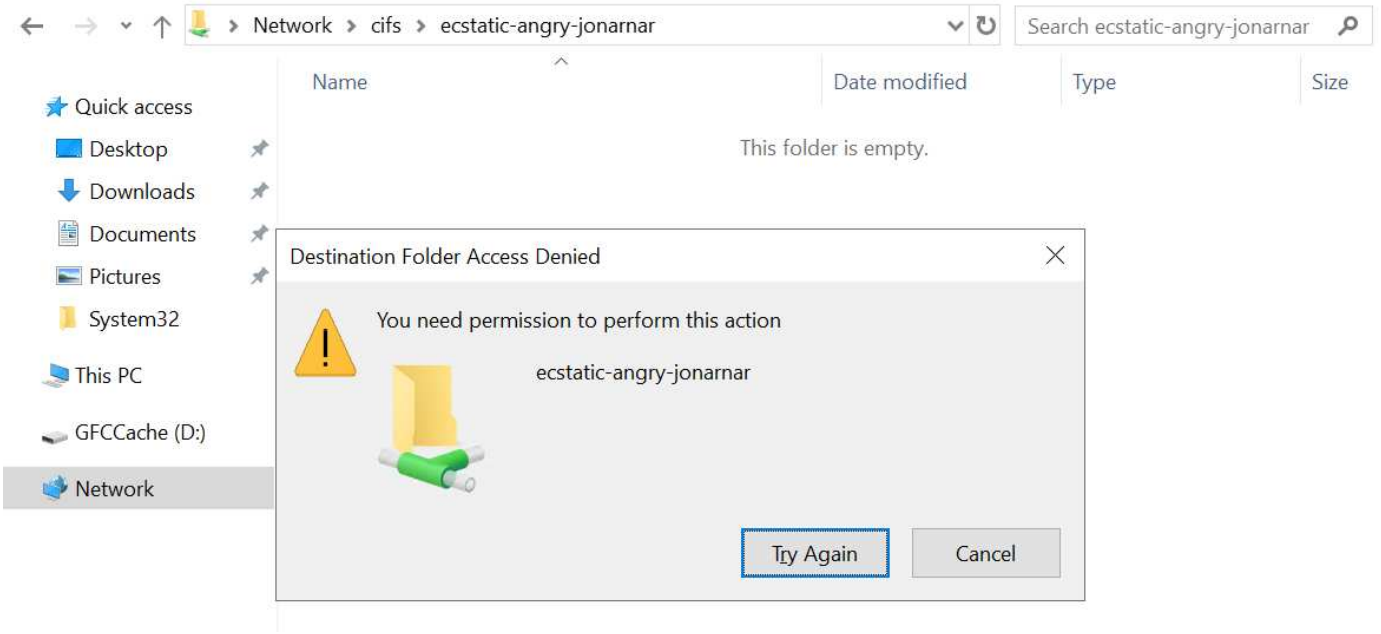
NFS 내보내기 정책 규칙은 IP 주소 또는 호스트 이름과 같은 호스트 기반 정보를 통해 액세스를 제어하지만 SMB 공유 권한은 공유 ACL에서 사용자 및 그룹 ACE를 사용하여 액세스를 제어할 수 있습니다. Windows 클라이언트 또는 Cloud Volumes Service 관리 UI에서 공유 ACL을 설정할 수 있습니다.

기본적으로 공유 ACL 및 초기 볼륨 ACL에는 모든 권한이 있는 모든 사용자가 포함됩니다. 파일 ACL은 변경되어야 하지만 공유 권한은 공유의 객체에 대한 파일 권한에 의해 무시됩니다.

예를 들어, 사용자가 Cloud Volumes Service 볼륨 파일 ACL에 대한 읽기 액세스만 허용되는 경우 다음 그림과 같이 공유 ACL이 모든 권한이 있는 사용자로 설정되어 있어도 파일 및 폴더 생성에 대한 액세스가 거부됩니다.







최상의 보안 결과를 얻으려면 다음을 수행하십시오.

- 공유 및 파일 ACL에서 모든 사용자를 제거하고 대신 사용자 또는 그룹에 대한 공유 액세스를 설정합니다.
- 개별 사용자 대신 그룹을 사용하여 액세스 제어를 수행할 수 있어 관리가 용이하고 그룹 관리를 통해 ACL을 공유할 사용자를 더 빠르게 제거/추가할 수 있습니다.
- 공유 권한에 있는 ACE에 대한 덜 제한적이고 보다 일반적인 공유 액세스를 허용하고 보다 세분화된 액세스 제어를 위한 파일 권한을 가진 사용자 및 그룹에 대한 액세스를 잠급니다.
- 명시적 거부 ACL은 ACL 허용 을 재정의하므로 일반적인 사용을 피합니다. 파일 시스템에 대한 액세스를 신속하게 제한해야 하는 사용자 또는 그룹의 명시적 거부 ACL 사용을 제한합니다.
- 에 주의를 기울이십시오 "ACL 상속" 사용 권한을 수정할 때 설정; 파일 수가 많은 디렉토리 또는 볼륨의 최상위

레벨에서 상속 플래그를 설정하면 해당 디렉토리 또는 볼륨 아래의 각 파일에 상속된 사용 권한이 추가되었음을 의미합니다. 의도하지 않은 액세스/거부 및 각 파일이 조정될 때 권한 수정 장기 이탈과 같은 원치 않는 동작이 발생할 수 있습니다.

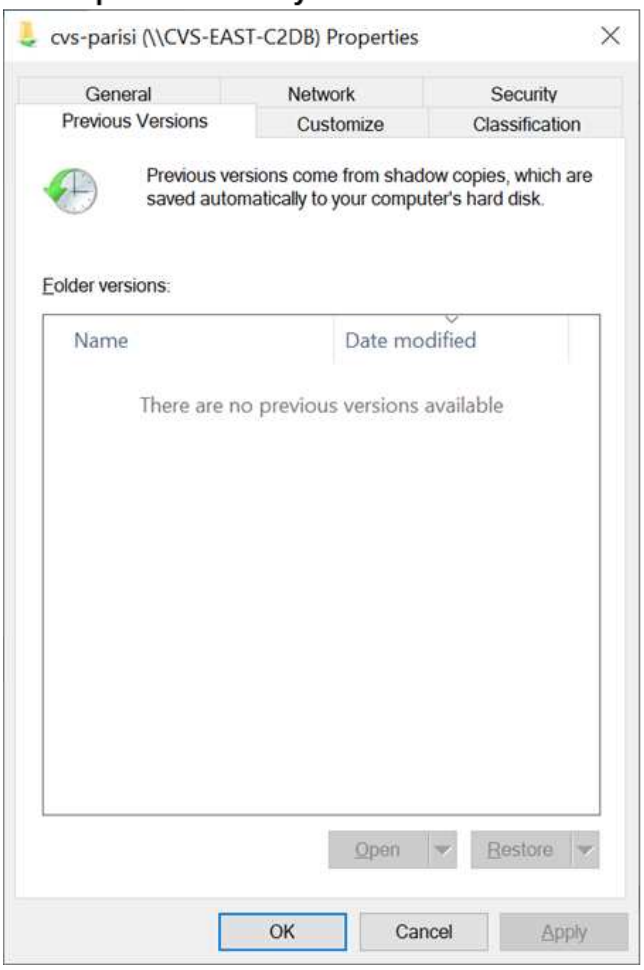
SMB는 보안 기능을 공유합니다

Cloud Volumes Service에서 SMB 액세스가 가능한 볼륨을 처음 생성하면 해당 볼륨을 보호하기 위한 일련의 선택 사항이 표시됩니다.

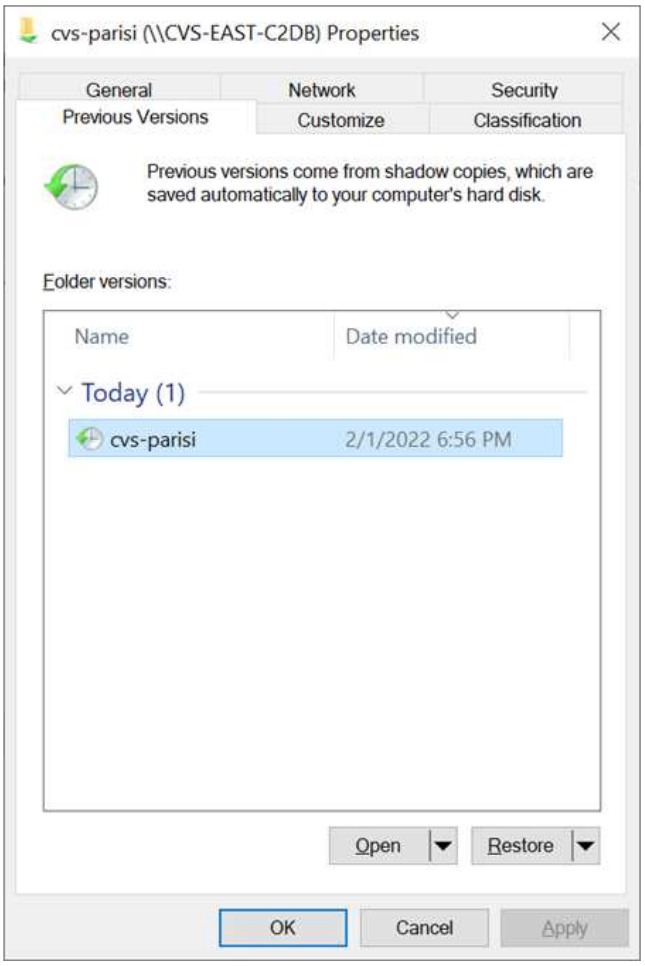
이러한 선택 사항 중 일부는 Cloud Volumes Service 레벨(성능 또는 소프트웨어)에 따라 달라지며 다음과 같은 옵션이 있습니다.

- * 스냅샷 디렉토리를 표시합니다(CVS - 성능 및 CVS - SW 모두에서 사용 가능). * 이 옵션은 SMB 클라이언트가 SMB 공유의 스냅샷 디렉토리에 액세스할 수 있는지 여부를 제어합니다('\\server\share\~snapshot' 및/또는 Previous Versions 탭). 기본 설정은 선택되지 않습니다. 즉, 볼륨이 기본적으로 `~snapshot' 디렉토리에 대한 액세스를 숨기거나 허용하지 않으며 볼륨의 이전 버전 탭에 스냅샷 복사본이 나타나지 않습니다.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



보안 상의 이유, 성능상의 이유(AV 스캔에서 이러한 폴더 숨기기) 또는 기본 설정을 위해 최종 사용자로부터 스냅샷 복사본을 숨기는 것이 좋습니다. Cloud Volumes Service 스냅샷은 읽기 전용이므로 이러한 스냅샷이 표시되는 경우에도 최종 사용자는 스냅샷 디렉토리의 파일을 삭제하거나 수정할 수 없습니다. 스냅샷 복사본이 생성된 시점의 파일 또는 폴더에 대한 파일 권한이 적용됩니다. 파일 또는 폴더의 사용 권한이 Snapshot 복사본 간에 변경되면 변경 내용이 Snapshot 디렉토리의 파일 또는 폴더에도 적용됩니다. 사용자 및 그룹은 권한에 따라 이러한 파일 또는 폴더에 액세스할 수 있습니다. 스냅샷 디렉토리에서 파일을 삭제하거나 수정할 수는 없지만 스냅샷 디렉토리에서 파일 또는 폴더를 복사할 수는 있습니다.

- * SMB 암호화 활성화(CVS - 성능 및 CVS - SW 모두에 사용 가능). * SMB 공유에서 SMB 암호화는 기본적으로 비활성화되어 있습니다(선택 취소됨). 이 확인란을 선택하면 SMB 암호화가 활성화됩니다. 즉, SMB 클라이언트와 서버 간의 트래픽은 협상된 가장 높은 암호화 수준으로 전송 중에 암호화됩니다. Cloud Volumes Service는 SMB에 대해 최대 AES-256 암호화를 지원합니다. SMB 암호화를 활성화하면 SMB 클라이언트에서 성능 저하가 발생할 수 있으며, 이는 대략 10~20% 범위에서 나타날 수도 있고 그렇지 않을 수도 있습니다. 테스트 결과, 성능 저하가 허용 가능한지 여부를 확인하는 것이 좋습니다.
- * SMB 공유 숨기기(CVS - 성능 및 CVS - SW 모두에 사용 가능) * 이 옵션을 설정하면 SMB 공유 경로가 일반 탐색에서 숨겨집니다. 즉, 공유 경로를 모르는 클라이언트는 기본 UNC 경로("\\CVS-SMB" 등)에 액세스할 때 공유를 볼 수 없습니다. 이 확인란을 선택하면 SMB 공유 경로를 명시적으로 알고 있거나 그룹 정책 개체에서 정의한 공유 경로를 가진 클라이언트만 액세스할 수 있습니다(난독 처리를 통한 보안).
- * ABE(액세스 기반 열거) 사용(CVS-SW만 해당). * SMB 공유를 숨기는 것과 비슷하지만, 공유 또는 파일이 개체에 액세스할 권한이 없는 사용자 또는 그룹에서만 숨겨지는 것을 제외하고는 차이가 있습니다. 예를 들어, Windows 사용자 'Joe'가 권한을 통한 읽기 액세스를 최소한 허용하지 않으면 Windows 사용자 'Joe'는 SMB 공유나 파일을 전혀 볼 수 없습니다. 이 기능은 기본적으로 비활성화되어 있으며 확인란을 선택하여 활성화할 수 있습니다. ABE에 대한 자세한 내용은 NetApp 기술 자료 문서를 참조하십시오 "ABE(Access Based Enumeration)는 어떻게 작동합니까?"
- * 지속적으로 사용 가능한(CA) 공유 지원 활성화(CVS - 성능만 해당) * "지속적으로 사용 가능한 SMB 공유" Cloud Volumes Service 백엔드 시스템의 노드 간에 잠금 상태를 복제하여 페일오버 이벤트 중에 애플리케이션 중단을 최소화할 수 있는 방법을 제공합니다. 이 기능은 보안 기능이 아니지만 전반적으로 더 뛰어난 복원력을 제공합니다. 현재 이 기능에는 SQL Server 및 FSLogix 애플리케이션만 지원됩니다.

숨겨진 기본 공유

SMB 서버가 Cloud Volumes Service에서 생성되면 서버가 생성됩니다 "숨겨진 관리 공유" ($ 명명 규칙 사용) - 데이터 볼륨 SMB 공유 이외에 생성됩니다. 여기에는 C$(네임스페이스 액세스) 및 IPC$(Microsoft Management Console(MMC) 액세스에 사용되는 RPC(원격 프로시저 호출)와 같은 프로그램 간 통신을 위한 명명된 파이프 공유)가 포함됩니다.

IPC$ 공유는 공유 ACL을 포함하지 않으며 수정할 수 없습니다. RPC 호출 및 에 엄격하게 사용됩니다 "Windows에서는 기본적으로 이러한 공유에 대한 익명 액세스를 허용하지 않습니다".

C$ 공유는 기본적으로 BUILTIN/Administrators 액세스를 허용하지만, Cloud Volumes Service 자동화는 공유 ACL을 제거하고, C$ 공유에 대한 액세스를 통해 Cloud Volumes Service 파일 시스템에 마운트된 모든 볼륨을 볼 수 있으므로 다른 사람에게 액세스를 허용하지 않습니다. 따라서 '\\server\C$'로 이동하려고 하면 실패합니다.

로컬/**BUILTIN** 관리자/백업 권한이 있는 계정

Cloud Volumes Service SMB 서버는 일부 도메인 사용자 및 그룹에 액세스 권한을 적용하는 로컬 그룹(예: BUILTIN\Administrators)이 있다는 점에서 일반 Windows SMB 서버와 유사한 기능을 유지합니다.

백업 사용자에 추가할 사용자를 지정하면 해당 Active Directory 연결을 사용하는 Cloud Volumes Service 인스턴스의 BUILTIN\Backup Operators 그룹에 사용자가 추가되고 이 그룹에 이 사용자가 추가됩니다 "SeBackupPrivilege 및 SeRestorePrivilege를 참조하십시오".

사용자를 보안 권한 사용자 에 추가하면 사용자에게 SeSecurityPrivilege 가 부여되며, 이 권한은 와 같은 일부 응용 프로그램 사용 사례에 유용합니다 "SMB 공유의 SQL Server".

Backup Users

Provide a comma separated list of domain users or a domain group name that require elevated privileges to access volumes created by Cloud Volumes Service.

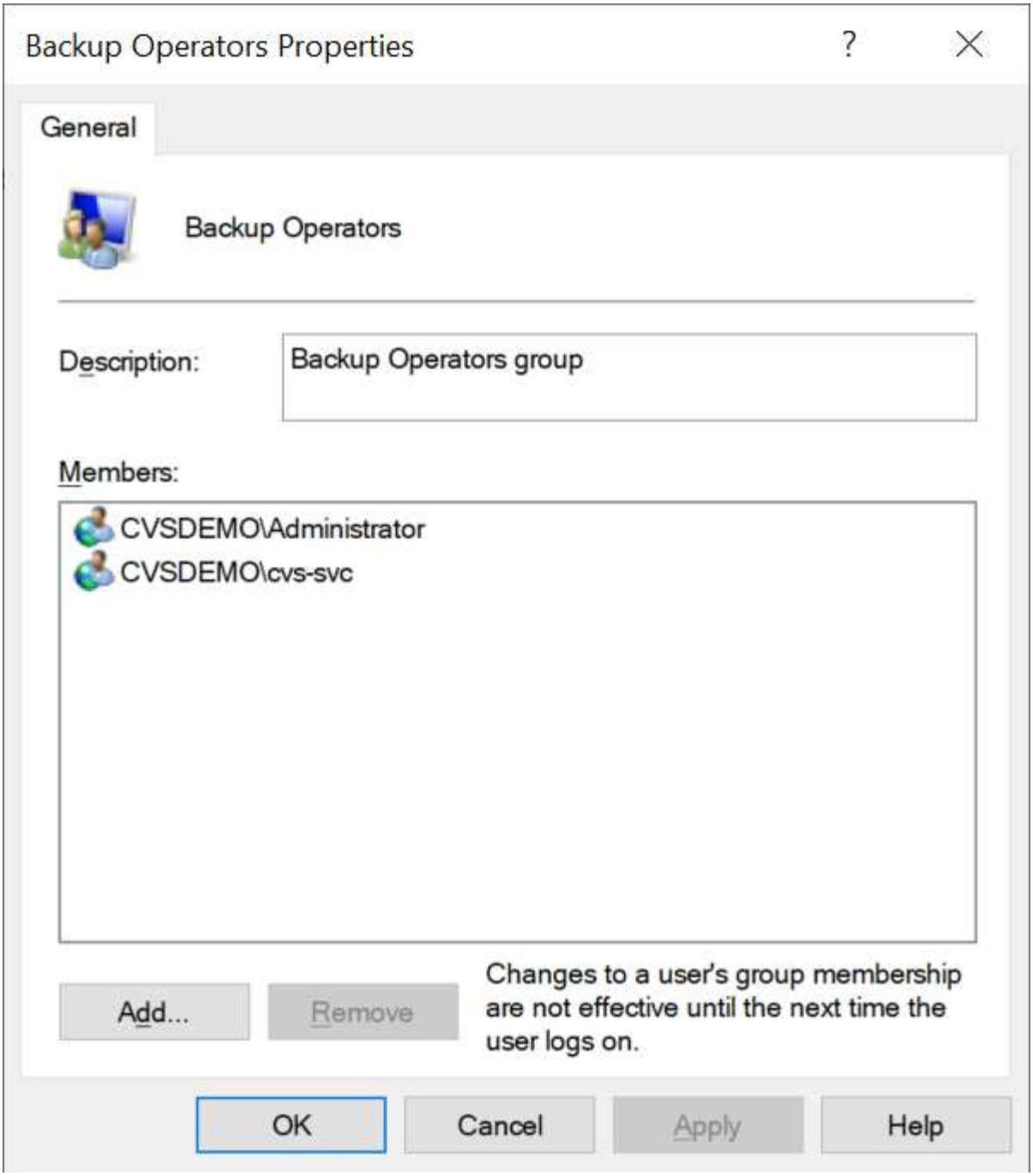
Accountnames
administrator,cvs-svc

Security Privilege Users

Provide a list of comma separated domain user accounts that require elevated privileges to manage security log for the Active Directory associated with Cloud Volumes Service.

Accountnames
administrator,cvs-svc

적절한 권한이 있는 MMC를 통해 Cloud Volumes Service 로컬 그룹 구성원 자격을 볼 수 있습니다. 다음 그림에서는 Cloud Volumes Service 콘솔을 사용하여 추가된 사용자를 보여 줍니다.

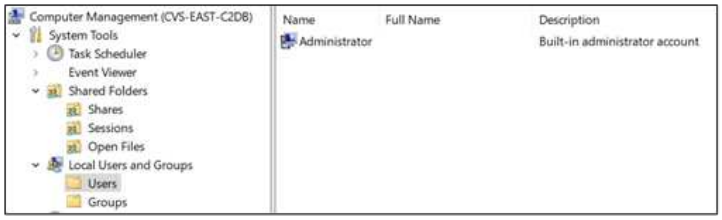


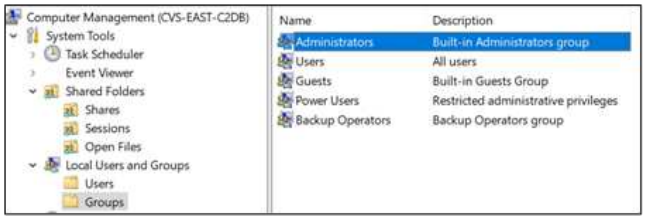
다음 표에서는 기본 BUILTIN 그룹 목록과 기본적으로 추가되는 사용자/그룹을 보여 줍니다.

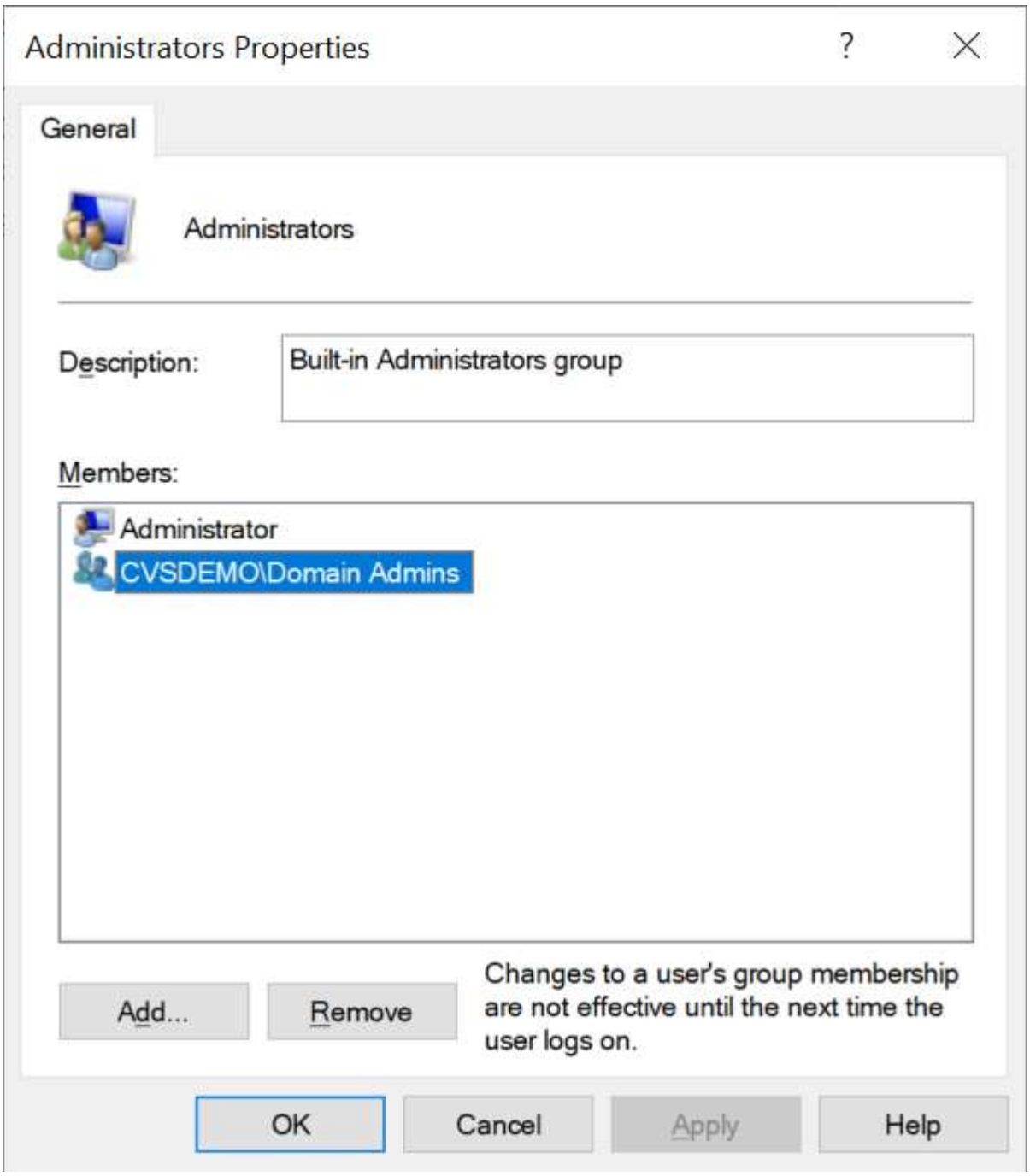
로컬/**BUILTIN** 그룹	기본 멤버
BUILTIN\Administrators *	Domain\Domain Admins입니다
BUILTIN\Backup Operators *	없음
BUILTIN\Guest입니다	도메인\도메인 게스트입니다
BUILTIN\고급 사용자	없음
BUILTIN\도메인 사용자	도메인\도메인 사용자

- Cloud Volumes Service Active Directory 연결 구성에서 그룹 멤버십이 제어됩니다.

MMC 창에서 로컬 사용자 및 그룹(및 그룹 구성원)을 볼 수 있지만 개체를 추가 또는 삭제하거나 이 콘솔에서 그룹 구성원을 변경할 수는 없습니다. 기본적으로 도메인 관리자 그룹 및 관리자만 Cloud Volumes Service의 BUILTIN\Administrators 그룹에 추가됩니다. 현재 수정할 수 없습니다.







MMC/컴퓨터 관리 액세스

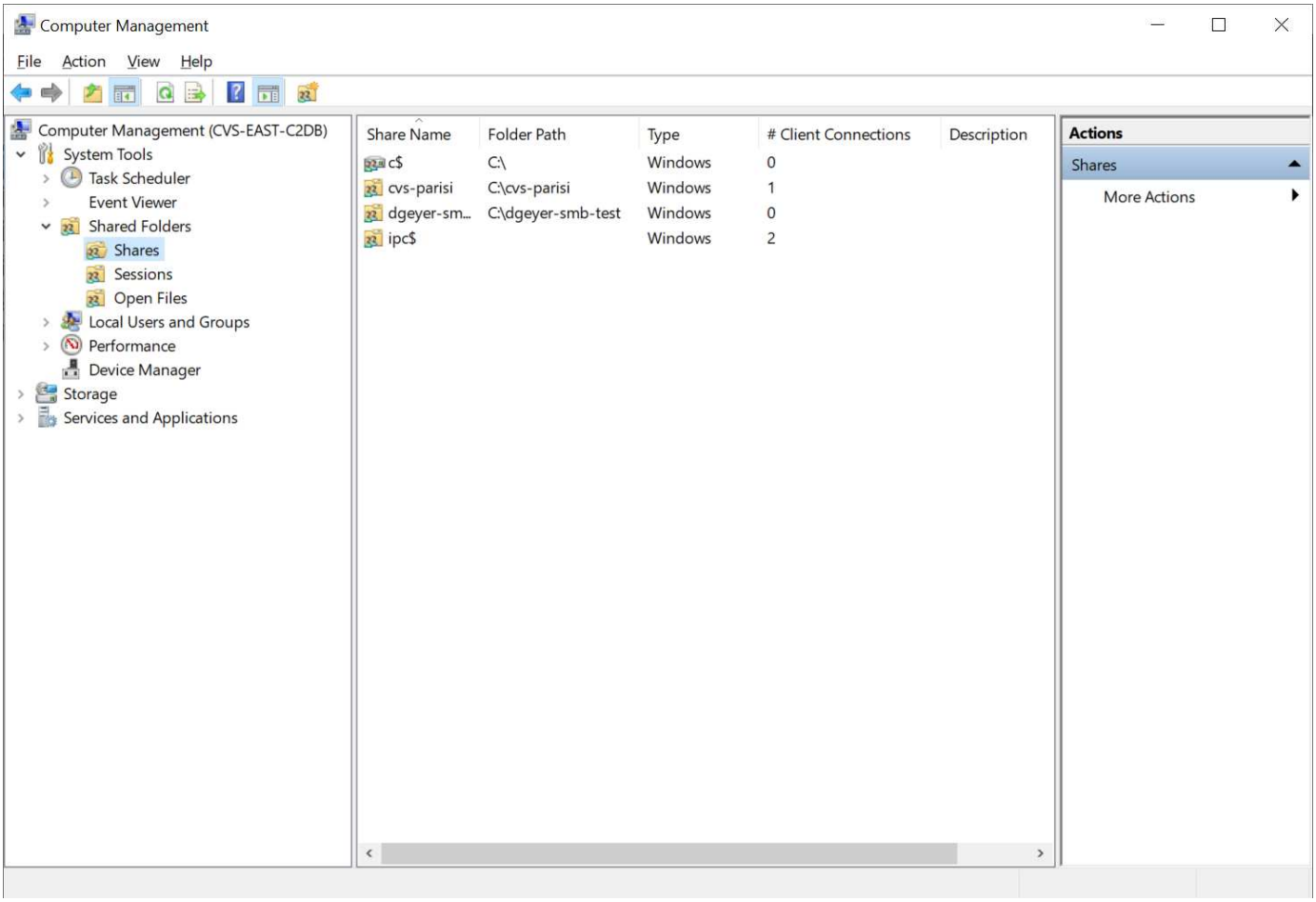
Cloud Volumes Service의 SMB 액세스는 공유를 보고, 공유 ACL을 관리하고, SMB 세션 및 열린 파일을 확인/관리할 수 있는 컴퓨터 관리 MMC에 대한 연결을 제공합니다.

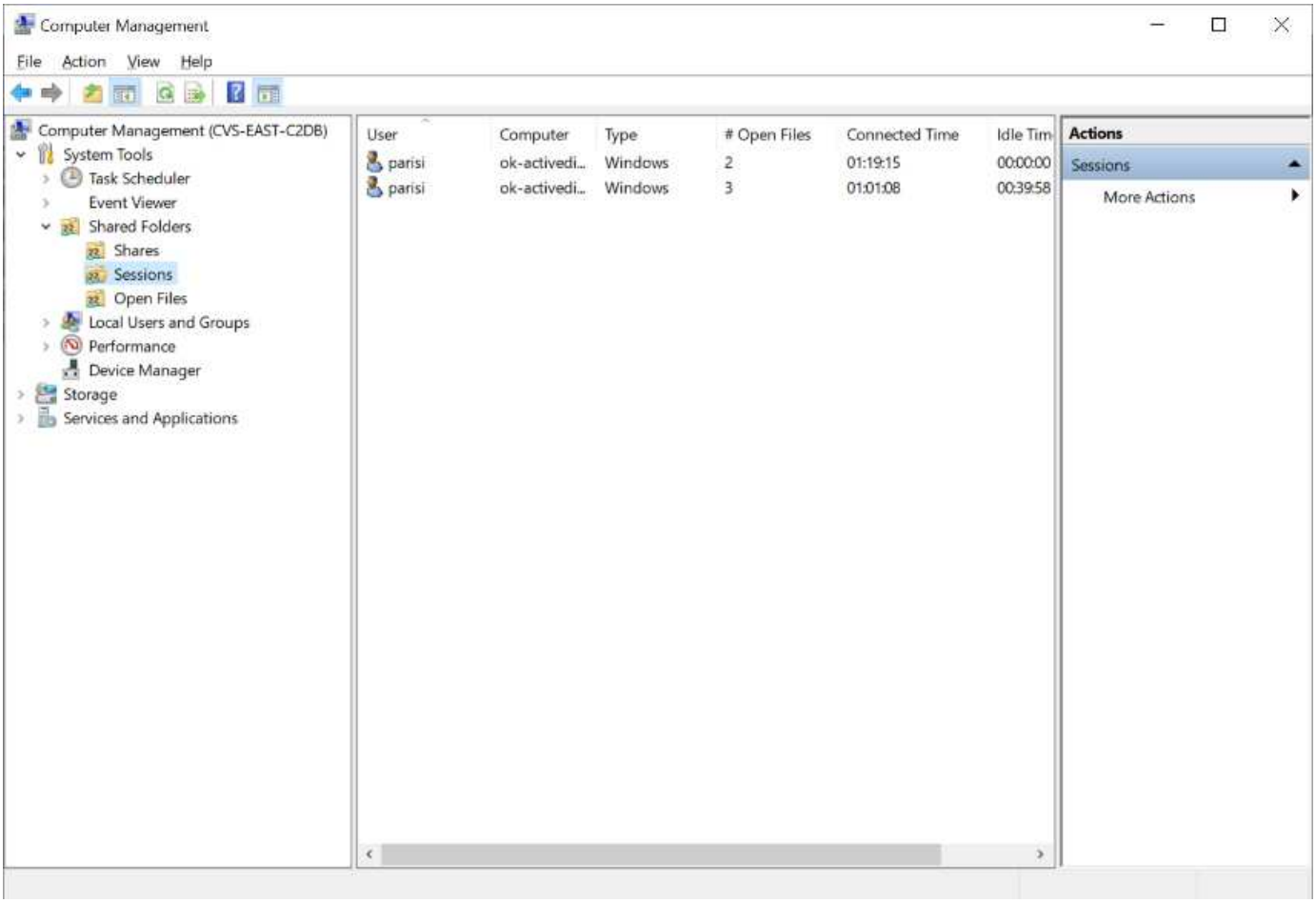
MMC를 사용하여 Cloud Volumes Service에서 SMB 공유 및 세션을 보려면 현재 로그인한 사용자가 도메인 관리자여야 합니다. 다른 사용자는 MMC에서 SMB 서버를 보거나 관리할 수 있으며 Cloud Volumes Service SMB 인스턴스에서 공유 또는 세션을 보려고 할 때 사용 권한 없음 대화 상자를 받을 수 있습니다.

SMB 서버에 연결하려면 컴퓨터 관리를 열고 컴퓨터 관리를 마우스 오른쪽 단추로 클릭한 다음 다른 컴퓨터에 연결을 선택합니다. 그러면 Cloud Volumes Service 볼륨 정보에 있는 SMB 서버 이름을 입력할 수 있는 컴퓨터 선택 대화 상자가 열립니다.

적절한 권한이 있는 SMB 공유를 보면 Active Directory 연결을 공유하는 Cloud Volumes Service 인스턴스에서 사용 가능한 모든 공유가 표시됩니다. 이 동작을 제어하려면 Cloud Volumes Service 볼륨 인스턴스에서 SMB 공유 숨기기 옵션을 설정합니다.

지역당 하나의 Active Directory 연결만 허용됩니다.





다음 표에는 MMC에서 지원/지원되지 않는 기능 목록이 나와 있습니다.

지원되는 함수	지원되지 않는 함수
• 공유 보기 • 활성 SMB 세션을 봅니다 • 열린 파일을 봅니다 • 로컬 사용자 및 그룹을 봅니다 • 로컬 그룹 구성원 자격을 봅니다 • 시스템의 세션, 파일 및 트리 연결 목록을 열거합니다 • 시스템에서 열려 있는 파일을 닫습니다 • 열려 있는 세션을 닫습니다 • 공유 생성/관리	• 새 로컬 사용자/그룹을 생성합니다 • 기존 로컬 사용자/그룹 관리/보기 • 이벤트 또는 성능 로그를 봅니다 • 스토리지 관리 • 서비스 및 애플리케이션 관리

SMB 서버 보안 정보

Cloud Volumes Service의 SMB 서버는 Kerberos 클록 편중, 티켓 사용 기간, 암호화 등 SMB 연결에 대한 보안 정책을 정의하는 일련의 옵션을 사용합니다.

다음 표에는 이러한 옵션, 기능, 기본 설정 및 Cloud Volumes Service를 사용하여 수정할 수 있는 경우 등이 나와

있습니다. 일부 옵션은 Cloud Volumes Service에는 적용되지 않습니다.

보안 옵션	기능	기본값	변경할 수 있습니까?
최대 Kerberos 클럭 비뚤어짐(분)	Cloud Volumes Service와 도메인 컨트롤러 간의 최대 시간 편중 시간 차이가 5분을 초과하면 Kerberos 인증이 실패합니다. 이 값은 Active Directory 기본값으로 설정됩니다.	5	아니요
Kerberos 티켓 수명(시간)	갱신이 요구되기 전에 Kerberos 티켓이 유효한 상태로 유지되는 최대 시간입니다. 10시간 전에 갱신이 발생하지 않으면 새 티켓을 받아야 합니다. Cloud Volumes Service는 이러한 갱신을 자동으로 수행합니다. Active Directory 기본값은 10시간입니다.	10	아니요
최대 Kerberos 티켓 갱신(일)	새 승인 요청이 필요해지기 전에 Kerberos 티켓을 갱신할 수 있는 최대 일 수입니다. Cloud Volumes Service는 SMB 연결에 대한 티켓을 자동으로 갱신합니다. 7일은 Active Directory 기본값입니다.	7	아니요
Kerberos KDC 연결 시간 초과(초)	KDC 연결이 시간 초과되기 전의 시간(초)입니다.	3	아니요
수신 SMB 트래픽에 서명 필요	SMB 트래픽에 서명 필요 로 설정합니다. true로 설정하면 서명을 지원하지 않는 클라이언트가 연결되지 않습니다.	거짓	
로컬 사용자 계정에 암호 복잡성 필요	로컬 SMB 사용자의 암호에 사용됩니다. Cloud Volumes Service는 로컬 사용자 생성을 지원하지 않으므로 이 옵션은 Cloud Volumes Service에는 적용되지 않습니다.	참	아니요
Active Directory LDAP 연결에 start_TLS를 사용합니다	Active Directory LDAP에 대한 TLS 연결 시작을 활성화하는 데 사용됩니다. Cloud Volumes Service에서는 현재 이 설정을 지원하지 않습니다.	거짓	아니요

보안 옵션	기능	기본값	변경할 수 있습니까?
Kerberos를 사용하도록 AES-128 및 AES-256 암호화를 사용합니다	Active Directory 연결에 AES 암호화를 사용할지 여부를 제어하고 Active Directory 연결을 생성/수정할 때 Active Directory 인증에 AES 암호화 사용 옵션을 사용하여 제어합니다.	거짓	예
LM 호환성 수준	Active Directory 연결에 대해 지원되는 인증 방언의 수준입니다. 자세한 내용은 " 단원을 참조하십시오SMB 인증 방언"를 참조하십시오.	NTLMv2 - KRB	아니요
수신 CIFS 트래픽에 SMB 암호화 필요	모든 공유에 SMB 암호화가 필요합니다. 이 기능은 Cloud Volumes Service에서 사용되지 않으며 대신 볼륨별로 암호화를 설정합니다(“ 절 참조)SMB는 보안 기능을 공유합니다").	거짓	아니요
클라이언트 세션 보안	LDAP 통신에 대한 서명 및/또는 봉인을 설정합니다. 이 설정은 현재 Cloud Volumes Service에 설정되어 있지 않지만 향후 릴리즈에서 필요할 수 있습니다. Windows 패치로 인한 LDAP 인증 문제에 대한 해결 방법은 섹션에서 설명합니다 ""LDAP 채널 바인딩.””.	없음	아니요
SMB2가 DC 연결에 대해 설정됩니다	DC 연결에 SMB2를 사용합니다. 기본적으로 사용됩니다.	System - 기본값입니다	아니요
LDAP 조회	여러 LDAP 서버를 사용하는 경우 조회 추적을 통해 첫 번째 서버에서 항목을 찾을 수 없을 때 클라이언트가 목록의 다른 LDAP 서버를 참조할 수 있습니다. 현재 Cloud Volumes Service에서는 지원되지 않습니다.	거짓	아니요
보안 Active Directory 연결에 LDAPS를 사용합니다	SSL을 통한 LDAP 사용을 활성화합니다. 현재 Cloud Volumes Service에서 지원되지 않습니다.	거짓	아니요

보안 옵션	기능	기본값	변경할 수 있습니까?
DC 연결에 암호화가 필요합니다	성공적인 DC 연결을 위해 암호화가 필요합니다. Cloud Volumes Service에서 기본적으로 비활성화되어 있습니다.	거짓	아니요

이중 프로토콜/멀티프로토콜

Cloud Volumes Service는 적절한 액세스 권한을 유지하면서 동일한 데이터 세트를 SMB 및 NFS 클라이언트 모두에 공유할 수 있는 기능을 제공합니다 ("이중 프로토콜")를 클릭합니다. 이는 프로토콜 간 ID 매핑을 조정하고 중앙 집중식 백엔드 LDAP 서버를 사용하여 Cloud Volumes Service에 UNIX ID를 제공하는 방식으로 수행됩니다. Windows Active Directory를 사용하여 Windows 및 UNIX 사용자를 모두 편리하게 제공할 수 있습니다.

액세스 제어

- * 공유 액세스 제어. * NAS 공유에 액세스할 수 있는 클라이언트 및/또는 사용자 및 그룹을 결정합니다. NFS의 경우 엑스포트 정책과 규칙을 사용하여 클라이언트 엑스포트 액세스를 제어합니다. NFS 내보내기는 Cloud Volumes Service 인스턴스에서 관리됩니다. SMB는 CIFS/SMB 공유를 사용하고 ACL을 공유하여 사용자 및 그룹 레벨에서 보다 세부적인 제어를 제공합니다. 을 사용하여 SMB 클라이언트의 공유 레벨 ACL만 구성할 수 있습니다 "MMC/컴퓨터 관리" Cloud Volumes Service 인스턴스에 대한 관리자 권한이 있는 계정(섹션 참조) "" 로컬/BUILTIN 관리자/백업 권한이 있는 계정.""를 클릭합니다.
- * 파일 액세스 제어. * 파일 또는 폴더 수준에서 권한을 제어하고 항상 NAS 클라이언트에서 관리합니다. NFS 클라이언트는 기존 모드 비트(rwx) 또는 NFSv4 ACL을 사용할 수 있습니다. SMB 클라이언트는 NTFS 권한을 활용합니다.

NFS와 SMB 모두에 데이터를 제공하는 볼륨의 액세스 제어는 사용 중인 프로토콜에 따라 다릅니다. 이중 프로토콜의 사용 권한에 대한 자세한 내용은 " 절을 참조하십시오권한 모델."

사용자 매핑

클라이언트가 볼륨에 액세스하면 Cloud Volumes Service는 들어오는 사용자를 반대 방향으로 유효한 사용자에게 매핑하려고 시도합니다. 이는 프로토콜 간에 적절한 액세스를 결정하고 액세스를 요청하는 사용자가 실제로 자신이 주장하는 사용자인지 확인하기 위해 필요합니다.

예를 들어, "joe"라는 Windows 사용자가 SMB를 통해 UNIX 사용 권한이 있는 볼륨에 액세스하려고 하면 Cloud Volumes Service는 검색을 수행하여 "joe"라는 해당 UNIX 사용자를 찾습니다. 이 파일이 있으면 Windows 사용자 Joe로 SMB 공유에 기록되는 파일이 NFS 클라이언트의 UNIX 사용자 Joe로 나타납니다.

또는 UNIX 사용자인 "Joe"가 Windows 사용 권한이 있는 Cloud Volumes Service 볼륨에 대한 액세스를 시도할 경우 UNIX 사용자는 유효한 Windows 사용자에게 매핑할 수 있어야 합니다. 그렇지 않으면 볼륨에 대한 액세스가 거부됩니다.

현재 LDAP를 사용하는 외부 UNIX ID 관리에는 Active Directory만 지원됩니다. 이 서비스에 대한 액세스 구성에 대한 자세한 내용은 을 참조하십시오 "AD 연결을 생성하는 중입니다".

권한 모델

이중 프로토콜 설정을 사용하는 경우 Cloud Volumes Service는 볼륨에 대한 보안 스타일을 사용하여 ACL 유형을

결정합니다. 이러한 보안 스타일은 지정된 NAS 프로토콜을 기반으로 설정되거나, 이중 프로토콜의 경우 Cloud Volumes Service 볼륨 생성 시 선택하는 것입니다.

- NFS만 사용하는 경우 Cloud Volumes Service 볼륨은 UNIX 사용 권한을 사용합니다.
- SMB만 사용하는 경우 Cloud Volumes Service 볼륨은 NTFS 권한을 사용합니다.

이중 프로토콜 볼륨을 생성하는 경우 볼륨 생성 시 ACL 스타일을 선택할 수 있습니다. 이 결정은 원하는 권한 관리를 기반으로 해야 합니다. 사용자가 Windows/SMB 클라이언트의 권한을 관리하는 경우 NTFS 를 선택합니다. 사용자가 NFS 클라이언트 및 chmod/chown을 사용하려는 경우 UNIX 보안 스타일을 사용합니다.

Active Directory 연결을 생성할 때의 고려 사항

Cloud Volumes Service를 사용하면 Cloud Volumes Service 인스턴스를 외부 Active Directory 서버에 연결하여 SMB 및 UNIX 사용자 모두의 ID 관리를 수행할 수 있습니다. Cloud Volumes Service에서 SMB를 사용하려면 Active Directory 연결을 생성해야 합니다.

이 구성은 보안을 고려해야 하는 몇 가지 옵션을 제공합니다. 외부 Active Directory 서버는 온-프레미스 인스턴스 또는 클라우드 네이티브 서버가 될 수 있습니다. 온-프레미스 Active Directory 서버를 사용하는 경우, 도메인을 외부 네트워크(예: DMZ 또는 외부 IP 주소)에 노출하지 마십시오. 대신 을 사용하여 사내 네트워크에 대한 보안 전용 터널 또는 VPN, 단방향 포리스트 트러스트 또는 전용 네트워크 연결을 사용합니다 "개인 Google 액세스". 에 대한 자세한 내용은 Google Cloud 설명서를 참조하십시오 "Google Cloud에서 Active Directory를 사용하는 모범 사례".

> CVS-SW를 사용하려면 Active Directory 서버가 동일한 지역에 있어야 합니다. CVS-SW에서 다른 지역으로 DC 연결을 시도하면 시도가 실패합니다. CVS-SW를 사용할 때는 Active Directory DC를 포함하는 Active Directory 사이트를 생성한 다음 Cloud Volumes Service에서 사이트를 지정하여 교차 지역 DC 연결 시도를 방지해야 합니다.

Active Directory 자격 증명

NFS용 SMB 또는 LDAP가 활성화된 경우 Cloud Volumes Service는 Active Directory 컨트롤러와 상호 작용하여 인증에 사용할 컴퓨터 계정 개체를 생성합니다. 이는 Windows SMB 클라이언트가 도메인에 가입하는 방식과 다르지 않으며 Active Directory의 OU(조직 구성 단위)에 동일한 액세스 권한이 필요합니다.

대부분의 경우 보안 그룹은 Cloud Volumes Service와 같은 외부 서버에서 Windows 관리자 계정 사용을 허용하지 않습니다. 경우에 따라 Windows 관리자 사용자는 보안 모범 사례로 완전히 비활성화됩니다.

SMB 시스템 계정을 생성하는 데 필요한 권한입니다

Cloud Volumes Service 컴퓨터 개체를 Active Directory에 추가하려면 도메인에 대한 관리 권한이 있거나 있는 계정입니다 "컴퓨터 계정 객체를 생성 및 수정하는 위임된 권한" 지정된 OU에 대한 필수 구성 요소입니다. Active Directory의 제어 위임 마법사를 사용하여 다음과 같은 액세스 권한이 있는 컴퓨터 개체를 생성/삭제할 수 있는 사용자 지정 작업을 만들어 이 작업을 수행할 수 있습니다.

- 읽기/쓰기
- 모든 자식 개체를 생성/삭제합니다
- 모든 속성 읽기/쓰기
- 암호 변경/재설정

이렇게 하면 정의된 사용자에 대한 보안 ACL이 Active Directory의 OU에 자동으로 추가되고 Active Directory 환경에 대한 액세스가 최소화됩니다. 사용자가 위임된 후에는 이 창에서 해당 사용자 이름과 암호를 Active Directory 자격

증명으로 제공할 수 있습니다.

Active Directory 도메인에 전달되는 사용자 이름과 암호는 컴퓨터 계정 개체 쿼리 및 생성 중에 Kerberos 암호화를 사용하여 보안을 강화합니다.

Active Directory 연결 세부 정보입니다

를 클릭합니다 "Active Directory 연결 세부 정보" 다음과 같은 컴퓨터 계정 배치에 대한 특정 Active Directory 스키마 정보를 관리자에게 제공하는 필드를 제공합니다.

- * Active Directory 연결 유형. * Cloud Volumes Service 또는 CVS 성능 서비스 유형의 볼륨에 대해 영역의 Active Directory 연결이 사용되는지 여부를 지정하는 데 사용됩니다. 기존 연결에서 이 설정을 잘못 설정하면 사용하거나 편집할 때 제대로 작동하지 않을 수 있습니다.
- * 도메인. * Active Directory 도메인 이름입니다.
- * 사이트. * 보안 및 성능을 위해 Active Directory 서버를 특정 사이트로 제한합니다 "고려 사항". Cloud Volumes Service는 현재 Cloud Volumes Service 인스턴스가 아닌 다른 영역에 있는 Active Directory 서버에 대한 Active Directory 인증 요청을 허용하지 않으므로 여러 Active Directory 서버가 여러 지역에 걸쳐 있는 경우 이 작업이 필요합니다. 예를 들어, Active Directory 도메인 컨트롤러는 CVS-Performance만 지원하는 영역에 있지만 CVS-SW 인스턴스에서 SMB 공유를 원할 수 있습니다.
- DNS 서버 * 이름 조회에 사용할 DNS 서버.
- NetBIOS 이름(선택 사항).* 필요한 경우 서버의 NetBIOS 이름입니다. 이 기능은 Active Directory 연결을 사용하여 새 컴퓨터 계정을 만들 때 사용됩니다. 예를 들어 NetBIOS 이름이 CVS-East로 설정된 경우 컴퓨터 계정 이름은 CVS-East-{1234}가 됩니다. 섹션을 참조하십시오 "Active Directory에 Cloud Volumes Service가 표시되는 방식" 를 참조하십시오.
- * OU(조직 단위) * 컴퓨터 계정을 만들 특정 OU. 이 기능은 컴퓨터 계정에 대해 특정 OU에 제어를 위임하는 경우에 유용합니다.
- * AES 암호화. * AD 인증에 AES 암호화 사용 확인란을 선택하거나 선택 취소할 수도 있습니다. Active Directory 인증에 AES 암호화를 사용하면 사용자 및 그룹 조회 중에 Cloud Volumes Service에서 Active Directory로 통신하는 데 추가적인 보안을 제공할 수 있습니다. 이 옵션을 활성화하기 전에 도메인 관리자에게 문의하여 Active Directory 도메인 컨트롤러가 AES 인증을 지원하는지 확인하십시오.

기본적으로 대부분의 Windows 서버는 약한 암호(예: DES 또는 RC4-HMAC)를 비활성화하지 않지만 약한 암호를 비활성화하도록 선택하는 경우 Cloud Volumes Service Active Directory 연결이 AES를 사용하도록 구성되었는지 확인합니다. 그렇지 않으면 인증 실패가 발생합니다. AES 암호화를 사용하도록 설정하면 약한 암호가 비활성화되지 않고 대신 Cloud Volumes Service SMB 시스템 계정에 AES 암호화에 대한 지원이 추가됩니다.

Kerberos 영역 세부 정보

이 옵션은 SMB 서버에는 적용되지 않습니다. 대신, Cloud Volumes Service 시스템에 NFS Kerberos를 구성할 때 사용됩니다. 이러한 세부 정보가 채워지면 NFS Kerberos 영역이 구성되고(Linux의 krb5.conf 파일과 유사), Active Directory 연결이 NFS Kerberos 메일 센터(KDC) 역할을 하므로 Cloud Volumes Service 볼륨 생성에 NFS Kerberos가 지정될 때 사용됩니다.

Windows 이외의 KDC는 현재 Cloud Volumes Service에서 사용할 수 없습니다.

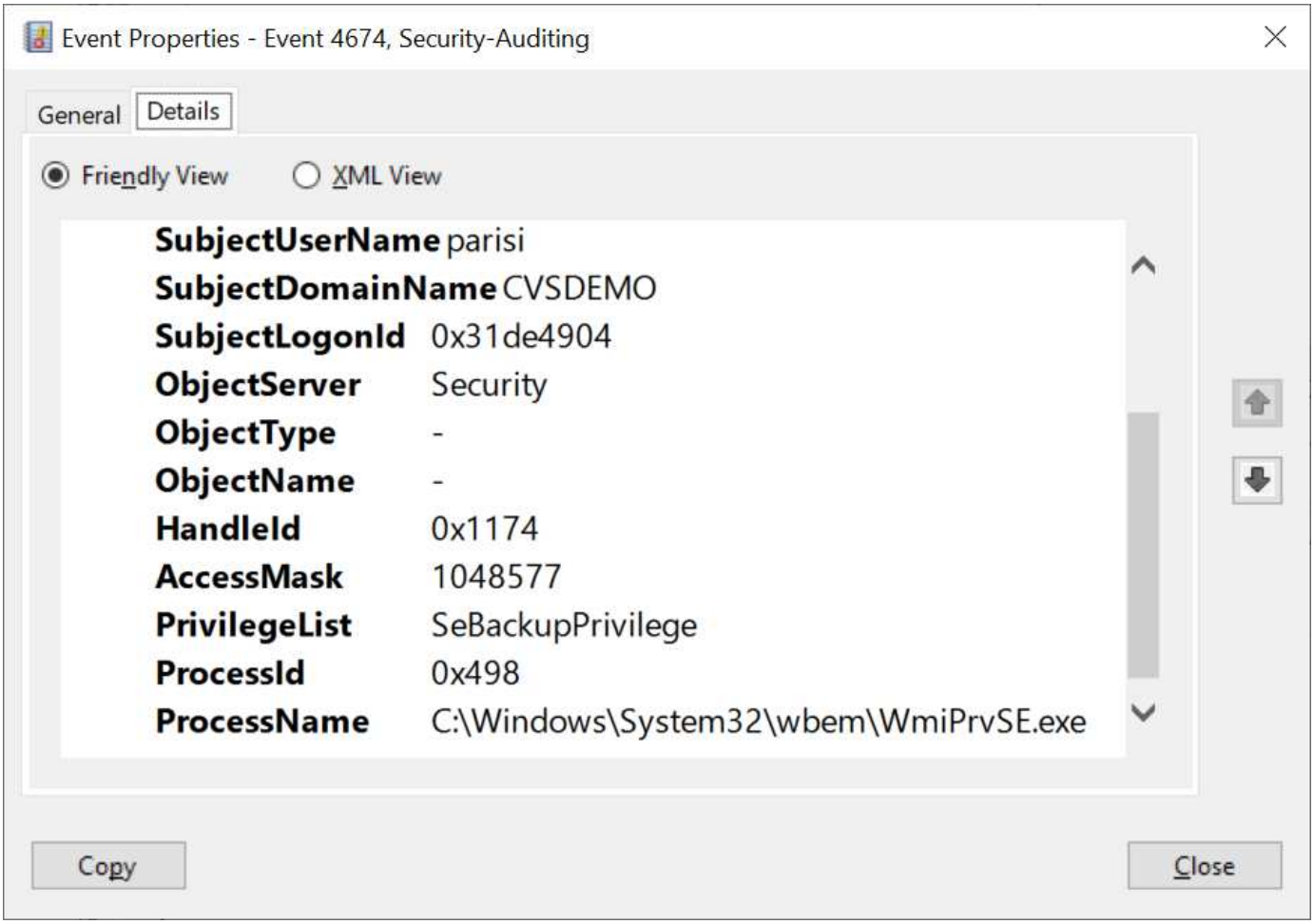
지역

영역을 사용하면 Active Directory 연결이 있는 위치를 지정할 수 있습니다. 이 영역은 Cloud Volumes Service 볼륨과 동일한 영역이어야 합니다.

- * LDAP를 사용하는 로컬 NFS 사용자 * 이 섹션에는 LDAP를 사용하는 로컬 NFS 사용자를 허용하는 옵션도 있습니다. UNIX 사용자 그룹 구성원 지원을 NFS(확장 그룹)의 16개 그룹 제한 이상으로 확장하려면 이 옵션을 선택하지 않아야 합니다. 그러나 확장된 그룹을 사용하려면 UNIX ID에 대해 구성된 LDAP 서버가 필요합니다. LDAP 서버가 없는 경우 이 옵션을 선택되지 않은 상태로 둡니다. LDAP 서버가 있고 로컬 UNIX 사용자(예: 루트)도 사용하려면 이 옵션을 선택합니다.

백업 사용자

이 옵션을 사용하면 Cloud Volumes Service 볼륨에 대한 백업 권한이 있는 Windows 사용자를 지정할 수 있습니다. NAS 볼륨의 데이터를 올바르게 백업 및 복원하려면 일부 애플리케이션에 백업 권한(SeBackupPrivilege)이 필요합니다. 이 사용자는 볼륨의 데이터에 대한 높은 수준의 액세스 권한을 가지고 있으므로 고려해야 합니다 "해당 사용자 액세스에 대한 감사를 설정합니다". 활성화된 감사 이벤트는 이벤트 뷰어 > Windows 로그 > 보안에 표시됩니다.



보안 권한 사용자

이 옵션을 사용하면 Cloud Volumes Service 볼륨에 대한 보안 수정 권한이 있는 Windows 사용자를 지정할 수 있습니다. 일부 응용 프로그램에는 보안 권한(SeSecurityPrivilege)이 필요합니다 ("SQL Server와 같은")를 클릭하여 설치 중에 권한을 적절하게 설정합니다. 이 권한은 보안 로그를 관리하는 데 필요합니다. 이 권한은 SeBackupPrivilege 권한만큼 강력하지는 않지만 NetApp이 권장합니다 "사용자의 사용자 액세스 감사" 필요한 경우 이 권한 수준을 사용합니다.

자세한 내용은 을 참조하십시오 "새 로그온에 할당된 특수 권한".

Active Directory에 **Cloud Volumes Service**가 표시되는 방식

Cloud Volumes Service는 Active Directory에 일반 컴퓨터 계정 개체로 표시됩니다. 명명 규칙은 다음과 같습니다.

- CIFS/SMB 및 NFS Kerberos는 별도의 시스템 계정 객체를 생성합니다.
- LDAP가 설정된 NFS는 Active Directory에서 Kerberos LDAP 바인드를 위한 컴퓨터 계정을 생성합니다.
- LDAP가 있는 이중 프로토콜 볼륨은 LDAP 및 SMB의 CIFS/SMB 시스템 계정을 공유합니다.
- CIFS/SMB 시스템 계정은 시스템 계정에 대해 이름-1234(10자 이름에 하이픈이 추가된 4자리 임의 ID)의 명명 규칙을 사용합니다. Active Directory 연결에서 NetBIOS 이름 설정을 사용하여 이름을 정의할 수 있습니다(“ 절 참조)Active Directory 연결 세부 정보입니다").
- NFS Kerberos에서는 nfs-name-1234를 명명 규칙(최대 15자)으로 사용합니다. 15자 이상을 사용하는 경우 이름은 nfs-duncated-name-1234입니다.
- NFS 전용 CVS - LDAP가 설정된 성능 인스턴스는 CIFS/SMB 인스턴스와 동일한 명명 규칙을 사용하여 LDAP 서버에 바인딩하기 위한 SMB 시스템 계정을 생성합니다.
- SMB 컴퓨터 계정이 생성되면 숨겨진 기본 관리자 공유가 생성됩니다(섹션 참조) "“숨겨진 기본 공유”")도 생성되지만(c$, admin$, ipc$) 해당 공유는 할당된 ACL이 없으며 액세스할 수 없습니다.
- 컴퓨터 계정 개체는 기본적으로 CN=Computers에 배치되지만 필요한 경우 다른 OU를 지정할 수 있습니다. 자세한 내용은 " 단원을 참조하십시오SMB 시스템 계정을 생성하는 데 필요한 권한입니다"Cloud Volumes Service에 대한 컴퓨터 계정 개체를 추가/제거하는 데 필요한 액세스 권한에 대한 정보를 제공합니다.

Cloud Volumes Service가 Active Directory에 SMB 컴퓨터 계정을 추가하면 다음 필드가 채워집니다.

- CN(지정된 SMB 서버 이름 포함)
- dNSHostName(SMBserver.domain.com 포함)
- msDS-SupportedEncryptionTypes (AES 암호화가 활성화되지 않은 경우 DES_CBC_MD5, RC4_HMAC_MD5 허용; AES 암호화가 활성화된 경우 DES_CBC_MD5, RC4_HMAC_MD5, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96은 SMB용 시스템 계정과 티켓 교환에 허용됨)
- 이름(SMB 서버 이름 포함)
- sAMAccountName(SMBserver$ 사용)
- servicePrincipalName(호스트 /smbserver.domain.com 및 Kerberos에 대한 호스트/smbserver SPN 포함)

컴퓨터 계정에서 약한 Kerberos 암호화 유형(enctype)을 비활성화하려면 컴퓨터 계정의 MSDS-SupportedEncryptionTypes 값을 다음 표의 값 중 하나로 변경하여 AES만 허용할 수 있습니다.

MSDS - SupportedEncryptionTypes 값입니다	**Enctype**이 활성화되었습니다
2	DES_CBC_MD5
4	RC4_HMAC
8	AES128_CTS_HMAC_SHA1_96만 해당
16	AES256_CTS_HMAC_SHA1_96만 해당
24	AES128_CTS_HMAC_SHA1_96 및 AES256_CTS_HMAC_SHA1_96

MSDS - SupportedEncryptionTypes 값입니다	**Enctype**이 활성화되었습니다
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 및 AES256_CTS_HMAC_SHA1_96

SMB 시스템 계정에 대해 AES 암호화를 활성화하려면 Active Directory 연결을 생성할 때 AD 인증에 AES 암호화 사용을 클릭합니다.

NFS Kerberos에서 AES 암호화를 사용하도록 설정하려면 "Cloud Volumes Service 설명서를 참조하십시오".

기타 **NAS** 인프라스트럭처 서비스 종속성**(KDC, LDAP** 및 **DNS)**

NAS 공유에 Cloud Volumes Service를 사용하는 경우 적절한 기능을 위해 외부 종속성이 필요할 수 있습니다. 이러한 종속성은 특정 상황에서 적용됩니다. 다음 표에는 다양한 구성 옵션과 종속 항목이 필요한 항목이 나와 있습니다.

구성	종속성이 필요합니다
NFSv3만 해당	없음
NFSv3 Kerberos만 해당	Windows Active Directory: * KDC * DNS * LDAP
NFSv4.1만 해당	클라이언트 ID 매핑 구성(/etc/idmap.conf)
NFSv4.1 Kerberos만 해당	• 클라이언트 ID 매핑 구성(/etc/idmap.conf) • Windows Active Directory: KDC DNS LDAP
SMB만 해당	Active Directory: * KDC * DNS
멀티프로토콜 NAS(NFS 및 SMB)	• 클라이언트 ID 매핑 구성(NFSv4.1 전용; /etc/idmap.conf) • Windows Active Directory: KDC DNS LDAP

시스템 계정 개체에 대한 **Kerberos** 키 탭 회전/암호 재설정

SMB 시스템 계정의 경우 Cloud Volumes Service는 SMB 시스템 계정에 대한 주기적인 암호 재설정을 예약합니다. 이러한 암호 재설정은 Kerberos 암호화를 사용하여 발생하며, 오후 11시부터 오전 1시 사이에 임의 시간에 매주 일요일 일정에 따라 작동합니다. 이러한 암호 재설정은 Kerberos 키 버전을 변경하고, Cloud Volumes Service 시스템에 저장된 키 탭을 회전하며, Cloud Volumes Service에서 실행되는 SMB 서버의 보안을 더욱 강화할 수 있도록 도와줍니다. 시스템 계정 암호는 무작위배정되며 관리자에게 알려져 있지 않습니다.

NFS Kerberos 시스템 계정의 경우 KDC와 새 키 탭이 생성/교환될 때만 암호 재설정이 적용됩니다. 현재 Cloud Volumes Service에서는 이 작업을 수행할 수 없습니다.

LDAP 및 **Kerberos**와 함께 사용할 네트워크 포트

LDAP 및 Kerberos를 사용하는 경우 이러한 서비스에서 사용 중인 네트워크 포트를 확인해야 합니다. 에서 Cloud Volumes Service에서 사용 중인 포트의 전체 목록을 찾을 수 있습니다 "보안 고려 사항에 대한 Cloud Volumes Service 문서".

LDAP를 지원합니다

Cloud Volumes Service는 LDAP 클라이언트 역할을 하며 UNIX ID에 대한 사용자 및 그룹 조회를 위해 표준 LDAP 검색 쿼리를 사용합니다. Cloud Volumes Service에서 제공하는 표준 기본 사용자 이외의 사용자 및 그룹을 사용하려면 LDAP가 필요합니다. NFS Kerberos를 사용자 보안 주체(예: user1@domain.com 사용할 계획이라면 LDAP도 필요합니다. 현재 Microsoft Active Directory를 사용하는 LDAP만 지원됩니다.

Active Directory를 UNIX LDAP 서버로 사용하려면 UNIX ID에 사용할 사용자 및 그룹에 필요한 UNIX 속성을 채워야 합니다. Cloud Volumes Service에서는 에 따라 특성을 쿼리하는 기본 LDAP 스키마 템플릿을 사용합니다 "RFC-2307-bis". 따라서 다음 표에서는 사용자 및 그룹에 채울 최소 필수 Active Directory 속성과 각 속성이 사용되는 특성을 보여 줍니다.

Active Directory에서 LDAP 속성을 설정하는 방법에 대한 자세한 내용은 을 참조하십시오 "이중 프로토콜 액세스 관리."

속성	기능
UID *	UNIX 사용자 이름을 지정합니다
uidNumber *	UNIX 사용자의 숫자 ID를 지정합니다
gidNumber *	UNIX 사용자의 기본 그룹 숫자 ID를 지정합니다
objectClass *	사용 중인 개체 유형을 지정합니다. Cloud Volumes Service에서는 "사용자"를 개체 클래스 목록에 포함해야 합니다(기본적으로 대부분의 Active Directory 배포에는 포함됨).
이름	계정에 대한 일반 정보(실제 이름, 전화 번호 등, gecos라고도 함)
unixUserPassword	NAS 인증을 위한 UNIX ID 조회에 사용되지 않으므로 설정할 필요가 없습니다. 이렇게 설정하면 구성된 unixUserPassword 값이 일반 텍스트로 설정됩니다.
unixHomeDirectory	사용자가 Linux 클라이언트에서 LDAP에 대해 인증할 때 UNIX 홈 디렉토리의 경로를 정의합니다. UNIX 홈 디렉토리 기능에 LDAP를 사용하려면 이 옵션을 설정합니다.
LoginShell입니다	사용자가 LDAP에 대해 인증할 때 Linux 클라이언트의 bash/profile 셸에 대한 경로를 정의합니다.

- 는 Cloud Volumes Service의 적절한 기능을 위해 특성이 필요함을 나타냅니다. 나머지 속성은 클라이언트 측 전용입니다.

속성	기능
CN *	UNIX 그룹 이름을 지정합니다. LDAP에 Active Directory를 사용하는 경우 개체를 처음 만들 때 설정되지만 나중에 변경할 수 있습니다. 이 이름은 다른 개체와 같을 수 없습니다. 예를 들어, user1이라는 UNIX 사용자가 Linux 클라이언트의 user1이라는 그룹에 속해 있는 경우 Windows에서는 cn 특성이 같은 두 개체를 허용하지 않습니다. 이 문제를 해결하려면 Windows 사용자의 이름을 고유한 이름(예: user1-UNIX)으로 바꿉니다. Cloud Volumes Service의 LDAP는 UNIX 사용자 이름에 uid 속성을 사용합니다.
gidNumber *	UNIX 그룹 숫자 ID를 지정합니다.
objectClass *	사용 중인 개체 유형을 지정합니다. Cloud Volumes Service에서는 개체 클래스 목록에 그룹을 포함해야 합니다. 이 특성은 기본적으로 대부분의 Active Directory 배포에 포함됩니다.
memberUid	UNIX 그룹의 구성원인 UNIX 사용자를 지정합니다. Cloud Volumes Service에서 Active Directory LDAP를 사용할 경우 이 필드는 필요하지 않습니다. Cloud Volumes Service LDAP 스키마는 그룹 구성원 자격에 구성원 필드를 사용합니다.
구성원 *	그룹 구성원 자격/보조 UNIX 그룹에 필요합니다. 이 필드는 Windows 그룹에 Windows 사용자를 추가하여 채워집니다. 그러나 Windows 그룹에 채워진 UNIX 특성이 없는 경우 UNIX 사용자의 그룹 구성원 목록에는 포함되지 않습니다. NFS에서 사용할 수 있어야 하는 모든 그룹은 이 표에 나열된 필수 UNIX 그룹 속성을 채워야 합니다.

- 는 Cloud Volumes Service의 적절한 기능을 위해 특성이 필요함을 나타냅니다. 나머지 속성은 클라이언트 측 전용입니다.

LDAP 바인딩 정보

LDAP에서 사용자를 쿼리하려면 Cloud Volumes Service가 LDAP 서비스에 바인딩(로그인)해야 합니다. 이 로그인에는 읽기 전용 권한이 있으며 디렉토리 조회를 위해 LDAP UNIX 속성을 쿼리하는 데 사용됩니다. 현재 LDAP 바인딩은 SMB 컴퓨터 계정을 통해서만 가능합니다.

'CVS 성능' 인스턴스에만 LDAP를 사용하도록 설정하고 NFSv3, NFSv4.1 또는 이중 프로토콜 볼륨에는 LDAP를 사용할 수 있습니다. LDAP 지원 볼륨을 성공적으로 배포하려면 Cloud Volumes Service 볼륨과 동일한 영역에 Active Directory 연결을 설정해야 합니다.

LDAP가 활성화된 경우 특정 시나리오에서 다음이 발생합니다.

- Cloud Volumes Service 프로젝트에 NFSv3이나 NFSv4.1만 사용되는 경우 Active Directory 도메인 컨트롤러에서 새 컴퓨터 계정이 생성되고 Cloud Volumes Service의 LDAP 클라이언트는 시스템 계정 자격 증명을 사용하여 Active Directory에 바인딩됩니다. NFS 볼륨 및 숨겨진 기본 관리 공유에 대해 SMB 공유가 생성되지 않습니다(섹션 참조) ""숨겨진 기본 공유"")의 공유 ACL이 제거되었습니다.
- Cloud Volumes Service 프로젝트에 이중 프로토콜 볼륨을 사용하는 경우 SMB 액세스용으로 생성된 단일 컴퓨터 계정만 Cloud Volumes Service의 LDAP 클라이언트를 Active Directory에 바인딩하는 데 사용됩니다. 추가 컴퓨터 계정이 생성되지 않습니다.

- 전용 SMB 볼륨이 별도로 생성된 경우(LDAP가 설정된 NFS 볼륨 이전 또는 이후에) LDAP 바인딩의 컴퓨터 계정이 SMB 시스템 계정과 공유됩니다.
- NFS Kerberos도 사용하도록 설정된 경우 두 개의 시스템 계정이 생성됩니다. 하나는 SMB 공유 및/또는 LDAP 바인드이고 다른 하나는 NFS Kerberos 인증입니다.

LDAP 쿼리입니다

LDAP 바인딩은 암호화되지만 일반 LDAP 포트 389를 사용하여 LDAP 쿼리가 일반 텍스트로 회선을 통해 전달됩니다. 이 잘 알려진 포트는 현재 Cloud Volumes Service에서 변경할 수 없습니다. 따라서 네트워크에서 패킷 스니핑에 액세스할 수 있는 사용자는 사용자 및 그룹 이름, 숫자 ID 및 그룹 구성원 자격을 볼 수 있습니다.

그러나 Google Cloud VM은 다른 VM의 유니캐스트 트래픽을 스니프할 수 없습니다. LDAP 트래픽에 활성 중인 VM(즉, 바인딩 가능)만 LDAP 서버의 트래픽을 볼 수 있습니다. Cloud Volumes Service의 패킷 스니핑에 대한 자세한 내용은 섹션을 참조하십시오 ""패킷 감지/추적 고려 사항""

LDAP 클라이언트 구성 기본값

Cloud Volumes Service 인스턴스에서 LDAP가 활성화되면 기본적으로 특정 구성 세부 정보를 사용하여 LDAP 클라이언트 구성이 생성됩니다. 경우에 따라 옵션이 Cloud Volumes Service(지원되지 않음)에 적용되지 않거나 구성할 수 없습니다.

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까?
LDAP 서버 목록	쿼리에 사용할 LDAP 서버 이름 또는 IP 주소를 설정합니다. Cloud Volumes Service에는 사용되지 않습니다. 대신 Active Directory 도메인을 사용하여 LDAP 서버를 정의합니다.	설정되지 않았습니다	아니요
Active Directory 도메인	LDAP 쿼리에 사용할 Active Directory 도메인을 설정합니다. Cloud Volumes Service는 DNS의 LDAP에 대한 SRV 레코드를 활용하여 도메인에서 LDAP 서버를 찾습니다.	Active Directory 연결에 지정된 Active Directory 도메인으로 설정합니다.	아니요
기본 Active Directory 서버	LDAP에 사용할 기본 Active Directory 서버를 설정합니다. Cloud Volumes Service에서 지원되지 않습니다. 대신 Active Directory 사이트를 사용하여 LDAP 서버 선택을 제어할 수 있습니다.	설정되지 않았습니다.	아니요

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까**?**
SMB 서버 자격 증명을 사용하여 바인딩합니다	SMB 시스템 계정을 사용하여 LDAP에 바인딩합니다. 현재 Cloud Volumes Service에서 지원되는 유일한 LDAP 바인딩 방법입니다.	참	아니요
스키마 템플릿	LDAP 쿼리에 사용되는 스키마 템플릿입니다.	MS-AD-BIS	아니요
LDAP 서버 포트입니다	LDAP 쿼리에 사용되는 포트 번호입니다. Cloud Volumes Service는 현재 표준 LDAP 포트 389만 사용합니다. LDAPS/포트 636은 현재 지원되지 않습니다.	389	아니요
LDAPS가 활성화되어 있습니다	SSL(Secure Sockets Layer)을 통한 LDAP가 쿼리 및 바인딩에 사용되는지 여부를 제어합니다. 현재 Cloud Volumes Service에서 지원되지 않습니다.	거짓	아니요
쿼리 시간 제한(초)	쿼리 시간이 초과되었습니다. 쿼리가 지정된 값보다 오래 걸면 쿼리가 실패합니다.	3	아니요
최소 바인딩 인증 레벨	지원되는 최소 바인딩 레벨입니다. Cloud Volumes Service는 LDAP 바인딩에 컴퓨터 계정을 사용하고 Active Directory는 기본적으로 익명 바인딩을 지원하지 않으므로 이 옵션은 보안을 위해 사용되지 않습니다.	익명	아니요
DN 바인딩	단순 바인딩이 사용될 때 바인딩에 사용되는 사용자 /고유 이름(DN)입니다. Cloud Volumes Service는 LDAP 바인딩에 시스템 계정을 사용하며 현재 단순 바인딩 인증을 지원하지 않습니다.	설정되지 않았습니다	아니요

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까**?**
기본 DN	LDAP 검색에 사용되는 기본 DN입니다.	Windows 도메인이 DN 형식(즉, DC=domain, DC=local)으로 Active Directory 연결에 사용됩니다.	아니요
기본 검색 범위	기본 DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service는 하위 트리 검색만 지원합니다.	하위 트리	아니요
사용자 DN	사용자가 LDAP 쿼리를 검색하는 DN을 정의합니다. 현재 Cloud Volumes Service에서는 지원되지 않으므로 모든 사용자 검색은 기본 DN에서 시작됩니다.	설정되지 않았습니다	아니요
사용자 검색 범위	사용자 DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service는 사용자 검색 범위 설정을 지원하지 않습니다.	하위 트리	아니요
그룹 DN	그룹 검색이 LDAP 쿼리를 시작하는 DN을 정의합니다. 현재 Cloud Volumes Service에 대해 지원되지 않으므로 모든 그룹 검색이 기본 DN에서 시작됩니다.	설정되지 않았습니다	아니요
그룹 검색 범위	그룹 DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service는 그룹 검색 범위 설정을 지원하지 않습니다.	하위 트리	아니요
넷그룹 DN입니다	넷그룹이 LDAP 쿼리를 검색하는 DN을 정의합니다. 현재 Cloud Volumes Service에 대해 지원되지 않으므로 모든 넷그룹 검색은 기본 DN에서 시작됩니다.	설정되지 않았습니다	아니요

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까**?**
넷그룹 검색 범위입니다	넷그룹 DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service에서는 넷그룹 검색 범위 설정을 지원하지 않습니다.	하위 트리	아니요
LDAP를 통해 start_tls를 사용합니다	포트 389를 통한 인증서 기반 LDAP 연결에 Start TLS를 활용합니다. 현재 Cloud Volumes Service에서 지원되지 않습니다.	거짓	아니요
Netgroup-by-host 조회를 설정합니다	넷그룹을 확장하여 모든 구성원을 나열하는 대신 호스트 이름별로 넷그룹 조회를 설정합니다. 현재 Cloud Volumes Service에서 지원되지 않습니다.	거짓	아니요
Netgroup-by-host DN입니다	넷그룹별 검색이 LDAP 쿼리를 시작하는 DN을 정의합니다. Cloud Volumes Service에 대해 현재 호스트별 넷그룹이 지원되지 않습니다.	설정되지 않았습니다	아니요
Netgroup-by-host 검색 범위입니다	Netgroup-by-host DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service에 대해 현재 호스트별 넷그룹이 지원되지 않습니다.	하위 트리	아니요
클라이언트 세션 보안	LDAP에서 사용하는 세션 보안 수준(서명, 봉인 또는 없음)을 정의합니다. LDAP 서명은 Active Directory에서 요청하는 경우 CVS - 성능에서 지원됩니다. CVS-SW는 LDAP 서명을 지원하지 않습니다. 두 서비스 유형 모두에서 봉인은 현재 지원되지 않습니다.	없음	아니요

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까**?**
LDAP 조회 추적	여러 LDAP 서버를 사용하는 경우 조회 추적을 통해 첫 번째 서버에서 항목을 찾을 수 없을 때 클라이언트가 목록의 다른 LDAP 서버를 참조할 수 있습니다. 현재 Cloud Volumes Service에서는 지원되지 않습니다.	거짓	아니요
그룹 구성원 필터	LDAP 서버에서 그룹 구성원을 검색할 때 사용할 사용자 지정 LDAP 검색 필터를 제공합니다. 현재 Cloud Volumes Service에서는 지원되지 않습니다.	설정되지 않았습니다	아니요

비대칭 이름 매핑에 **LDAP**를 사용합니다

Cloud Volumes Service는 기본적으로 특별한 구성 없이 양방향으로 동일한 사용자 이름을 가진 Windows 사용자와 UNIX 사용자를 매핑합니다. Cloud Volumes Service가 유효한 UNIX 사용자(LDAP 사용)를 찾을 수 있는 한 1:1 이름 매핑이 발생합니다. 예를 들어, 윈도우 사용자인 'johnsmith'를 사용하는 경우, Cloud Volumes Service가 LDAP에서 johnsmith라는 UNIX 사용자를 찾을 수 있다면, 해당 사용자에 대한 이름 매핑이 성공하면, johnsmith로 생성된 모든 파일/폴더에 올바른 사용자 소유권이 표시됩니다. 또한 사용 중인 NAS 프로토콜에 관계없이 "johnsmith"에 영향을 주는 모든 ACL이 적용됩니다. 이것을 대칭 이름 매핑이라고 합니다.

비대칭 이름 매핑은 Windows 사용자 및 UNIX 사용자 ID가 일치하지 않는 경우를 나타냅니다. 예를 들어, 윈도우 사용자인 주스미스(jsmith)가 유닉스의 ID를 갖고 있다면, Cloud Volumes Service는 그 변이에 대한 정보를 얻을 수 있는 방법이 필요합니다. Cloud Volumes Service는 현재 정적 이름 매핑 규칙 생성을 지원하지 않으므로, LDAP를 사용하여 Windows 및 UNIX ID 모두의 사용자 ID를 조회하여 파일 및 폴더의 올바른 소유권과 예상되는 권한을 확인해야 합니다.

기본적으로 Cloud Volumes Service는 이름 맵 데이터베이스 인스턴스의 ns-switch에 LDAP를 포함하므로 비대칭 이름에 LDAP를 사용하여 이름 매핑 기능을 제공하려면 Cloud Volumes Service의 모양을 반영하기 위해 일부 사용자/그룹 속성만 수정하면 됩니다.

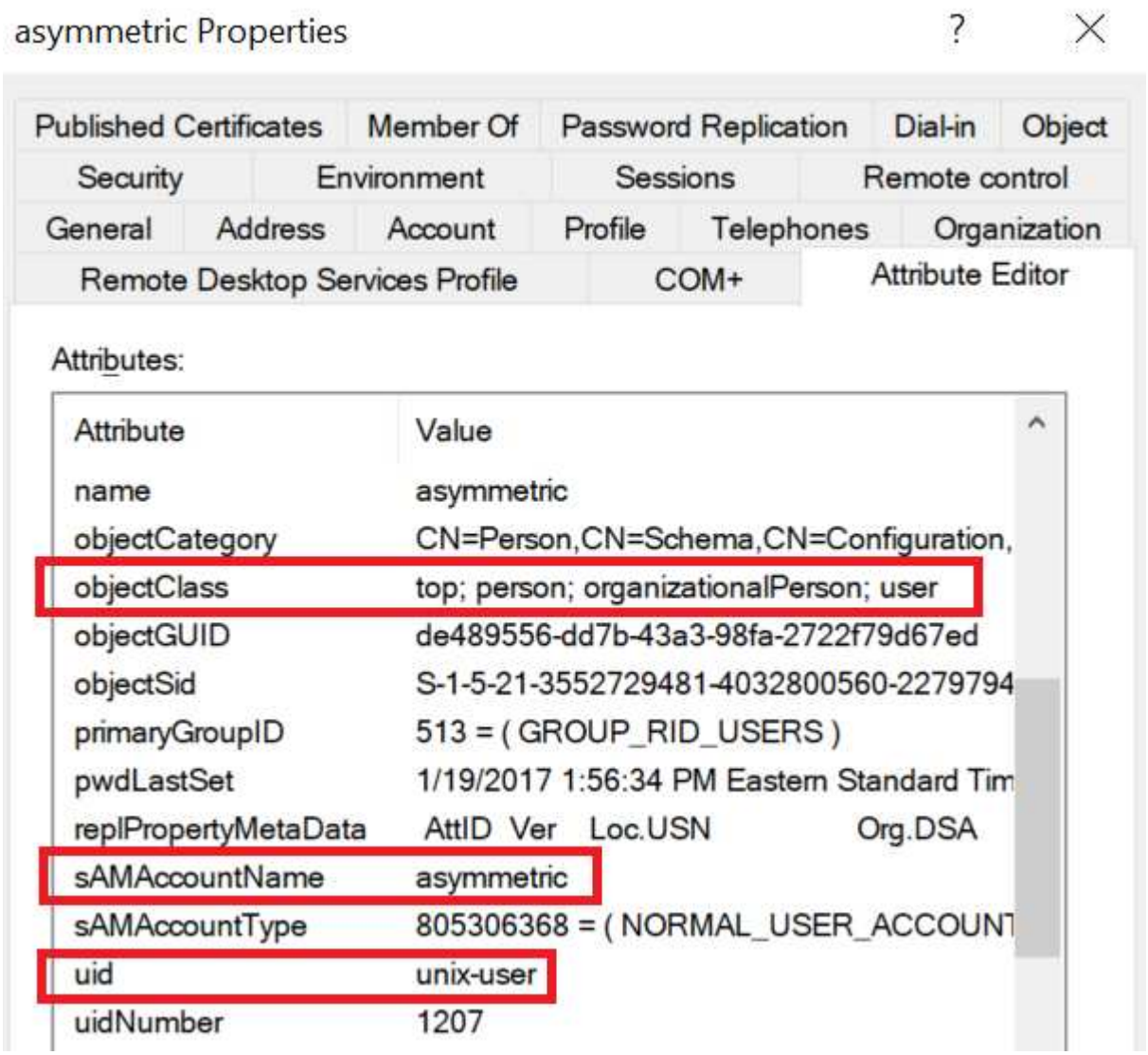
다음 표에서는 비대칭 이름 매핑 기능을 위해 LDAP에 채워야 하는 특성을 보여 줍니다. 대부분의 경우 Active Directory는 이미 이 작업을 수행하도록 구성되어 있습니다.

Cloud Volumes Service 특성입니다	기능	**Cloud Volumes Service**에서 이름 매핑에 사용하는 값입니다
Windows에서 UNIX로의 객체 클래스	사용 중인 개체의 형식을 지정합니다. (즉, 사용자, 그룹, posixAccount 등)	사용자를 포함해야 합니다(필요한 경우 다른 값을 여러 개 포함할 수 있음).
Windows에서 UNIX로의 속성	그러면 생성 시 Windows 사용자 이름이 정의됩니다. Cloud Volumes Service는 Windows에서 UNIX로의 조회에 이 기능을 사용합니다.	여기에서 변경할 필요가 없습니다. sAMAccountName은 Windows 로그인 이름과 동일합니다.
UID	UNIX 사용자 이름을 정의합니다.	원하는 UNIX 사용자 이름입니다.

Cloud Volumes Service는 현재 LDAP 조회에서 도메인 접두사를 사용하지 않으므로 LDAP 이름 맵 조회에서 여러 도메인 LDAP 환경이 제대로 작동하지 않습니다.

다음 예에서는 Windows 이름 "비대칭", UNIX 이름 "UNIX-user"를 가진 사용자와 SMB 및 NFS에서 파일을 쓸 때 나타나는 동작을 보여 줍니다.

다음 그림에서는 LDAP 특성이 Windows 서버에서 어떻게 표시되는지 보여 줍니다.



NFS 클라이언트에서 UNIX 이름을 쿼리할 수 있지만 Windows 이름은 쿼리할 수 없습니다.

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

NFS에서 UNIX-USER로 파일을 쓸 때 NFS 클라이언트의 결과는 다음과 같습니다.

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

Windows 클라이언트에서 파일 소유자가 올바른 Windows 사용자로 설정되어 있는지 확인할 수 있습니다.

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

반대로, SMB 클라이언트에서 Windows 사용자 '비대칭'으로 생성된 파일은 다음 텍스트에서와 같이 적절한 UNIX 소유자를 표시합니다.

SMB:

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS:

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

LDAP 채널 바인딩

Windows Active Directory 도메인 컨트롤러의 취약점으로 인해 "Microsoft 보안 권고 ADV190023" DC에서 LDAP 바인드를 허용하는 방법을 변경합니다.

Cloud Volumes Service에 미치는 영향은 모든 LDAP 클라이언트와 동일합니다. Cloud Volumes Service는 현재 채널 바인딩을 지원하지 않습니다. Cloud Volumes Service는 협상을 통해 기본적으로 LDAP 서명을 지원하므로 LDAP 채널 바인딩은 문제가 되지 않습니다. 채널 바인딩이 설정된 LDAP에 바인딩하는 데 문제가 있는 경우 ADV190023의 개선 단계를 수행하여 Cloud Volumes Service에서 LDAP 바인딩이 성공하도록 허용합니다.

DNS

Active Directory와 Kerberos 모두 호스트 이름 대 IP/IP 대 호스트 이름 확인에 대한 DNS에 대한 종속성을 가집니다. DNS를 열려면 포트 53이 열려 있어야 합니다. Cloud Volumes Service는 DNS 레코드를 수정하지 않으며 현재 의 사용을 지원하지 않습니다 "다이나믹 DNS" 네트워크 인터페이스.

DNS 레코드를 업데이트할 수 있는 서버를 제한하도록 Active Directory DNS를 구성할 수 있습니다. 자세한 내용은 을 참조하십시오 "Windows DNS 보안".

Google 프로젝트 내의 리소스는 기본적으로 Active Directory DNS와 연결되지 않은 Google Cloud DNS를 사용합니다. 클라우드 DNS를 사용하는 클라이언트는 Cloud Volumes Service에서 반환하는 UNC 경로를 확인할 수 없습니다. Active Directory 도메인에 참가한 Windows 클라이언트는 Active Directory DNS를 사용하도록 구성되어 있으며 이러한 UNC 경로를 확인할 수 있습니다.

Active Directory에 클라이언트를 연결하려면 Active Directory DNS를 사용하도록 해당 DNS 구성을 구성해야 합니다. 필요에 따라 Active Directory DNS로 요청을 전달하도록 Cloud DNS를 구성할 수 있습니다. 을 참조하십시오 "클라이언트가 SMB NetBIOS 이름을 확인할 수 없는 이유는 무엇입니까?"를 참조하십시오.

Cloud Volumes Service는 현재 DNSSEC를 지원하지 않으며 DNS 쿼리는 일반 텍스트로 수행됩니다.

파일 액세스 감사

현재 Cloud Volumes Service에서 지원되지 않습니다.

안티바이러스 보호

클라이언트의 Cloud Volumes Service에서 NAS 공유에 대한 바이러스 백신 검사를 수행해야 합니다. 현재 Cloud Volumes Service와 통합된 기본 바이러스 백신이 없습니다.

서비스 작업

Cloud Volumes Service 팀은 Google Cloud에서 백엔드 서비스를 관리하고 여러 전략을 사용하여 플랫폼을 보호하고 원치 않는 액세스를 방지합니다.

각 고객은 기본적으로 다른 고객으로부터 액세스 펜싱된 고유한 서브넷을 받게 되며, Cloud Volumes Service의 모든 테넌트는 전체 데이터 격리를 위한 고유한 네임스페이스와 VLAN을 갖게 됩니다. 사용자가 인증되면 SDE(Service Delivery Engine)는 해당 테넌트와 관련된 구성 데이터만 읽을 수 있습니다.

물리적 보안

적절한 사전 승인을 받은 경우, 현장 엔지니어와 NetApp 내부 현장 지원 엔지니어(FSE)만 물리적 작업을 위한 케이지 및 랙에 액세스할 수 있습니다. 스토리지 및 네트워크 관리는 허용되지 않습니다. 이러한 현장 리소스만 하드웨어 유지 관리 작업을 수행할 수 있습니다.

현장 엔지니어의 경우 랙 ID 및 장치 위치(RU)가 포함된 SOW(Statement of Work)에 대한 티켓이 발행되고 기타 모든 세부 정보가 티켓에 포함됩니다. NetApp FSE의 경우 COLO를 통해 사이트 방문 티켓을 제기해야 하며 티켓에는 감사 목적을 위한 방문자의 세부 정보, 날짜 및 시간이 포함됩니다. FSE용 SOW는 내부적으로 NetApp에 전달됩니다.

운영팀

Cloud Volumes Service의 운영 팀은 운영 엔지니어링과 SRE(Site Reliability Engineer)로 구성되며, 클라우드 볼륨 서비스를 위한 NetApp 현장 지원 엔지니어 및 파트너는 하드웨어에 대해 구성됩니다. 모든 운영 팀 구성원은 Google Cloud에서 작업할 수 있도록 인증되었으며, 제기된 모든 티켓에 대해 자세한 작업 기록이 유지됩니다. 또한 엄격한 변경 관리 및 승인 프로세스를 통해 각 결정이 적절하게 검토되는지 확인할 수 있습니다.

SRE 팀은 컨트롤 플레인을 관리하고 데이터가 UI 요청에서 백엔드 하드웨어 및 Cloud Volumes Service 소프트웨어로 라우팅되는 방식을 관리합니다. SRE 팀은 또한 볼륨 및 inode 최대값과 같은 시스템 리소스를 관리합니다. SRE는 고객 데이터와 상호 작용하거나 고객 데이터에 액세스할 수 없습니다. 또한 SRE는 백엔드 하드웨어에 대한 새 디스크 또는

메모리 교체 요청과 같은 RMA(Return Material Authorizations)와 함께 조정을 제공합니다.

고객의 책임

Cloud Volumes Service 고객은 조직의 Active Directory 및 사용자 역할 관리와 볼륨 및 데이터 작업을 관리합니다. 고객은 NetApp과 Google Cloud(관리자 및 뷰어)가 제공하는 두 가지 사전 정의된 역할을 사용하여 관리 역할을 수행하고 동일한 Google Cloud 프로젝트 내의 다른 최종 사용자에게 권한을 위임할 수 있습니다.

관리자는 고객 프로젝트 내의 모든 VPC를 고객이 적절하다고 판단한 Cloud Volumes Service에 연결할 수 있습니다. 고객은 Google Cloud Marketplace 구독에 대한 액세스를 관리하고 데이터 평면에 액세스할 수 있는 VPC를 관리해야 합니다.

악성 **SRE** 보호

악성 SRE가 있거나 SRE 자격 증명이 손상된 경우 Cloud Volumes Service가 이를 어떻게 보호합니까?

운영 환경에 대한 액세스는 제한된 수의 SRE 사용자만 가능합니다. 관리 권한은 소수의 숙련된 관리자에게만 더욱 제한됩니다. Cloud Volumes Service 운영 환경의 모든 작업이 기록되고 기준 또는 의심스러운 활동에 대한 모든 이상 사항은 SIEM(Security Information and Event Management) 위협 인텔리전스 플랫폼에서 탐지됩니다. 따라서 Cloud Volumes Service 백엔드에 너무 많은 손상이 발생하기 전에 악의적인 작업을 추적하고 완화할 수 있습니다.

볼륨 수명 주기

Cloud Volumes Service는 볼륨 내의 데이터가 아니라 서비스 내의 객체만 관리합니다. 볼륨에 액세스하는 클라이언트만 데이터, ACL, 파일 소유자 등을 관리할 수 있습니다. 이러한 볼륨의 데이터는 유휴 상태로 암호화되며 액세스는 Cloud Volumes Service 인스턴스 테넌트로 제한됩니다.

Cloud Volumes Service의 볼륨 라이프사이클은 create-update-delete입니다. 볼륨은 볼륨이 삭제될 때까지 볼륨의 스냅샷 복사본을 유지하며, 검증된 Cloud Volumes Service 관리자만 Cloud Volumes Service의 볼륨을 삭제할 수 있습니다. 관리자가 볼륨 삭제를 요청하는 경우 삭제를 확인하려면 볼륨 이름을 추가로 입력해야 합니다. 볼륨이 삭제된 후에는 볼륨이 사라지고 복구할 수 없습니다.

Cloud Volumes Service 계약이 종료된 경우 NetApp은 특정 기간 이후에 삭제할 볼륨을 표시합니다. 이 기간이 만료되기 전에 고객의 요청에 따라 볼륨을 복구할 수 있습니다.

인증

Cloud Volumes Services for Google Cloud는 현재 ISO/IEC 27001:2013 및 ISO/IEC 27018:2019 표준에 따라 인증되었습니다. 또한 이 서비스는 최근 SOC2 Type I Attestation 보고서를 받았습니다. 데이터 보안 및 개인 정보 보호에 대한 NetApp의 약속에 대한 자세한 내용은 을 참조하십시오 "규정 준수: 데이터 보안 및 데이터 개인 정보 보호".

GDPR을 참조하십시오

개인 정보 보호 및 GDPR 준수에 대한 NetApp의 약속은 당사의 다양한 규정으로 제공됩니다 "고객 계약"있습니다 "고객 데이터 처리 부록"를 포함합니다 "표준 계약 조항" 유럽 위원회에서 제공. 또한 NetApp은 개인 정보 보호 정책에 이러한 의무를 이행하며, 이는 기업 행동 강령에 명시된 핵심 가치를 기반으로 합니다.

추가 정보 및 연락처 정보

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹 사이트를 검토하십시오.

- Cloud Volumes Service용 Google Cloud 설명서

"https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"

- Google 전용 서비스 액세스

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- NetApp 제품 설명서

  "https://www.netapp.com/support-and-training/documentation/"

- 암호화 검증 모듈 프로그램 — NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- 랜섬웨어용 NetApp 솔루션

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616: ONTAP에서 NFS Kerberos

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

문의하기

이 기술 보고서를 개선할 방법을 알려주십시오.

이메일: mailto:doccomments@netapp.com [doccomments@netapp.com^]로 연락해 주십시오. 제목 줄에 기술 보고서 4918 포함.

BlueXP 백업 및 복구

VM용 BlueXP 백업 및 복구

VM용 SnapCenter 플러그인 및 BlueXP 백업 및 복구를 통한 VMware용 3-2-1 데이터 보호

저자: Josh Powell - NetApp 솔루션 엔지니어링

개요

3-2-1 백업 전략은 업계에서 인정하는 데이터 보호 방법으로서 중요한 데이터를 보호하기 위한 포괄적인 접근 방식을 제공합니다. 이 전략은 신뢰할 수 있으며 예상치 못한 재해 발생 시에도 데이터 사본이 계속 사용될 수 있습니다.

이 전략은 다음과 같은 세 가지 기본 규칙으로 구성됩니다.

1. 데이터의 복사본을 3개 이상 유지해야 합니다. 이렇게 하면 한 복사본이 손실되거나 손상된 경우에도 남아 있는 복사본이 두 개 이상 남아 있습니다.
2. 두 개의 백업 복사본을 서로 다른 저장소 미디어 또는 장치에 저장합니다. 다양한 저장 미디어를 사용하면 장치별 또는 미디어별 장애로부터 보호할 수 있습니다. 한 장치가 손상되었거나 한 유형의 미디어가 실패하는 경우 다른 백업 사본은 영향을 받지 않습니다.
3. 마지막으로 하나 이상의 백업 복제본이 오프사이트에 있는지 확인합니다. 오프사이트 스토리지는 화재 또는 홍수와 같은 지역화된 재해에 대해 장애 발생 시 현장 복제본을 사용할 수 없게 됩니다.

이 솔루션 문서에서는 SCV(VMware vSphere)용 SnapCenter 플러그인을 사용하여 온프레미스 가상 머신의 운영 및 2차 백업을 생성하는 3-2-1 백업 솔루션과 가상 머신의 데이터 복사본을 클라우드 스토리지 또는 StorageGRID에 백업하는 가상 머신에 대한 BlueXP 백업 및 복구를 다룹니다.

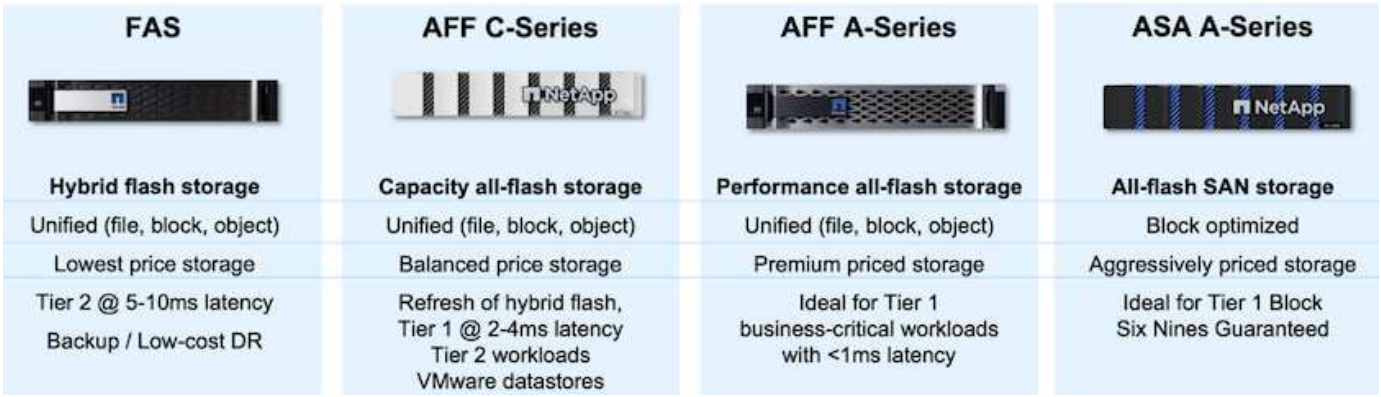
사용 사례

이 솔루션은 다음과 같은 사용 사례를 해결합니다.

- VMware vSphere용 SnapCenter 플러그인을 사용하여 사내 가상 머신 및 데이터 저장소를 백업 및 복원합니다.
- ONTAP 클러스터에서 호스팅되고 가상 머신에 대한 BlueXP 백업 및 복구를 사용하여 온프레미스 가상 머신 및 데이터 저장소를 백업 및 복원하고 오브젝트 스토리지에 백업합니다.

NetApp ONTAP 데이터 스토리지

ONTAP은 NetApp의 업계 최고 스토리지 솔루션으로, SAN 또는 NAS 프로토콜을 통해 액세스할 수 있는 유니파이드 스토리지를 제공합니다. 3-2-1 백업 전략을 통해 사내 데이터를 둘 이상의 미디어 유형에서 보호할 수 있고 NetApp은 고속 플래시에서 저렴한 미디어에 이르는 플랫폼을 제공합니다.



NetApp의 모든 하드웨어 플랫폼에 대해 자세히 알아보십시오 "NetApp 데이터 스토리지".

VMware vSphere용 SnapCenter 플러그인

VMware vSphere용 SnapCenter 플러그인은 VMware vSphere와 긴밀하게 통합되어 가상 머신의 백업 및 복원을 쉽게 관리할 수 있는 데이터 보호 오퍼링입니다. 이러한 솔루션의 일부로 SnapMirror는 보조 ONTAP 스토리지 클러스터에 가상 머신 데이터의 변경 불가능한 두 번째 백업 복사본을 빠르고 안정적으로 생성할 수 있는 방법을 제공합니다. 이 아키텍처를 사용하면 운영 또는 보조 백업 위치에서 가상 머신 복구 작업을 쉽게 시작할 수 있습니다.

SCV는 OVA 파일을 사용하여 Linux 가상 어플라이언스로 구축됩니다. 이제 플러그인에서 원격 플러그인을 사용합니다 있을 겁니다. 원격 플러그인은 vCenter 서버 외부에서 실행되며 SCV 가상 어플라이언스에서 호스팅됩니다.

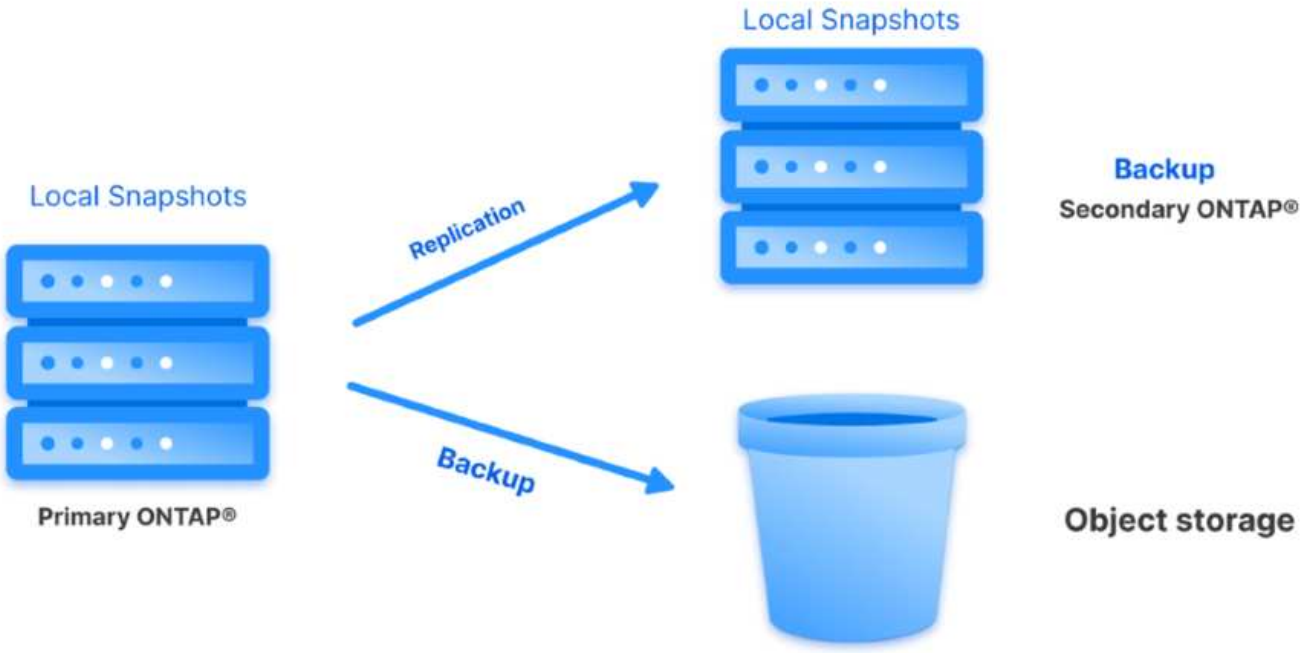
SCV에 대한 자세한 내용은 을 참조하십시오 "VMware vSphere용 SnapCenter 플러그인 설명서".

가상 머신에 대한 BlueXP 백업 및 복구

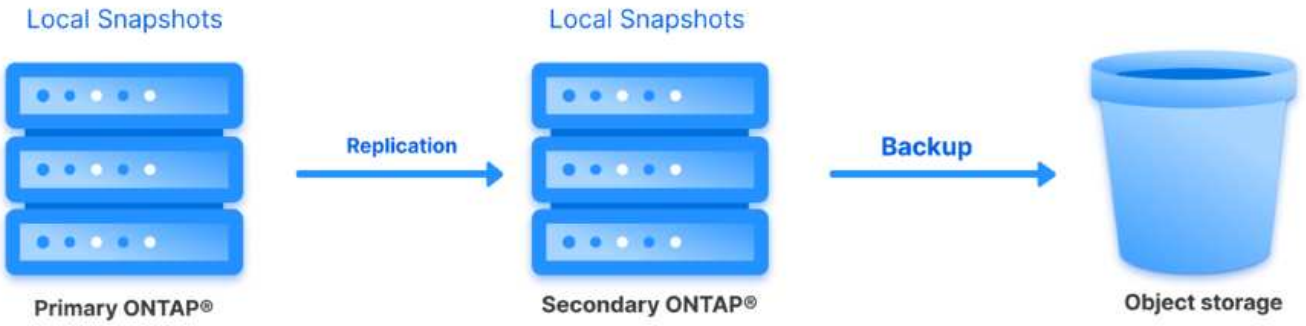
BlueXP 백업 및 복구는 데이터 관리를 위한 클라우드 기반 툴로서 온프레미스와 클라우드 환경 모두에서 다양한 백업 및 복구 작업을 위한 단일 제어 플레인을 제공합니다. NetApp BlueXP 백업 및 복구 제품군의 일부는 VMware vSphere(사내)용 SnapCenter 플러그인과 통합되어 데이터 복사본을 클라우드의 오브젝트 스토리지로 확장하는 기능입니다. 이렇게 하면 운영 또는 보조 스토리지 백업에서 가져온 세 번째 오프사이트 데이터 복제본이 설정됩니다. BlueXP 백업 및 복구를 사용하면 두 개의 온프레미스 위치 중 하나에서 데이터 복사본을 전송하는 스토리지 정책을 쉽게 설정할 수 있습니다.

BlueXP 백업 및 복구에서 기본 백업과 보조 백업 중에서 소스로 선택하면 다음 두 가지 토폴로지 중 하나가 구현됩니다.

- 팬아웃 토폴로지 * – VMware vSphere용 SnapCenter 플러그인에 의해 백업이 시작되면 로컬 스냅샷이 즉시 생성됩니다. 그런 다음 SCV가 최신 스냅샷을 보조 ONTAP 클러스터에 복제하는 SnapMirror 작업을 시작합니다. BlueXP 백업 및 복구에서 정책은 기본 ONTAP 클러스터를 선택한 클라우드 공급자의 오브젝트 스토리지로 전송할 데이터의 스냅샷 복사본의 소스로 지정합니다.



계단식 토폴로지 – SCV를 사용하여 기본 및 보조 데이터 사본을 만드는 것은 위에서 언급한 팬아웃 토폴로지와 동일합니다. 하지만 이번에는 BlueXP 백업 및 복구에 정책이 생성되어 오브젝트 스토리지에 대한 백업이 2차 ONTAP 클러스터에서 시작되도록 지정합니다.



BlueXP 백업 및 복구를 통해 온프레미스 ONTAP 스냅샷의 백업 복사본을 AWS Glacier, Azure Blob 및 GCP 아카이브 스토리지에 생성할 수 있습니다.

AWS Glacier and Deep Glacier

Azure Blob Archive

GCP Archive Storage

또한 NetApp StorageGRID를 오브젝트 스토리지 백업 타겟으로 사용할 수 있습니다. StorageGRID에 대한 자세한 내용은 를 참조하십시오 "StorageGRID 랜딩 페이지".

솔루션 구축 개요

이 목록에는 이 솔루션을 구성하고 SCV 및 BlueXP 백업 및 복구에서 백업 및 복원 작업을 실행하는 데 필요한 상위 단계가 나와 있습니다.

1. 운영 및 2차 데이터 복사본에 사용할 ONTAP 클러스터 간에 SnapMirror 관계를 구성합니다.
2. VMware vSphere용 SnapCenter 플러그인을 구성합니다.
   a. 스토리지 시스템을 추가합니다
   b. 백업 정책을 생성합니다
   c. 리소스 그룹을 생성합니다
   d. 백업 첫 번째 백업 작업을 실행합니다
3. 가상 머신에 대한 BlueXP 백업 및 복구 구성
   a. 작업 환경을 추가합니다
   b. SCV 및 vCenter 어플라이언스를 검색합니다
   c. 백업 정책을 생성합니다
   d. 백업을 활성화합니다
4. SCV를 사용하여 기본 및 보조 스토리지에서 가상 머신을 복구합니다.
5. BlueXP 백업 및 복원을 사용하여 오브젝트 스토리지에서 가상 머신을 복원합니다.

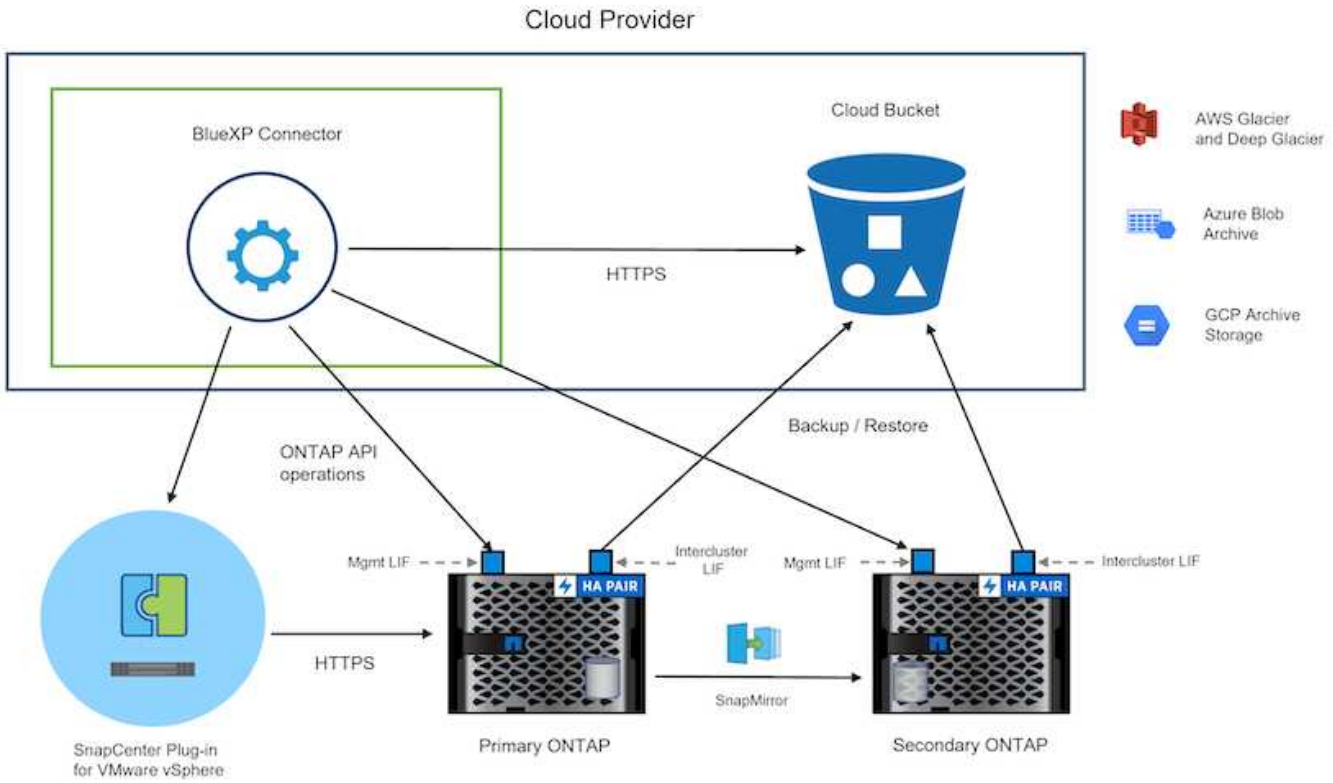
필수 구성 요소

이 솔루션의 목적은 VMware vSphere에서 실행되고 NetApp ONTAP에서 호스팅하는 NFS 데이터 저장소에 있는 가상 시스템의 데이터 보호를 시연하는 것입니다. 이 솔루션에서는 다음 구성 요소가 구성되어 사용할 준비가 되어 있다고 가정합니다.

1. VMware vSphere에 연결된 NFS 또는 VMFS 데이터 저장소가 있는 ONTAP 스토리지 클러스터 NFS 및 VMFS 데이터 저장소가 모두 지원됩니다. 이 솔루션에는 NFS 데이터 저장소가 사용되었습니다.
2. NFS 데이터 저장소에 사용되는 볼륨에 대해 SnapMirror 관계가 설정된 보조 ONTAP 스토리지 클러스터
3. 오브젝트 스토리지 백업에 사용되는 클라우드 공급자용으로 BlueXP 커넥터가 설치되었습니다.
4. 백업할 가상 머신은 운영 ONTAP 스토리지 클러스터에 상주하는 NFS 데이터 저장소에 있습니다.
5. BlueXP 커넥터와 온프레미스 ONTAP 스토리지 클러스터 관리 인터페이스 간의 네트워크 연결
6. BlueXP 커넥터와 사내 SCV 어플라이언스 VM 간의 네트워크 연결, 그리고 BlueXP connector와 vCenter 간의 네트워크 연결
7. 온프레미스 ONTAP 인터클러스터 LIF와 오브젝트 스토리지 서비스 간의 네트워크 연결
8. 1차 및 2차 ONTAP 스토리지 클러스터의 관리 SVM을 위해 구성된 DNS 자세한 내용은 을 참조하십시오 "호스트 이름 확인을 위해 DNS를 구성합니다".

고급 아키텍처

이 솔루션의 테스트/검증은 최종 배포 환경과 일치하거나 일치하지 않을 수 있는 랩에서 수행되었습니다.



솔루션 구축

이 솔루션에서 NetApp은 VMware vSphere용 SnapCenter 플러그인을 BlueXP 백업 및 복구와 함께 사용하여 사내 데이터 센터에 있는 VMware vSphere 클러스터 내에서 Windows 및 Linux 가상 머신에 대한 백업 및 복구를 수행하는 솔루션을 구축하고 검증하는 상세한 지침을 제공합니다. 이 설정의 가상 머신은 ONTAP A300 스토리지 클러스터에서 호스팅하는 NFS 데이터 저장소에 저장됩니다. 또한 별도의 ONTAP A300 스토리지 클러스터가 SnapMirror를 사용하여 복제된 볼륨의 보조 대상으로 사용됩니다. 또한 Amazon Web Services 및 Azure Blob에서 호스팅되는 오브젝트 스토리지는 데이터의 세 번째 복사본의 타겟으로 사용되었습니다.

SCV로 관리되는 백업의 보조 복사본에 대한 SnapMirror 관계 생성과 SCV 및 BlueXP 백업 및 복구 모두에서 백업 작업에 대한 구성을 살펴보겠습니다.

VMware vSphere용 SnapCenter 플러그인에 대한 자세한 내용은 를 참조하십시오 "VMware vSphere용 SnapCenter 플러그인 설명서".

BlueXP 백업 및 복구에 대한 자세한 내용은 를 참조하십시오 "BlueXP 백업 및 복구 설명서".

ONTAP 클러스터 간 **SnapMirror** 관계 설정

VMware vSphere용 SnapCenter 플러그인은 ONTAP SnapMirror 기술을 사용하여 보조 SnapMirror 및/또는 SnapVault 복사본을 보조 ONTAP 클러스터로 전송하는 작업을 관리합니다.

SCV 백업 정책에는 SnapMirror 또는 SnapVault 관계를 사용하는 옵션이 있습니다. 주된 차이점은 SnapMirror 옵션을 사용할 경우 정책의 백업에 대해 구성된 보존 일정이 운영 위치와 보조 위치에서 동일하다는 점입니다. SnapVault는 아카이빙용으로 설계되었으며, 이 옵션을 사용할 경우 보조 ONTAP 스토리지 클러스터에 있는 스냅샷 복사본에 대한 SnapMirror 관계를 통해 별도의 보존 일정을 설정할 수 있습니다.

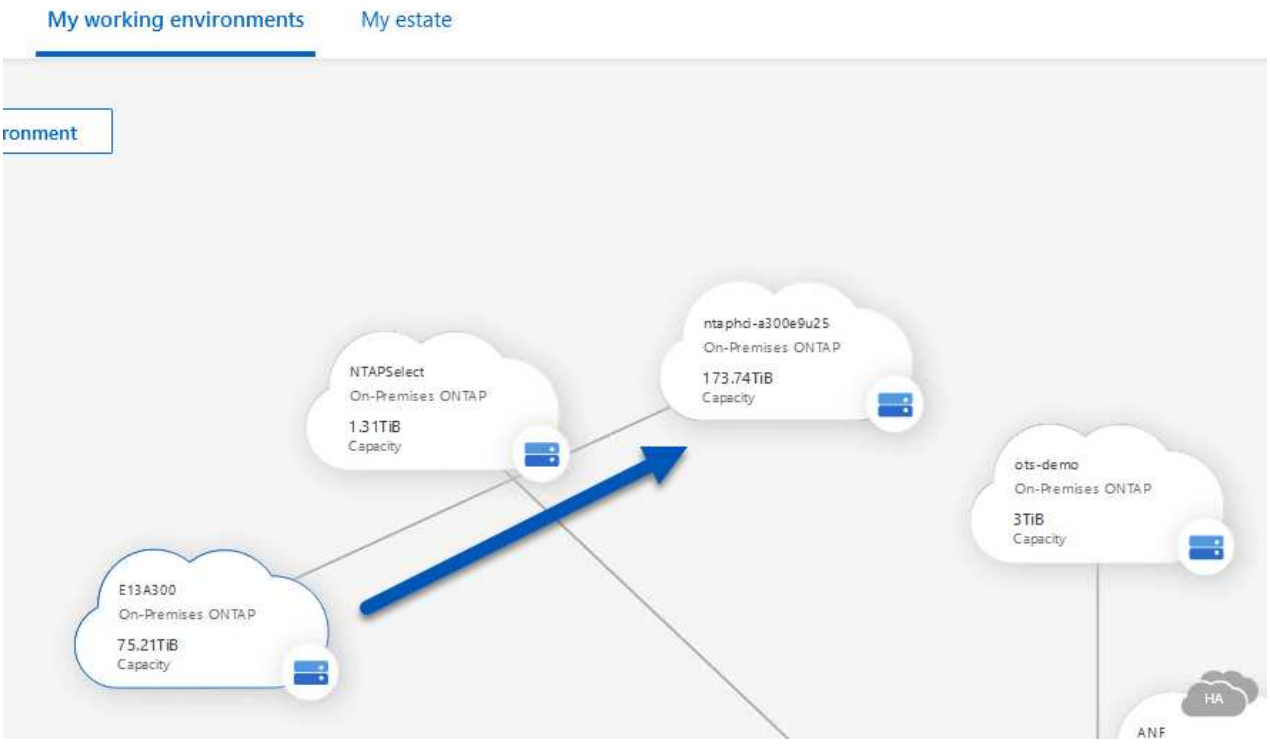
SnapMirror 관계를 설정하는 작업은 다양한 단계가 자동화된 BlueXP에서 수행할 수 있으며, System Manager와 ONTAP CLI를 사용하여 수행할 수도 있습니다. 이러한 모든 방법은 아래에 설명되어 있습니다.

BlueXP와 **SnapMirror** 관계 설정

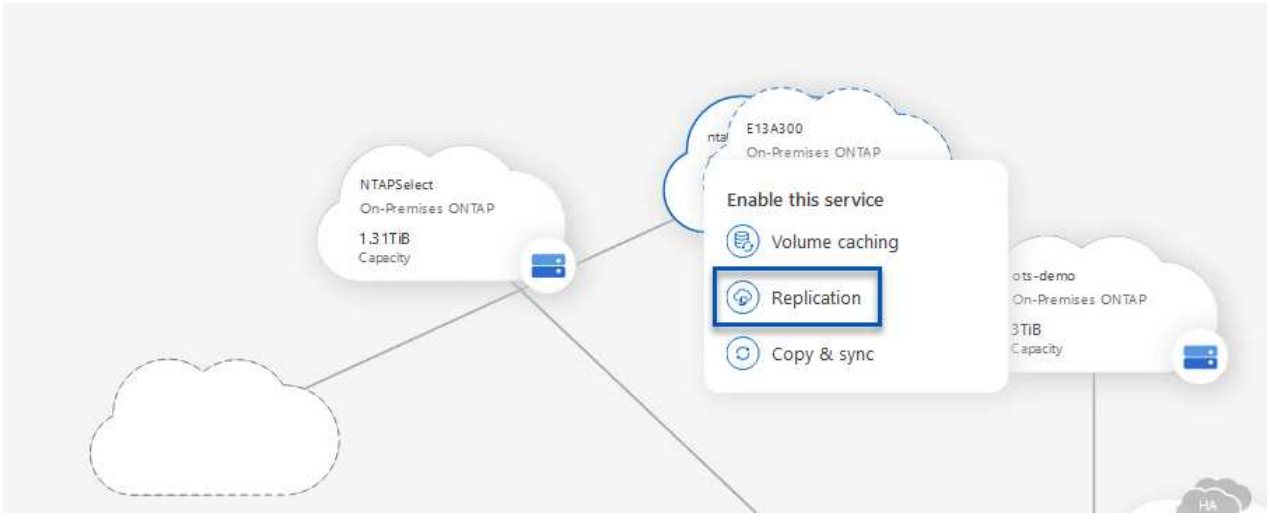
BlueXP 웹 콘솔에서 다음 단계를 완료해야 합니다.

먼저 BlueXP 웹 콘솔에 로그인하고 Canvas로 이동합니다.

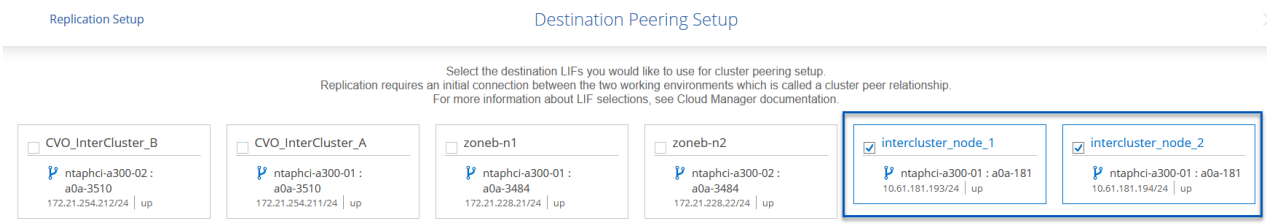
1. 소스(운영) ONTAP 스토리지 시스템을 대상(2차) ONTAP 스토리지 시스템으로 끌어다 놓으십시오.



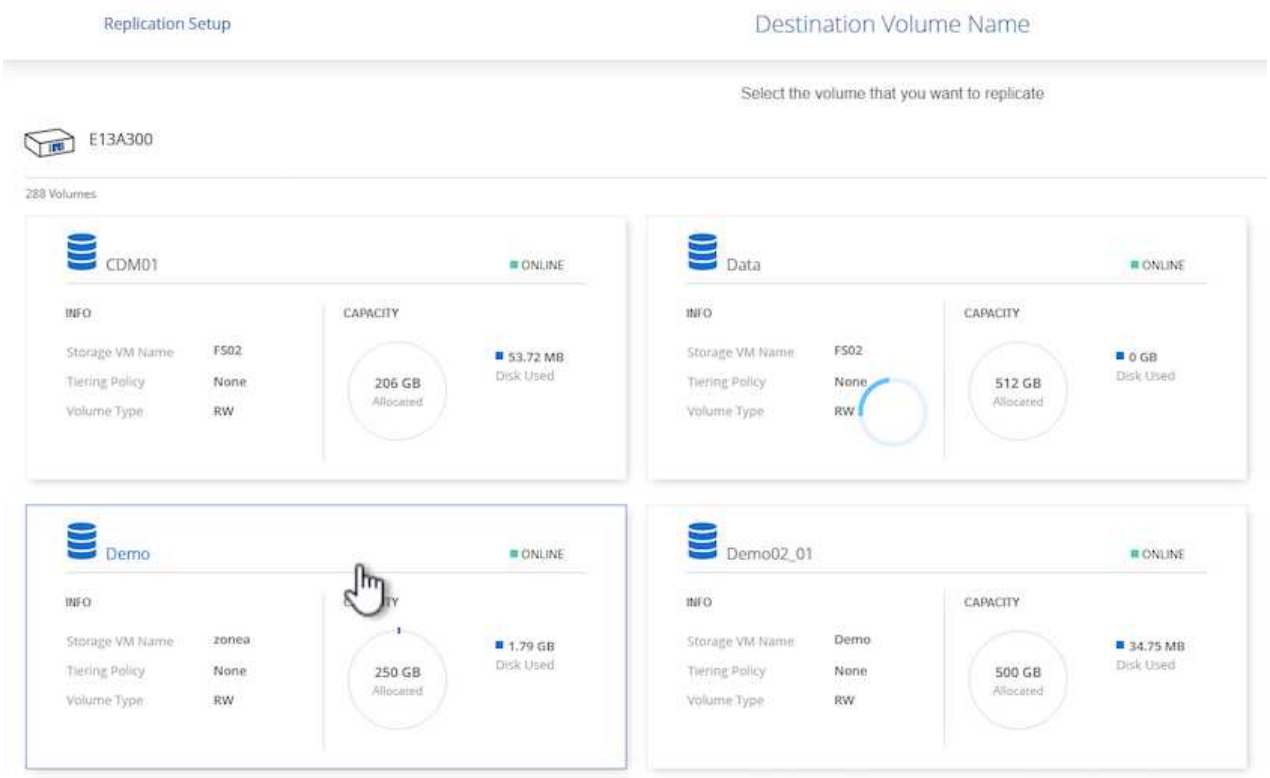
2. 나타나는 메뉴에서 * Replication * 을 선택합니다.



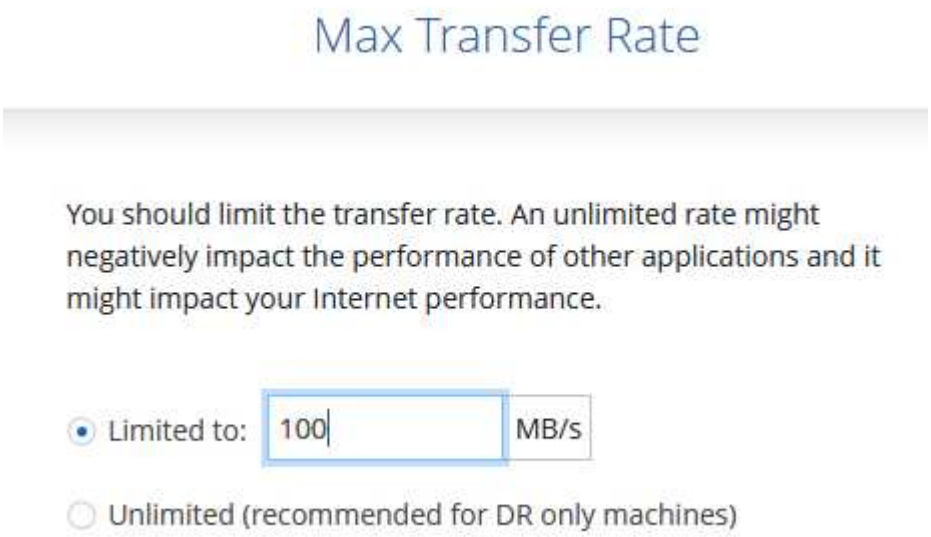
3. Destination 피어링 Setup * 페이지에서 스토리지 시스템 간 연결에 사용할 대상 클러스터 LIF를 선택합니다.



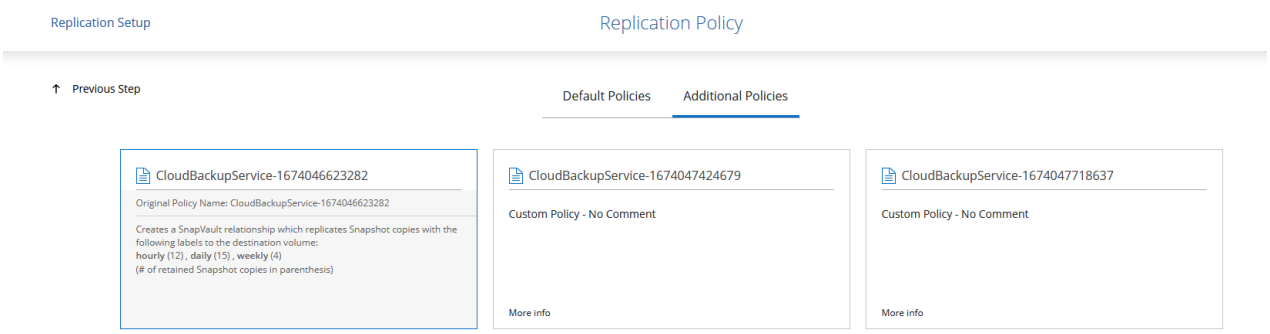
4. Destination Volume Name * 페이지에서 먼저 소스 볼륨을 선택한 다음 대상 볼륨 이름을 입력하고 대상 SVM 및 애그리게이트를 선택합니다. 계속하려면 * 다음 * 을 클릭하십시오.



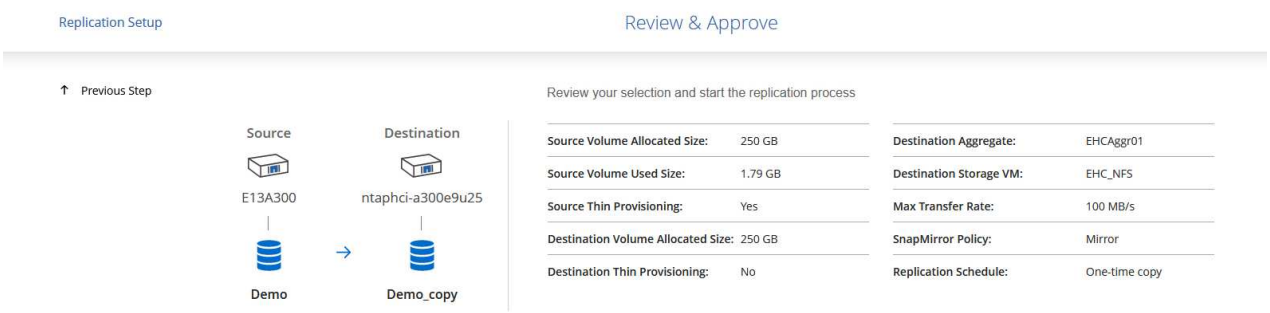
5. 에서 복제를 수행할 최대 전송 속도를 선택합니다.



6. 보조 백업의 보존 일정을 결정할 정책을 선택합니다. 이 정책은 미리 생성하거나(* 스냅샷 보존 정책 만들기 * 단계에서 아래의 수동 프로세스 참조) 원하는 경우 변경 후 변경할 수 있습니다.



7. 마지막으로 모든 정보를 검토하고 * Go * 버튼을 클릭하여 복제 설정 프로세스를 시작합니다.



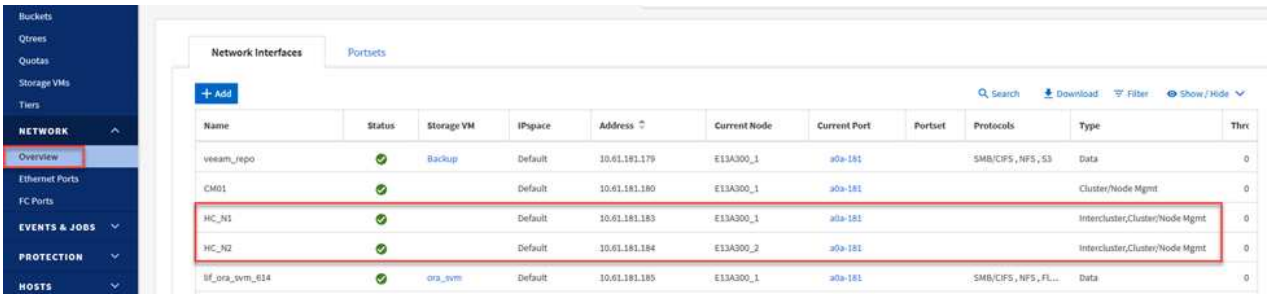
System Manager 및 ONTAP CLI와 SnapMirror 관계 설정

SnapMirror 관계를 설정하는 데 필요한 모든 단계는 System Manager 또는 ONTAP CLI를 사용하여 수행할 수 있습니다. 다음 섹션에서는 두 가지 방법에 대한 자세한 정보를 제공합니다.

소스 및 대상 클러스터간 논리 인터페이스를 기록합니다

소스 및 대상 ONTAP 클러스터의 경우 System Manager 또는 CLI에서 클러스터 간 LIF 정보를 검색할 수 있습니다.

1. ONTAP System Manager에서 네트워크 개요 페이지로 이동하여 FSx가 설치된 AWS VPC와 통신하도록 구성된 Type:Intercluster의 IP 주소를 검색합니다.



2. CLI를 사용하여 Intercluster IP 주소를 검색하려면 다음 명령을 실행합니다.

```
ONTAP-Dest::> network interface show -role intercluster
```

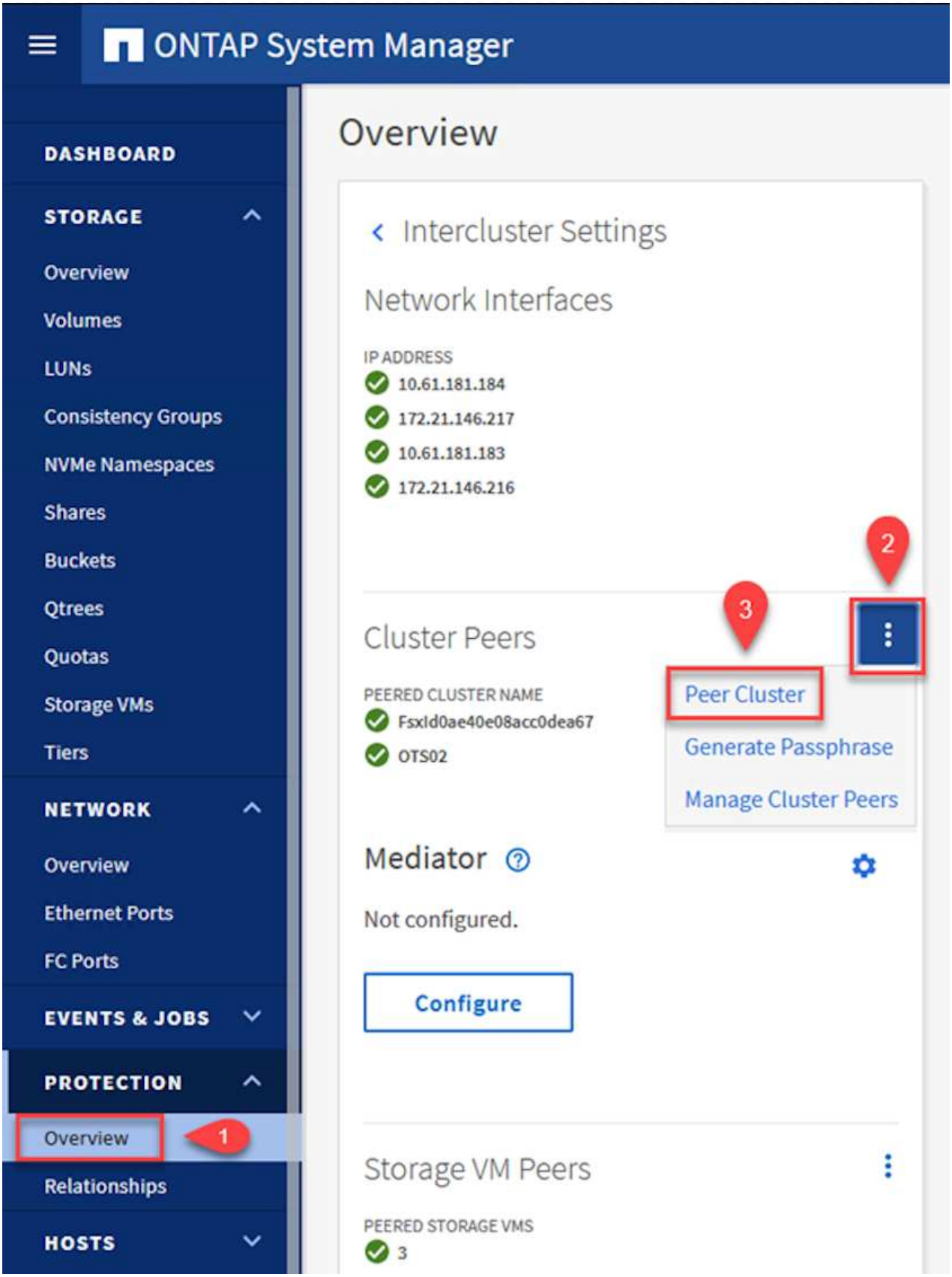
ONTAP 클러스터 간 클러스터 피어링을 설정합니다

ONTAP 클러스터 간에 클러스터 피어링을 설정하려면 시작 ONTAP 클러스터에 입력된 고유한 암호가 다른 피어 클러스터에서 확인되어야 합니다.

1. 를 사용하여 타겟 ONTAP 클러스터의 피어링을 설정합니다 `cluster peer create` 명령. 메시지가 표시되면 소스 클러스터에서 나중에 사용되는 고유한 암호를 입력하여 생성 프로세스를 마칩니다.

```
ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

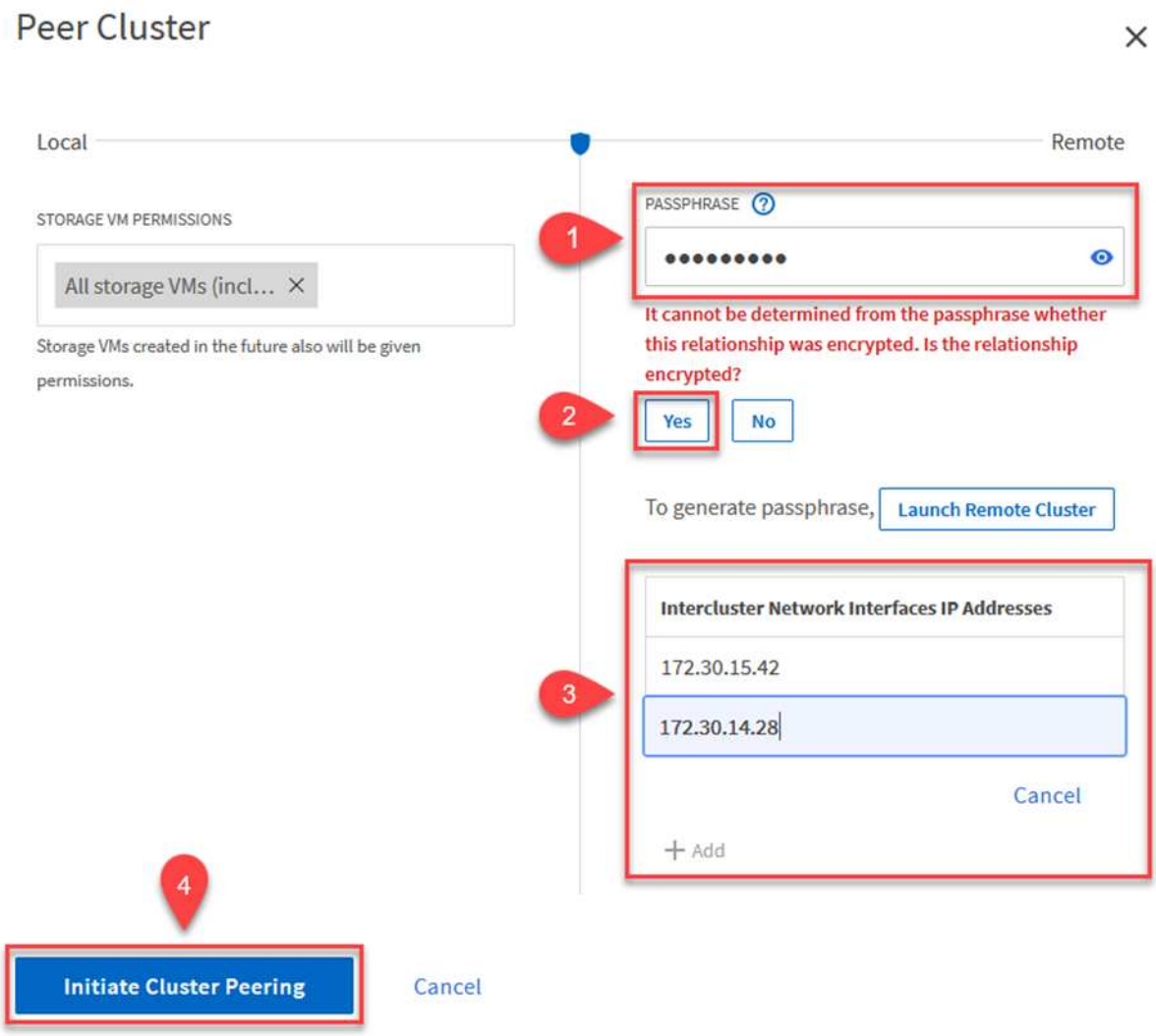
2. 소스 클러스터에서 ONTAP System Manager 또는 CLI를 사용하여 클러스터 피어 관계를 설정할 수 있습니다. ONTAP 시스템 관리자에서 보호 > 개요 로 이동하고 피어 클러스터 를 선택합니다.



3. 피어 클러스터 대화 상자에서 필요한 정보를 입력합니다.
   a. 대상 ONTAP 클러스터에서 피어 클러스터 관계를 설정하는 데 사용된 암호를 입력합니다.
   b. 암호화된 관계를 설정하려면 Yes를 선택합니다.

c. 대상 ONTAP 클러스터의 인터클러스터 LIF IP 주소를 입력합니다.

d. 클러스터 피어링 시작 을 클릭하여 프로세스를 마칩니다.



4. 다음 명령을 사용하여 대상 ONTAP 클러스터에서 클러스터 피어 관계의 상태를 확인합니다.

```
ONTAP-Dest::> cluster peer show
```

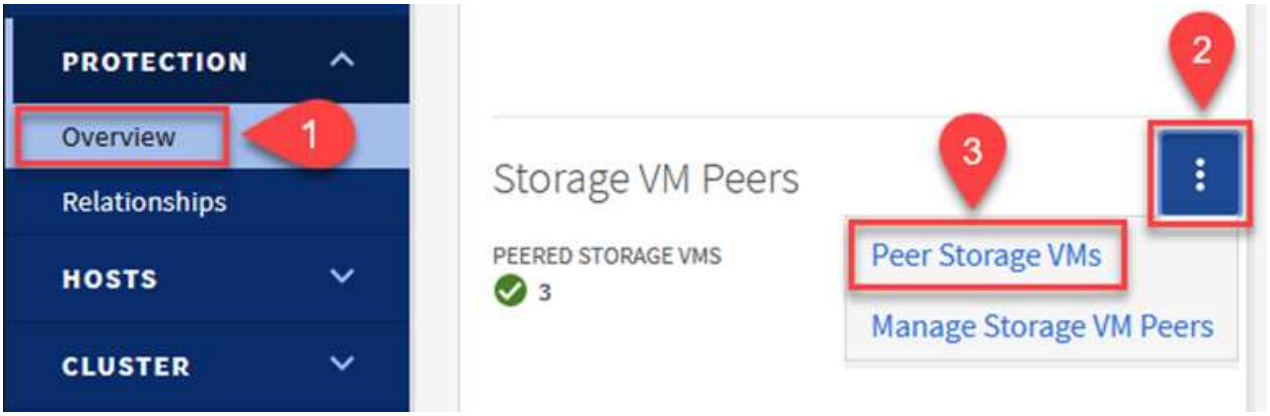
SVM 피어링 관계를 설정합니다

다음 단계는 SnapMirror 관계에 있는 볼륨을 포함하는 소스 스토리지 가상 시스템과 타겟 스토리지 가상 시스템 간에 SVM 관계를 설정하는 것입니다.

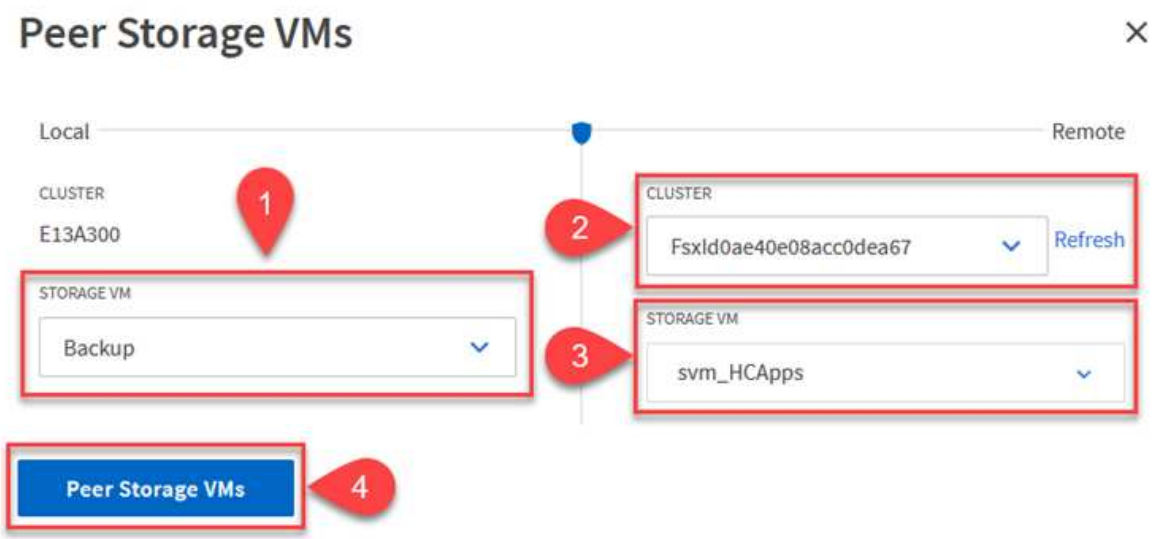
1. 대상 ONTAP 클러스터에서 CLI에서 다음 명령을 사용하여 SVM 피어 관계를 생성합니다.

```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. 소스 ONTAP 클러스터에서 ONTAP System Manager 또는 CLI와 피어링 관계를 수락합니다.
3. ONTAP 시스템 관리자에서 보호 > 개요 로 이동하고 스토리지 VM 피어 아래에서 피어 스토리지 VM 을 선택합니다.



4. 피어 스토리지 VM 대화 상자에서 필수 필드를 입력합니다.
   - 소스 스토리지 VM입니다
   - 타겟 클러스터
   - 대상 스토리지 VM입니다



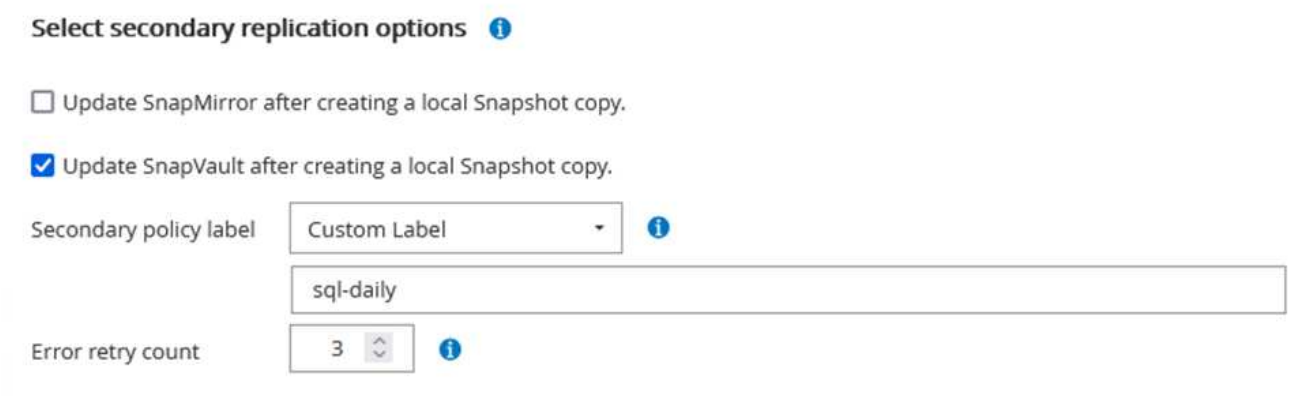
5. 피어 스토리지 VM 을 클릭하여 SVM 피어링 프로세스를 완료합니다.

SnapCenter는 운영 스토리지 시스템에서 스냅샷 복사본으로 존재하는 백업의 보존 일정을 관리합니다. SnapCenter에서 정책을 생성할 때 설정됩니다. SnapCenter는 보조 스토리지 시스템에 보존되는 백업에 대한 보존 정책을 관리하지 않습니다. 이러한 정책은 보조 FSx 클러스터에서 생성되고 소스 볼륨과 SnapMirror 관계에 있는 대상 볼륨에 연결된 SnapMirror 정책을 통해 별도로 관리됩니다.

SnapCenter 정책을 생성할 때 SnapCenter 백업을 수행할 때 생성되는 각 스냅샷의 SnapMirror 레이블에 추가되는 2차 정책 레이블을 지정할 수 있습니다.

ⓘ 보조 스토리지에서 이러한 레이블은 스냅샷 보존을 적용하기 위해 대상 볼륨과 관련된 정책 규칙과 일치합니다.

다음 예제는 SQL Server 데이터베이스 및 로그 볼륨의 일일 백업에 사용되는 정책의 일부로 생성된 모든 스냅샷에 존재하는 SnapMirror 레이블을 보여줍니다.



SQL Server 데이터베이스에 대한 SnapCenter 정책을 만드는 방법에 대한 자세한 내용은 을 참조하십시오 "SnapCenter 설명서".

우선 유지할 스냅샷 복사본 수를 결정하는 규칙을 사용하여 SnapMirror 정책을 생성해야 합니다.

1. FSx 클러스터에서 SnapMirror 정책을 생성합니다.

```
ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. SnapCenter 정책에 지정된 2차 정책 레이블과 일치하는 SnapMirror 레이블을 사용하여 정책에 규칙을 추가합니다.

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

다음 스크립트는 정책에 추가할 수 있는 규칙의 예를 제공합니다.

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest
-policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

각 SnapMirror 레이블과 유지할 스냅샷 수(보존 기간)에 대한 추가 규칙을 생성합니다.

대상 볼륨을 생성합니다

ONTAP에서 소스 볼륨의 스냅샷 복사본을 받을 대상 볼륨을 생성하려면 대상 ONTAP 클러스터에서 다음 명령을 실행합니다.

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

소스 볼륨과 타겟 볼륨 간의 **SnapMirror** 관계를 생성합니다

소스 볼륨과 타겟 볼륨 간에 SnapMirror 관계를 생성하려면 대상 ONTAP 클러스터에서 다음 명령을 실행하십시오.

```
ONTAP-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

SnapMirror 관계 초기화

SnapMirror 관계를 초기화합니다. 이 프로세스에서는 소스 볼륨에서 생성된 새 스냅샷을 시작하여 타겟 볼륨에 복사합니다.

볼륨을 생성하려면 대상 ONTAP 클러스터에서 다음 명령을 실행하십시오.

```
ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

VMware vSphere용 **SnapCenter** 플러그인을 구성합니다

설치가 완료되면 vCenter Server Appliance 관리 인터페이스에서 VMware vSphere용 SnapCenter 플러그인을 액세스할 수 있습니다. SCV는 ESXi 호스트에 마운트되고 Windows 및 Linux VM이 포함된 NFS 데이터 저장소에 대한 백업을 관리합니다.

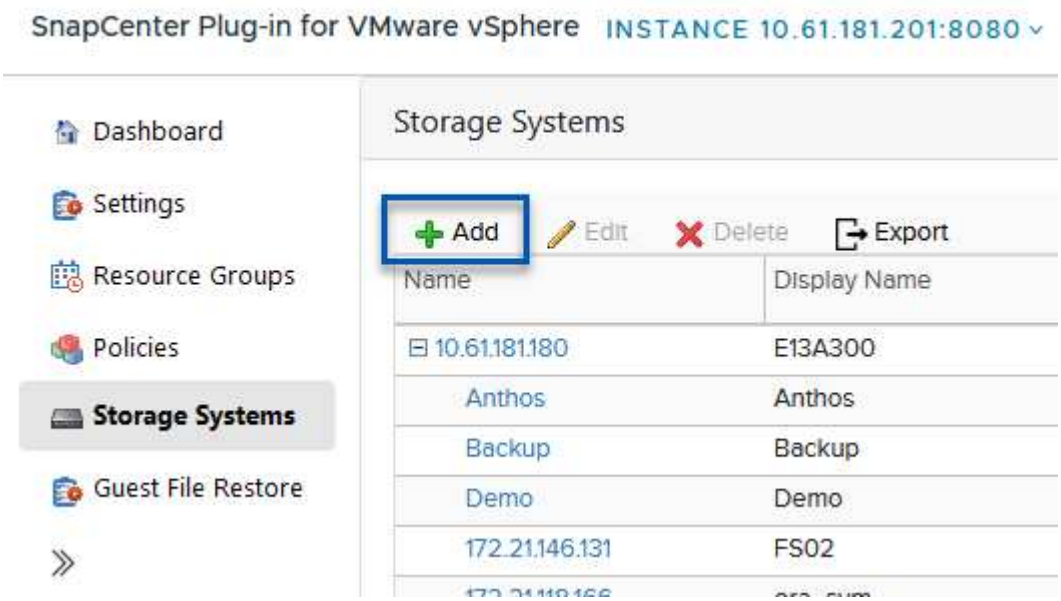
를 검토합니다 "데이터 보호 워크플로우" 백업 구성 단계에 대한 자세한 내용은 SCV 설명서의 섹션을 참조하십시오.

가상 머신 및 데이터 저장소의 백업을 구성하려면 플러그인 인터페이스에서 다음 단계를 완료해야 합니다.

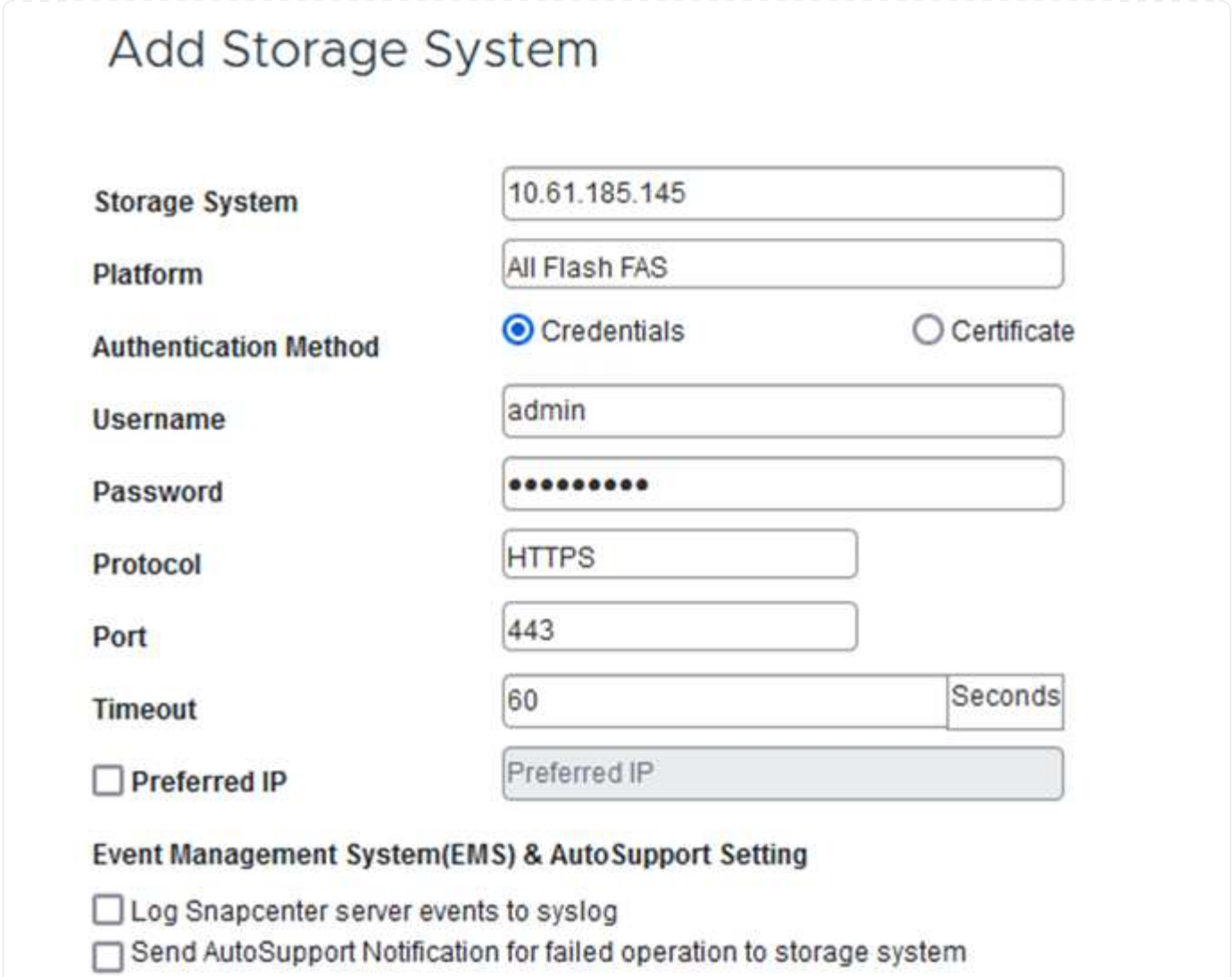
Discovery ONTAP 스토리지 시스템

운영 백업과 보조 백업에 모두 사용할 ONTAP 스토리지 클러스터를 검색합니다.

1. VMware vSphere용 SnapCenter 플러그인에서 왼쪽 메뉴의 * 스토리지 시스템 * 으로 이동한 후 * 추가 * 버튼을 클릭합니다.



2. 운영 ONTAP 스토리지 시스템의 자격 증명 및 플랫폼 유형을 입력하고 * Add * 를 클릭합니다.



3. 보조 ONTAP 스토리지 시스템에 대해 이 절차를 반복합니다.

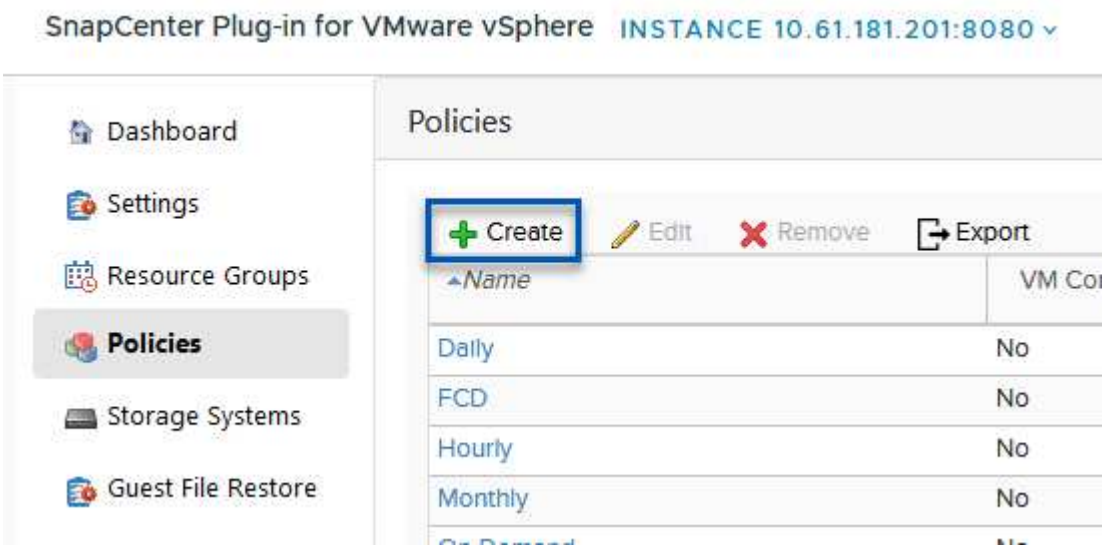
SCV 백업 정책을 생성합니다

정책은 SCV로 관리되는 백업의 보존 기간, 빈도 및 복제 옵션을 지정합니다.

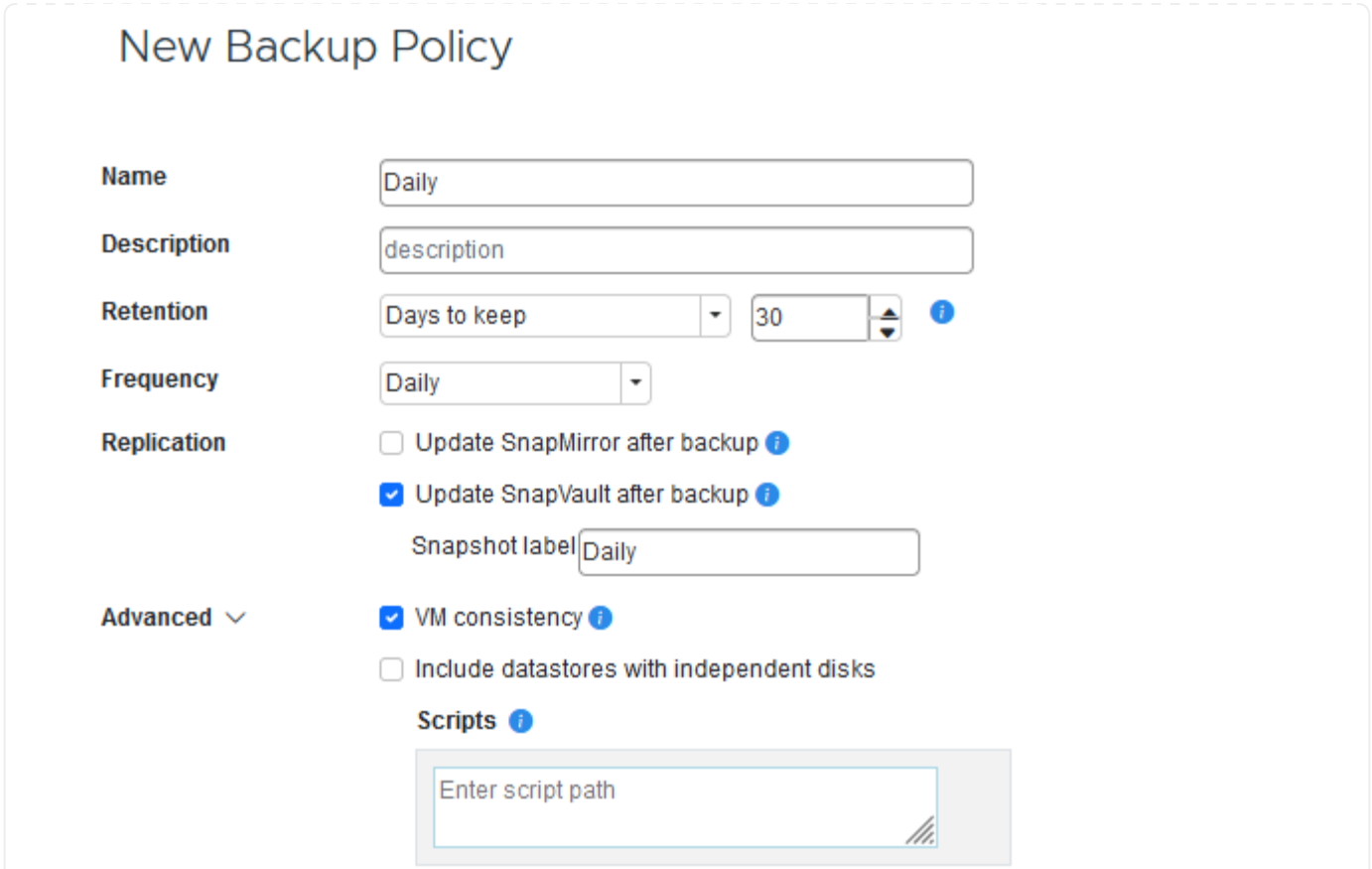
를 검토합니다 "VM 및 데이터 저장소에 대한 백업 정책을 생성합니다" 섹션을 참조하십시오.

백업 정책을 생성하려면 다음 단계를 수행하십시오.

1. VMware vSphere용 SnapCenter 플러그인에서 왼쪽 메뉴의 * Policies * 로 이동한 후 * Create * 버튼을 클릭합니다.



2. 정책 이름, 보존 기간, 빈도 및 복제 옵션, 스냅샷 레이블을 지정합니다.



SnapCenter 플러그인에서 정책을 생성하면 SnapMirror 및 SnapVault에 대한 옵션이 표시됩니다. SnapMirror를 선택하는 경우 정책에 지정된 보존 일정은 운영 스냅샷과 보조 스냅샷에 모두 동일합니다. SnapVault를 선택하는 경우 보조 스냅샷의 보존 일정은 SnapMirror 관계에 구현된 별도의 일정을 기반으로 합니다. 이 기능은 보조 백업에 더 긴 보존 기간을 원할 때 유용합니다.

스냅샷 레이블은 보조 ONTAP 클러스터에 복제된 SnapVault 복사본에 대해 특정 보존 기간을 지정하여 정책을 수립하는 데 사용할 수 있다는 점에서 유용합니다. SCV를 BlueXP 백업 및 복원과 함께 사용할 때는 스냅샷 레이블 필드를 비워 두거나 [밑줄] #match #BlueXP 백업 정책에 지정된 레이블을 지정해야 합니다.

3. 필요한 각 정책에 대해 절차를 반복합니다. 예를 들어 매일, 매주 및 매월 백업에 대한 별도의 정책을 사용할 수 있습니다.

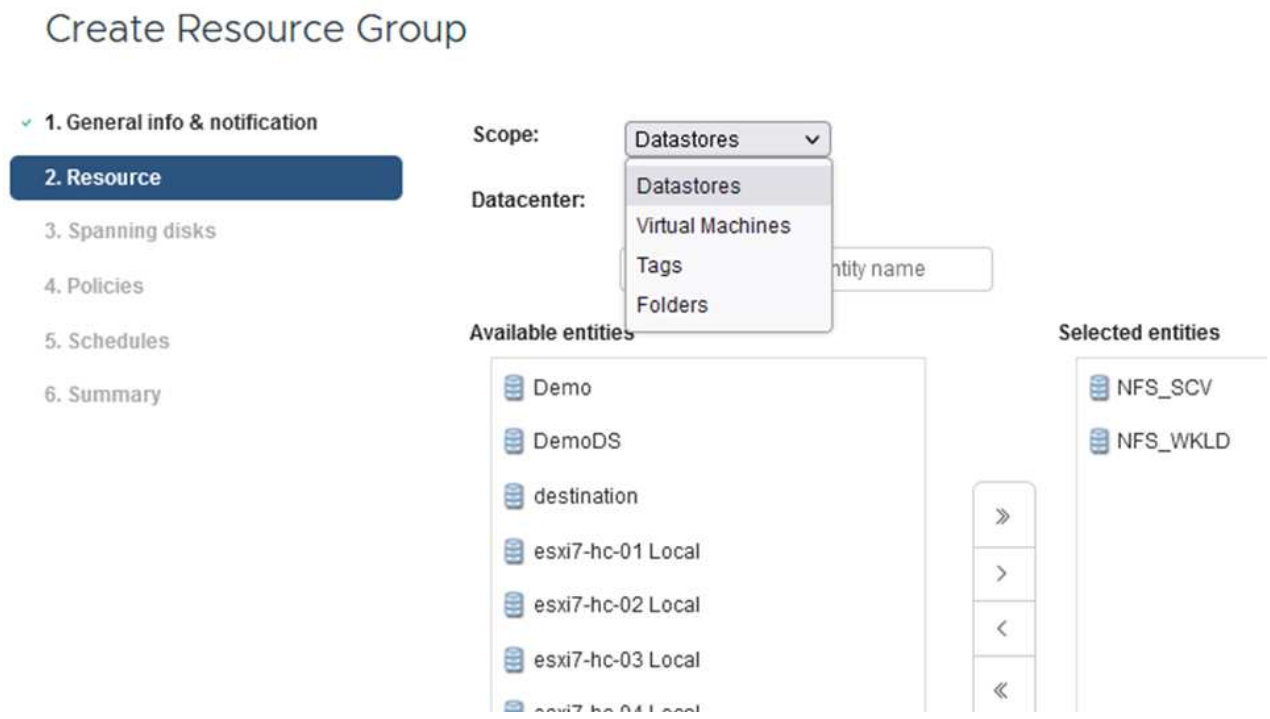
리소스 그룹에는 백업 작업에 포함될 데이터 저장소 및 가상 머신과 관련 정책 및 백업 일정이 포함됩니다.

를 검토합니다 "리소스 그룹을 생성합니다" 섹션을 참조하십시오.

리소스 그룹을 만들려면 다음 단계를 완료하십시오.

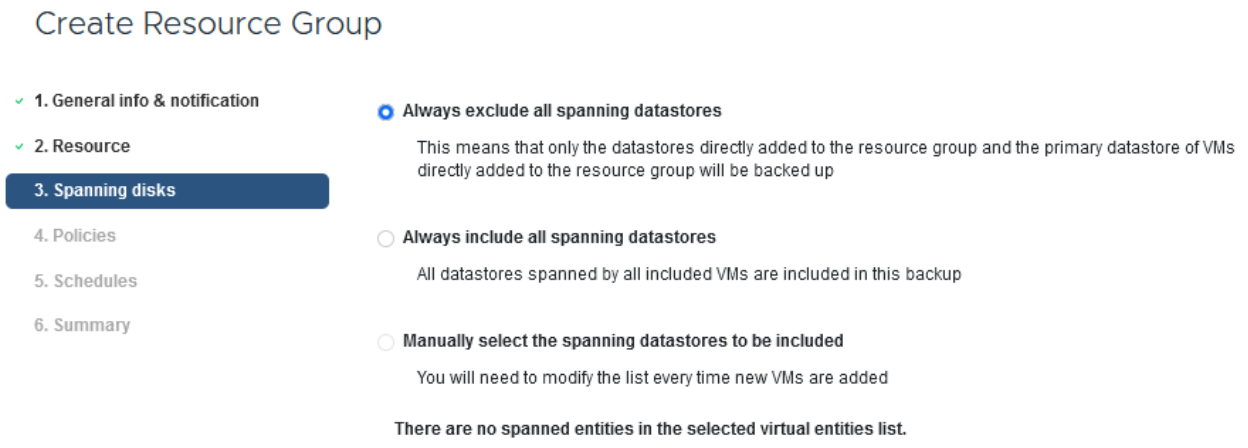
1. VMware vSphere용 SnapCenter 플러그인에서 왼쪽 메뉴의 * 리소스 그룹 * 으로 이동한 후 * 생성 * 버튼을 클릭합니다.

2. 리소스 그룹 만들기 마법사에서 그룹의 이름 및 설명과 알림을 받는 데 필요한 정보를 입력합니다. 다음 * 을 클릭합니다
3. 다음 페이지에서 백업 작업에 포함할 데이터 저장소와 가상 머신을 선택하고 * Next * 를 클릭합니다.



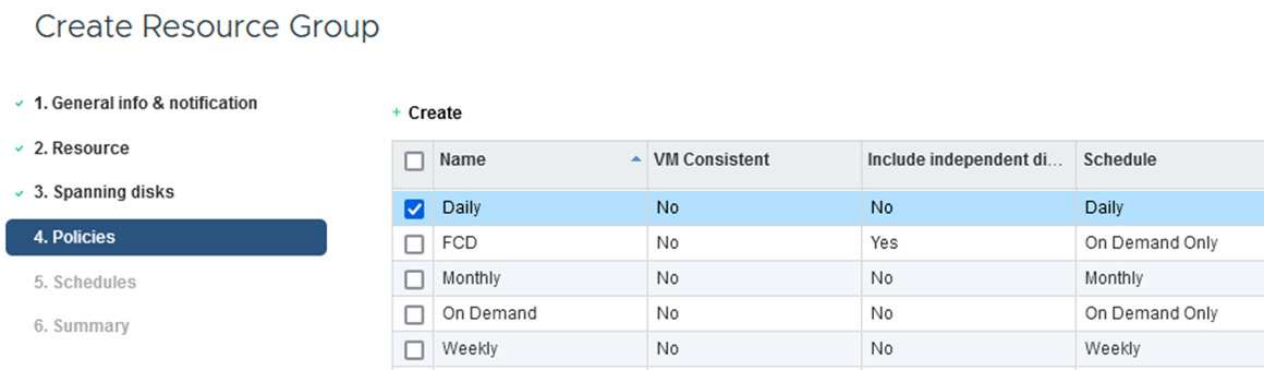
특정 VM 또는 전체 데이터 저장소를 선택할 수 있습니다. 백업이 기본 볼륨의 스냅샷을 생성한 결과이기 때문에 선택한 유형에 관계없이 전체 볼륨 및 데이터 저장소가 백업됩니다. 대부분의 경우 전체 데이터 저장소를 선택하는 것이 가장 쉽습니다. 그러나 복원 시 사용 가능한 VM의 목록을 제한하려는 경우 백업용 VM의 하위 집합만 선택할 수 있습니다.

4. 여러 데이터 저장소에 상주하는 VMDK가 있는 VM의 데이터 저장소 스패닝 옵션을 선택한 후 * Next * 를 클릭합니다.



BlueXP 백업 및 복구는 현재 여러 데이터 저장소를 확장하는 VMDK를 사용하는 VM 백업을 지원하지 않습니다.

5. 다음 페이지에서 리소스 그룹과 연결할 정책을 선택하고 * 다음 * 을 클릭합니다.



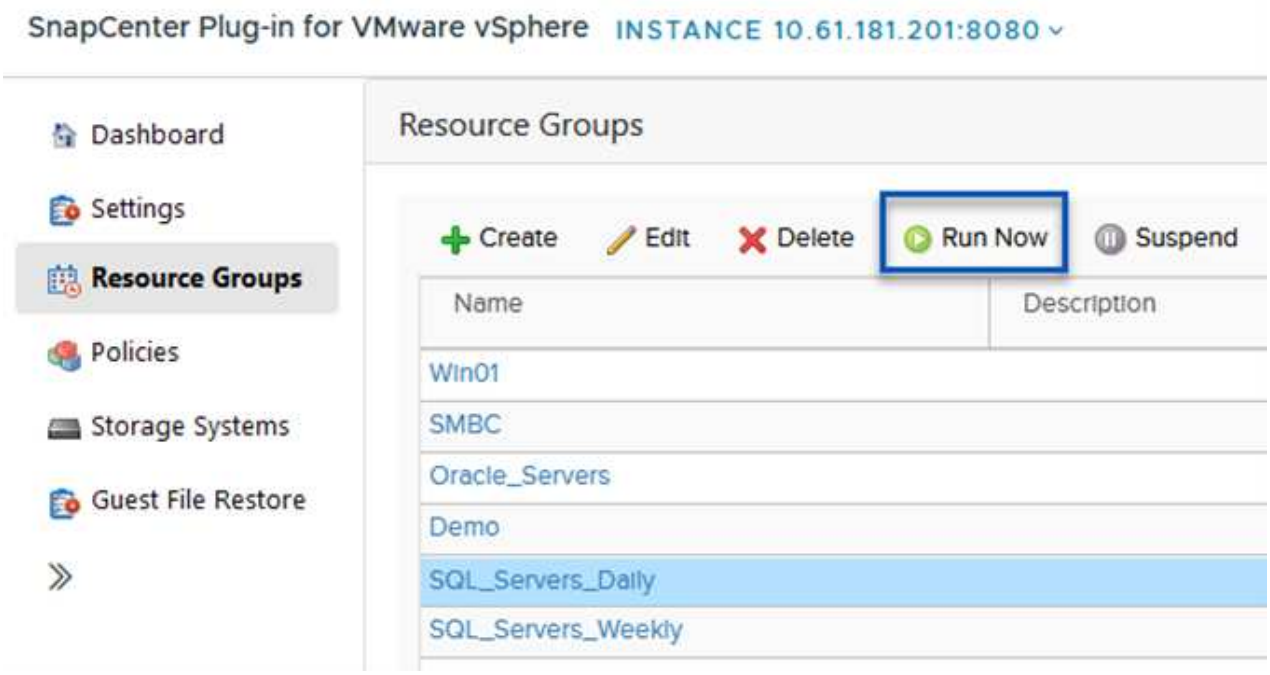
BlueXP 백업 및 복구를 사용하여 SCV 관리 스냅샷을 오브젝트 스토리지에 백업할 경우 각 리소스 그룹은 단일 정책에만 연결될 수 있습니다.

6. 백업이 실행되는 시간을 결정하는 일정을 선택합니다. 다음 * 을 클릭합니다.

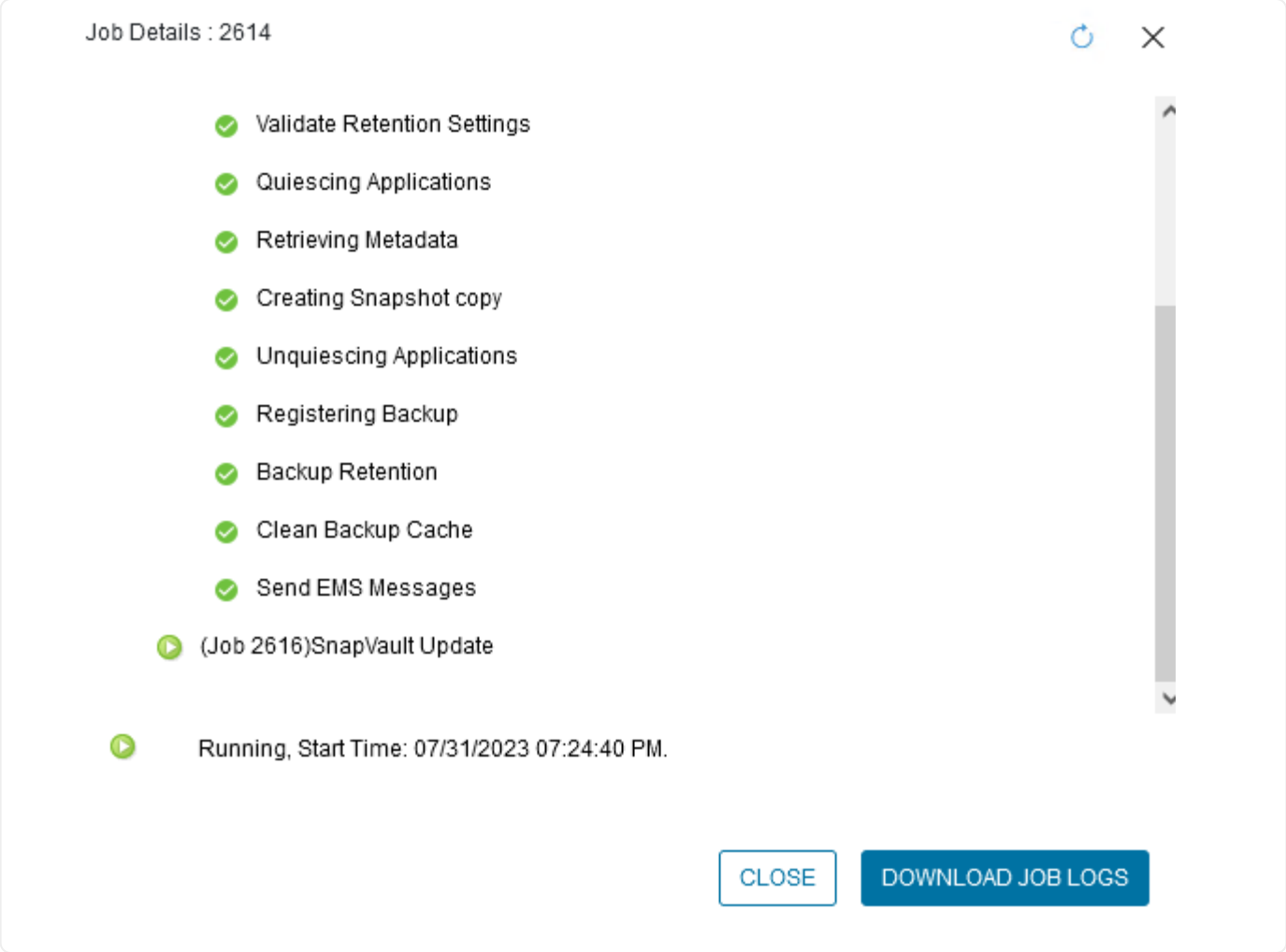
7. 마지막으로 요약 페이지를 검토한 후 * Finish * 를 클릭하여 리소스 그룹 생성을 완료합니다.

이 마지막 단계에서는 백업 작업을 실행하고 진행 상황을 모니터링합니다. BlueXP 백업 및 복구에서 리소스를 검색하려면 먼저 SCV에서 하나 이상의 백업 작업을 성공적으로 완료해야 합니다.

1. VMware vSphere용 SnapCenter 플러그인에서 왼쪽 메뉴의 * 리소스 그룹 * 으로 이동합니다.
2. 백업 작업을 시작하려면 원하는 리소스 그룹을 선택하고 * 지금 실행 * 버튼을 클릭합니다.



3. 백업 작업을 모니터링하려면 왼쪽 메뉴에서 * Dashboard * 로 이동합니다. 최근 작업 활동 * 에서 작업 ID 번호를 클릭하여 작업 진행 상황을 모니터링합니다.



BlueXP 백업 및 복구에서 오브젝트 스토리지에 백업을 구성합니다

BlueXP를 효과적으로 관리하려면 Connector를 사전에 설치해야 합니다. 커넥터는 리소스 검색 및 데이터 작업 관리와 관련된 작업을 실행합니다.

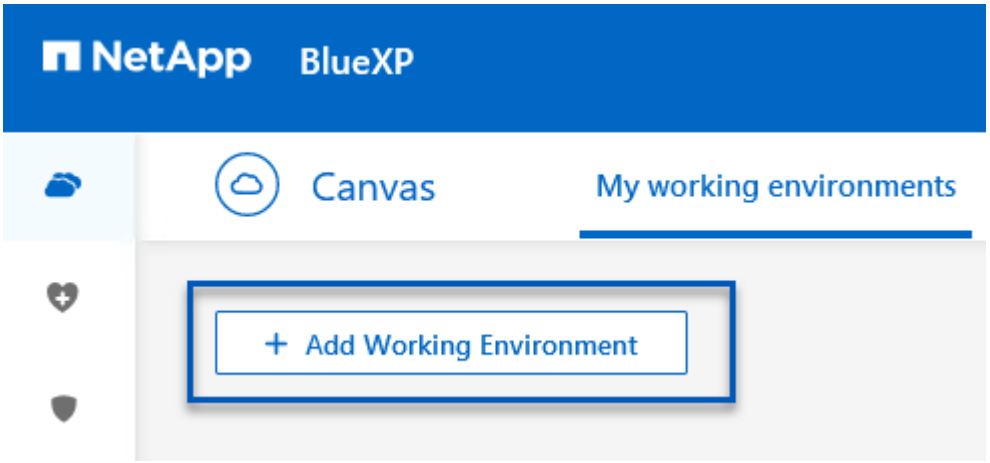
BlueXP Connector에 대한 자세한 내용은 을 참조하십시오 "커넥터에 대해 자세히 알아보십시오" 검토합니다.

사용 중인 클라우드 공급자용으로 커넥터가 설치되면 개체 스토리지의 그래픽 표현을 Canvas에서 볼 수 있습니다.

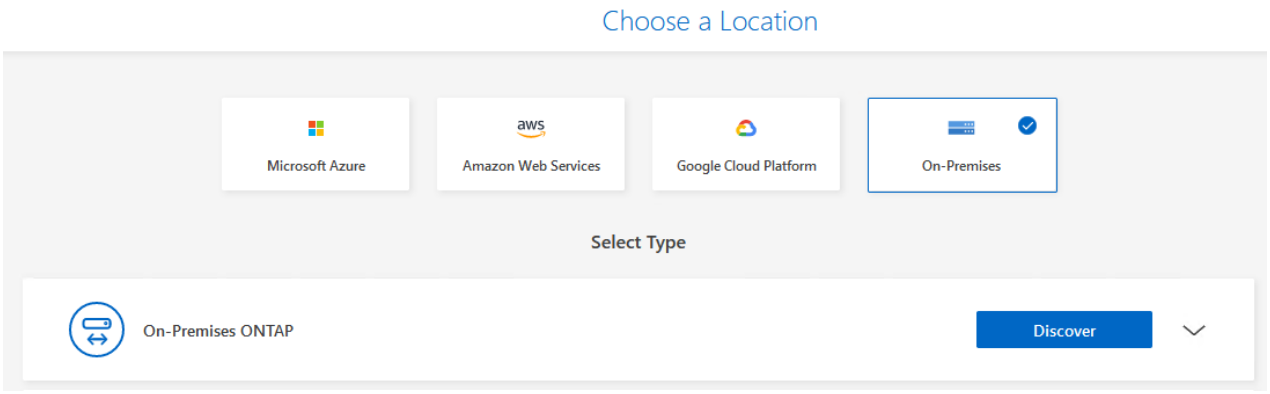
사내의 SCV에서 관리하는 백업 데이터에 대해 BlueXP 백업 및 복구를 구성하려면 다음 단계를 완료하십시오.

첫 번째 단계는 온프레미스 ONTAP 스토리지 시스템을 BlueXP에 추가하는 것입니다

1. Canvas에서 * 작업 환경 추가 * 를 선택하여 시작합니다.



2. 선택한 위치에서 * 온-프레미스 * 를 선택한 다음 * 검색 * 버튼을 클릭합니다.



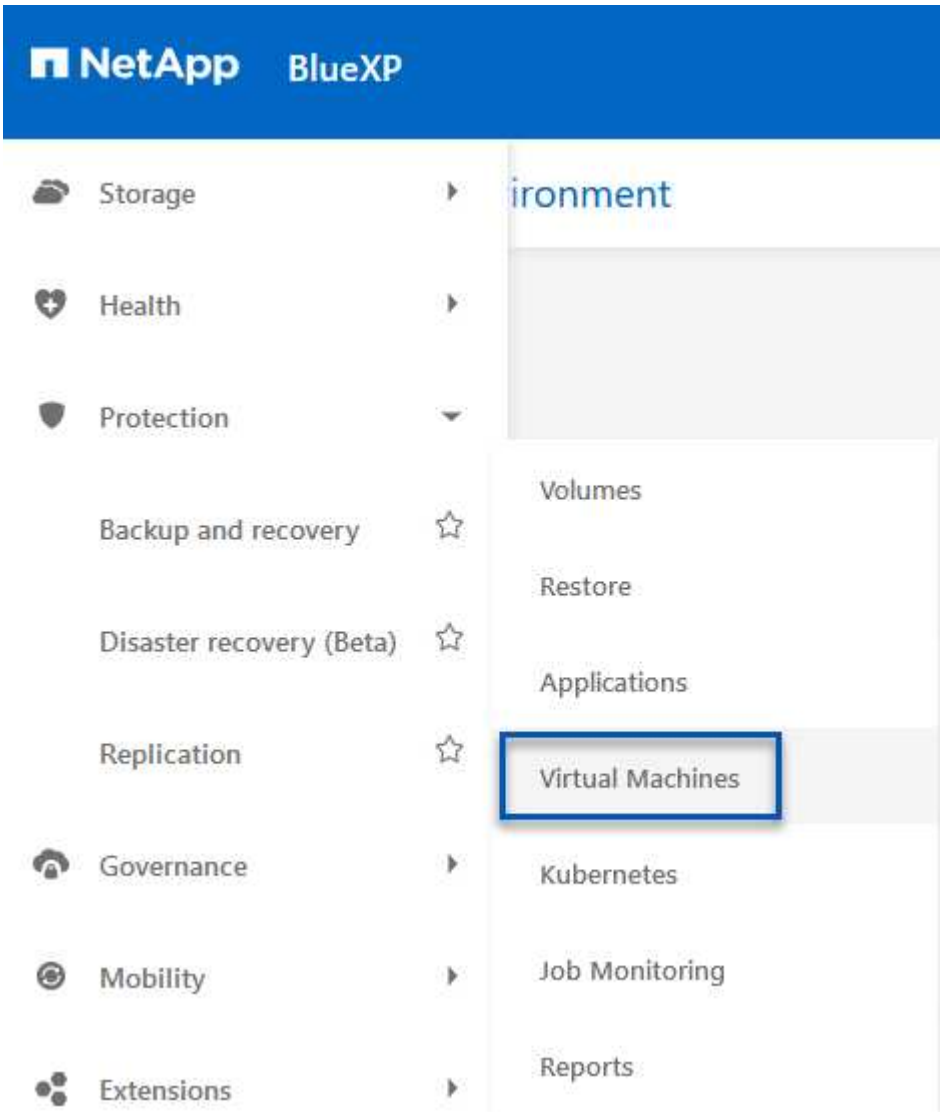
3. ONTAP 스토리지 시스템에 대한 자격 증명을 작성하고 * 검색 * 버튼을 클릭하여 작업 환경을 추가합니다.


ONTAP Cluster IP
10.61.181.180
User Name
admin
Password

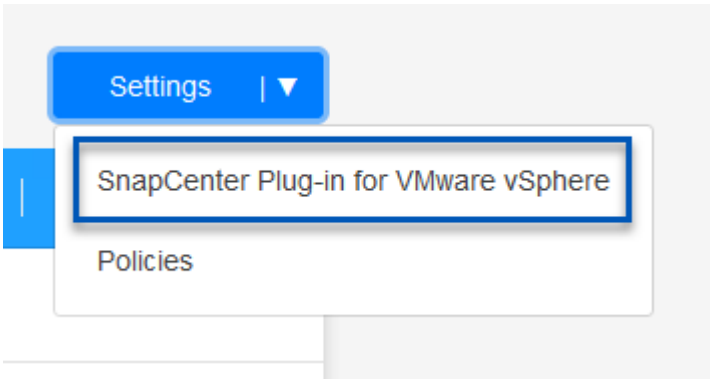
온-프레미스 SCV 어플라이언스 및 vCenter에 대해 알아봅니다

온-프레미스 데이터 저장소 및 가상 머신 리소스를 검색하려면 vCenter 관리 어플라이언스에 대한 SCV 데이터 브로커에 대한 정보와 자격 증명을 추가합니다.

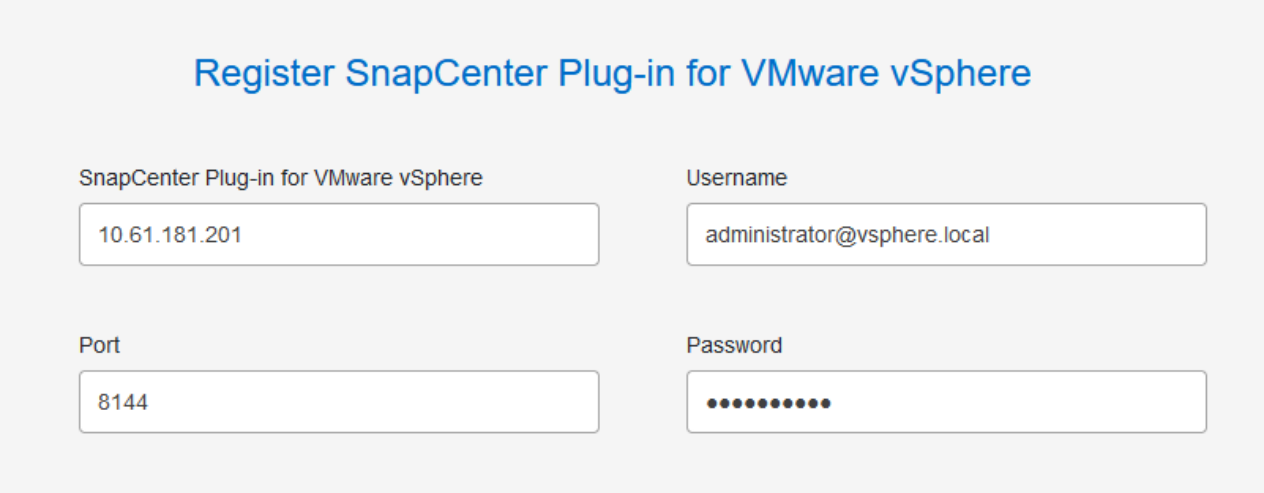
1. BlueXP 왼쪽 메뉴에서 선택 * 보호 > 백업 및 복구 > 가상 머신 * 을 선택합니다



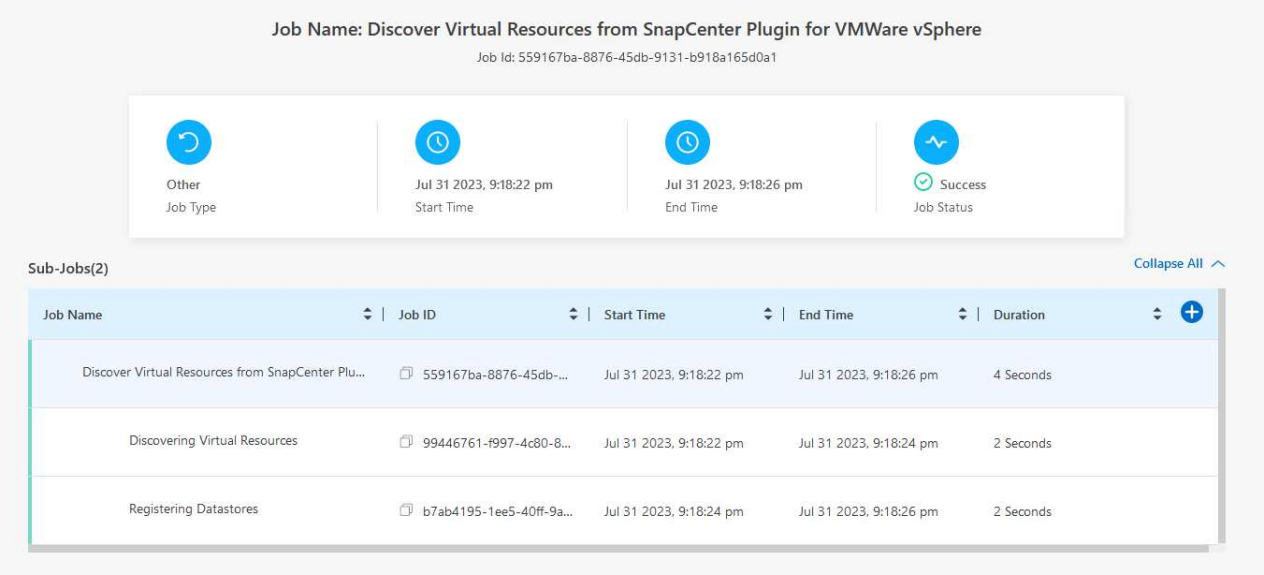
2. 가상 머신 기본 화면에서 * 설정 * 드롭다운 메뉴에 액세스하고 * SnapCenter Plug-in for VMware vSphere * 를 선택합니다.



3. 등록 * 버튼을 클릭한 다음 SnapCenter 플러그인 어플라이언스의 IP 주소 및 포트 번호와 vCenter 관리 어플라이언스의 사용자 이름 및 암호를 입력합니다. 검색 프로세스를 시작하려면 * 등록 * 버튼을 클릭하십시오.



4. 작업 진행률은 작업 모니터링 탭에서 모니터링할 수 있습니다.



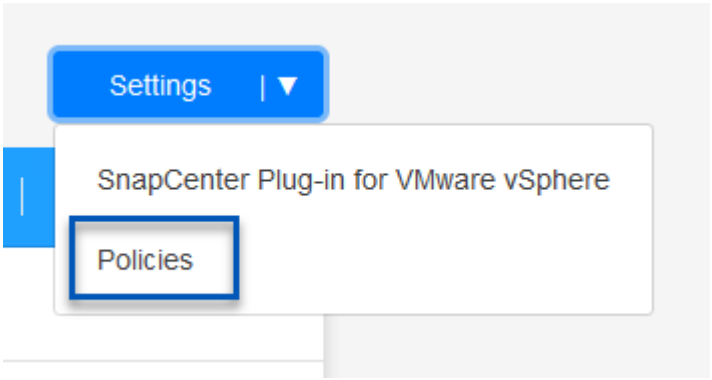
5. 검색이 완료되면 검색된 모든 SCV 어플라이언스에 걸쳐 데이터 저장소 및 가상 머신을 볼 수 있습니다. 를 누릅니다
이미지: bxp-scv-hybrid-23.png [사용 가능한 리소스 보기]

BlueXP 백업 정책을 생성합니다

가상 머신의 BlueXP 백업 및 복구에서 보존 기간, 백업 소스 및 아카이브 정책을 지정하는 정책을 생성합니다.

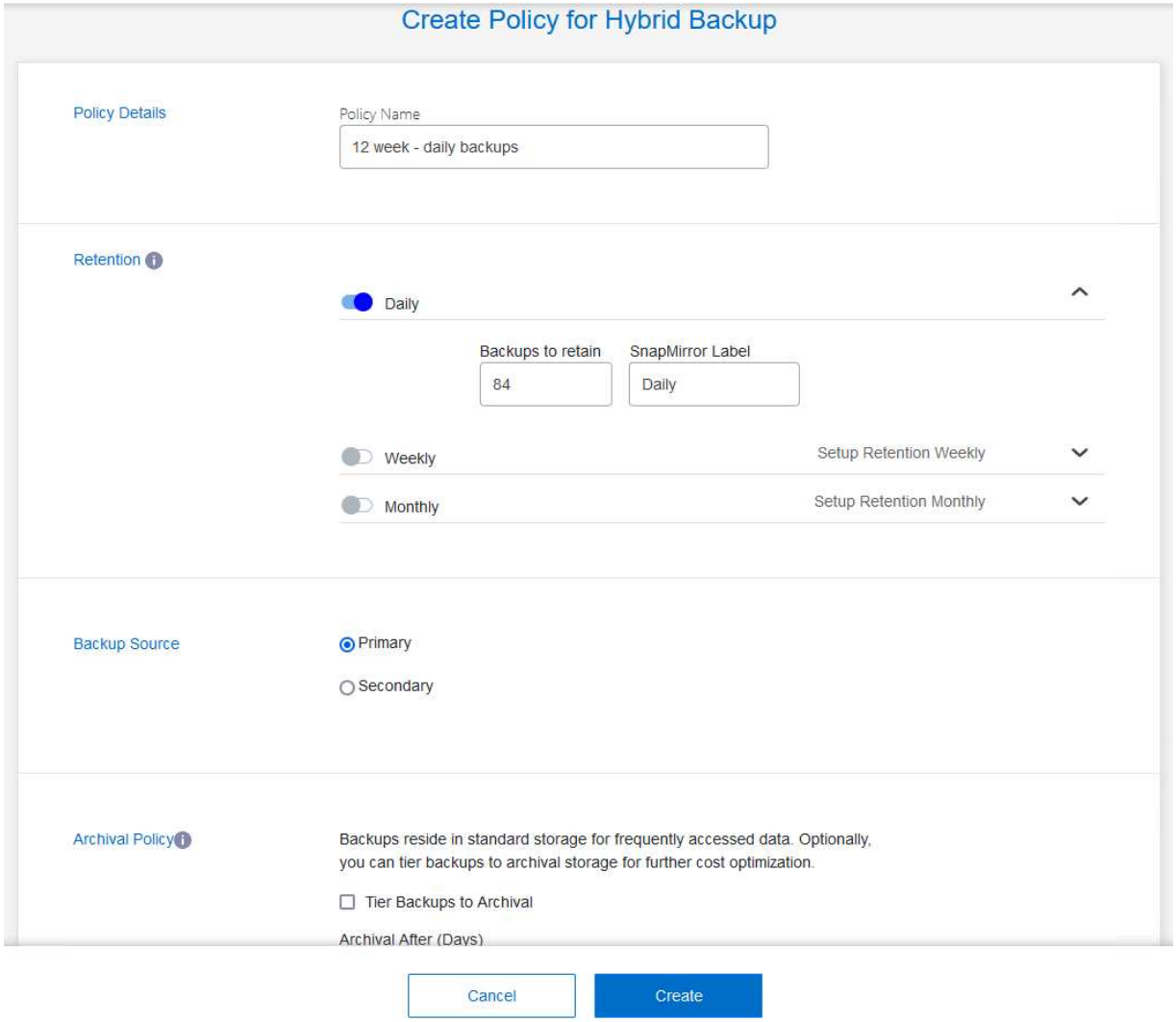
정책 생성에 대한 자세한 내용은 을 참조하십시오 "데이터 저장소를 백업하는 정책을 생성합니다".

1. 가상 머신에 대한 BlueXP 백업 및 복구 기본 페이지에서 * Settings * 드롭다운 메뉴에 액세스하고 * Policies * 를 선택합니다.



2. Create Policy * 를 클릭하여 * Create Policy for Hybrid Backup * 창에 액세스합니다.

   a. 정책 이름을 추가합니다
   b. 원하는 보존 기간을 선택합니다
   c. 운영 또는 보조 사내 ONTAP 스토리지 시스템에서 백업을 소싱할지 선택합니다
   d. 필요에 따라 추가 비용 절감을 위해 백업이 보관 스토리지로 계층화되는 기간 후를 지정합니다.



여기에 입력한 SnapMirror 레이블을 사용하여 정책을 적용할 백업을 식별합니다. 레이블 이름은 해당 온-프레미스 SCV 정책의 레이블 이름과 일치해야 합니다.

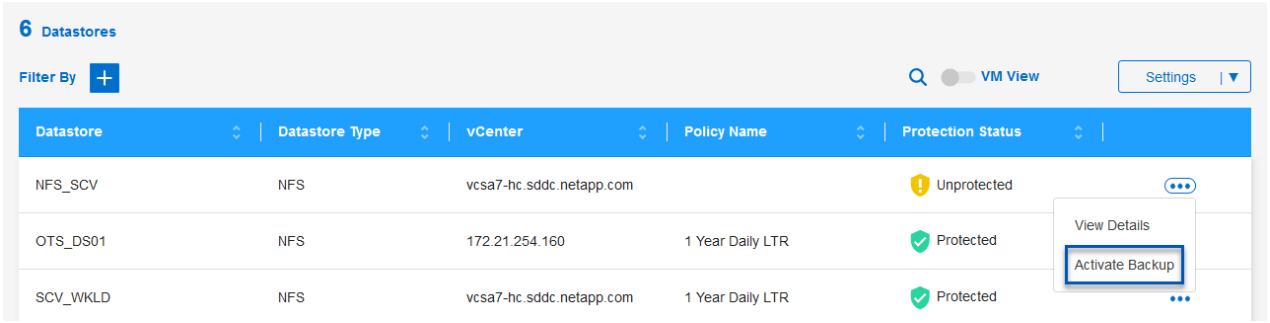
3. Create * 를 클릭하여 정책 생성을 완료합니다.

Amazon Web Services에 데이터 저장소를 백업합니다

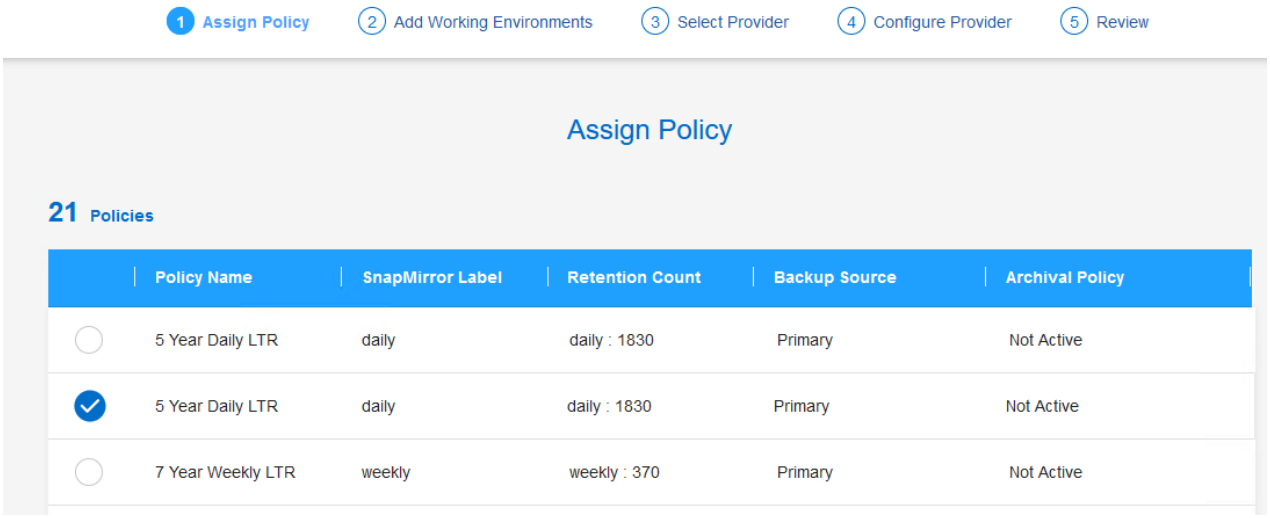
마지막 단계는 개별 데이터 저장소 및 가상 시스템에 대한 데이터 보호를 활성화하는 것입니다. 다음 단계에서는 AWS로 백업을 활성화하는 방법을 간략하게 설명합니다.

자세한 내용은 을 참조하십시오 "Amazon Web Services에 데이터 저장소를 백업합니다".

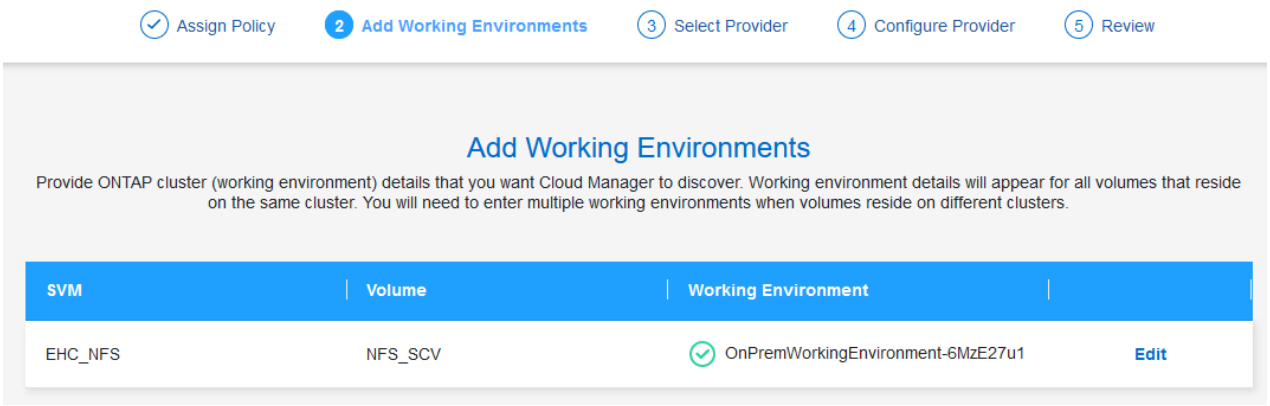
1. BlueXP 백업 및 복구 for Virtual Machines 기본 페이지에서 백업할 데이터 저장소에 대한 설정 드롭다운에 액세스하고 * Activate Backup * 을 선택합니다.



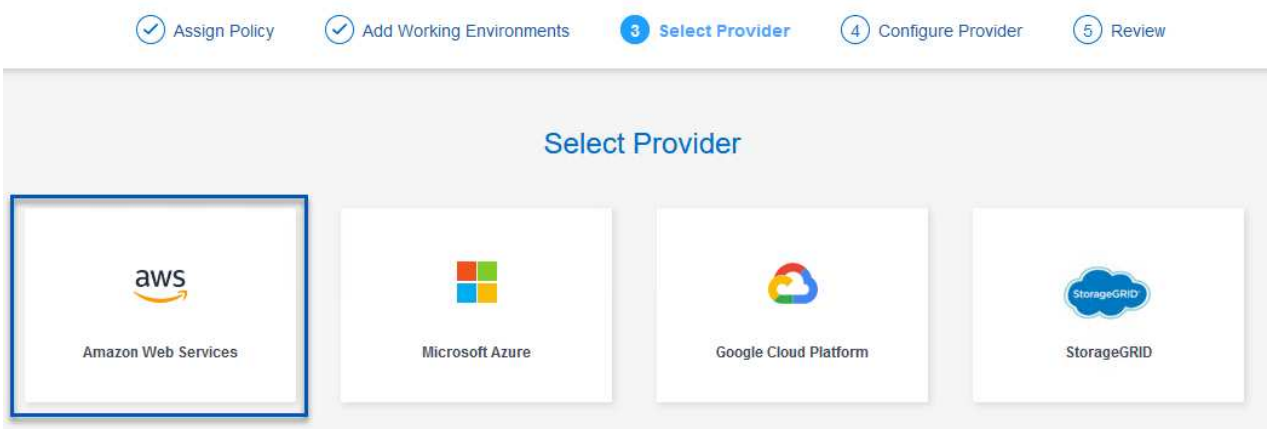
2. 데이터 보호 작업에 사용할 정책을 할당하고 * Next * 를 클릭합니다.



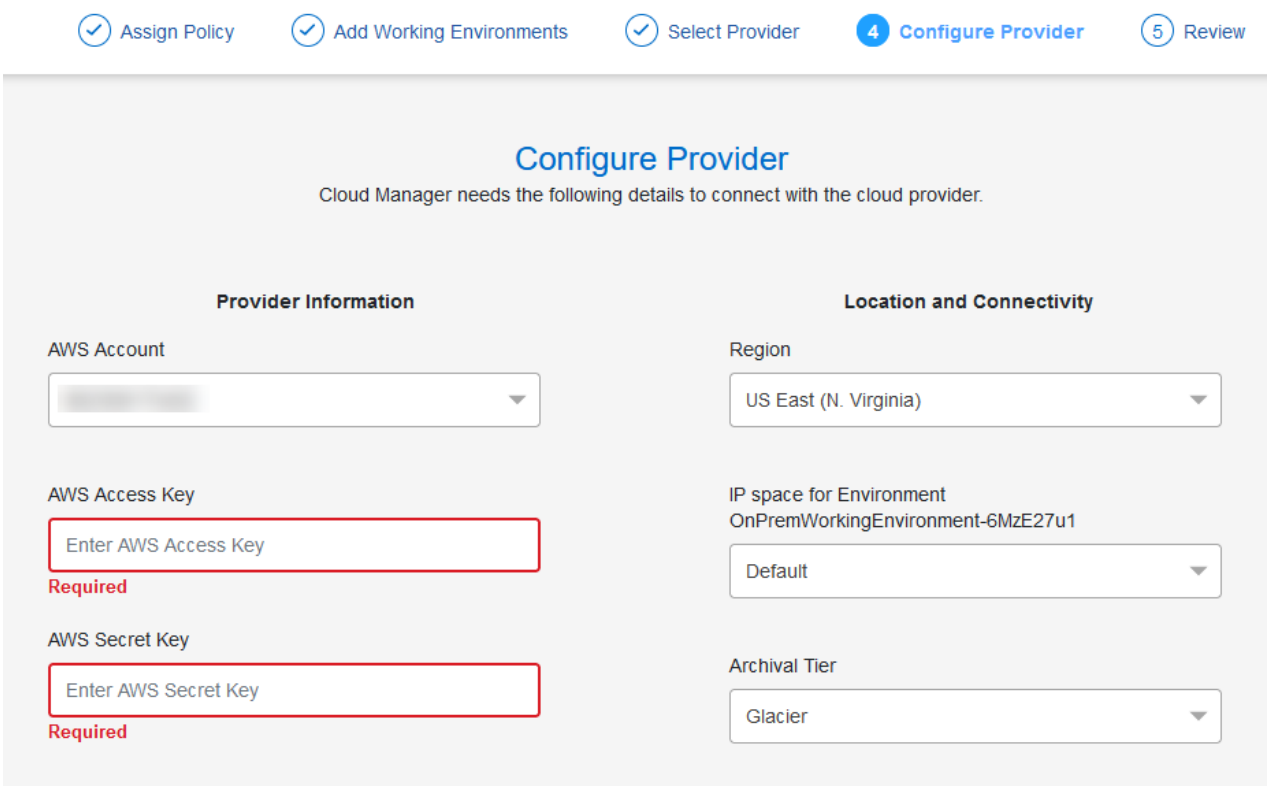
3. 작업 환경이 이전에 검색된 경우 * Add Working Environments * 페이지에서 데이터 저장소 및 작업 환경이 확인 표시와 함께 표시됩니다. 작업 환경이 이전에 검색되지 않은 경우 여기에 추가할 수 있습니다. 계속하려면 * 다음 * 을 클릭하십시오.



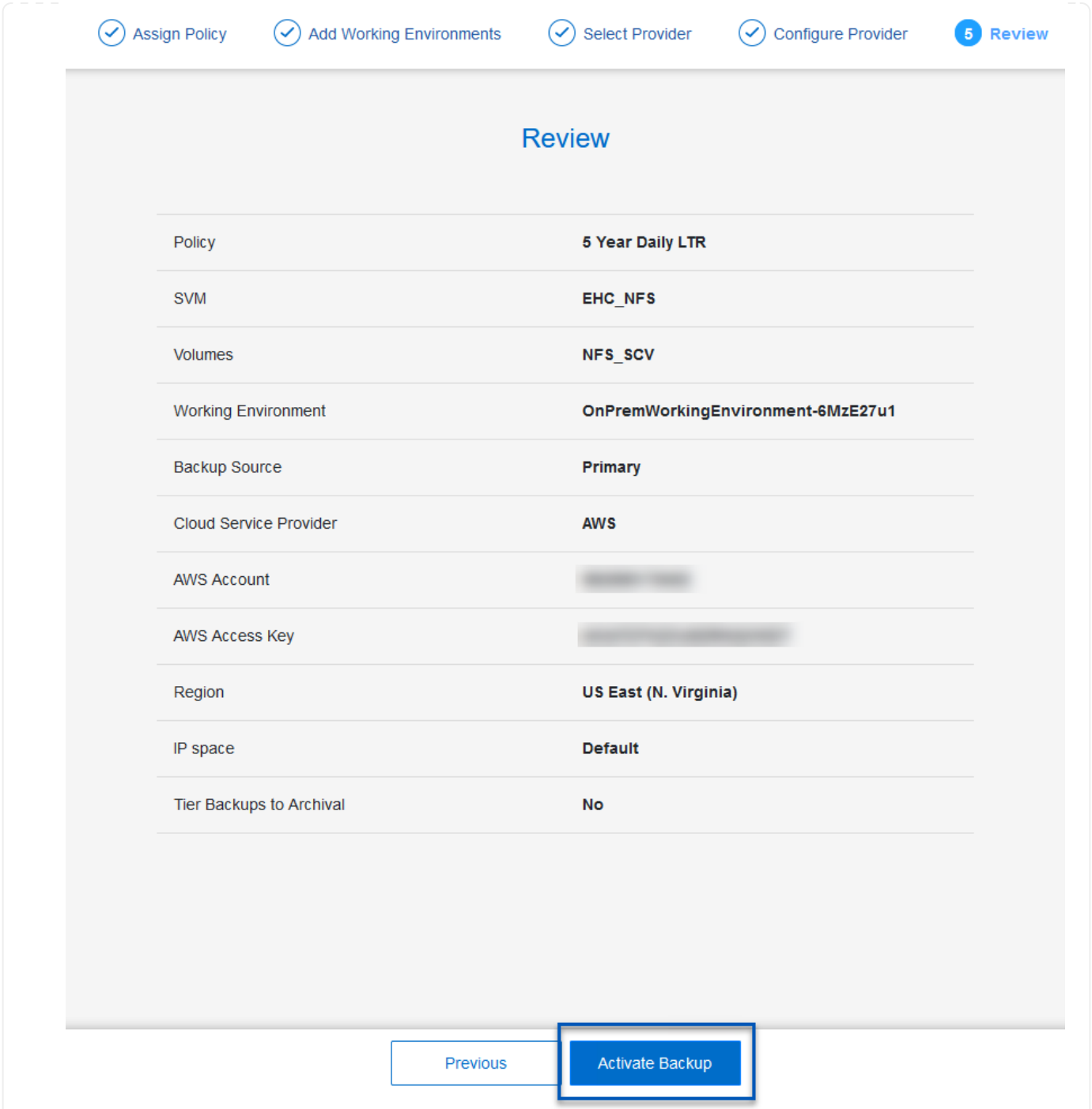
4. 공급자 선택 * 페이지에서 AWS를 클릭한 후 * 다음 * 버튼을 클릭하여 계속합니다.



5. 사용할 AWS 액세스 키와 비밀 키, 지역, 아카이브 계층 등 AWS에 대한 공급자별 자격 증명 정보를 입력합니다. 또한 온프레미스 ONTAP 스토리지 시스템의 ONTAP IP 공간을 선택합니다. 다음 * 을 클릭합니다.



6. 마지막으로 백업 작업 세부 정보를 검토하고 * Activate Backup * 버튼을 클릭하여 데이터 저장소의 데이터 보호를 시작합니다.



이때 데이터 전송이 즉시 시작되지 않을 수 있습니다. BlueXP 백업 및 복구는 매시간마다 미해결 스냅샷을 검색한 다음 이를 오브젝트 스토리지로 전송합니다.

데이터 손실 시 가상 머신 복구

데이터를 보호하는 것은 포괄적인 데이터 보호의 한 가지 측면에 불과합니다. 여기도 중요한 것은 데이터 손실 또는 랜섬웨어 공격이 발생했을 때 어느 위치에서나 데이터를 즉시 복원할 수 있는 능력입니다. 이 기능은 원활한 비즈니스 운영을 유지하고 복구 시점 목표를 달성하는 데 매우 중요합니다.

NetApp는 매우 적응성이 뛰어난 3-2-1 전략을 제공하여 운영, 보조 및 오브젝트 스토리지 위치에서 보존 일정을 사용자

지정할 수 있도록 합니다. 이 전략은 특정 요구사항에 맞게 데이터 보호 접근 방식을 조정할 수 있는 유연성을 제공합니다.

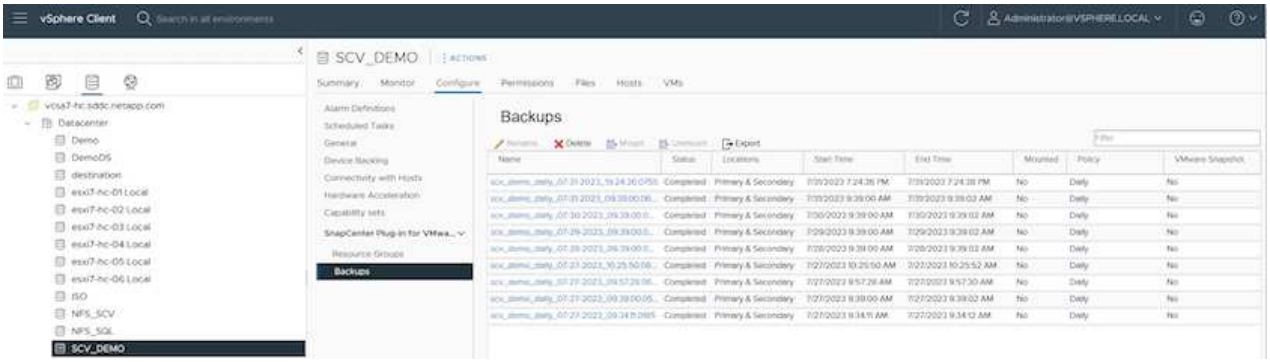
이 섹션에서는 VMware vSphere용 SnapCenter 플러그인과 가상 머신에 대한 BlueXP 백업 및 복구 모두에서 데이터 복원 프로세스를 개괄적으로 설명합니다.

VMware vSphere용 SnapCenter 플러그인에서 가상 머신 복구

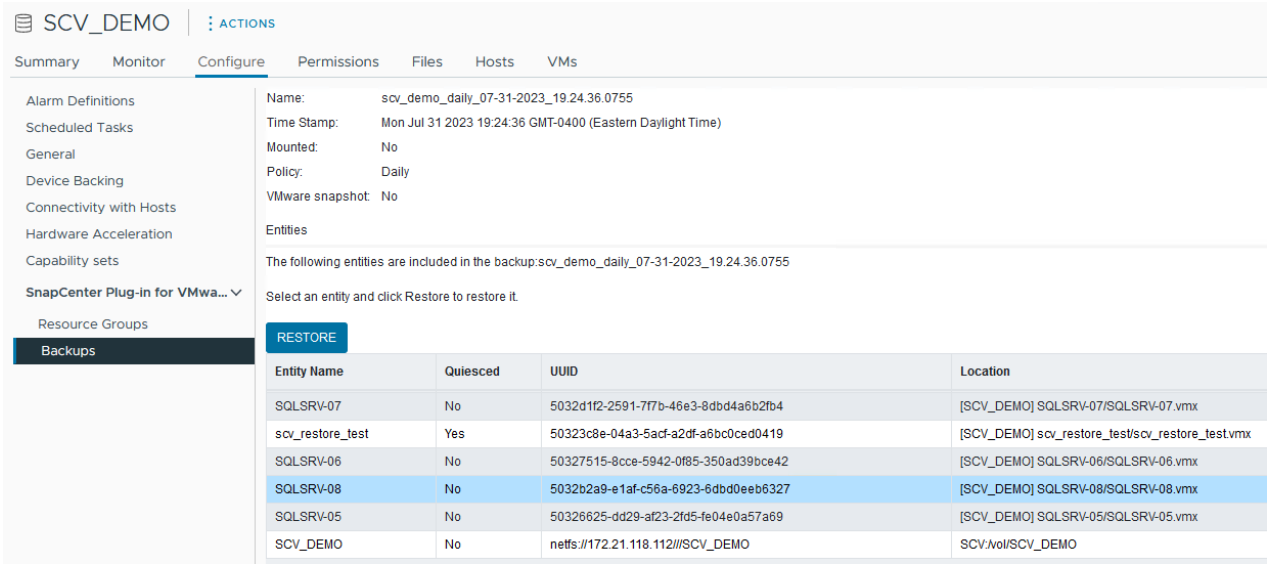
이 솔루션의 경우 가상 머신이 원래 위치와 대체 위치로 복구되었습니다. SCV의 데이터 복원 기능의 모든 측면을 이 솔루션에서 다루지 않습니다. SCV가 제공하는 모든 기능에 대한 자세한 내용은 을 참조하십시오 "백업에서 VM을 복원합니다" 참조하십시오.

운영 또는 보조 스토리지에서 가상 머신 복구를 복구하려면 다음 단계를 완료하십시오.

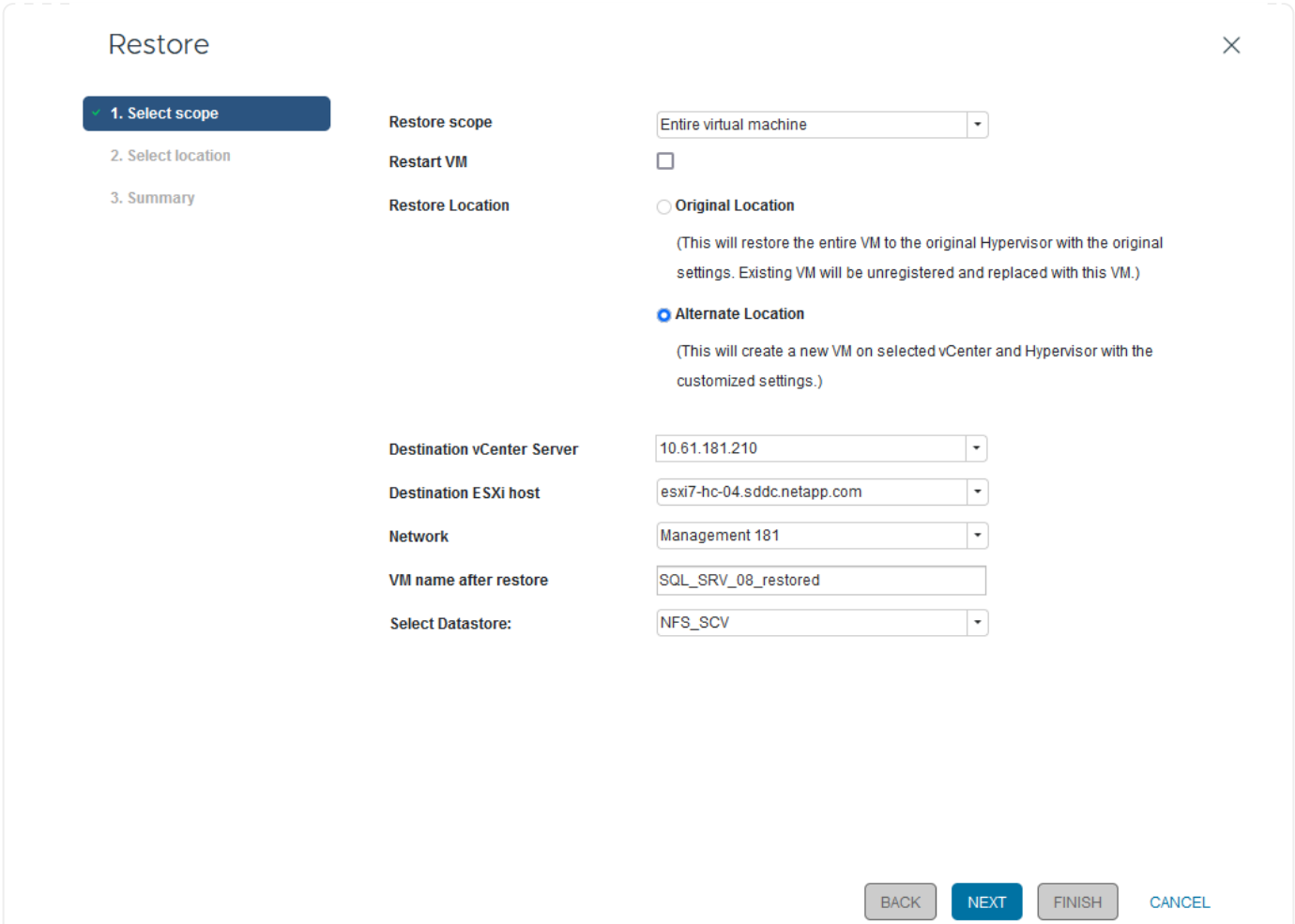
1. vCenter 클라이언트에서 * Inventory > Storage * 로 이동하고 복원할 가상 머신이 포함된 데이터 저장소를 클릭합니다.
2. Configure * 탭에서 * Backups * 를 클릭하여 사용 가능한 백업 목록에 액세스합니다.



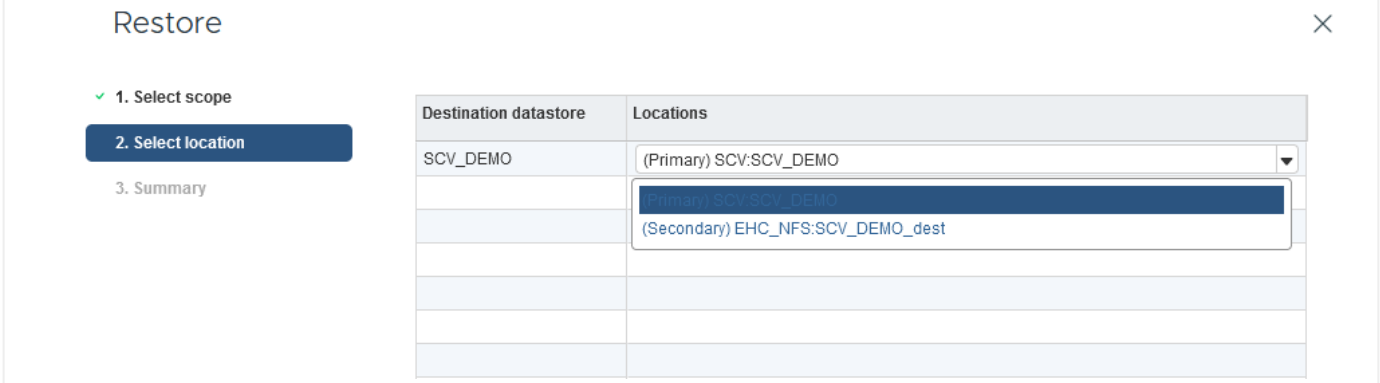
3. 백업을 클릭하여 VM 목록에 액세스한 다음 복구할 VM을 선택합니다. Restore * 를 클릭합니다.



4. 복구 마법사에서 전체 가상 머신 또는 특정 VMDK를 복구하도록 선택합니다. 원래 위치 또는 대체 위치에 설치하고 복구 후 VM 이름 및 대상 데이터 저장소를 제공하려면 선택합니다. 다음 * 을 클릭합니다.



5. 운영 또는 보조 스토리지 위치에서 백업하도록 선택합니다.



6. 마지막으로 백업 작업의 요약을 검토하고 Finish를 클릭하여 복구 프로세스를 시작합니다.

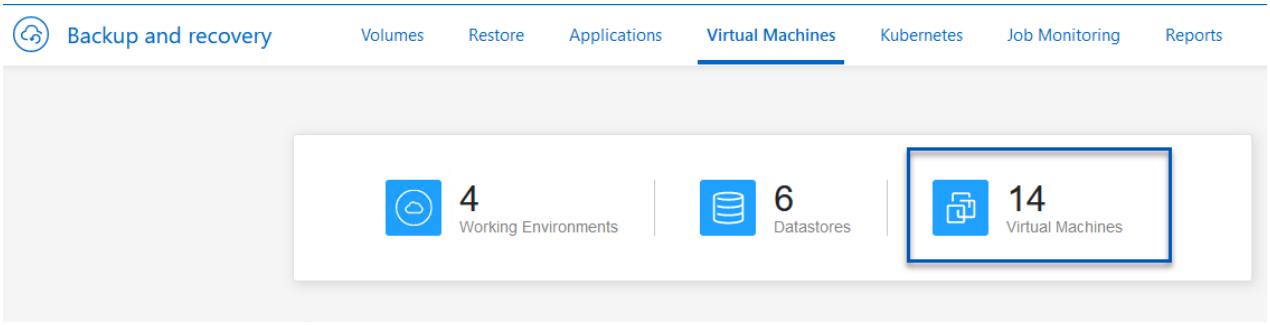
가상 머신에 대한 **BlueXP** 백업 및 복구에서 가상 머신 복원

가상 머신의 BlueXP 백업 및 복구를 사용하면 가상 머신을 원래 위치에 복구할 수 있습니다. 복원 기능은 BlueXP 웹 콘솔을 통해 액세스할 수 있습니다.

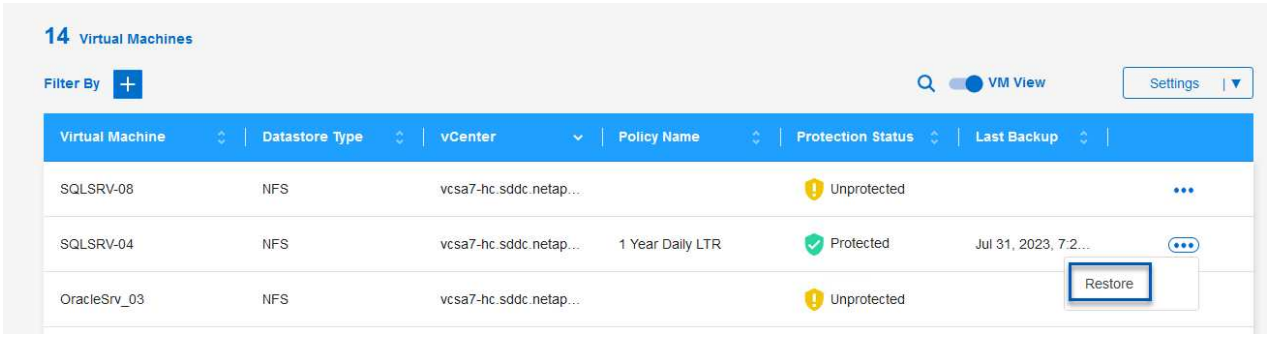
자세한 내용은 을 참조하십시오 "클라우드에서 가상 머신 데이터를 복원합니다".

BlueXP 백업 및 복구에서 가상 머신을 복원하려면 다음 단계를 완료하십시오.

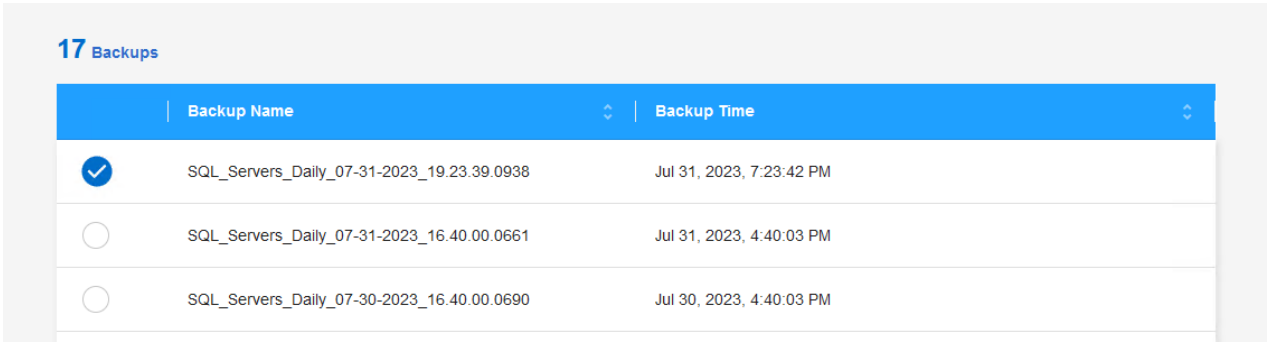
1. Protection > Backup and Recovery > Virtual Machines * 로 이동하고 Virtual Machines * 를 클릭하여 복원할 수 있는 가상 머신 목록을 표시합니다.



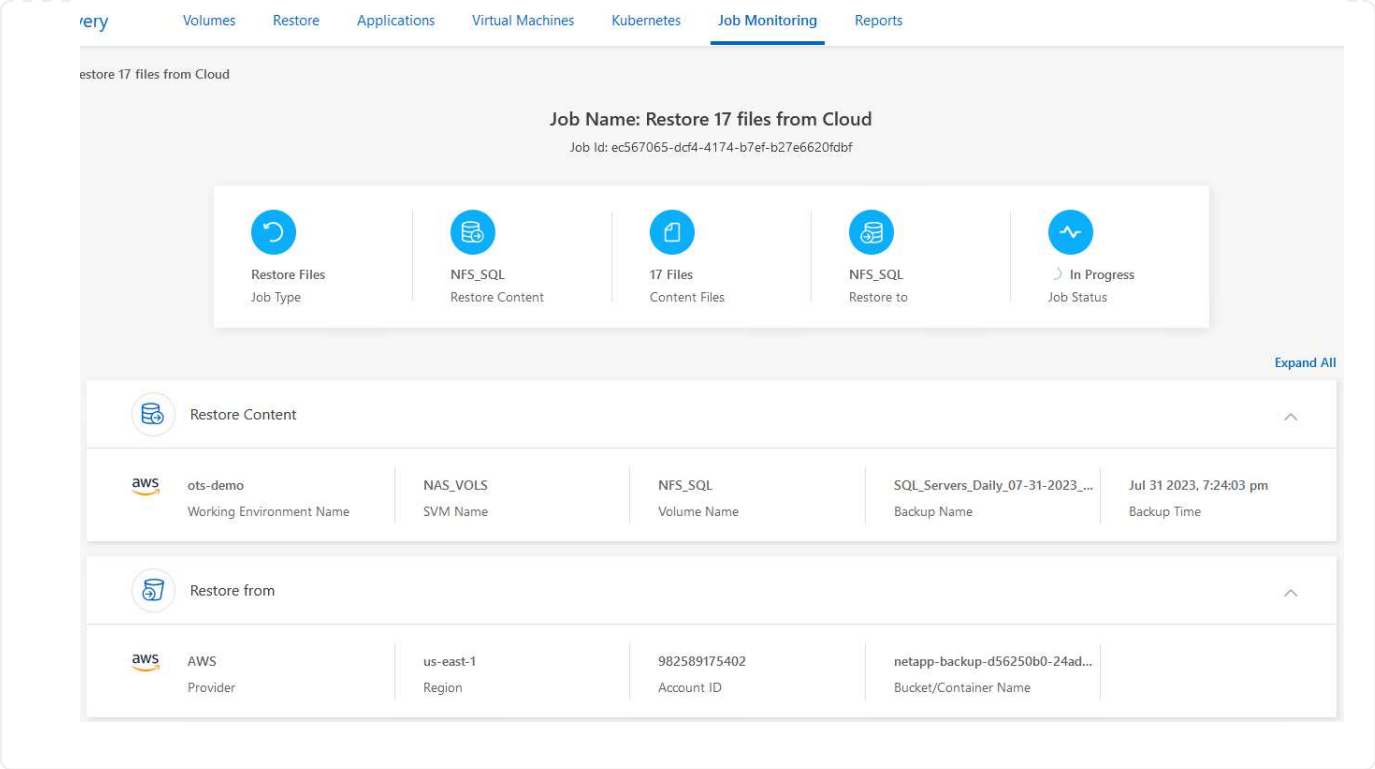
2. 복구할 VM에 대한 설정 드롭다운 메뉴에 액세스하고 를 선택합니다



3. 복원할 백업을 선택하고 * 다음 * 을 클릭합니다.



4. 백업 작업의 요약을 검토하고 * Restore * 를 클릭하여 복원 프로세스를 시작합니다.
5. 작업 모니터링 * 탭에서 복원 작업의 진행 상황을 모니터링합니다.



결론

VMware vSphere용 SnapCenter 플러그인 및 가상 머신용 BlueXP 백업 및 복구와 함께 구현되는 3-2-1 백업 전략은 데이터 보호를 위한 강력하고 안정적이며 비용 효율적인 솔루션을 제공합니다. 이 전략은 데이터 중복성과 접근성을 보장할 뿐 아니라 온프레미스 ONTAP 스토리지 시스템과 클라우드 기반 오브젝트 스토리지 모두에서 데이터를 유연하게 복원할 수 있도록 합니다.

이 설명서에 나와 있는 사용 사례는 NetApp, VMware와 업계 최고 수준의 클라우드 공급자 간의 통합을 강조한 검증된 데이터 보호 기술에 중점을 둡니다. VMware vSphere용 SnapCenter 플러그인은 VMware vSphere와 원활하게 통합되므로 데이터 보호 작업을 중앙에서 효율적으로 관리할 수 있습니다. 이러한 통합을 통해 가상 머신의 백업 및 복구 프로세스가 간소화되므로 VMware 에코시스템 내에서 간편한 예약, 모니터링 및 유연한 복구 작업을 수행할 수 있습니다. 가상 머신용 BlueXP 백업 및 복구는 가상 머신 데이터를 클라우드 기반 오브젝트 스토리지에 에어갭 방식으로 안전하게 백업하여 3-2-1로 1을 제공합니다. 직관적인 인터페이스와 논리적 워크플로는 중요 데이터의 장기 보관을 위한 안전한 플랫폼을 제공합니다.

추가 정보

이 솔루션에 제공되는 기술에 대한 자세한 내용은 다음 추가 정보를 참조하십시오.

- "VMware vSphere용 SnapCenter 플러그인 설명서"
- "BlueXP 설명서"

VMware Sovereign 클라우드

Sovereign Cloud를 위한 VMware 리소스

NetApp와 VMware Sovereign Cloud의 약어입니다

VMware Sovereign Cloud 개요

주권의 개념은 국가 및 주 정부 등 매우 민감한 데이터를 처리하고 유지하는 많은 주체와 금융 및 의료 등 고도로 규제되는 산업 분야에서 클라우드 컴퓨팅의 필수 구성 요소로 부상하고 있습니다. 또한 디지털 경제 능력을 확대하고 클라우드 서비스에 대한 다국적 기업의 의존도를 줄이고자 합니다.

VMware Sovereign 클라우드 이니셔티브

VMware는 주권 클라우드를 다음과 같이 정의합니다.

- 민간 및 공공 부문 조직 모두에 대한 중요 데이터(예: 국가 데이터, 기업 데이터 및 개인 데이터)의 가치를 보호하고 잠금 해제합니다
- 디지털 경제를 위한 국가적 역량을 제공합니다
- 감사된 보안 제어를 통해 데이터를 보호합니다
- 데이터 개인정보 보호법을 준수하도록 보장합니다
- 데이터 상주 및 데이터 주권을 모두 관할하는 완벽하게 제어함으로써 데이터 제어 개선

신뢰할 수 있는 VMware Sovereign Cloud Service Provider와 협력

성공을 보장하기 위해 조직은 자신들이 신뢰하는 파트너들과 함께 공인하고 자율적인 주권 클라우드 플랫폼을 호스팅할 수 있는 역량이 있어야 합니다. VMware Sovereign Cloud 이니셔티브 내에서 인정을 받은 VMware 클라우드 공급업체는 VMware Sovereign Cloud 프레임워크에 설명된 주요 원칙과 모범 사례를 구현하는 최신 소프트웨어 정의 아키텍처를 기반으로 클라우드 솔루션을 설계하고 운영하기 위해 노력하고 있습니다.

- * 데이터 주권 및 관할권 관리 * – 모든 데이터는 해당 데이터가 수집된 국가 국가의 배타적 통제 및 권한을 따릅니다. 작업은 관할 지역 내에서 완전히 관리됩니다
- * 데이터 액세스 및 무결성 * – 클라우드 인프라는 탄력적이며 관할 지역 내의 두 데이터 센터 위치에서 사용할 수 있으며 보안 및 개인 연결 옵션을 사용할 수 있습니다.
- * 데이터 보안 및 규정 준수 * – 정보 보안 관리 시스템 제어는 업계에서 인정하는 글로벌(또는 지역) 표준에 따라 인증되고 정기적으로 감사를 받습니다.
- * 데이터 독립성 및 이동성 * – 벤더의 클라우드 종속을 방지하고 애플리케이션 이동성과 독립성을 지원하는 최신 애플리케이션 아키텍처 지원

VMware에 대한 자세한 내용은 다음 사이트를 참조하십시오.

- "VMware Sovereign Cloud 개요"
- "VMware Sovereign Cloud란 무엇입니까?"
- "새로운 VMware Sovereign Cloud Initiative를 소개합니다"
- "VMware Sovereign 클라우드 기술 백서"

VMware Sovereign Cloud를 사용한 Netpp: 활용 사례

NetApp는 여러 NetApp 기술을 통합하여 VMware Sovereign Cloud 개념을 지원합니다.

다음 링크를 사용하여 NetApp 기술과 VMware Sovereign Cloud의 통합에 대해 자세히 알아보십시오.

- "개체 저장소 확장으로 사용되는 NetApp StorageGRID"

개체 저장소 확장으로 사용되는 **NetApp StorageGRID**

NetApp는 VMware와 협력하여 VMware 소버린 클라우드를 지원하기 위해 NetApp StorageGRID를 VMware Cloud Director에 통합했습니다. 이 VMware Cloud Director 플러그인을 사용하면 서비스 제공업체가 사용 사례에 관계없이 StorageGRID를 오브젝트 스토리지 오퍼링으로 사용할 수 있으며 서비스 제공업체가 오퍼링 카탈로그의 다른 부분을 관리하는 데 사용하는 것과 동일한 VMware 멀티 테넌트 솔루션(VMware Cloud Director)을 통해 StorageGRID 관리를 수행할 수 있습니다.

VMware 소버린 클라우드를 제공하는 파트너는 NetApp StorageGRID를 선택하여 비정형 데이터를 통해 클라우드 환경을 관리하고 유지할 수 있습니다. Amazon S3 API와 같은 업계 표준 API에 대한 기본 지원에서 범용 호환성은 다양한 클라우드 환경에서 원활한 상호 운용성을 보장하며, 자동화된 라이프사이클 관리와 같은 고유한 혁신을 통해 보다 비용 효율적인 보호, 스토리지 및 고객의 비정형 데이터를 장기간 보존하도록 지원합니다.

NetApp의 Sovereign Cloud와 Cloud Director 공급자 고객 통합:

- 메타데이터를 비롯한 중요 데이터가 여전히 주권의 통제하에 있으며, 데이터 개인 정보 보호법을 위반할 수 있는 외부 기관의 액세스를 방지합니다.
- 보안 및 규정 준수를 강화하여 빠르게 진화하는 공격 벡터로부터 애플리케이션과 데이터를 보호하고 신뢰할 수 있는 로컬에 대한 지속적인 규정 준수를 유지합니다. 인프라, 기본 제공 프레임워크 및 로컬 전문가
- 미래 지향형 인프라로 변화하는 데이터 개인 정보 보호 규정, 보안 위협, 지정학에 빠르게 대응합니다.
- 안전한 데이터 공유 및 분석을 통해 데이터의 가치를 극대화하여 개인 정보 보호법을 위반하지 않고 혁신을 주도할 수 있습니다. 데이터 무결성이 보호되어 정확한 인사이트를 보장합니다.

StorageGRID 통합에 대한 자세한 내용은 다음을 참조하십시오.

- "NetApp 공지"

Red Hat OpenShift Container 워크로드를 지원하는 NetApp 하이브리드 멀티 클라우드

Red Hat OpenShift Container 워크로드를 위한 NetApp 하이브리드 멀티 클라우드 솔루션

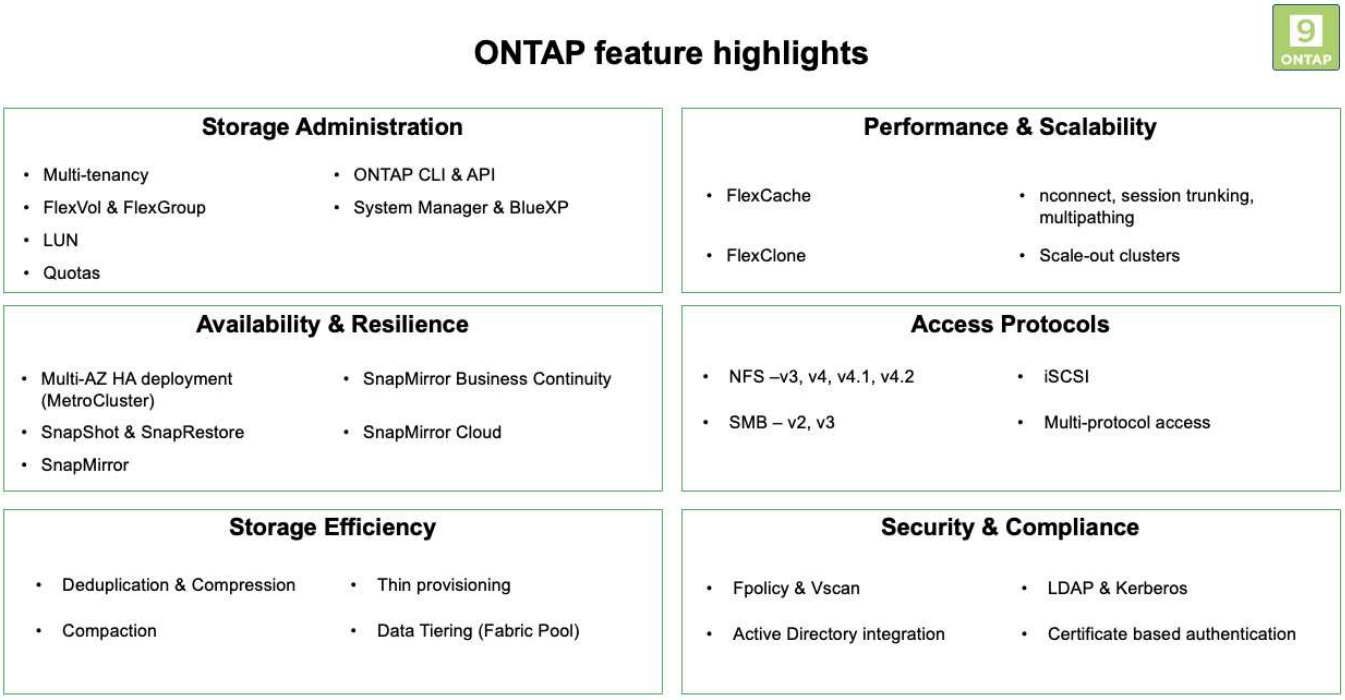
개요

NetApp은 기존 엔터프라이즈 애플리케이션을 현대화하고 Kubernetes를 기반으로 구축된 컨테이너 및 오케스트레이션 플랫폼을 사용하여 새로운 애플리케이션을 구축하는 고객이 크게 증가하고 있습니다. Red Hat OpenShift Container Platform은 많은 고객이 채택한 한 가지 예입니다.

점점 더 많은 고객이 기업 내에 컨테이너를 채택하기 시작함에 따라 NetApp은 상태 저장 애플리케이션의 영구 스토리지 요구사항과 데이터 보호, 데이터 보안, 데이터 마이그레이션과 같은 기존의 데이터 관리 요구사항을 충족할 수 있는 완벽한 위치를 선점하고 있습니다. 그러나 이러한 요구 사항은 서로 다른 전략, 도구 및 방법을 사용하여 충족됩니다.

- NetApp ONTAP** 아래에 나열된 스토리지 옵션을 사용하여 컨테이너 및 Kubernetes 구축을 위한 보안, 데이터 보호, 안정성 및 유연성을 확보할 수 있습니다.
  - 사내 자가 관리형 스토리지:

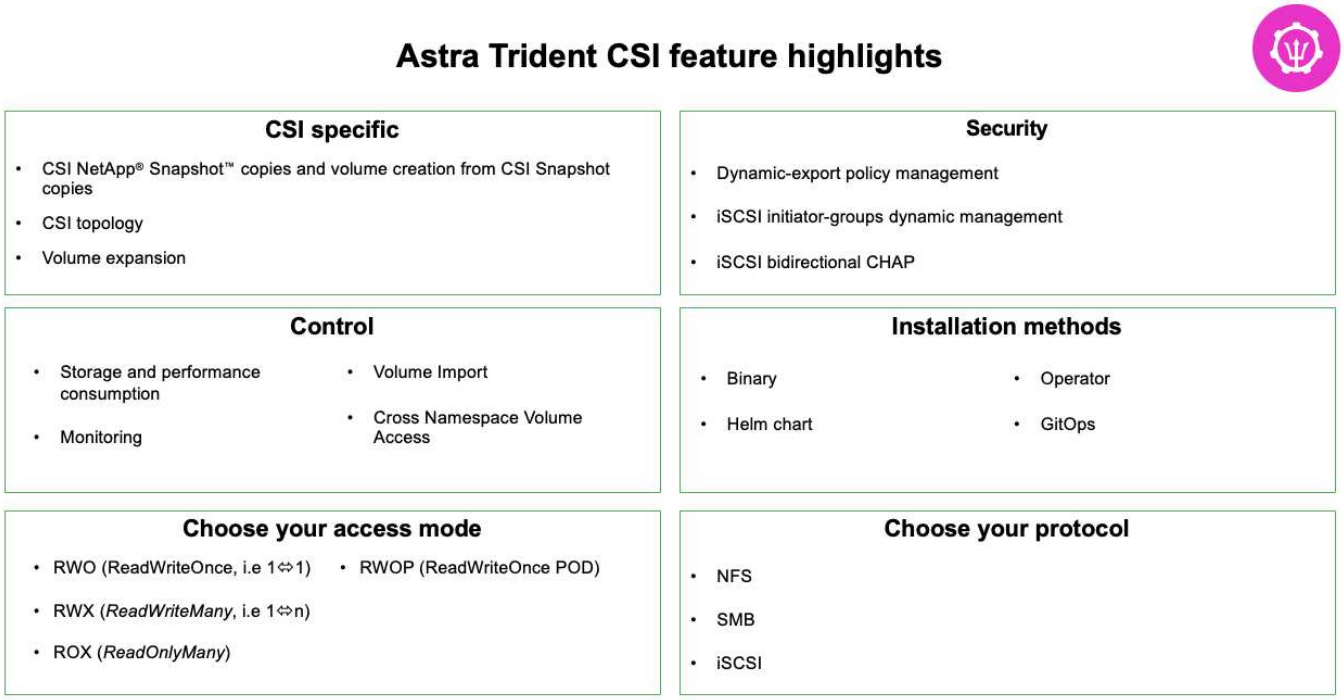
- NetApp 패브릭 연결 스토리지(FAS), NetApp All Flash FAS 어레이(AFF), NetApp All SAN 어레이(ASA) 및 ONTAP Select
    - 온프레미스에서 공급자 관리 스토리지:
- NetApp Keystone, STaaS(서비스형 스토리지) 제공
    - 클라우드에서 자가 관리 스토리지:
- NetApp Cloud Volumes ONTAP(CVO)은 하이퍼스케일러에 자가 관리하는 스토리지를 제공합니다
    - 클라우드 내 공급자 관리 스토리지:
- Cloud Volumes Service for Google Cloud(CVS), Azure NetApp Files(ANF), Amazon FSx for NetApp ONTAP는 하이퍼스케일러에 완전 관리형 스토리지를 제공합니다



- NetApp BlueXP** - 단일 제어 플레인/인터페이스에서 모든 스토리지 및 데이터 자산을 관리할 수 있습니다.

BlueXP를 사용하여 클라우드 스토리지(예: Cloud Volumes ONTAP 및 Azure NetApp Files)를 생성 및 관리하고, 데이터를 이동, 보호 및 분석하며, 많은 사내 및 에지 스토리지 장치를 제어할 수 있습니다.

- NetApp Astra Trident**는 CSI 규정 준수 스토리지 오케스트레이터로서, 위에서 언급한 다양한 NetApp 스토리지 옵션을 통해 영구 스토리지를 빠르고 쉽게 사용할 수 있습니다. NetApp에서 관리 및 지원하는 오픈 소스 소프트웨어입니다.



비즈니스 크리티컬 컨테이너 워크로드에는 영구 볼륨 이상의 용량이 필요합니다. 이들의 데이터 관리 요구사항에 따라 애플리케이션 Kubernetes 객체의 보호 및 마이그레이션이 필요합니다.

애플리케이션 데이터에는 사용자 데이터 외에도 Kubernetes 객체가 포함됩니다. 몇 가지 예는 다음과 같습니다. POD 사양, PVC, 구축, 서비스 맞춤형 구성 개체(예: 구성 맵 및 암호), 스냅샷 복사본, 백업, CRS, CRD와 같은 클론 맞춤형 리소스 등의 영구 데이터)가 있습니다

- NetApp Astra Control**, 완전 관리형 및 자가 관리 소프트웨어로 모두 사용 가능하며, 강력한 애플리케이션 데이터 관리를 위한 오케스트레이션을 제공합니다. 을 참조하십시오 "Astra 문서" Astra 제품군에 대한 자세한 내용은

이 참조 문서는 NetApp Astra Control Center를 사용하여 RedHat OpenShift 컨테이너 플랫폼에 배포된 컨테이너 기반 애플리케이션의 마이그레이션 및 보호를 검증합니다. 또한 이 솔루션은 컨테이너 플랫폼 관리를 위한 Red Hat Advanced Cluster Management(ACM)의 배포 및 사용에 대한 자세한 정보를 제공합니다. 또한, Astra Trident CSI 프로비저닝을 사용하여 NetApp 스토리지를 Red Hat OpenShift 컨테이너 플랫폼과 통합하기 위한 세부 정보도 제공합니다. Astra Control Center는 허브 클러스터에 구축되며 컨테이너 애플리케이션 및 영구 스토리지 라이프사이클을 관리하는 데 사용됩니다. 마지막으로, NetApp FSx for NetApp ONTAP(FSxN)를 영구 스토리지로 사용하는 AWS(Rosa)의 관리되는 Red Hat OpenShift 클러스터에서 복제, 페일오버 및 컨테이너 워크로드에 대한 페일백용 솔루션을 제공합니다.

Red Hat OpenShift Container 워크로드를 위한 **NetApp** 하이브리드 멀티 클라우드 솔루션의 가치 제안

대부분의 고객은 기존 인프라를 사용하지 않고 Kubernetes 기반 환경을 구축하는 것만을 시작하고 있지 않습니다. 가상 머신(예: 대규모 VMware 환경)에서 대부분의 엔터프라이즈 애플리케이션을 실행하는 기존 IT 환경일 수 있습니다. 그런 다음 최신 애플리케이션 개발 팀의 요구사항을 충족하기 위해 소규모 컨테이너 기반 환경을 구축하기 시작합니다. 이러한 이니셔티브는 일반적으로 소규모로 시작하여 팀이 새로운 기술과 기술을 익히고 이러한 기술을 채택함으로써 얻을 수 있는 많은 이점을 인식함에 따라 점차 널리 보급되기 시작합니다. 좋은 소식은 NetApp이 두 환경의 요구사항을 모두 충족할 수 있다는 것입니다. NetApp 고객은 Red Hat OpenShift를 사용하여 하이브리드 멀티 클라우드를 위한 이 솔루션 세트를 사용하여 전체

인프라와 조직을 정비하지 않고도 최신 클라우드 기술 및 서비스를 채택할 수 있습니다. 고객 애플리케이션과 데이터가 사내, 클라우드, 가상 머신 또는 컨테이너에서 호스팅되는 경우 NetApp은 일관된 데이터 관리, 보호, 보안 및 이동성을 제공할 수 있습니다. 새로운 솔루션을 통해 사내 데이터 센터 환경에서 NetApp이 수십 년 동안 제공해온 것과 동일한 가치를 재정비하거나 새로운 기술을 습득하거나 새로운 팀을 구축할 필요가 없이 기업 전체 데이터 수평선에서 사용할 수 있게 됩니다. NetApp은 고객이 클라우드 전환의 어떤 단계에 있든 관계없이 이러한 비즈니스 과제를 해결하도록 지원하기에 유리한 위치에 있습니다.

Red Hat OpenShift를 포함하는 NetApp 하이브리드 멀티 클라우드:

- NetApp 기반 스토리지 솔루션과 Red Hat OpenShift를 사용할 경우 고객이 데이터 및 애플리케이션을 관리, 보호, 보안, 마이그레이션할 수 있는 최상의 방법을 보여주는 검증된 설계와 사례를 제공합니다.
- VMware 환경, 베어 메탈 인프라 또는 이 둘을 조합하여 NetApp 스토리지와 Red Hat OpenShift를 실행하는 고객에게 모범 사례 제공
- 온프레미스 환경과 클라우드 환경 모두에서, 그리고 둘 다 사용되는 하이브리드 환경에 대한 전략과 옵션을 보여줍니다.

Red Hat OpenShift Container 워크로드를 위한 **NetApp** 하이브리드 멀티 클라우드 지원 솔루션

이 솔루션은 OpenShift 컨테이너 플랫폼(OCP), OpenShift Advanced Cluster Manager(ACM), NetApp ONTAP, NetApp BlueXP, NetApp Astra Control Center(ACC)를 사용해 마이그레이션 및 중앙 집중식 데이터 보호를 테스트하고 검증합니다.

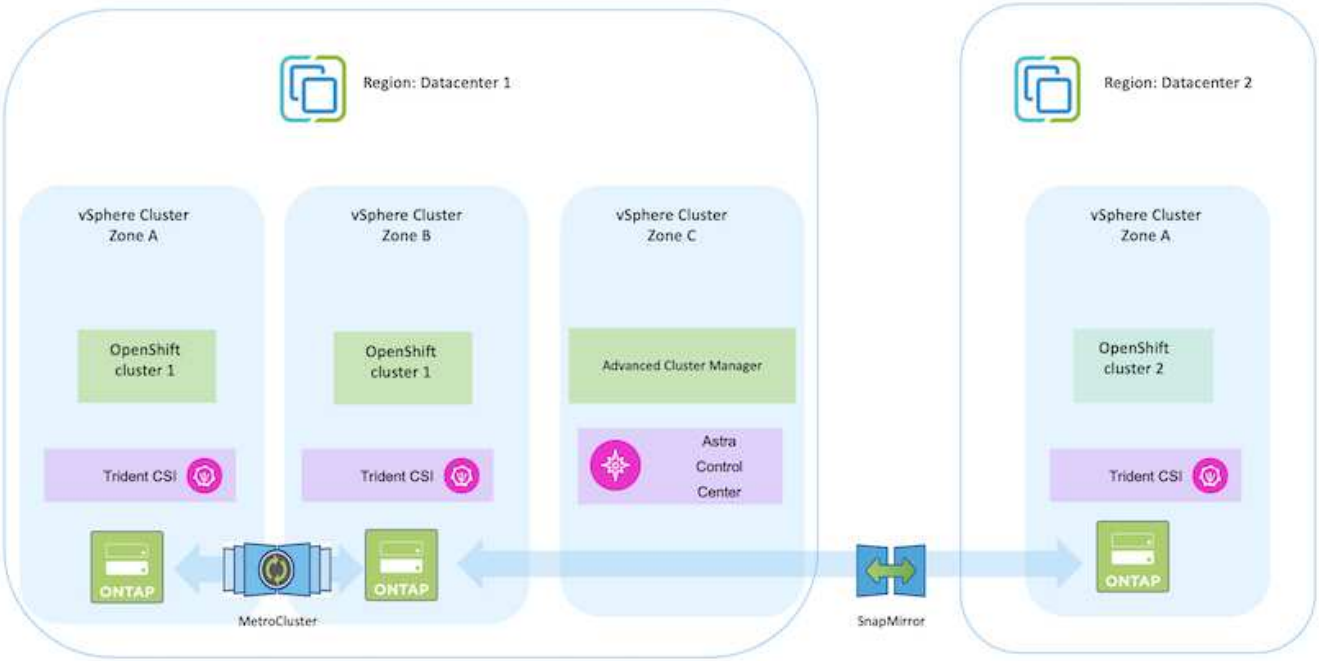
이 솔루션의 경우 다음 시나리오가 NetApp에서 테스트 및 검증되었습니다. 이 솔루션은 다음과 같은 특성을 기반으로 여러 시나리오로 구분됩니다.

- 온프레미스
- 클라우드
  - 자가 관리형 OpenShift 클러스터와 자가 관리형 NetApp 스토리지
  - 공급자가 관리하는 OpenShift 클러스터와 공급자 관리 NetApp 스토리지
  - 앞으로 추가 솔루션과 사용 사례를 구축하게 될 것입니다.**

시나리오 **1: ACC**를 사용하여 사내 환경 내에서 데이터 보호 및 마이그레이션

- 사내: 자체 관리형 OpenShift 클러스터와 자가 관리형 NetApp 스토리지**
  - ACC를 사용하여 데이터 보호를 위한 스냅샷 복사본, 백업 및 복원을 생성합니다.
  - ACC를 사용하여 컨테이너 애플리케이션의 SnapMirror 복제를 수행하십시오.

시나리오 **1**

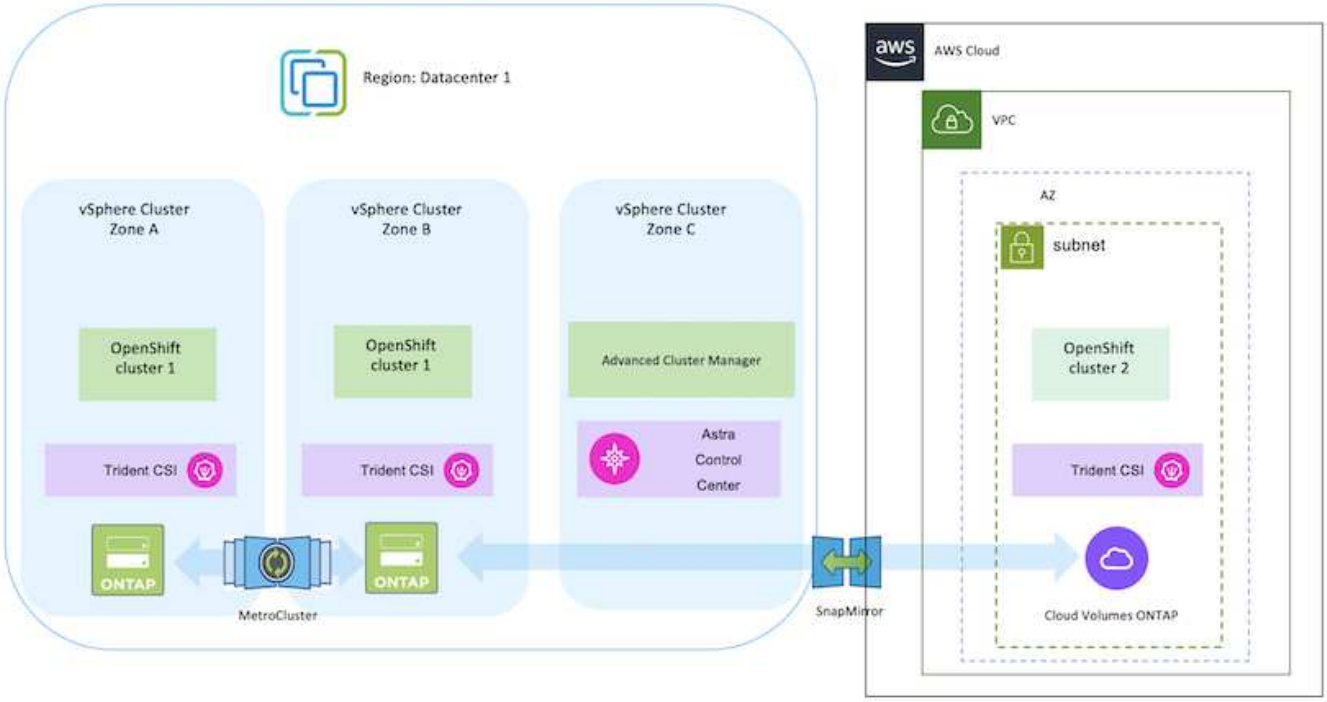


시나리오 **2: ACC**를 사용하여 사내 환경에서 **AWS** 환경으로 데이터 보호 및 마이그레이션

온프레미스: 자체 관리되는 OpenShift 클러스터와 자체 관리되는 스토리지 **AWS** 클라우드**:** 자체 관리되는 **OpenShift** 클러스터와 자체 관리되는 스토리지

- ACC를 사용하여 데이터 보호를 위한 백업 및 복원을 수행합니다.
- ACC를 사용하여 컨테이너 애플리케이션의 SnapMirror 복제를 수행하십시오.

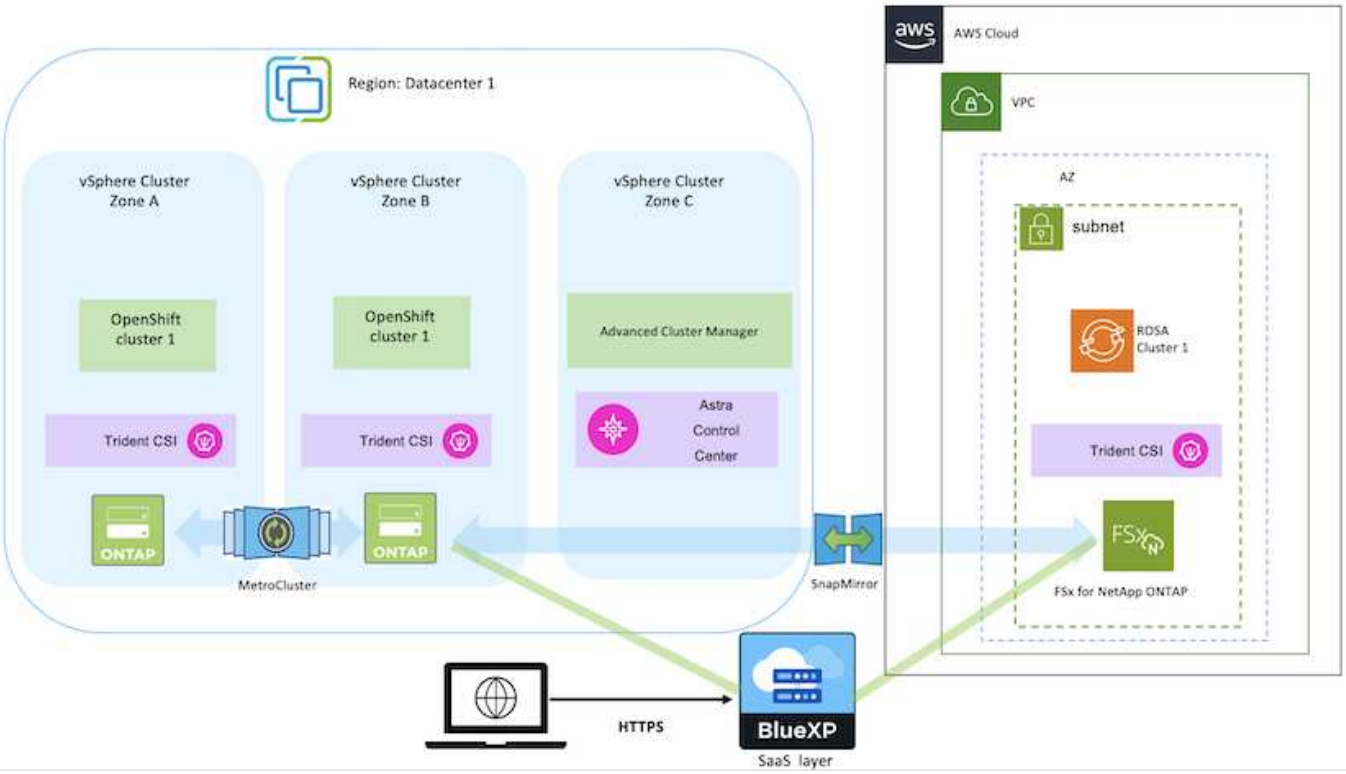
시나리오 **2**



시나리오 **3:** 사내 환경에서 **AWS** 환경으로 데이터 보호 및 마이그레이션

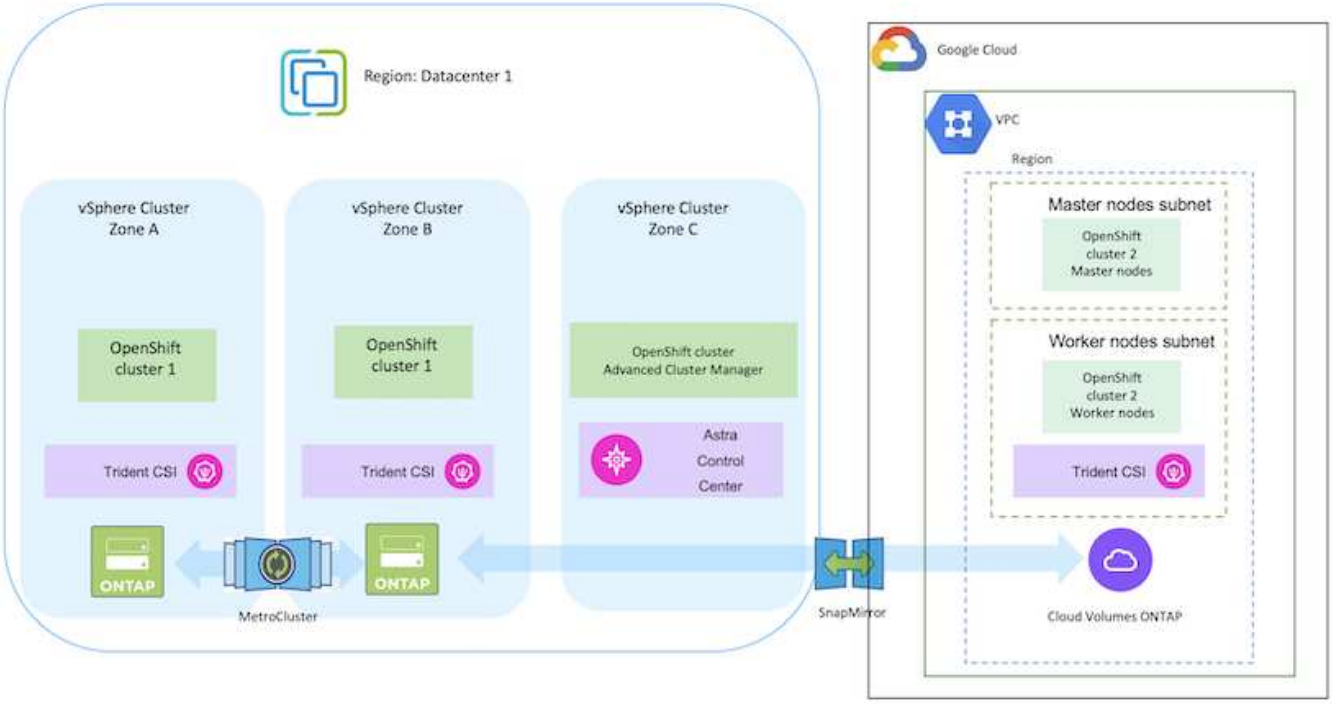
- 온프레미스: 자체 관리되는 OpenShift 클러스터와 자체 관리되는 스토리지** **AWS Cloud:** 공급자 관리 **OpenShift** 클러스터**(Rosa)** 및 공급자 관리 스토리지**(FSxN)**
  - BlueXP를 사용하여 영구 볼륨(FSxN)의 복제를 수행합니다.
  - OpenShift GitOps를 사용하여 애플리케이션 메타데이터를 다시 생성합니다.

시나리오 **3**



시나리오 **4: ACC**를 사용하여 온프레미스 환경에서 **GCP** 환경으로 데이터 보호 및 마이그레이션

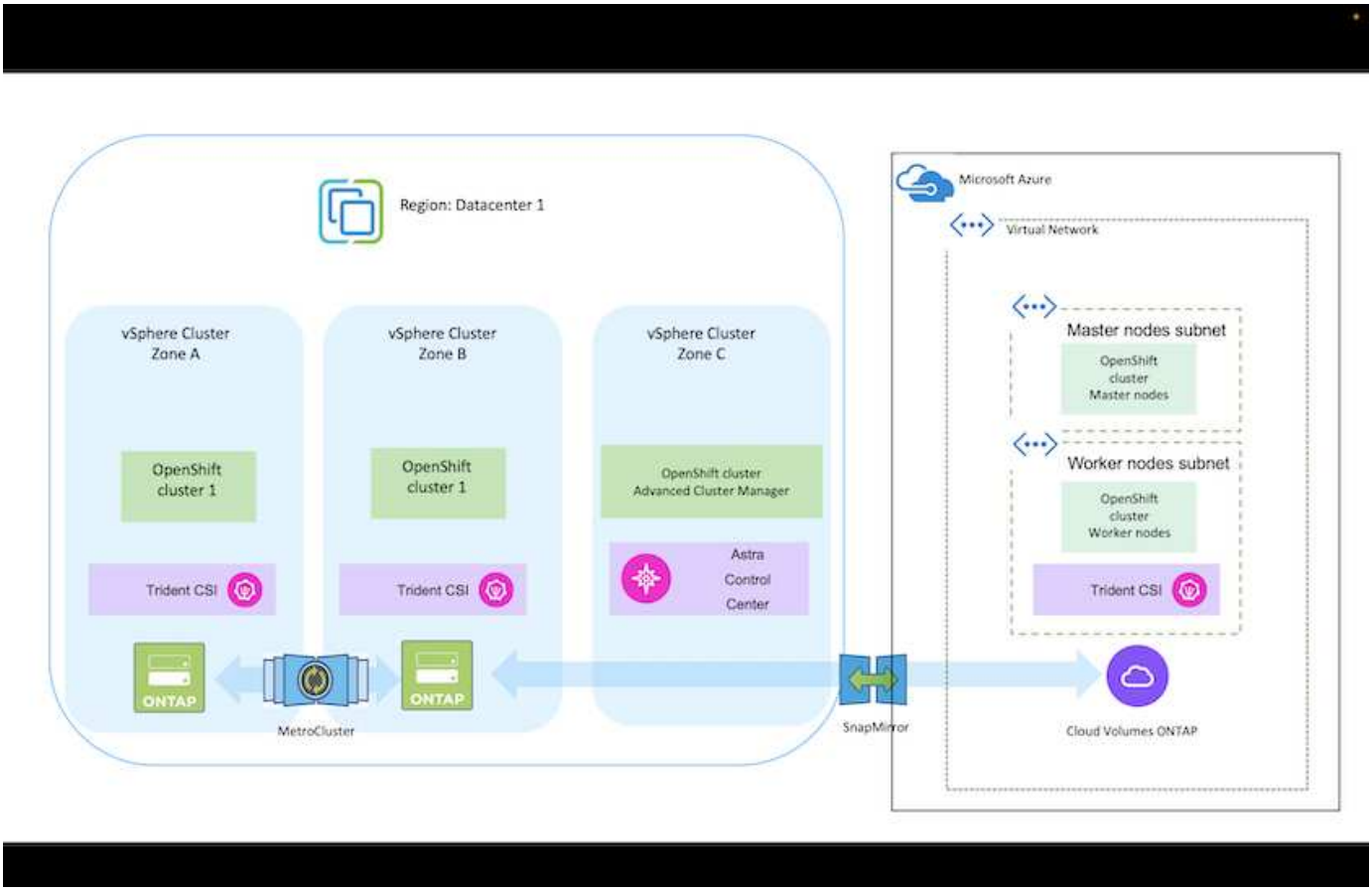
- 온프레미스: 자체 관리형 OpenShift 클러스터 및 자체 관리형 스토리지**
- Google Cloud: 자체 관리형 OpenShift 클러스터 및 자체 관리형 스토리지**
  - ACC를 사용하여 데이터 보호를 위한 백업 및 복원을 수행합니다.
  - ACC를 사용하여 컨테이너 애플리케이션의 SnapMirror 복제를 수행하십시오.



MetroCluster 구성에서 ONTAP를 사용할 때의 고려 사항은 을 참조하십시오 "여기".

시나리오 **5: ACC**를 사용하여 온프레미스 환경에서 **Azure** 환경으로 데이터 보호 및 마이그레이션

- 온프레미스: 자체 관리형 OpenShift 클러스터 및 자체 관리형 스토리지**
- Azure Cloud: 자체 관리형 OpenShift 클러스터 및 자체 관리형 스토리지**
  - ACC를 사용하여 데이터 보호를 위한 백업 및 복원을 수행합니다.
  - ACC를 사용하여 컨테이너 애플리케이션의 SnapMirror 복제를 수행하십시오.



MetroCluster 구성에서 ONTAP를 사용할 때의 고려 사항은 을 참조하십시오 "여기".

솔루션 검증에 사용된 다양한 구성 요소의 버전입니다

이 솔루션은 OpenShift 컨테이너 플랫폼, OpenShift Advanced Cluster Manager, NetApp ONTAP, NetApp Astra Control Center를 사용하여 마이그레이션 및 중앙 집중식 데이터 보호를 테스트하고 검증합니다.

솔루션의 시나리오 1, 2 및 3은 아래 표에 표시된 버전을 사용하여 검증되었습니다.

* 구성 요소 *	* 버전 *
* VMware *	vSphere Client 버전 8.0.0.10200 VMware ESXi, 8.0.0, 20842819
* 허브 클러스터 *	OpenShift 4.11.34
* 소스 및 대상 클러스터 *	OpenShift 4.12.9 사내 및 AWS
* NetApp Astra Trident *	Trident 서버 및 클라이언트 23.04.0
* NetApp Astra Control Center * 에서 확인할 수 있습니다	ACC 22.11.0-82
* NetApp ONTAP *	ONTAP 9.12.1
NetApp ONTAP * 용 * AWS FSx	싱글 AZ

솔루션의 시나리오 4는 아래 표에 표시된 버전을 사용하여 검증되었습니다.

* 구성 요소 *	* 버전 *
* VMware *	vSphere Client 버전 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
* 허브 클러스터 *	OpenShift 4.13.13
* 소스 및 대상 클러스터 *	OpenShift 4.13.12 데이터를 더 많이 활용하십시오
* NetApp Astra Trident *	Trident 서버 및 클라이언트 23.07.0
* NetApp Astra Control Center * 에서 확인할 수 있습니다	ACC 23.07.0-25
* NetApp ONTAP *	ONTAP 9.12.1
* Cloud Volumes ONTAP *	단일 AZ, 단일 노드, 9.14.0

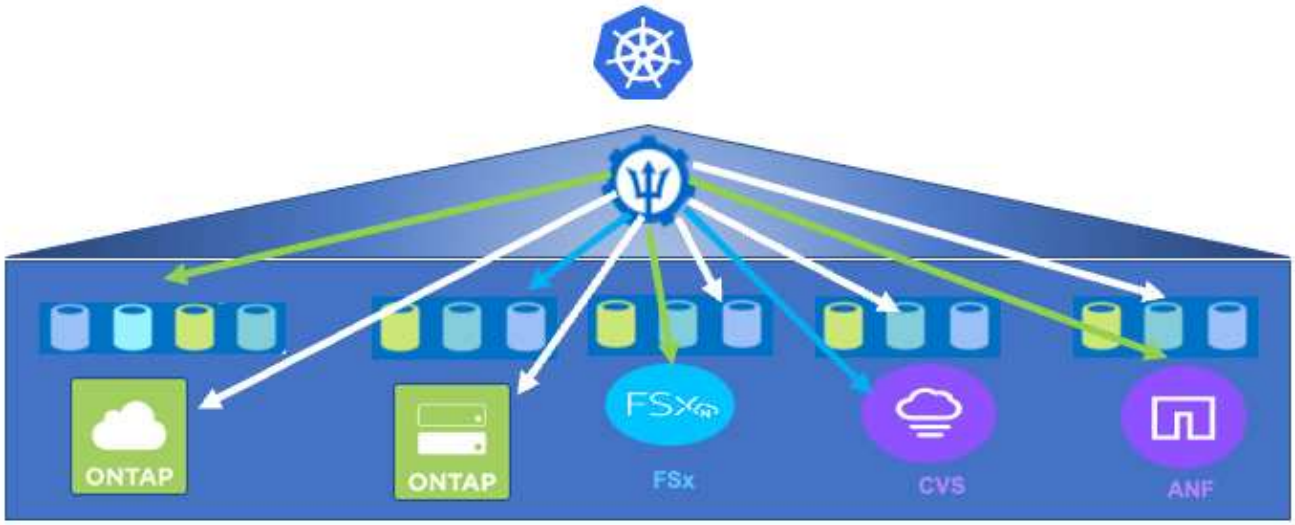
솔루션의 시나리오 5는 아래 표에 표시된 버전을 사용하여 검증되었습니다.

* 구성 요소 *	* 버전 *
* VMware *	vSphere Client 버전 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
* 소스 및 대상 클러스터 *	OpenShift 4.13.25 데이터를 더 많이 활용하십시오
* NetApp Astra Trident *	Trident Server, Client 및 Astra Control Provisioner 23.10.0 을 참조하십시오
* NetApp Astra Control Center * 에서 확인할 수 있습니다	ACC 23.10
* NetApp ONTAP *	ONTAP 9.12.1
* Cloud Volumes ONTAP *	단일 AZ, 단일 노드, 9.14.0

Red Hat Open Shift 컨테이너와의 **NetApp** 스토리지 통합을 지원했습니다

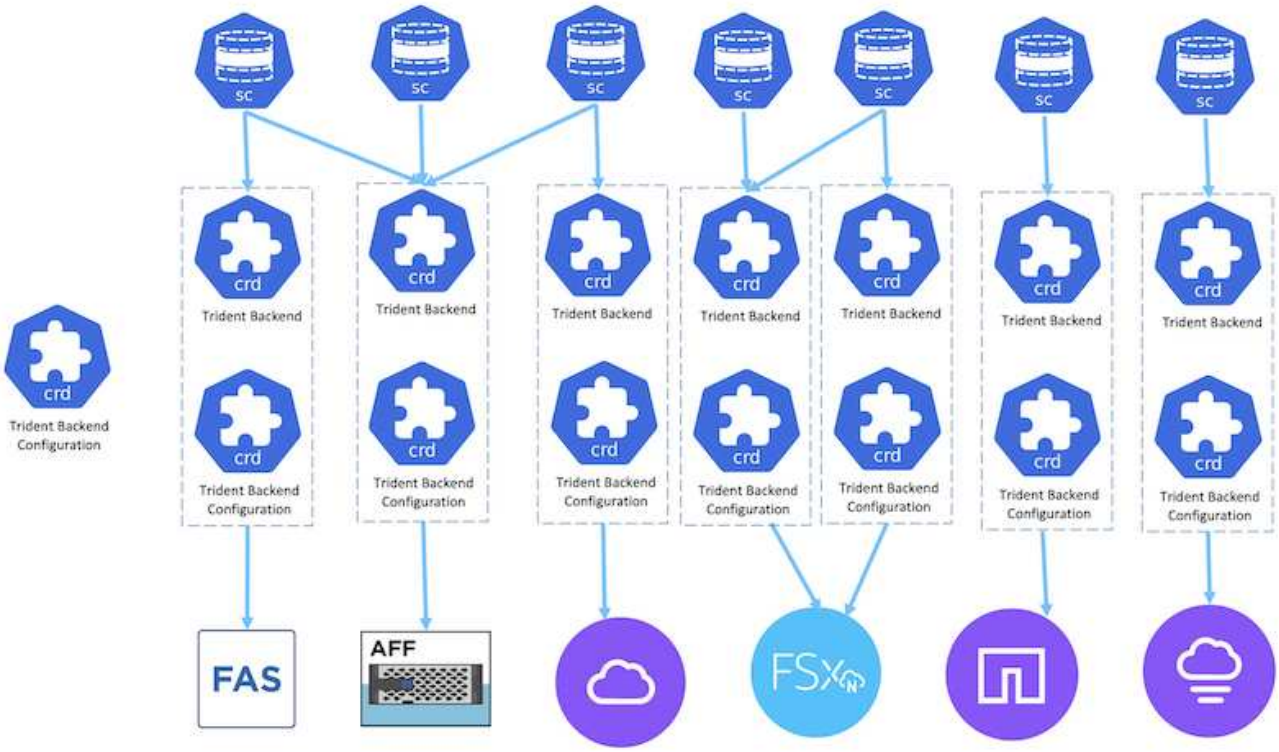
Red Hat Open Shift 컨테이너를 VMware에서 실행하거나 하이퍼스케일러에서 실행하는 경우, NetApp Astra Trident를 지원하는 다양한 백엔드 NetApp 스토리지의 CSI 프로비저닝 용도로 사용할 수 있습니다.

다음 다이어그램은 NetApp Astra Trident를 사용하여 OpenShift 클러스터와 통합할 수 있는 다양한 백엔드 NetApp 스토리지를 보여 줍니다.

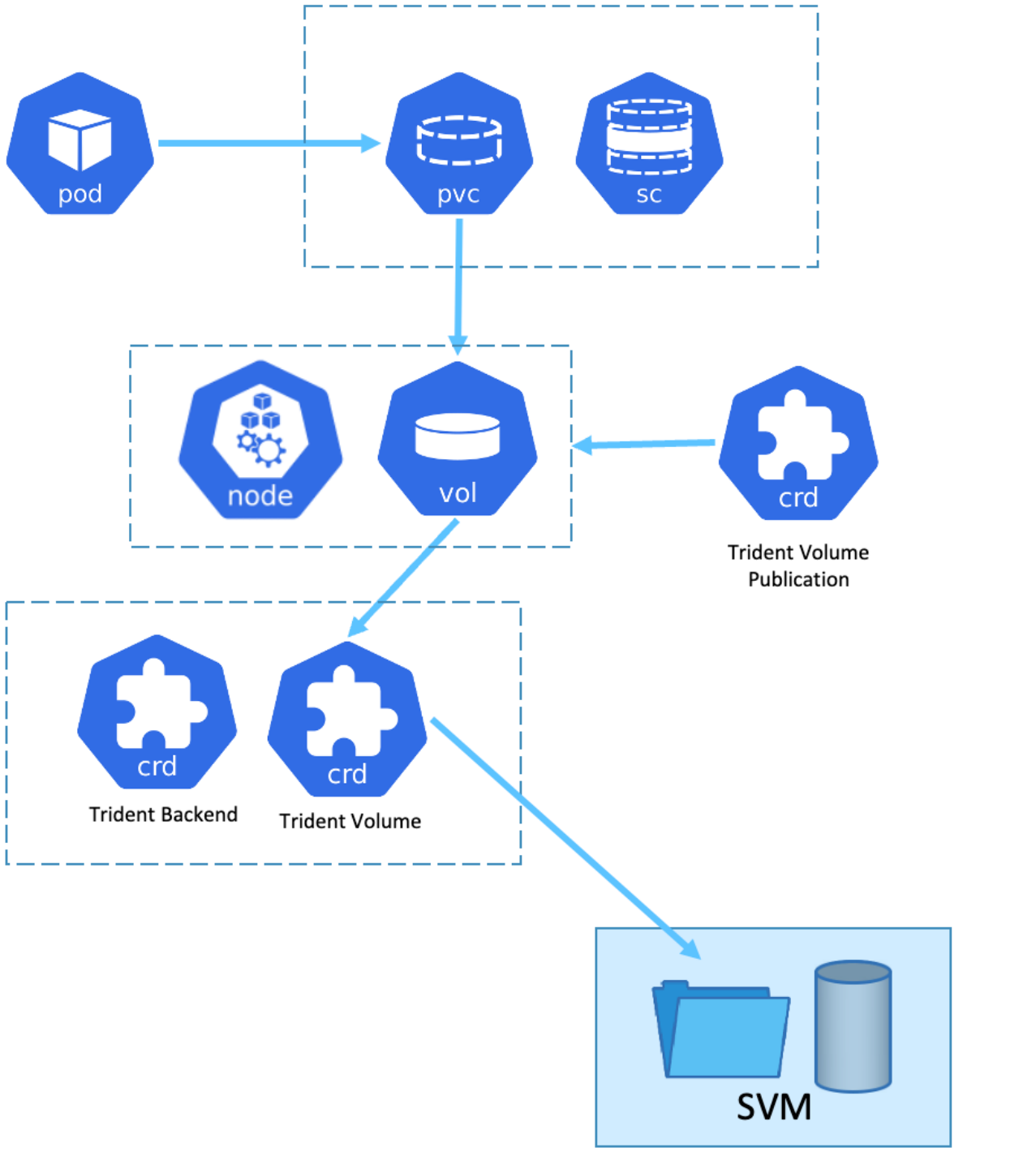


ONTAP SVM(스토리지 가상 머신)은 안전한 멀티 테넌시를 제공합니다. 단일 OpenShift 클러스터는 단일 SVM이나 여러 SVM, 심지어 여러 ONTAP 클러스터에 연결할 수 있습니다. 스토리지 클래스는 매개 변수 또는 레이블을 기준으로 백엔드 스토리지를 필터링합니다. 스토리지 관리자는 삼중 백엔드 구성을 사용하여 스토리지 시스템에 접속할 매개 변수를 정의합니다. 접속 설정에 성공하면 트리덴트 백엔드를 생성하고 스토리지 클래스가 필터링할 수 있는 정보를 채웁니다.

스토리지 플랫폼과 백엔드 간의 관계가 아래에 나와 있습니다.



애플리케이션 소유자가 스토리지 클래스를 사용하여 영구 볼륨을 요청합니다. 스토리지 클래스는 백엔드 스토리지를 필터링합니다. POD와 백엔드 스토리지 간의 관계가 아래에 나와 있습니다.



컨테이너 스토리지 인터페이스**(CSI)** 옵션

vSphere 환경에서 고객은 VMware CSI 드라이버 및/또는 Astra Trident CSI를 선택하여 ONTAP와 통합할 수 있습니다. VMware CSI에서는 영구 볼륨이 로컬 SCSI 디스크로 사용되는 반면, Trident에서는 네트워크에서 사용됩니다. VMware CSI는 ONTAP에서 rwx 액세스 모드를 지원하지 않으므로 rwx 모드가 필요한 경우 애플리케이션이 Trident CSI를 사용해야 합니다. FC 기반 구축을 통해 VMware CSI가 선호되고 SMBC(SnapMirror

Business Continuity)는 존 레벨 고가용성을 제공합니다.

VMware CSI는 를 지원합니다

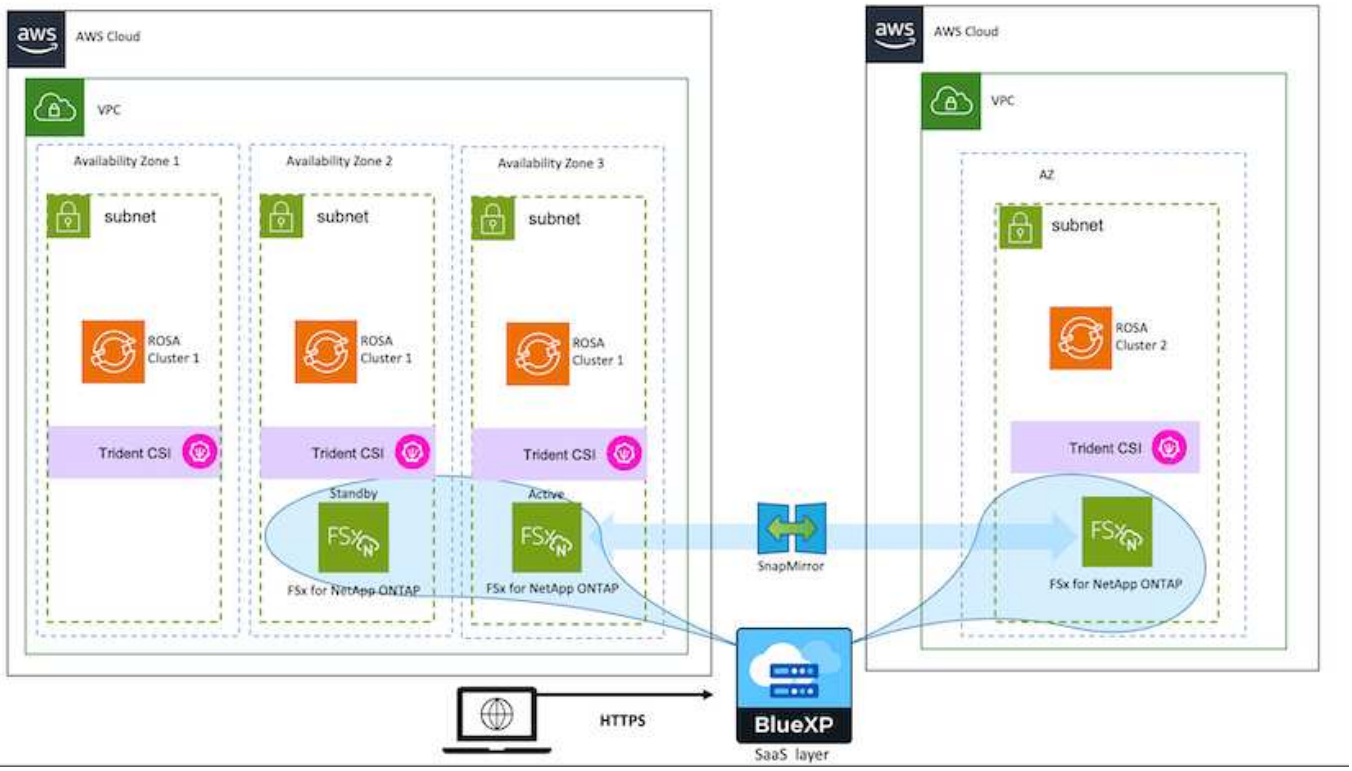
- 코어 블록 기반 데이터 저장소(FC, FCoE, iSCSI, NVMeoF)
- 핵심 파일 기반 데이터 저장소(NFS v3, v4)
- VVOL 데이터 저장소(블록 및 파일)

Trident에는 **ONTAP**를 지원하는 다음과 같은 드라이버가 있습니다

- ONTAP-SAN(전용 볼륨)
- ONTAP-SAN-이코노미(공유 볼륨)
- ONTAP-NAS(전용 볼륨)
- ONTAP-NAS-이코노미(공유 볼륨)
- ONTAP-NAS-Flexgroup(대규모 전용 볼륨)

VMware CSI 및 Astra Trident CSI 모두에서 ONTAP는 NFS 및 다중 경로, CHAP 인증 등에 대한 nconnect, 세션 트렁킹, Kerberos 등을 지원합니다.

AWS에서 FSx for NetApp ONTAP(FSxN)는 AZ(단일 가용성 영역) 또는 AZ에 구축할 수 있습니다. 고가용성이 요구되는 운영 워크로드의 경우, Multi-AZ는 조널 레벨 내결함성을 제공하며 단일 AZ에 비해 더 나은 NVMe 읽기 캐시를 제공합니다. 자세한 내용은 을 참조하십시오 "AWS 성능 지침".
재해 복구 사이트 비용을 절약하기 위해 단일 AZ FSx ONTAP를 활용할 수 있습니다.



FSx ONTAP에서 지원되는 SVM 수는 를 참조하십시오 "FSx ONTAP 스토리지 가상 머신 관리"

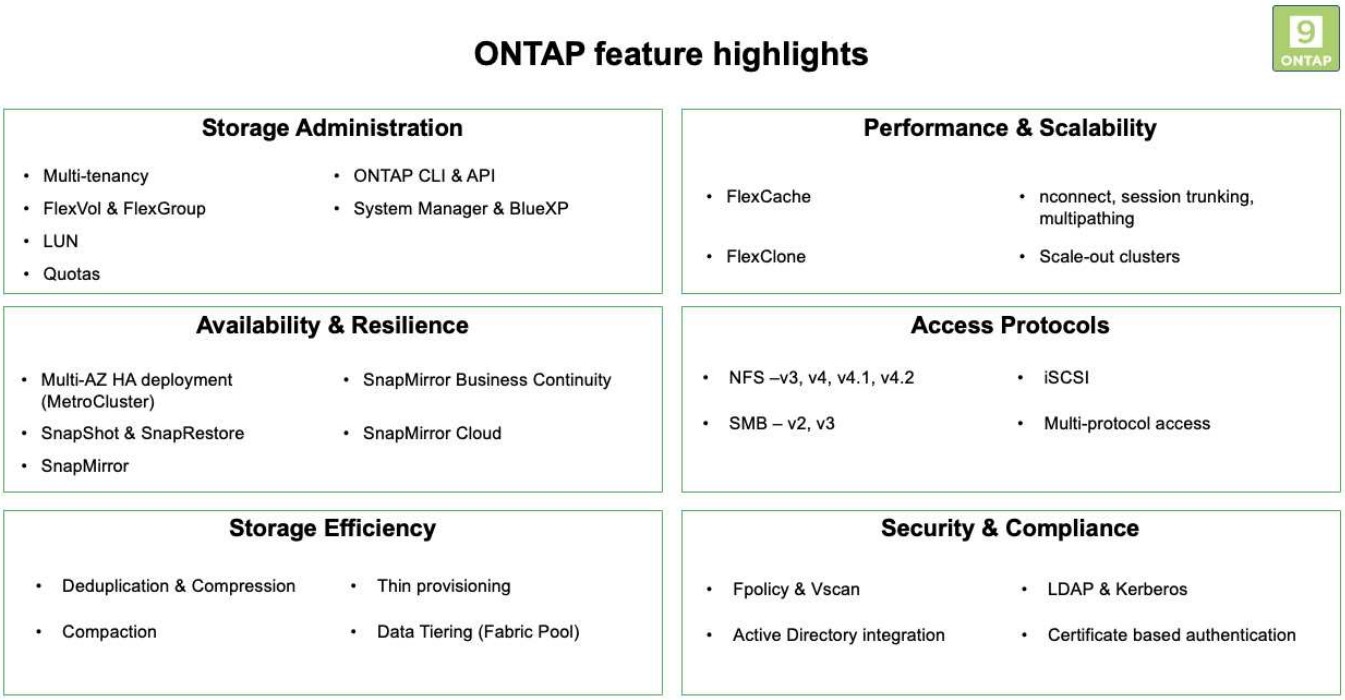
Red Hat OpenShift Container 워크로드를 위한 NetApp 하이브리드 멀티 클라우드 솔루션

개요

NetApp은 기존 엔터프라이즈 애플리케이션을 현대화하고 Kubernetes를 기반으로 구축된 컨테이너 및 오케스트레이션 플랫폼을 사용하여 새로운 애플리케이션을 구축하는 고객이 크게 증가하고 있습니다. Red Hat OpenShift Container Platform은 많은 고객이 채택한 한 가지 예입니다.

점점 더 많은 고객이 기업 내에 컨테이너를 채택하기 시작함에 따라 NetApp은 상태 저장 애플리케이션의 영구 스토리지 요구사항과 데이터 보호, 데이터 보안, 데이터 마이그레이션과 같은 기존의 데이터 관리 요구사항을 충족할 수 있는 완벽한 위치를 선점하고 있습니다. 그러나 이러한 요구 사항은 서로 다른 전략, 도구 및 방법을 사용하여 충족됩니다.

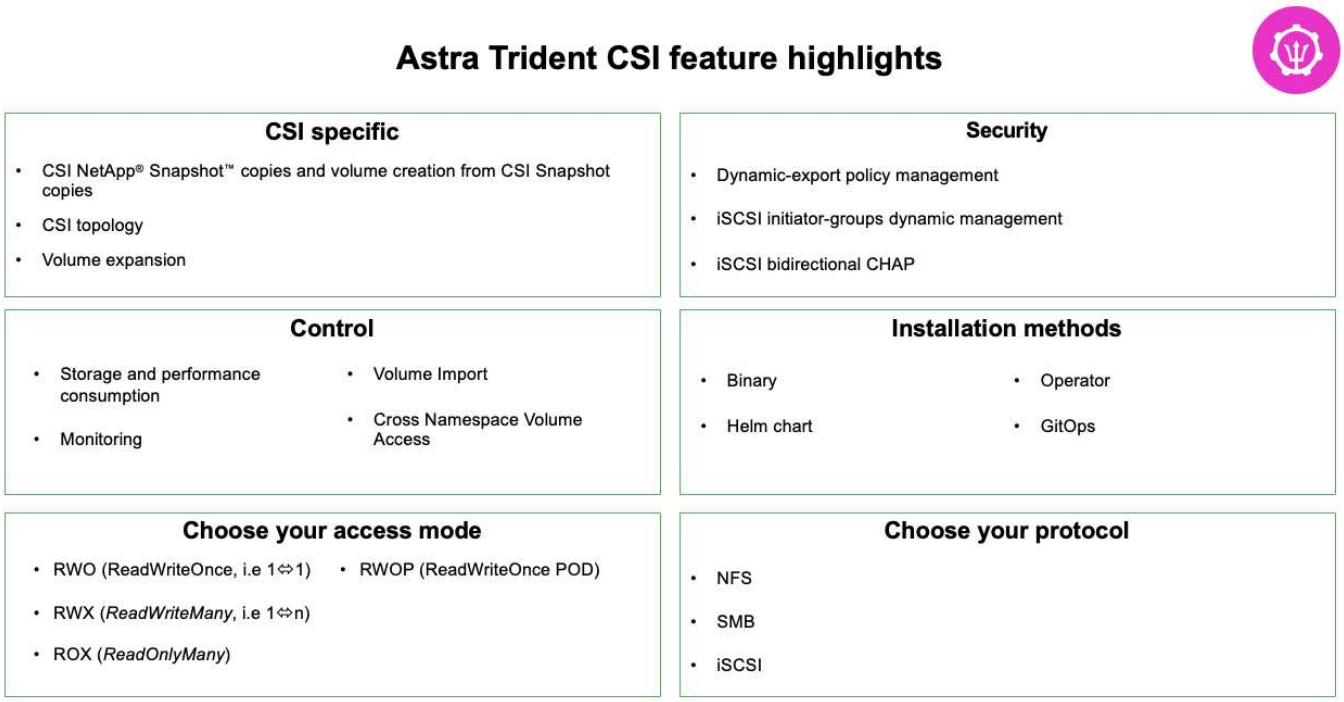
- NetApp ONTAP** 아래에 나열된 스토리지 옵션을 사용하여 컨테이너 및 Kubernetes 구축을 위한 보안, 데이터 보호, 안정성 및 유연성을 확보할 수 있습니다.
  - 사내 자가 관리형 스토리지:
- NetApp 패브릭 연결 스토리지(FAS), NetApp All Flash FAS 어레이(AFF), NetApp All SAN 어레이(ASA) 및 ONTAP Select
  - 온프레미스에서 공급자 관리 스토리지:
- NetApp Keystone, STaaS(서비스형 스토리지) 제공
  - 클라우드에서 자가 관리 스토리지:
- NetApp Cloud Volumes ONTAP(CVO)은 하이퍼스케일러에 자가 관리하는 스토리지를 제공합니다
  - 클라우드 내 공급자 관리 스토리지:
- Cloud Volumes Service for Google Cloud(CVS), Azure NetApp Files(ANF), Amazon FSx for NetApp ONTAP는 하이퍼스케일러에 완전 관리형 스토리지를 제공합니다



- NetApp BlueXP** - 단일 제어 플레인/인터페이스에서 모든 스토리지 및 데이터 자산을 관리할 수 있습니다.

BlueXP를 사용하여 클라우드 스토리지(예: Cloud Volumes ONTAP 및 Azure NetApp Files)를 생성 및 관리하고, 데이터를 이동, 보호 및 분석하며, 많은 사내 및 에지 스토리지 장치를 제어할 수 있습니다.

- NetApp Astra Trident**는 CSI 규정 준수 스토리지 오케스트레이터로서, 위에서 언급한 다양한 NetApp 스토리지 옵션을 통해 영구 스토리지를 빠르고 쉽게 사용할 수 있습니다. NetApp에서 관리 및 지원하는 오픈 소스 소프트웨어입니다.



비즈니스 크리티컬 컨테이너 워크로드에는 영구 볼륨 이상의 용량이 필요합니다. 이들의 데이터 관리 요구사항에 따라 애플리케이션 Kubernetes 객체의 보호 및 마이그레이션이 필요합니다.

애플리케이션 데이터에는 사용자 데이터 외에도 Kubernetes 객체가 포함됩니다. 몇 가지 예는 다음과 같습니다. POD 사양, PVC, 구축, 서비스 맞춤형 구성 개체(예: 구성 맵 및 암호), 스냅샷 복사본, 백업, CRS, CRD와 같은 클론 맞춤형 리소스 등의 영구 데이터)가 있습니다

- NetApp Astra Control**, 완전 관리형 및 자가 관리 소프트웨어로 모두 사용 가능하며, 강력한 애플리케이션 데이터 관리를 위한 오케스트레이션을 제공합니다. 을 참조하십시오 "Astra 문서" Astra 제품군에 대한 자세한 내용은

이 참조 문서는 NetApp Astra Control Center를 사용하여 RedHat OpenShift 컨테이너 플랫폼에 배포된 컨테이너 기반 애플리케이션의 마이그레이션 및 보호를 검증합니다. 또한 이 솔루션은 컨테이너 플랫폼 관리를 위한 Red Hat Advanced Cluster Management(ACM)의 배포 및 사용에 대한 자세한 정보를 제공합니다. 또한, Astra Trident CSI 프로비저닝을 사용하여 NetApp 스토리지를 Red Hat OpenShift 컨테이너 플랫폼과 통합하기 위한 세부 정보도 제공합니다. Astra Control Center는 허브 클러스터에 구축되며 컨테이너 애플리케이션 및 영구 스토리지 라이프사이클을 관리하는 데 사용됩니다. 마지막으로, NetApp FSx for NetApp ONTAP(FSxN)를 영구 스토리지로 사용하는 AWS(Rosa)의 관리되는 Red Hat OpenShift 클러스터에서 복제, 페일오버 및 컨테이너 워크로드에 대한 페일백용 솔루션을 제공합니다.

VMware 기반의 **Red Hat OpenShift Container** 플랫폼 워크로드를 지원하는 **NetApp** 솔루션

고객이 프라이빗 데이터 센터의 인프라에서 최신 컨테이너식 애플리케이션을 실행해야 하는 경우, 그렇게 할 수 있습니다. 컨테이너 워크로드를 배포할 수 있는 성공적인 생산 준비 환경을

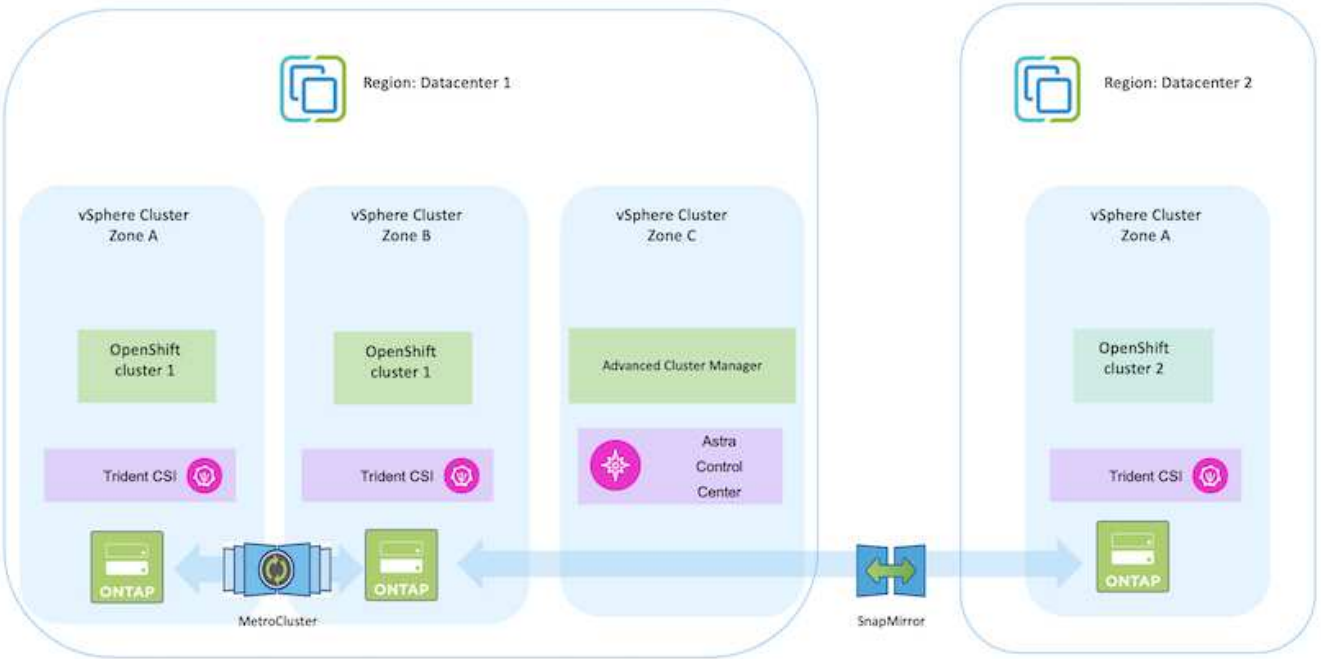
위해 Red Hat OpenShift 컨테이너 플랫폼(OCP)을 계획하고 배포해야 합니다. OCP 클러스터는 VMware 또는 베어 메탈에 구축할 수 있습니다.

NetApp ONTAP 스토리지는 컨테이너 구축을 위한 데이터 보호, 안정성 및 유연성을 제공합니다. Astra Trident는 동적 스토리지 프로비저닝을 통해 고객의 상태 저장 애플리케이션에 영구 ONTAP 스토리지를 사용합니다. Astra Control Center는 데이터 보호, 마이그레이션, 비즈니스 연속성 등 상태 저장 애플리케이션의 다양한 데이터 관리 요구 사항을 조율하는 데 사용할 수 있습니다.

VMware vSphere를 통해 NetApp ONTAP 툴은 데이터 저장소 프로비저닝에 사용할 수 있는 vCenter 플러그인을 제공합니다. 태그를 적용하고 노드 구성 및 데이터를 저장하기 위해 OpenShift와 함께 사용합니다. NVMe 기반 스토리지는 낮은 지연 시간과 고성능을 제공합니다.

이 솔루션은 Astra Control Center를 사용하여 컨테이너 워크로드의 데이터 보호 및 마이그레이션에 대한 세부 정보를 제공합니다. 이 솔루션의 경우 컨테이너 워크로드가 온프레미스 환경 내에서 vSphere의 Red Hat OpenShift 클러스터에 배포됩니다. 참고: 향후 베어 메탈에서 OpenShift 클러스터의 컨테이너 워크로드에 대한 솔루션을 제공할 예정입니다.

Astra Control Center를 사용하는 **OpenShift Container** 워크로드를 위한 데이터 보호 및 마이그레이션 솔루션

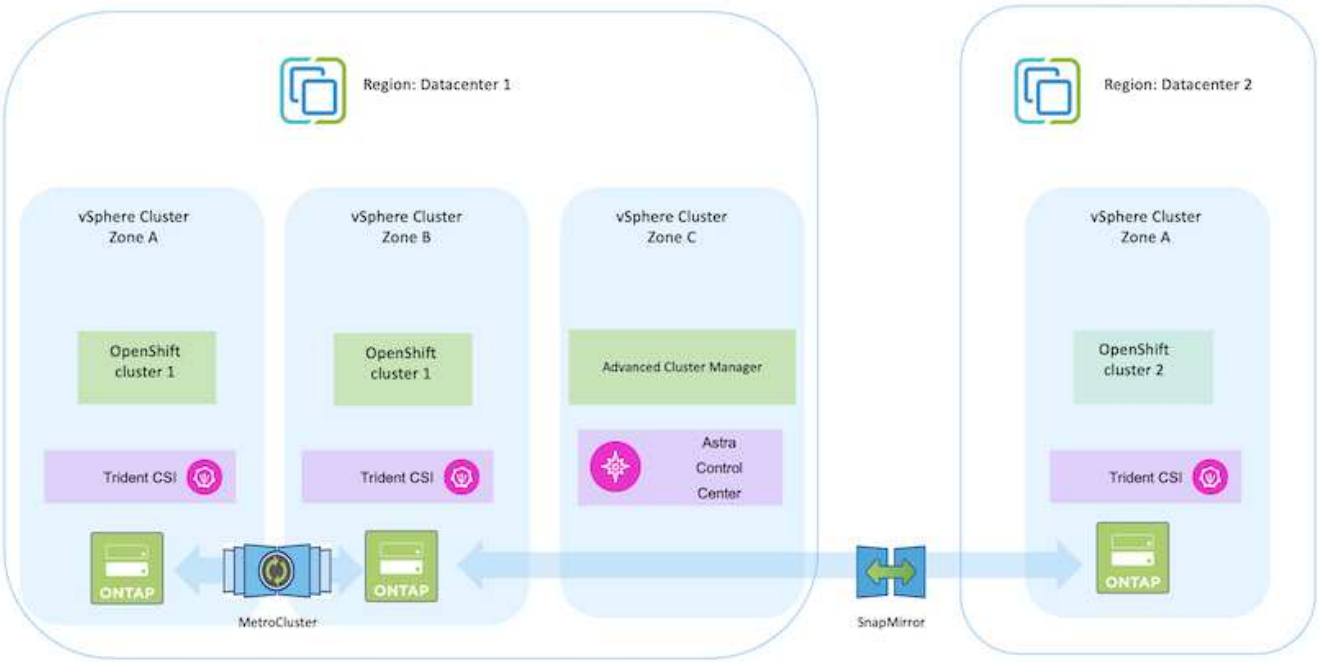


VMware에서 **Red Hat OpenShift Container** 플랫폼을 배포하고 구성합니다

이 섹션에서는 OpenShift 클러스터를 설정 및 관리하고 이를 기반으로 상태 저장 애플리케이션을 관리하는 방법에 대한 고급 워크플로우를 설명합니다. 또한, 영구 볼륨을 제공하는 Astra Trident의 도움을 받아 NetApp ONTAP 스토리지 어레이를 사용하는 모습을 보여 줍니다. 상태 저장 애플리케이션에 대한 데이터 보호 및 마이그레이션 작업을 수행하기 위해 Astra Control Center를 사용하는 방법에 대한 세부 정보가 제공됩니다.

Red Hat OpenShift Container 플랫폼 클러스터를 배포하는 방법에는 여러 가지가 있습니다. 설정에 대한 이 고급 설명은 사용된 특정 방법에 대한 설명서 링크를 제공합니다. 에 제공된 관련 링크에서 다른 방법을 참조할 수 있습니다 "리소스 섹션을 참조하십시오".

다음은 데이터 센터의 VMware에 구축된 클러스터를 보여 주는 다이어그램입니다.



설치 프로세스는 다음 단계로 나눌 수 있습니다.

CentOS VM 배포 및 구성

- VMware vSphere 환경에 구축됩니다.
- 이 VM은 NetApp Astra Trident 및 NetApp Astra Control Center와 같은 일부 구성요소를 구축하는 데 사용됩니다.
- 설치 중에 이 VM에 루트 사용자가 구성됩니다.

VMware vSphere(허브 클러스터)에서 **OpenShift Container Platform** 클러스터 배포 및 구성

의 지침을 참조하십시오 "보조 배포" OCP 클러스터 구축 방법

다음 사항을 기억하십시오. - ssh 공용 및 개인 키를 생성하여 설치 프로그램에 제공합니다. 이러한 키는 필요한 경우 마스터 및 작업자 노드에 로그인하는 데 사용됩니다. - 지원되는 설치 프로그램에서 설치 프로그램을 다운로드합니다. 이 프로그램은 마스터 노드와 작업자 노드에 대해 VMware vSphere 환경에서 생성한 VM을 부팅하는 데 사용됩니다. VM에는 최소 CPU, 메모리 및 하드 디스크 요구 사항이 있어야 합니다. (에서 VM create 명령을 참조하십시오 "여기" 마스터 및 이 정보를 제공하는 작업자 노드에 대한 페이지) - 모든 VM에서 diskUUID를 활성화해야 합니다. - 마스터에 대해 최소 3개의 노드를 만들고 작업자에 대해 3개의 노드를 만듭니다. 설치 관리자가 검색한 후 VMware vSphere 통합 전환 버튼을 설정합니다.

허브 클러스터에 고급 클러스터 관리를 설치합니다

허브 클러스터의 고급 클러스터 관리 운영자를 사용하여 설치됩니다. 지침을 참조하십시오 "여기".

허브 클러스터에 내부 **Red Hat Quay** 레지스트리를 설치합니다**.**

- Astra 이미지를 푸시하려면 내부 레지스트리가 필요합니다. 키 내부 레지스트리는 허브 클러스터의 오퍼레이터를 사용하여 설치됩니다.
- 지침을 참조하십시오 "여기"

추가 **OCP** 클러스터 **2**개 설치**(**소스 및 대상**)**

- 허브 클러스터의 ACM을 사용하여 추가 클러스터를 구축할 수 있습니다.
- 지침을 참조하십시오 "여기".

NetApp ONTAP 스토리지를 구성합니다

- VMware 환경에서 OCP VM에 연결된 ONTAP 클러스터를 설치합니다.
- SVM을 생성합니다.
- SVM에서 스토리지에 액세스할 수 있도록 NAS 데이터 거짓을 구성합니다.

OCP 클러스터에 **NetApp Trident**를 설치합니다

- 허브, 소스, 타겟 클러스터의 3개 클러스터 모두에 NetApp Trident를 설치합니다
- 지침을 참조하십시오 "여기".
- ONTAP-NAS에 대한 스토리지 백엔드를 생성합니다.
- ONTAP-NAS의 스토리지 클래스를 생성합니다.
- 지침을 참조하십시오 "여기".

NetApp Astra Control Center를 설치합니다

- NetApp Astra Control Center는 허브 클러스터의 Astra Operator를 사용하여 설치됩니다.
- 지침을 참조하십시오 "여기".

기억하십시오. * 지원 사이트에서 NetApp Astra Control Center 이미지를 다운로드하십시오. * 이미지를 내부 레지스트리로 푸시합니다. * 여기 에서 지침을 참조하십시오.

소스 클러스터에 애플리케이션을 배포합니다

OpenShift GitOps를 사용하여 애플리케이션을 배포합니다. (예: Postgres, 고스트)

Astra Control Center에 소스 및 대상 클러스터를 추가합니다**.**

Astra Control 관리에 클러스터를 추가한 후 클러스터(Astra Control 외부)에 앱을 설치한 다음 Astra Control의 애플리케이션 페이지로 이동하여 앱과 리소스를 정의할 수 있습니다. 을 참조하십시오 "Astra Control Center의 앱 관리 섹션을 시작합니다".

다음 단계는 데이터 보호 및 데이터 마이그레이션을 위한 Astra Control Center를 소스에서 타겟 클러스터로 마이그레이션하는 것입니다.

Astra를 사용한 데이터 보호

이 페이지에는 Astra Control Center(ACC)를 사용하여 VMware vSphere에서 실행되는 Red Hat OpenShift Container 기반 애플리케이션에 대한 데이터 보호 옵션이 나와 있습니다.

사용자가 Red Hat OpenShift를 사용하여 애플리케이션을 현대화하는 과정에서 실수로 인한 삭제나 기타 인적 오류로부터 애플리케이션을 보호하기 위한 데이터 보호 전략이 마련되어야 합니다. 규정 또는 규정 준수 목적으로도 데이터 마스터를 보호하기 위해 보호 전략이 필요한 경우가 많습니다.

데이터 보호 요구 사항은 사람의 개입 없이 시점 복사본으로 되돌려서 다른 장애 도메인으로 자동 페일오버하는 것에서부터 다릅니다. 많은 고객들이 멀티 테넌시, 멀티 프로토콜, 고성능 및 용량 제공 기능, 멀티 사이트 위치의 복제 및 캐싱, 보안, 유연성 등과 같은 다양한 기능 때문에 Kubernetes 애플리케이션을 위한 기본 스토리지 플랫폼으로 ONTAP를 선택하고 있습니다.

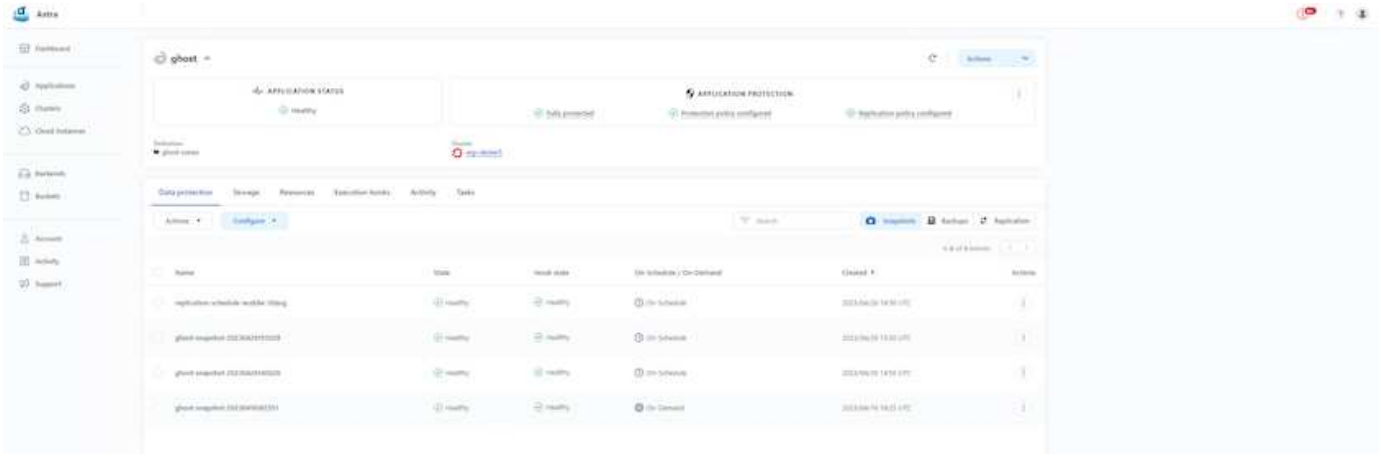
ONTAP의 데이터 보호는 임시 또는 정책 제어 - 스냅샷 - 백업 및 복원 을 사용하여 수행할 수 있습니다

Snapshot 복사본 및 백업은 다음 유형의 데이터를 보호합니다.- 응용 프로그램의 상태를 나타내는 응용 프로그램 메타데이터 - 응용 프로그램과 연결된 모든 영구 데이터 볼륨 - 응용 프로그램에 속하는 모든 리소스 아티팩트

ACC를 사용한 스냅샷

ACC의 Snapshot을 사용하여 데이터의 시점 복제본을 캡처할 수 있습니다. 보호 정책은 유지할 스냅샷 복사본 수를 정의합니다. 사용 가능한 최소 스케줄 옵션은 매시간 입니다. 수동 온디맨드 스냅샷 복사본은 예약된 스냅샷 복사본보다 언제든지 더 짧은 간격으로 생성할 수 있습니다. 스냅샷 복사본은 앱과 동일한 프로비저닝된 볼륨에 저장됩니다.

ACC로 스냅샷 구성

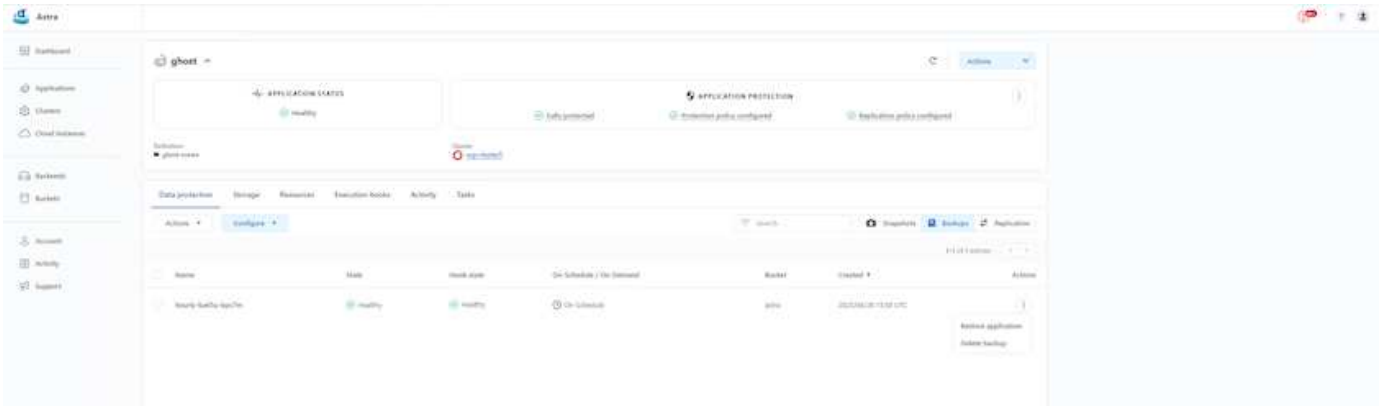


ACC를 사용한 백업 및 복구

백업은 스냅샷을 기반으로 합니다. ACC는 CSI를 사용하여 스냅샷 복사본을 생성하고 시점 스냅샷 복사본을 사용하여 백업을 수행할 수 있습니다. 백업은 외부 오브젝트 저장소(ONTAP S3를 비롯한 다른 위치의 호환 S3)에 저장됩니다. 예약된 백업과 유지할 백업 버전 수에 대해 보호 정책을 구성할 수 있습니다. 최소 RPO는 1시간입니다.

ACC를 사용하여 백업에서 애플리케이션 복구

ACC는 백업이 저장되는 S3 버킷에서 애플리케이션을 복구합니다.



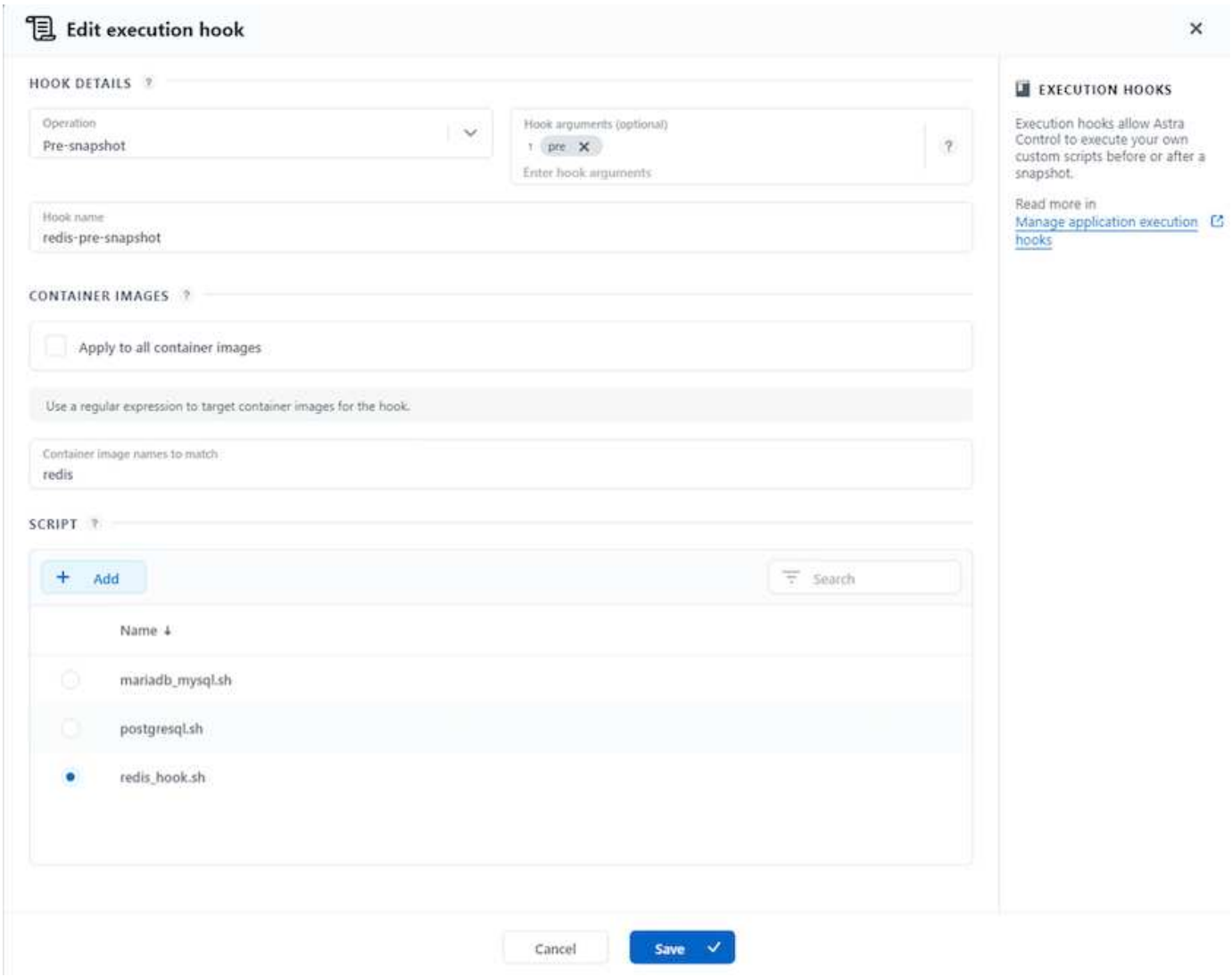
응용 프로그램별 실행 후크

또한 실행 후크는 관리되는 앱의 데이터 보호 작업과 함께 실행되도록 구성할 수 있습니다. 스토리지 시스템 레벨 데이터 보호 기능을 사용할 수 있지만 백업 및 복구를 수행하기 위해 추가 단계가 필요한 경우가 많으며, 애플리케이션 정합성이 보장됩니다. 앱별 추가 단계는 다음과 같습니다. - 스냅샷 복사본 생성 이전 또는 이후에 - 백업을 생성하기 전이나 후에 - 스냅샷 복사본 또는 백업에서 복원한 후

Astra Control은 실행 후크라고 하는 사용자 정의 스크립트로 코드화된 이러한 앱 관련 단계를 실행할 수 있습니다.

"NetApp Verda GitHub 프로젝트" 널리 사용되는 클라우드 네이티브 애플리케이션을 위한 실행 후크를 제공하여 애플리케이션을 간편하고, 강력하고, 쉽게 조정할 수 있도록 합니다. 리포지토리에 없는 응용 프로그램에 대한 충분한 정보가 있는 경우 해당 프로젝트에 자유롭게 참여할 수 있습니다.

redis 애플리케이션의 사전 스냅샷을 위한 샘플 실행 후크



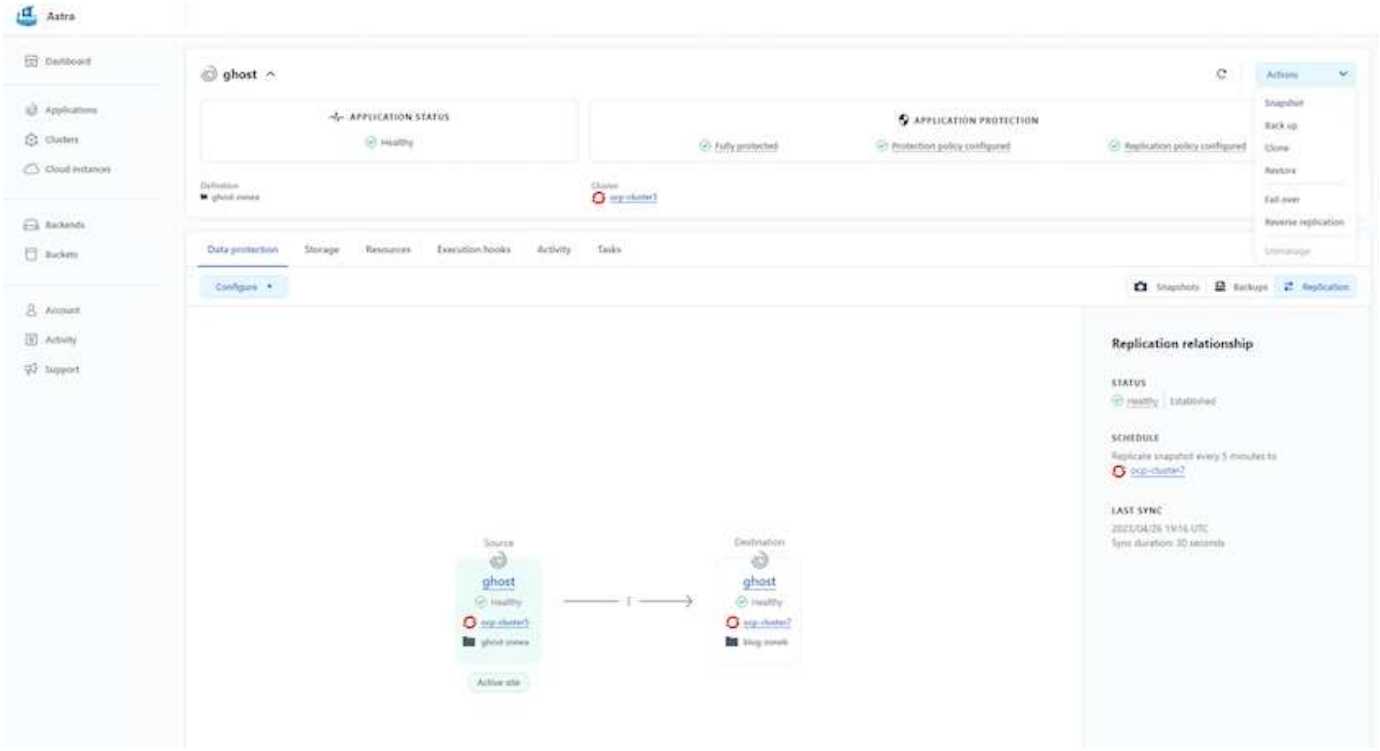
ACC를 통한 복제

지역 보호를 위해 또는 낮은 RPO 및 RTO 솔루션을 위해 애플리케이션을 다른 지역의 가급적이면 다른 지역에서 실행되는 다른 Kubernetes 인스턴스로 복제할 수 있습니다. ACC는 5분 이내에 ONTAP 비동기식 SnapMirror를 사용합니다. 복제는 ONTAP로 복제하여 수행되면 페일오버로 타겟 클러스터에 Kubernetes 리소스를 생성합니다.

복제는 백업이 S3로 수행되고 복원이 수행되는 백업 및 복원과 다릅니다. 두 가지 데이터 보호 유형 간의 차이점에 대한 자세한 내용은 here 참조하십시오.

을 참조하십시오 "여기" SnapMirror 설정 지침을 보려면

ACC가 장착된 **SnapMirror**



SAN 경제형 및 NAS 경제형 스토리지 드라이버는 복제 기능을 지원하지 않습니다. 을 참조하십시오 "여기" 를 참조하십시오.

데모 비디오:

"Astra Control Center를 사용한 재해 복구 데모 비디오"

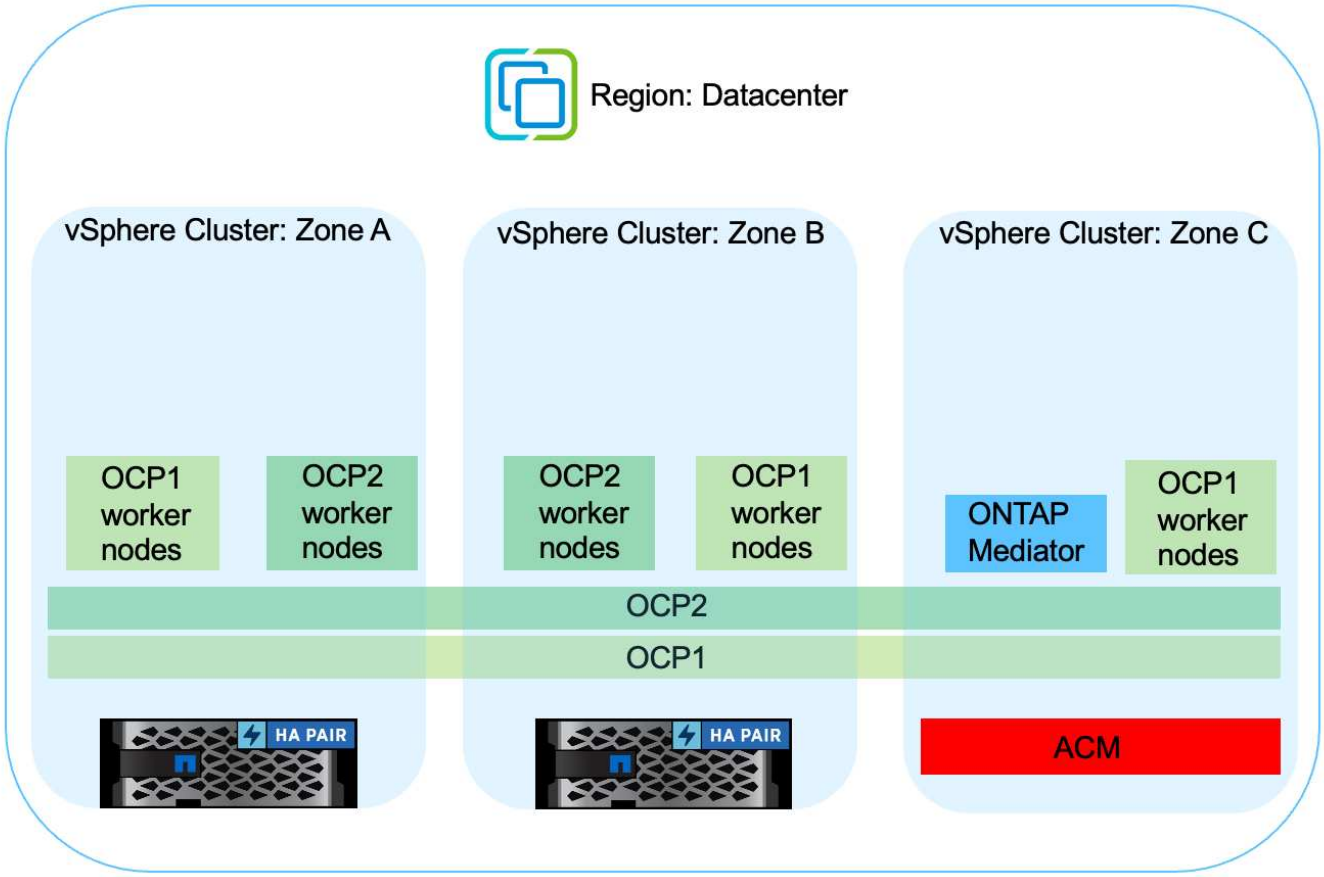
Astra Control Center를 통한 데이터 보호

MetroCluster를 통한 비즈니스 연속성

대부분의 ONTAP용 하드웨어 플랫폼에는 고가용성 기능이 있어 장치 장애로부터 보호하므로 DIaster 복구를 수행할 필요가 없습니다. 하지만 화재 또는 기타 재난으로부터 보호하고 RPO가 0이고 RTO가 낮은 비즈니스를 계속 운영하려면 MetroCluster 솔루션이 자주 사용됩니다.

현재 ONTAP 시스템을 사용 중인 고객은 영역 수준 재해 복구 기능을 제공하기 위해 거리 제한 내에서 지원되는 ONTAP 시스템을 추가하여 MetroCluster로 확장할 수 있습니다. Astra Trident, CSI(컨테이너 스토리지 인터페이스)는 MetroCluster 구성을 포함한 NetApp ONTAP와 Cloud Volumes ONTAP, Azure NetApp Files, AWS FSx for NetApp ONTAP 등의 기타 옵션을 지원합니다 Astra Trident는 ONTAP를 위한 5가지 스토리지 드라이버 옵션을 제공하며 모든 옵션이 MetroCluster 구성에 지원됩니다. 을 참조하십시오 "여기" Astra Trident에서 지원하는 ONTAP 스토리지 드라이버에 대한 자세한 내용은

MetroCluster 솔루션은 두 오류 도메인에서 동일한 네트워크 주소에 액세스하려면 계층 2 네트워크 확장 또는 기능이 필요합니다. MetroCluster 구성이 완료되면 MetroCluster svm의 모든 볼륨이 보호되고 SyncMirror(제로 RPO)의 이점을 얻을 수 있으므로 애플리케이션 소유자는 솔루션을 투명하게 사용할 수 있습니다.



Trident 백엔드 구성(TBC)의 경우 MetroCluster 구성을 사용할 때 데이터 LIF 및 SVM을 지정하지 마십시오. 관리 LIF에 SVM 관리 IP를 지정하고 vsadmin 역할 자격 증명을 사용합니다.

Astra Control Center 데이터 보호 기능에 대한 자세한 내용을 확인할 수 있습니다 "여기"

Astra Control Center를 사용한 데이터 마이그레이션

이 페이지에는 Astra Control Center(ACC)가 있는 Red Hat OpenShift 클러스터의 컨테이너 워크로드에 대한 데이터 마이그레이션 옵션이 나와 있습니다.

Kubernetes 애플리케이션은 한 환경에서 다른 환경으로 이동해야 하는 경우가 많습니다. 애플리케이션의 영구적 데이터와 함께 애플리케이션을 마이그레이션하려면 NetApp ACC를 활용할 수 있습니다.

서로 다른 **Kubernetes** 환경 간의 데이터 마이그레이션

ACC는 Google Anthos, Red Hat OpenShift, Tanzu Kubernetes Grid, Rancher Kubernetes Engine, Upstream Kubernetes, 등 자세한 내용은 을 참조하십시오 "여기".

한 클러스터에서 다른 클러스터로 애플리케이션을 마이그레이션하려면 ACC의 다음 기능 중 하나를 사용할 수 있습니다.

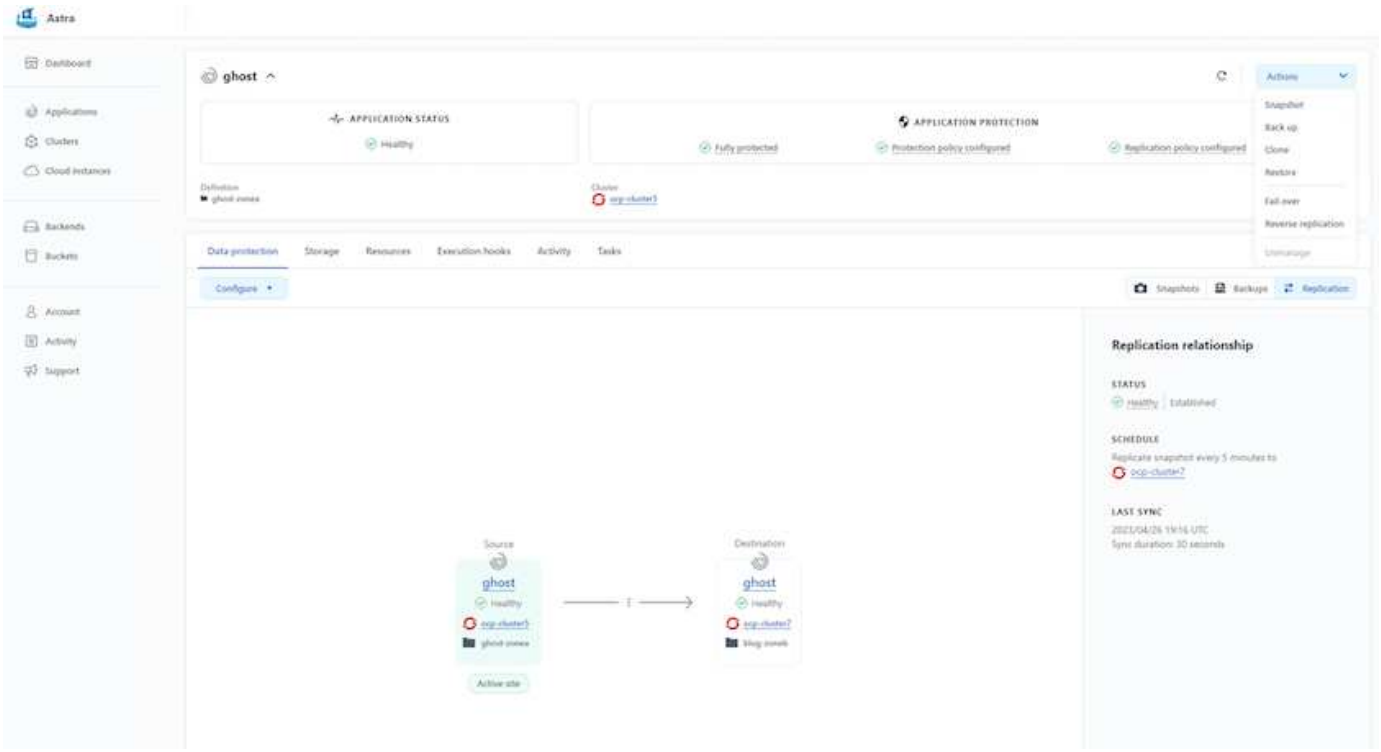
- 복제**
- 백업 및 복구
- 복제

을 참조하십시오 "데이터 보호 섹션을 참조하십시오" 복제 및 백업 및 복구** 옵션에 대해 설명합니다.

을 참조하십시오 "여기" 복제 에 대한 자세한 내용을 확인하십시오.

Astra Replication 기능은 Trident CSI(Container Storage Interface)에서만 지원됩니다. 그러나 NAS – 이코노미 및 SAN – 이코노미 동인은 복제를 지원하지 않습니다.

ACC를 사용하여 데이터 복제 수행



Red Hat OpenShift Container 워크로드를 위한 **NetApp** 하이브리드 멀티 클라우드 솔루션

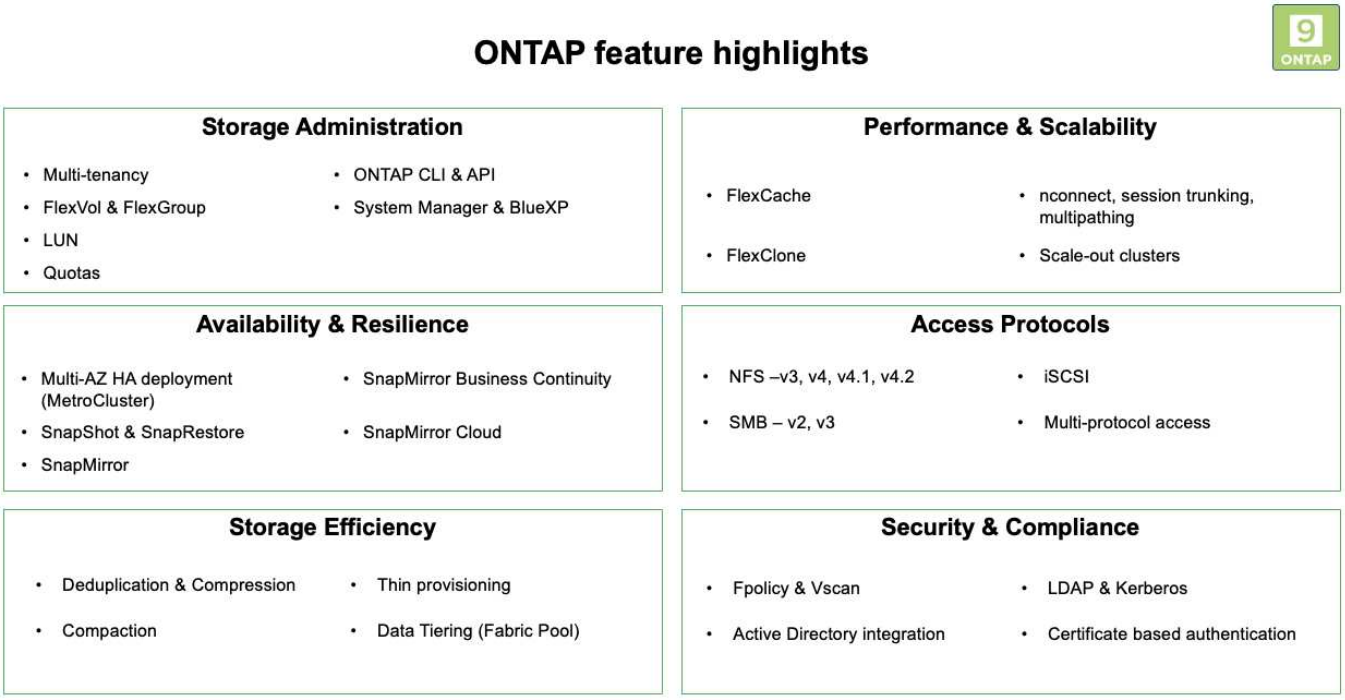
개요

NetApp은 기존 엔터프라이즈 애플리케이션을 현대화하고 Kubernetes를 기반으로 구축된 컨테이너 및 오케스트레이션 플랫폼을 사용하여 새로운 애플리케이션을 구축하는 고객이 크게 증가하고 있습니다. Red Hat OpenShift Container Platform은 많은 고객이 채택한 한 가지 예입니다.

점점 더 많은 고객이 기업 내에 컨테이너를 채택하기 시작함에 따라 NetApp은 상태 저장 애플리케이션의 영구 스토리지 요구사항과 데이터 보호, 데이터 보안, 데이터 마이그레이션과 같은 기존의 데이터 관리 요구사항을 충족할 수 있는 완벽한 위치를 선점하고 있습니다. 그러나 이러한 요구 사항은 서로 다른 전략, 도구 및 방법을 사용하여 충족됩니다.

- NetApp ONTAP** 아래에 나열된 스토리지 옵션을 사용하여 컨테이너 및 Kubernetes 구축을 위한 보안, 데이터 보호, 안정성 및 유연성을 확보할 수 있습니다.
  - 사내 자가 관리형 스토리지:
- NetApp 패브릭 연결 스토리지(FAS), NetApp All Flash FAS 어레이(AFF), NetApp All SAN 어레이(ASA) 및 ONTAP Select
  - 온프레미스에서 공급자 관리 스토리지:

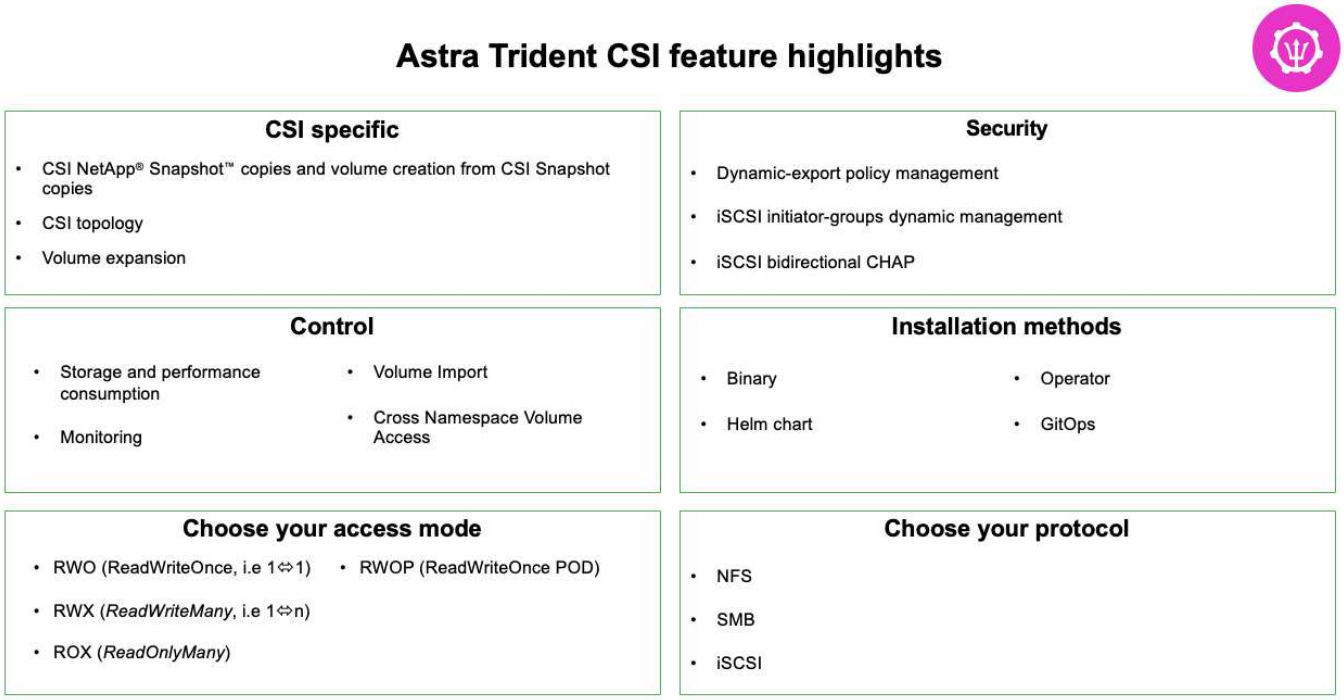
- NetApp Keystone, STaaS(서비스형 스토리지) 제공
  - 클라우드에서 자가 관리 스토리지:
- NetApp Cloud Volumes ONTAP(CVO)은 하이퍼스케일러에 자가 관리하는 스토리지를 제공합니다
  - 클라우드 내 공급자 관리 스토리지:
- Cloud Volumes Service for Google Cloud(CVS), Azure NetApp Files(ANF), Amazon FSx for NetApp ONTAP는 하이퍼스케일러에 완전 관리형 스토리지를 제공합니다



- NetApp BlueXP** - 단일 제어 플레인/인터페이스에서 모든 스토리지 및 데이터 자산을 관리할 수 있습니다.

BlueXP를 사용하여 클라우드 스토리지(예: Cloud Volumes ONTAP 및 Azure NetApp Files)를 생성 및 관리하고, 데이터를 이동, 보호 및 분석하며, 많은 사내 및 에지 스토리지 장치를 제어할 수 있습니다.

- NetApp Astra Trident**는 CSI 규정 준수 스토리지 오케스트레이터로서, 위에서 언급한 다양한 NetApp 스토리지 옵션을 통해 영구 스토리지를 빠르고 쉽게 사용할 수 있습니다. NetApp에서 관리 및 지원하는 오픈 소스 소프트웨어입니다.



비즈니스 크리티컬 컨테이너 워크로드에는 영구 볼륨 이상의 용량이 필요합니다. 이들의 데이터 관리 요구사항에 따라 애플리케이션 Kubernetes 객체의 보호 및 마이그레이션이 필요합니다.

애플리케이션 데이터에는 사용자 데이터 외에도 Kubernetes 객체가 포함됩니다. 몇 가지 예는 다음과 같습니다. POD 사양, PVC, 구축, 서비스 맞춤형 구성 개체(예: 구성 맵 및 암호), 스냅샷 복사본, 백업, CRS, CRD와 같은 클론 맞춤형 리소스 등의 영구 데이터)가 있습니다

- NetApp Astra Control**, 완전 관리형 및 자가 관리 소프트웨어로 모두 사용 가능하며, 강력한 애플리케이션 데이터 관리를 위한 오케스트레이션을 제공합니다. 을 참조하십시오 "Astra 문서" Astra 제품군에 대한 자세한 내용은

이 참조 문서는 NetApp Astra Control Center를 사용하여 RedHat OpenShift 컨테이너 플랫폼에 배포된 컨테이너 기반 애플리케이션의 마이그레이션 및 보호를 검증합니다. 또한 이 솔루션은 컨테이너 플랫폼 관리를 위한 Red Hat Advanced Cluster Management(ACM)의 배포 및 사용에 대한 자세한 정보를 제공합니다. 또한, Astra Trident CSI 프로비저닝을 사용하여 NetApp 스토리지를 Red Hat OpenShift 컨테이너 플랫폼과 통합하기 위한 세부 정보도 제공합니다. Astra Control Center는 허브 클러스터에 구축되며 컨테이너 애플리케이션 및 영구 스토리지 라이프사이클을 관리하는 데 사용됩니다. 마지막으로, NetApp FSx for NetApp ONTAP(FSxN)를 영구 스토리지로 사용하는 AWS(Rosa)의 관리되는 Red Hat OpenShift 클러스터에서 복제, 페일오버 및 컨테이너 워크로드에 대한 페일백용 솔루션을 제공합니다.

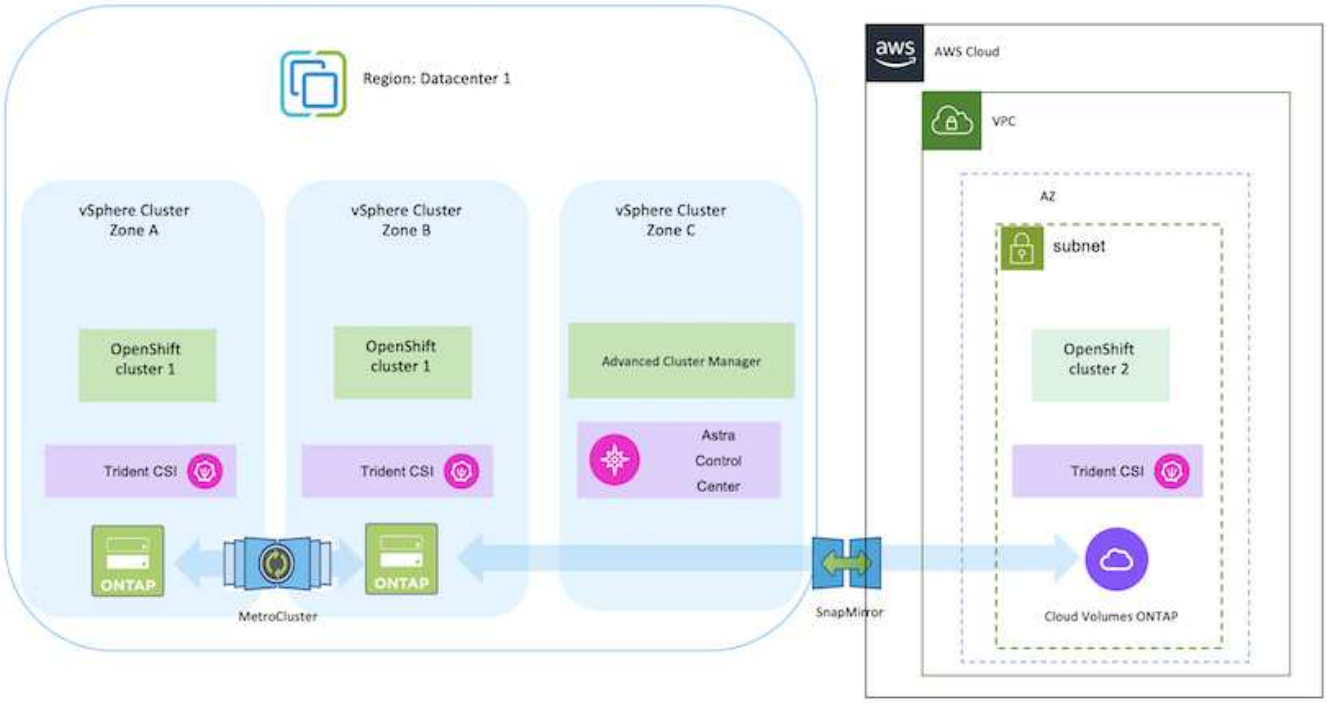
하이브리드 클라우드의 **Red Hat OpenShift Container** 플랫폼 워크로드를 지원하는 **NetApp** 솔루션

고객은 일부 특정 워크로드 또는 모든 워크로드를 데이터 센터에서 클라우드로 이동할 준비가 되었을 때 현대화 과정에서 한 시점에 있을 수 있습니다. 고객은 다양한 이유로 클라우드에서 자가 관리 OpenShift 컨테이너와 자가 관리 NetApp 스토리지를 사용할 수 있습니다. 컨테이너 워크로드를 데이터 센터에서 마이그레이션하기 위한 성공적인 프로덕션 준비 환경을 위해 클라우드에 Red Hat OpenShift Container Platform(OCP)을 계획하고 배포해야 합니다. OCP 클러스터는 데이터 센터의 VMware 또는 베어 메탈과 클라우드 환경의 AWS, Azure 또는 Google Cloud에 구축할 수 있습니다.

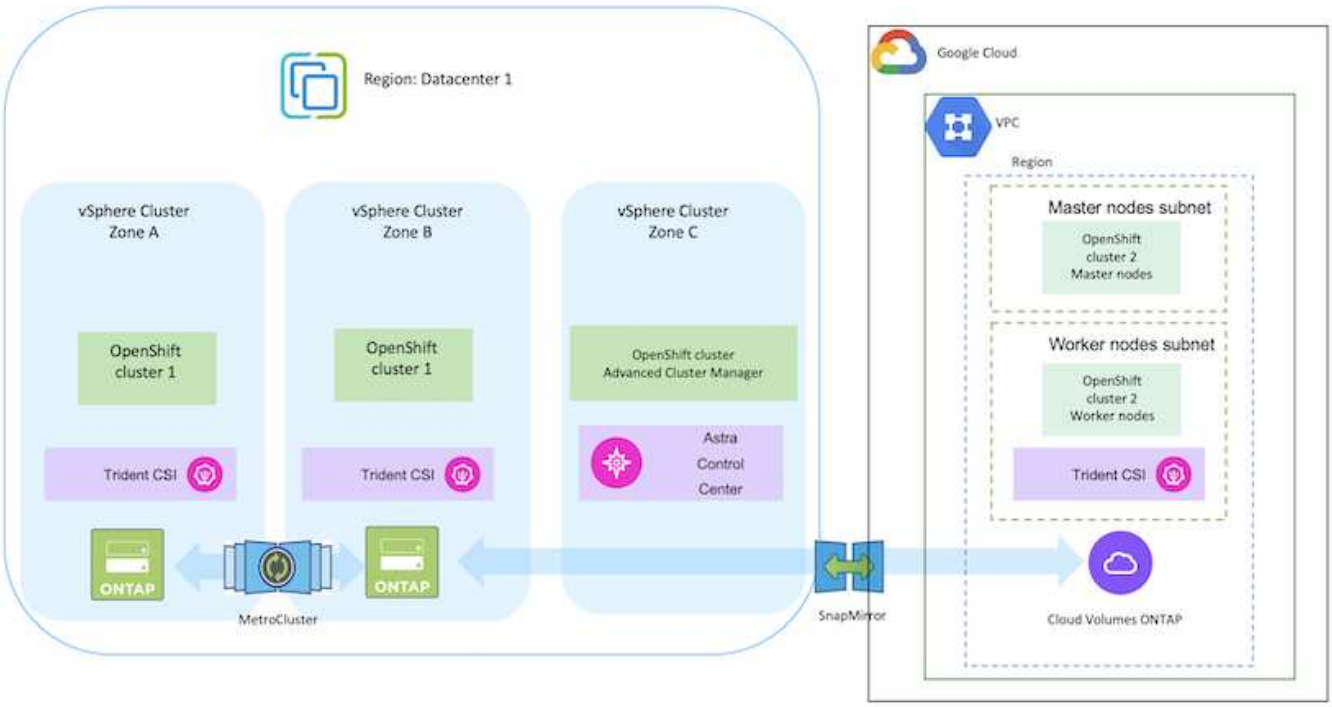
NetApp Cloud Volumes ONTAP 스토리지는 AWS, Azure 및 Google Cloud의 컨테이너 구축을 위한 데이터 보호, 안정성 및 유연성을 제공합니다. Astra Trident는 동적 스토리지 프로비저닝을 통해 고객의 상태 저장 애플리케이션에 영구 Cloud Volumes ONTAP 스토리지를 사용합니다. Astra Control Center는 데이터 보호, 마이그레이션, 비즈니스 연속성 등 상태 저장 애플리케이션의 다양한 데이터 관리 요구 사항을 조율하는 데 사용할 수 있습니다.

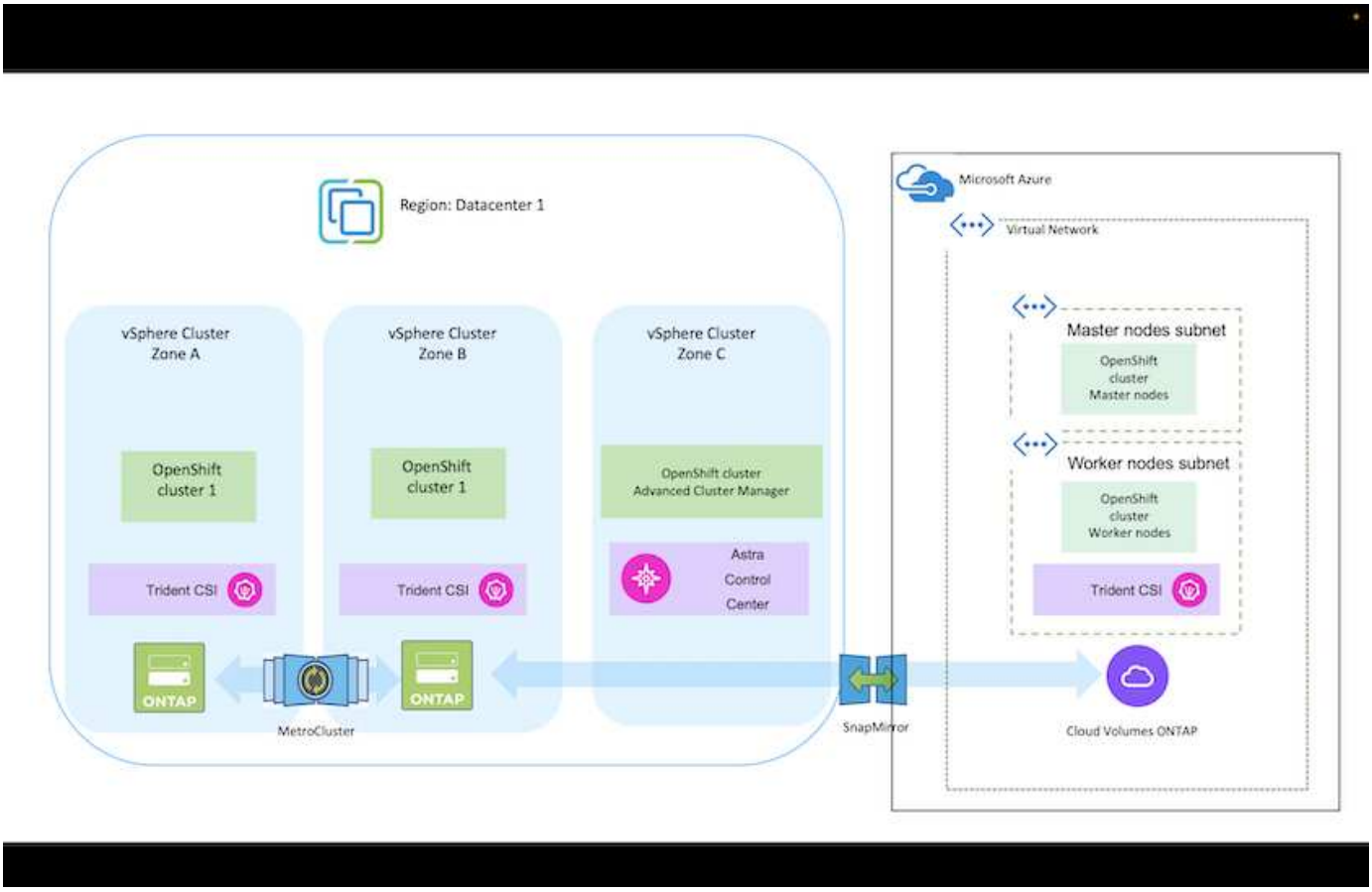
Astra Control Center를 사용하는 하이브리드 클라우드의 **OpenShift Container** 워크로드를 위한 데이터 보호 및 마이그레이션 솔루션

온프레미스 및 AWS



온프레미스 및 Google Cloud



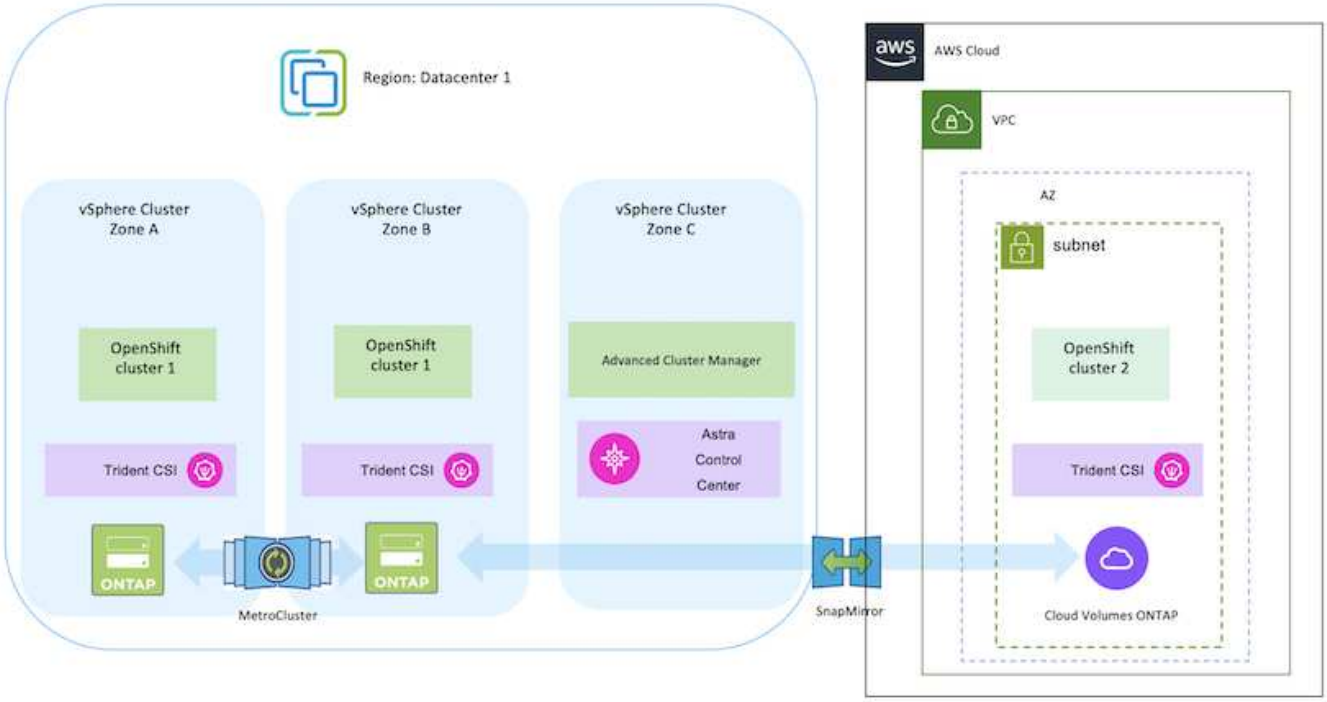


AWS에서 **Red Hat OpenShift Container** 플랫폼을 구축 및 구성합니다

이 섹션에서는 AWS에서 OpenShift 클러스터를 설정 및 관리하고 stateful 애플리케이션을 배포하는 방법에 대한 고급 워크플로우를 설명합니다. 또한, 영구 볼륨을 제공하는 Astra Trident의 도움을 받아 NetApp Cloud Volumes ONTAP 스토리지를 사용하는 모습을 보여 줍니다. 상태 저장 애플리케이션에 대한 데이터 보호 및 마이그레이션 작업을 수행하기 위해 Astra Control Center를 사용하는 방법에 대한 세부 정보가 제공됩니다.

AWS에서 Red Hat OpenShift Container 플랫폼 클러스터를 배포하는 방법은 여러 가지가 있습니다. 설정에 대한 이 고급 설명은 사용된 특정 방법에 대한 설명서 링크를 제공합니다. 에 제공된 관련 링크에서 다른 방법을 참조할 수 있습니다 "리소스 섹션을 참조하십시오".

이 다이어그램은 AWS에 구축되고 VPN을 사용하여 데이터 센터에 연결된 클러스터를 보여 줍니다.



설치 프로세스는 다음 단계로 나눌 수 있습니다.

고급 클러스터 관리 에서 **AWS**에 **OCP** 클러스터를 설치합니다**.**

- pfSense를 사용하여 사이트 간 VPN 연결을 통해 VPC를 생성하여 온-프레미스 네트워크에 연결합니다.
- 온-프레미스 네트워크에는 인터넷 연결이 있습니다.
- 3개의 다른 AZs에 3개의 개인 서브넷을 생성합니다.
- VPC용 Route 53 전용 호스팅 영역 및 DNS 리졸버를 생성합니다.

ACM(Advanced Cluster Management) 마법사에서 AWS에서 OpenShift Cluster를 생성합니다. 지침을 참조하십시오 "여기".

OpenShift 하이브리드 클라우드 콘솔에서 AWS에서 클러스터를 생성할 수도 있습니다. 을 참조하십시오 "여기" 를 참조하십시오.

ACM을 사용하여 클러스터를 생성할 때 양식 보기에서 세부 정보를 입력한 후 YAML 파일을 편집하여 설치를 사용자 지정할 수 있습니다. 클러스터를 생성한 후 문제 해결 또는 추가 수동 구성을 위해 ssh를 통해 클러스터 노드에 로그인할 수 있습니다. 설치 중에 제공한 ssh 키와 사용자 이름 코어를 사용하여 로그인합니다.

BlueXP를 사용하여 **AWS**에 **Cloud Volumes ONTAP**를 구축합니다.

- 사내 VMware 환경에 커넥터를 설치합니다. 지침을 참조하십시오 "여기".
- 커넥터를 사용하여 AWS에 CVO 인스턴스를 구축합니다. 지침을 참조하십시오 "여기".

커넥터는 클라우드 환경에도 설치할 수 있습니다. 을 참조하십시오 "여기" 자세한 내용은 를 참조하십시오.

OCP 클러스터에 **Astra Trident**를 설치합니다

- Hrom을 사용하여 Trident 연산자 배포 지침을 참조하십시오 "여기"
- 백엔드 및 스토리지 클래스를 생성합니다. 지침을 참조하십시오 "여기".

AWS의 **OCP** 클러스터를 **Astra Control Center**에 추가합니다.

AWS의 OCP 클러스터를 Astra Control Center에 추가합니다.

멀티 존 아키텍처용 **Trident**의 **CSI** 토폴로지 기능 사용

현재 클라우드 공급자는 Kubernetes/OpenShift 클러스터 관리자가 영역 기반 클러스터의 노드를 생성할 수 있도록 지원합니다. 노드는 지역 내 또는 여러 지역의 여러 가용성 영역에 위치할 수 있습니다. Astra Trident는 다중 영역 아키텍처에서 워크로드용 볼륨 프로비저닝을 지원하기 위해 CSI 토폴로지를 사용합니다. CSI 토폴로지 기능을 사용하면 지역 및 가용성 영역에 따라 볼륨에 대한 액세스가 노드의 하위 집합으로 제한될 수 있습니다. 을 참조하십시오 "여기" 를 참조하십시오.

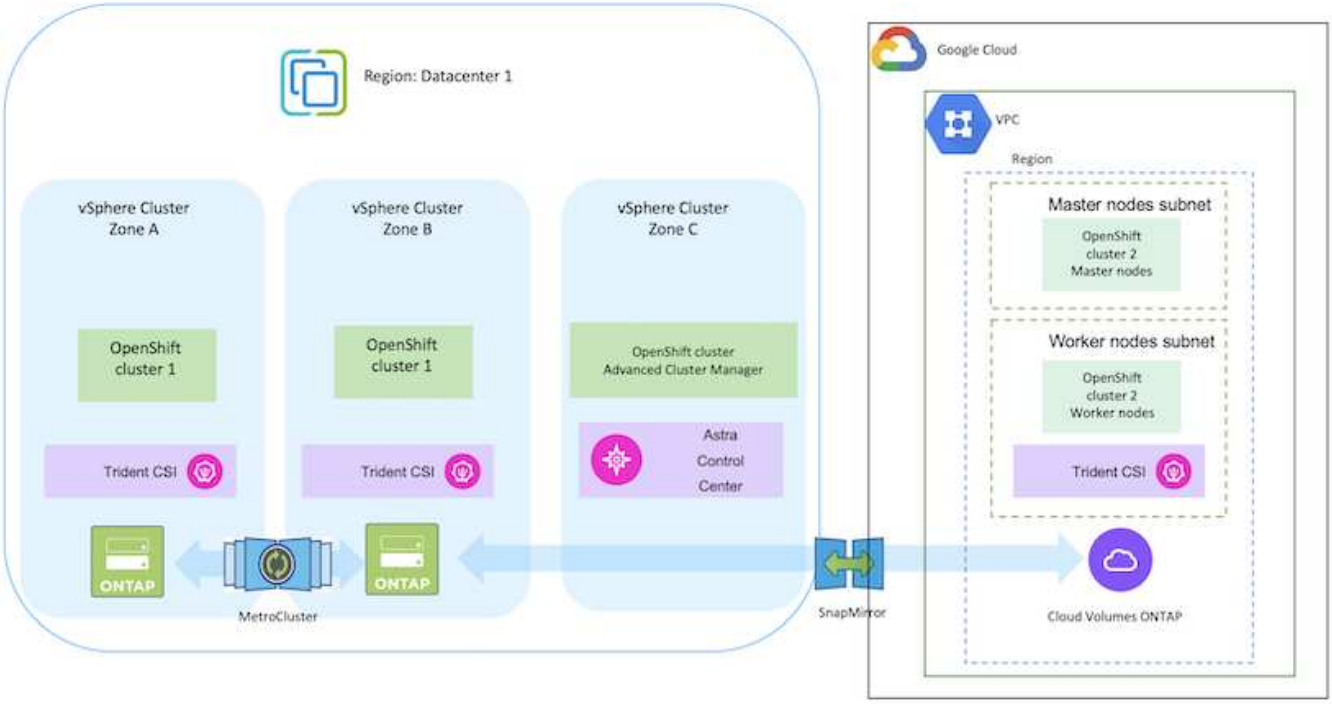
Kubernetes는 두 가지 볼륨 바인딩 모드를 지원합니다. -***VolumeBindingMode***_가 ***_immediate*** (기본값)로 설정되어 있으면 Astra Trident가 토폴로지 인식 없이 볼륨을 생성합니다. 영구 볼륨은 요청 포드의 예약 요구 사항에 의존하지 않고 생성됩니다. -***VolumeBindingMode_set to_WaitForFirstConsumer*** 경우 PVC를 사용하는 POD가 예약 및 생성될 때까지 PVC에 대한 영구 볼륨의 생성 및 바인딩이 지연됩니다. 이렇게 하면 토폴로지 요구 사항에 따라 적용되는 일정 제한을 충족하기 위해 볼륨이 생성됩니다. Astra Trident 스토리지 백엔드는 가용성 영역(토폴로지 인식 백엔드)을 기반으로 볼륨을 선택적으로 프로비저닝하도록 설계할 수 있습니다. 이러한 백엔드를 사용하는 StorageClasses의 경우 지원되는 영역/영역에서 예약된 애플리케이션에서 요청하는 경우에만 볼륨이 생성됩니다. (Topology-Aware StorageClass) 를 참조하십시오 "여기" 를 참조하십시오.

GCP에서 **Red Hat OpenShift Container** 플랫폼을 구축하고 구성합니다

GCP에서 **Red Hat OpenShift Container** 플랫폼을 구축하고 구성합니다

이 섹션에서는 GCP에서 OpenShift 클러스터를 설정 및 관리하고 이러한 클러스터에 상태 저장 애플리케이션을 배포하는 방법에 대한 고급 워크플로우를 설명합니다. 또한, 영구 볼륨을 제공하는 Astra Trident의 도움을 받아 NetApp Cloud Volumes ONTAP 스토리지를 사용하는 모습을 보여 줍니다. 상태 저장 애플리케이션에 대한 데이터 보호 및 마이그레이션 작업을 수행하기 위해 Astra Control Center를 사용하는 방법에 대한 세부 정보가 제공됩니다.

다음은 GCP에 구축되고 VPN을 사용하여 데이터 센터에 연결된 클러스터를 보여 주는 다이어그램입니다.



GCP에서 Red Hat OpenShift Container Platform 클러스터를 배포하는 방법에는 여러 가지가 있습니다. 설정에 대한 이 고급 설명은 사용된 특정 방법에 대한 설명서 링크를 제공합니다. 에 제공된 관련 링크에서 다른 방법을 참조할 수 있습니다 "리소스 섹션을 참조하십시오".

설치 프로세스는 다음 단계로 나눌 수 있습니다.

CLI에서 **GCP**에 **OCP** 클러스터를 설치합니다**.**

- 명시된 모든 사전 요구 사항을 충족했는지 확인합니다 "여기".
- 온프레미스와 GCP 간 VPN 연결을 위해 pfSense VM을 생성 및 구성했습니다. 자세한 내용은 을 참조하십시오 "여기".
  - pfSense의 원격 게이트웨이 주소는 Google Cloud Platform에서 VPN 게이트웨이를 생성한 후에만 구성할 수 있습니다.
  - 2단계의 원격 네트워크 IP 주소는 OpenShift 클러스터 설치 프로그램이 실행되고 클러스터의 인프라 구성 요소를 생성한 후에만 구성할 수 있습니다.
  - Google Cloud의 VPN은 설치 프로그램에서 클러스터의 인프라 구성 요소를 생성한 후에만 구성할 수 있습니다.
- 이제 GCP에 OpenShift 클러스터를 설치합니다.
  - 설치 프로그램 및 풀 암호를 확인하고 설명서에 제공된 단계에 따라 클러스터를 구축합니다 "여기".
  - 설치 시 Google Cloud Platform에 VPC 네트워크가 생성됩니다. 또한 Cloud DNS에서 개인 영역을 만들고 레코드를 추가합니다.
    - VPC 네트워크의 CIDR 블록 주소를 사용하여 pfSense를 구성하고 VPN 연결을 설정합니다. 방화벽이 올바르게 설정되었는지 확인합니다.
    - Google Cloud DNS의 A 레코드에 있는 IP 주소를 사용하여 온-프레미스 환경의 DNS에 레코드를 추가합니다.
  - 클러스터 설치가 완료되고 kubeconfig 파일과 사용자 이름 및 암호를 제공하여 클러스터의 콘솔에 로그인합니다.

BlueXP를 사용하여 **GCP**에 **Cloud Volumes ONTAP**을 구축합니다**.**

- Google Cloud에 커넥터를 설치합니다. 지침을 참조하십시오 "여기".
- 커넥터를 사용하여 Google Cloud에 CVO 인스턴스를 배포합니다. 여기 에서 지침을 참조하십시오. https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html

GCP의 **OCP** 클러스터에 **Astra Trident**를 설치합니다

- 그림과 같이 Astra Trident를 구축하는 방법은 여러 가지가 있습니다 "여기".
- 이 프로젝트의 경우 지침에 따라 Astra Trident Operator를 수동으로 구축하여 Astra Trident를 설치했습니다 "여기".
- 백엔드 및 스토리지 클래스를 생성합니다. 지침을 참조하십시오 "여기".

GCP의 **OCP** 클러스터를 **Astra Control Center**에 추가합니다**.**

- Astra Control에서 관리하는 클러스터를 관리하는 데 필요한 최소 권한이 포함된 클러스터 역할을 사용하여 별도의 KubeConfig 파일을 생성합니다. 지침을 찾을 수 있습니다 "여기".
- 지침에 따라 Astra Control Center에 클러스터를 추가합니다 "여기"

멀티 존 아키텍처용 **Trident**의 **CSI** 토폴로지 기능 사용

현재 클라우드 공급자는 Kubernetes/OpenShift 클러스터 관리자가 영역 기반 클러스터의 노드를 생성할 수 있도록 지원합니다. 노드는 지역 내 또는 여러 지역의 여러 가용성 영역에 위치할 수 있습니다. Astra Trident는 다중 영역 아키텍처에서 워크로드용 볼륨 프로비저닝을 지원하기 위해 CSI 토폴로지를 사용합니다. CSI 토폴로지 기능을 사용하면 지역 및 가용성 영역에 따라 볼륨에 대한 액세스가 노드의 하위 집합으로 제한될 수 있습니다. 을 참조하십시오 "여기" 를 참조하십시오.

Kubernetes는 두 가지 볼륨 바인딩 모드를 지원합니다. -***VolumeBindingMode***_가 ***_immediate*** (기본값)로 설정되어 있으면 Astra Trident가 토폴로지 인식 없이 볼륨을 생성합니다. 영구 볼륨은 요청 포드의 예약 요구 사항에 의존하지 않고 생성됩니다. -***VolumeBindingMode_set to_WaitForFirstConsumer*** 경우 PVC를 사용하는 POD가 예약 및 생성될 때까지 PVC에 대한 영구 볼륨의 생성 및 바인딩이 지연됩니다. 이렇게 하면 토폴로지 요구 사항에 따라 적용되는 일정 제한을 충족하기 위해 볼륨이 생성됩니다. Astra Trident 스토리지 백엔드는 가용성 영역(토폴로지 인식 백엔드)을 기반으로 볼륨을 선택적으로 프로비저닝하도록 설계할 수 있습니다. 이러한 백엔드를 사용하는 StorageClasses의 경우 지원되는 영역/영역에서 예약된 애플리케이션에서 요청하는 경우에만 볼륨이 생성됩니다. (Topology-Aware StorageClass) 를 참조하십시오 "여기" 를 참조하십시오.

[밑줄]# * 데모 비디오 * #

Google Cloud Platform에 OpenShift Cluster 설치

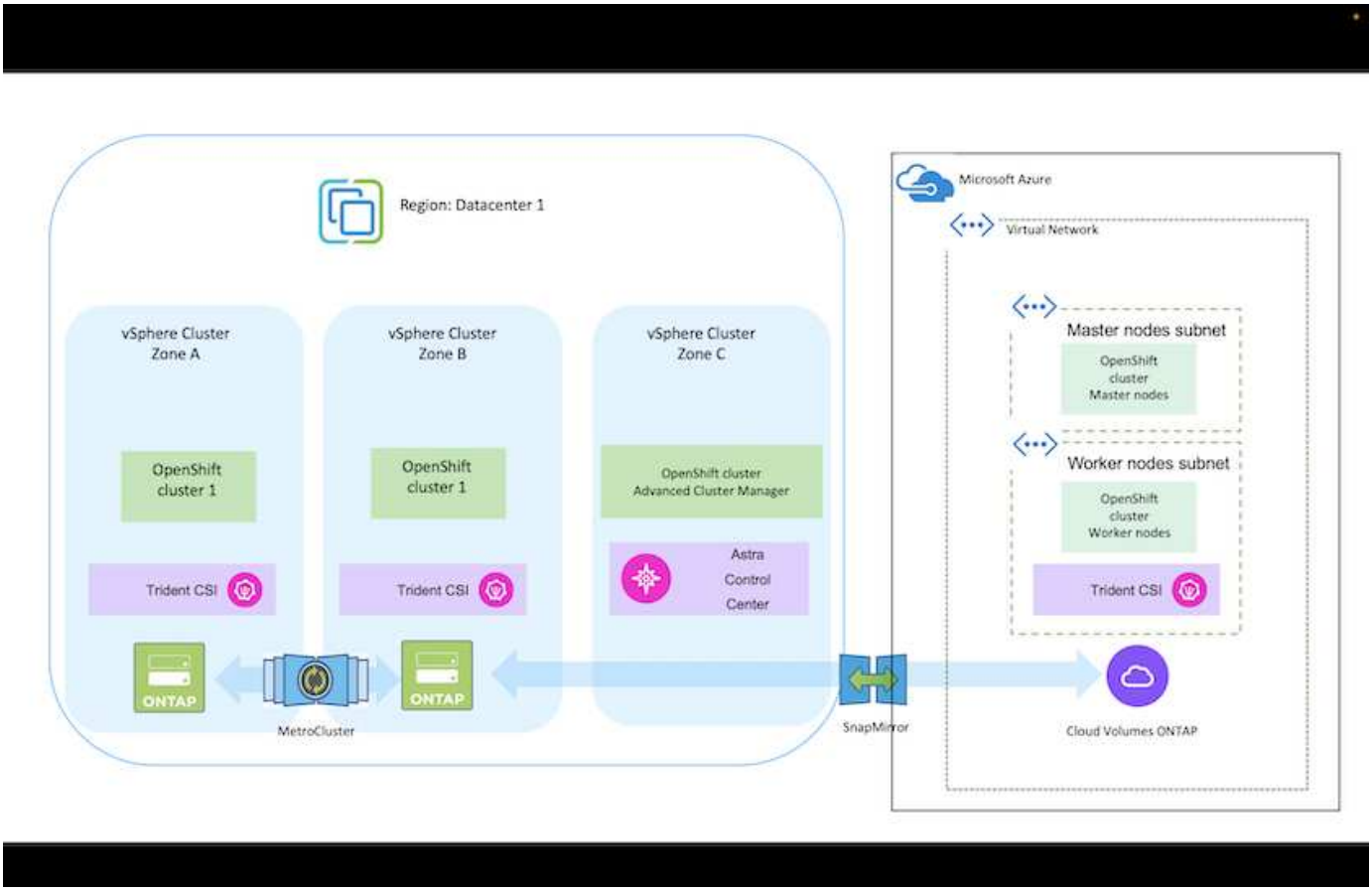
OpenShift 클러스터를 Astra Control Center로 가져오기

Azure에서 **Red Hat OpenShift Container** 플랫폼을 배포 및 구성합니다

Azure에서 **Red Hat OpenShift Container** 플랫폼을 배포 및 구성합니다

이 섹션에서는 Azure에서 OpenShift 클러스터를 설정 및 관리하고 이러한 클러스터에 상태 저장 애플리케이션을 배포하는 방법에 대한 고급 워크플로를 설명합니다. 이 게시판에서는 Astra Trident/Astra Control Provisioner를 통해 NetApp Cloud Volumes ONTAP 스토리지를 사용하여 영구 볼륨을 제공하는 것을 보여 줍니다. 상태 저장 애플리케이션에 대한 데이터 보호 및 마이그레이션 작업을 수행하기 위해 Astra Control Center를 사용하는 방법에 대한 세부 정보가 제공됩니다.

다음은 Azure에 배포되고 VPN을 사용하여 데이터 센터에 연결된 클러스터를 보여 주는 다이어그램입니다.



Azure에서 Red Hat OpenShift Container Platform 클러스터를 배포하는 방법에는 여러 가지가 있습니다. 설정에 대한 이 고급 설명은 사용된 특정 방법에 대한 설명서 링크를 제공합니다. 에 제공된 관련 링크에서 다른 방법을 참조할 수 있습니다 "리소스 섹션을 참조하십시오".

설치 프로세스는 다음 단계로 나눌 수 있습니다.

CLI에서 **Azure**에 **OCP** 클러스터를 설치합니다.

- 명시된 모든 사전 요구 사항을 충족했는지 확인합니다 "여기".
- VPN, 서브넷 및 네트워크 보안 그룹과 개인 DNS 영역을 만듭니다. VPN 게이트웨이 및 사이트 간 VPN 연결을 만듭니다.
- 온프레미스와 Azure 간 VPN 연결을 위해 pfSense VM을 생성 및 구성했습니다. 자세한 내용은 을 참조하십시오 "여기".
- 설치 프로그램 및 풀 암호를 확인하고 설명서에 제공된 단계에 따라 클러스터를 구축합니다 "여기".
- 클러스터 설치가 완료되고 kubeconfig 파일과 사용자 이름 및 암호를 제공하여 클러스터의 콘솔에 로그인합니다.

다음은 install-config.yaml 파일의 예입니다.

```
apiVersion: v1
baseDomain: sddc.netapp.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
      type: Standard_D2s_v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
      type: Standard_D8s_v3
      ultraSSDCapability: Disabled
  replicas: 3
```

```
metadata:
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
        diskType: "StandardSSD_LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:
```

BlueXP를 사용하여 **Azure**에서 **Cloud Volumes ONTAP**를 구축하십시오.

- Azure에서 커넥터를 설치합니다. 지침을 참조하십시오 "여기".
- 커넥터를 사용하여 Azure에서 CVO 인스턴스를 배포합니다. 지침 링크: https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html [여기]를 참조하십시오.

Azure의 **OCP** 클러스터에 **Astra Control Provisioner**를 설치합니다

- 이 프로젝트를 위해 Astra Control Provisioner(ACP)가 모든 클러스터(Astra Control Center가 구축된 온프레미스 클러스터 및 Azure의 클러스터)에 설치되었습니다. Astra Control Provisioner에 대해 자세히 알아보십시오 "여기".
- 백엔드 및 스토리지 클래스를 생성합니다. 지침을 참조하십시오 "여기".

Azure의 **OCP** 클러스터를 **Astra Control Center**에 추가합니다.

- Astra Control에서 관리하는 클러스터를 관리하는 데 필요한 최소 권한이 포함된 클러스터 역할을 사용하여 별도의 KubeConfig 파일을 생성합니다. 지침을 찾을 수 있습니다 "여기".
- 지침에 따라 Astra Control Center에 클러스터를 추가합니다 "여기"

멀티 존 아키텍처용 **Trident**의 **CSI** 토폴로지 기능 사용

현재 클라우드 공급자는 Kubernetes/OpenShift 클러스터 관리자가 영역 기반 클러스터의 노드를 생성할 수 있도록 지원합니다. 노드는 지역 내 또는 여러 지역의 여러 가용성 영역에 위치할 수 있습니다. Astra Trident는 다중 영역 아키텍처에서 워크로드용 볼륨 프로비저닝을 지원하기 위해 CSI 토폴로지를 사용합니다. CSI 토폴로지 기능을 사용하면 지역 및 가용성 영역에 따라 볼륨에 대한 액세스가 노드의 하위 집합으로 제한될 수 있습니다. 을 참조하십시오 "여기" 를 참조하십시오.

Kubernetes는 두 가지 볼륨 바인딩 모드를 지원합니다. -***VolumeBindingMode***_가 ***_immediate*** (기본값)로 설정되어 있으면 Astra Trident가 토폴로지 인식 없이 볼륨을 생성합니다. 영구 볼륨은 요청 포드의 예약 요구 사항에 의존하지 않고 생성됩니다. -***VolumeBindingMode_set to_WaitForFirstConsumer*** 경우 PVC를 사용하는 POD가 예약 및 생성될 때까지 PVC에 대한 영구 볼륨의 생성 및 바인딩이 지연됩니다. 이렇게 하면 토폴로지 요구 사항에 따라 적용되는 일정 제한을 충족하기 위해 볼륨이 생성됩니다. Astra Trident 스토리지 백엔드는 가용성 영역(토폴로지 인식 백엔드)을 기반으로 볼륨을 선택적으로 프로비저닝하도록 설계할 수 있습니다. 이러한 백엔드를 사용하는 StorageClasses의 경우 지원되는 영역/영역에서 예약된 애플리케이션에서 요청하는 경우에만 볼륨이 생성됩니다. (Topology-Aware StorageClass) 를 참조하십시오 "여기" 를 참조하십시오.

[밑줄]# * 데모 비디오 * #

애플리케이션 장애 조치 및 장애 복구를 위해 Astra Control을 사용합니다

Astra Control Center를 사용하여 데이터를 보호합니다

이 페이지에는 VMware vSphere 또는 ACC(Astra Control Center)를 사용하는 클라우드에서 실행되는 Red Hat OpenShift Container 기반 애플리케이션에 대한 데이터 보호 옵션이 나와 있습니다.

사용자가 Red Hat OpenShift를 사용하여 애플리케이션을 현대화하는 과정에서 실수로 인한 삭제나 기타 인적 오류로부터 애플리케이션을 보호하기 위한 데이터 보호 전략이 마련되어야 합니다. 규정 또는 규정 준수 목적으로도 데이터 마스터를 보호하기 위해 보호 전략이 필요한 경우가 많습니다.

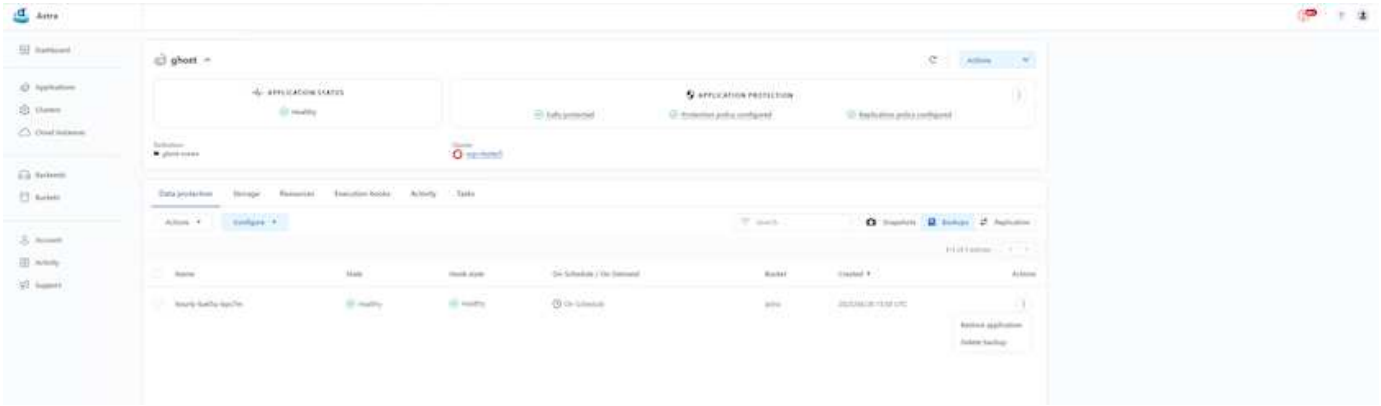
데이터 보호 요구 사항은 사람의 개입 없이 시점 복사본으로 되돌려서 다른 장애 도메인으로 자동 페일오버하는 것에서부터 다릅니다. 많은 고객들이 멀티 테넌시, 멀티 프로토콜, 고성능 및 용량 제공 기능, 멀티 사이트 위치의 복제 및 캐싱, 보안, 유연성 등과 같은 다양한 기능 때문에 Kubernetes 애플리케이션을 위한 기본 스토리지 플랫폼으로 ONTAP를 선택하고 있습니다.

고객은 클라우드 환경을 데이터 센터로 확장할 수 있으므로 클라우드의 이점을 활용하고 나중에 워크로드를 이동할 수 있습니다. 이러한 고객은 OpenShift 애플리케이션과 데이터를 클라우드 환경으로 백업하는 것이 불가피한 선택이라고 할 수 있습니다. 그런 다음 애플리케이션과 관련 데이터를 클라우드의 OpenShift 클러스터나 데이터 센터에 복원할 수 있습니다.

ACC를 사용한 백업 및 복구

애플리케이션 소유자는 ACC에서 검색된 응용 프로그램을 검토하고 업데이트할 수 있습니다. ACC는 CSI를 사용하여 스냅샷 복사본을 생성하고 시점 스냅샷 복사본을 사용하여 백업을 수행할 수 있습니다. 백업 대상은 클라우드 환경에서 오브젝트 저장소로 사용할 수 있습니다. 예약된 백업과 유지할 백업 버전 수에 대해 보호 정책을 구성할 수 있습니다. 최소 RPO는 1시간입니다.

ACC를 사용하여 백업에서 애플리케이션 복구

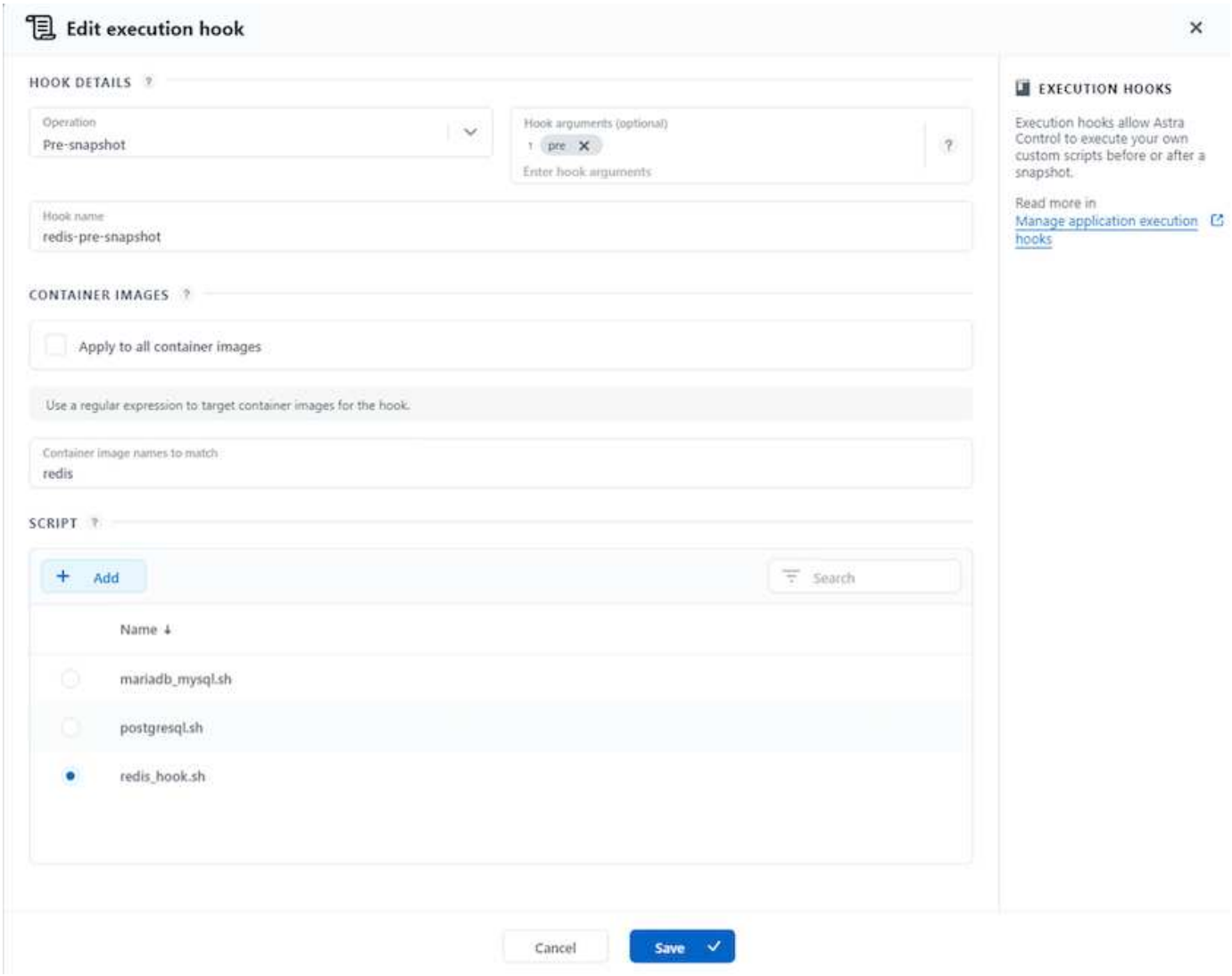


응용 프로그램별 실행 후크

스토리지 레벨 데이터 보호 기능을 사용할 수 있지만 백업 및 복구 애플리케이션의 정합성을 유지하기 위해 추가 단계가 필요한 경우가 많습니다. 앱별 추가 단계는 다음과 같습니다. - 스냅샷 복사본 생성 이전 또는 이후에 - 백업을 생성하기 전이나 후에 - 스냅샷 복사본 또는 백업에서 복원한 후 Astra Control은 실행 후크라고 하는 사용자 정의 스크립트로 코드화된 이러한 앱 관련 단계를 실행할 수 있습니다.

NetApp의 "오픈 소스 프로젝트 Verda" 널리 사용되는 클라우드 네이티브 애플리케이션을 위한 실행 후크를 제공하여 애플리케이션을 간편하고, 강력하고, 쉽게 조정할 수 있도록 합니다. 리포지토리에 없는 응용 프로그램에 대한 충분한 정보가 있는 경우 해당 프로젝트에 자유롭게 참여할 수 있습니다.

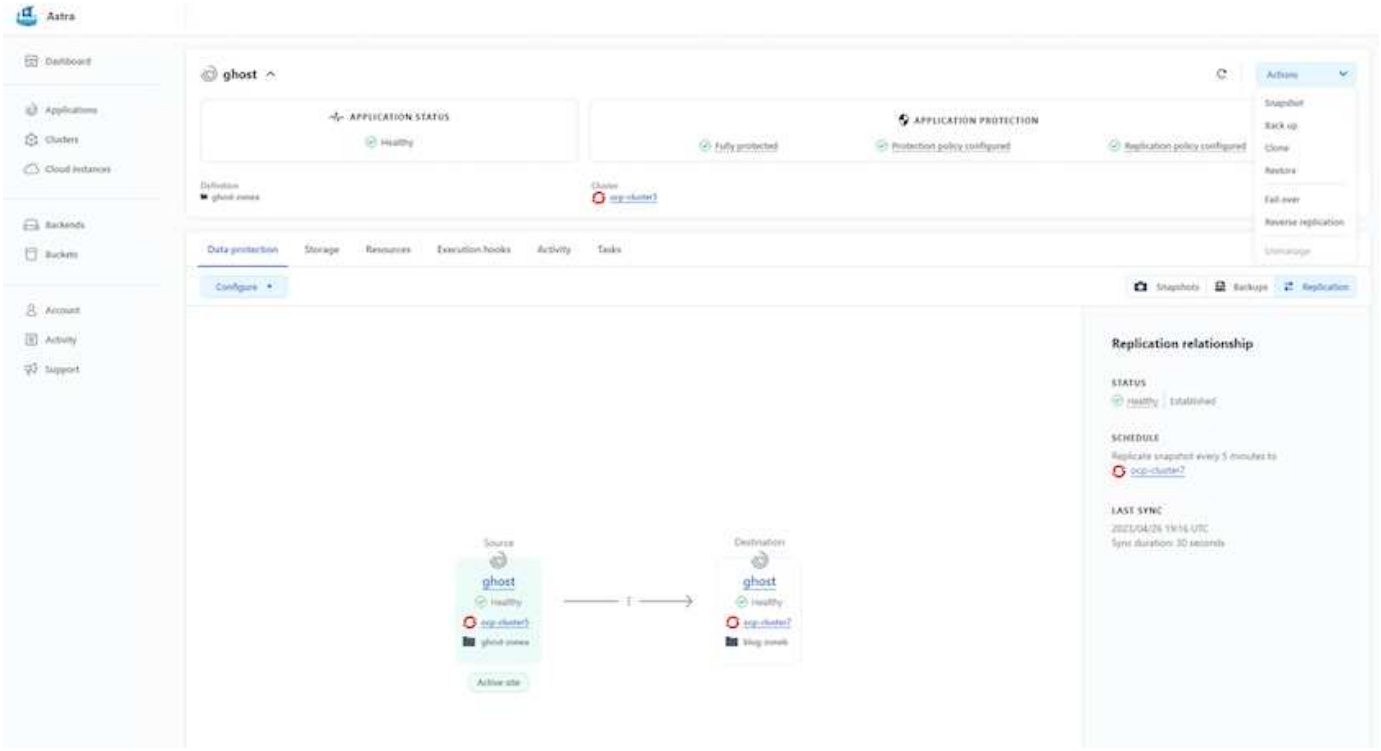
redis 애플리케이션의 사전 스냅샷을 위한 샘플 실행 후크



ACC를 통한 복제

지역 보호를 위해 또는 낮은 RPO 및 RTO 솔루션을 위해 애플리케이션을 다른 지역의 가급적이면 다른 지역에서 실행되는 다른 Kubernetes 인스턴스로 복제할 수 있습니다. ACC는 5분 이내에 ONTAP 비동기식 SnapMirror를 사용합니다. 을 참조하십시오 "여기" SnapMirror 설정 지침을 보려면

ACC가 장착된 **SnapMirror**



SAN 경제형 및 NAS 경제형 스토리지 드라이버는 복제 기능을 지원하지 않습니다. 을 참조하십시오 "여기" 를 참조하십시오.

데모 비디오:

"Astra Control Center를 사용한 재해 복구 데모 비디오"

Astra Control Center를 통한 데이터 보호

Astra Control Center 데이터 보호 기능에 대한 자세한 내용을 확인할 수 있습니다 "여기"

ACC를 사용한 재해 복구(복제를 사용한 페일오버 및 페일백

애플리케이션 장애 조치 및 장애 복구를 위해 Astra Control을 사용합니다

Astra Control Center를 사용한 데이터 마이그레이션

이 페이지에는 Astra Control Center(ACC)가 있는 Red Hat OpenShift 클러스터의 컨테이너 워크로드에 대한 데이터 마이그레이션 옵션이 나와 있습니다. 특히, 고객은 ACC를 사용하여 일부 선택된 워크로드 또는 모든 워크로드를 사내 데이터 센터에서 클라우드로 이동할 수 있으며, 테스트 목적으로 앱을 클라우드로 클론 복제하거나 데이터 센터에서 클라우드로 이동할 수 있습니다

데이터 마이그레이션

한 환경에서 다른 환경으로 애플리케이션을 마이그레이션하려면 ACC의 다음 기능 중 하나를 사용할 수 있습니다.

- 복제**

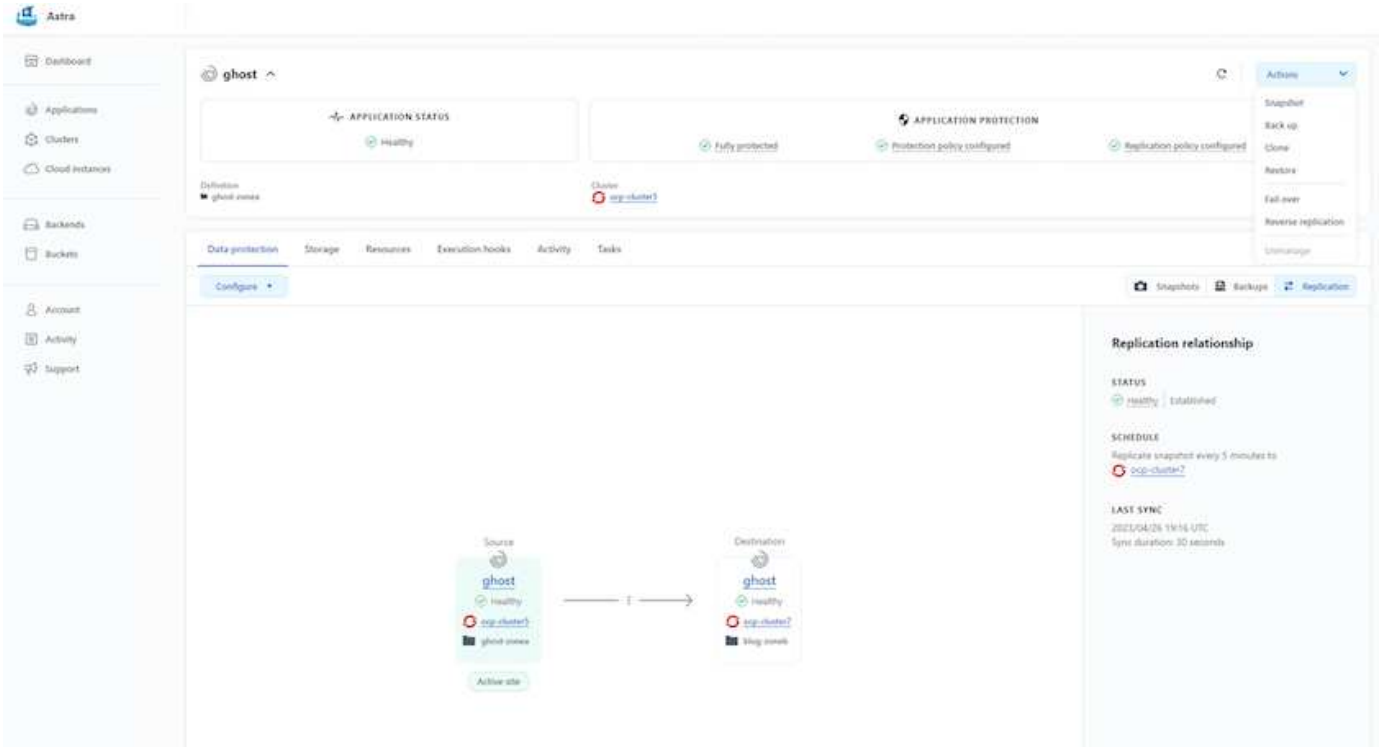
- 백업 및 복구
- 복제

을 참조하십시오 "데이터 보호 섹션을 참조하십시오" 복제 및 백업 및 복구** 옵션에 대해 설명합니다.

을 참조하십시오 "여기" 복제 에 대한 자세한 내용을 확인하십시오.

Astra Replication 기능은 Trident CSI(Container Storage Interface)에서만 지원됩니다. 그러나 NAS – 이코노미 및 SAN – 이코노미 동인은 복제를 지원하지 않습니다.

ACC를 사용하여 데이터 복제 수행



Red Hat OpenShift Container 워크로드를 위한 NetApp 하이브리드 멀티 클라우드 솔루션

개요

NetApp은 기존 엔터프라이즈 애플리케이션을 현대화하고 Kubernetes를 기반으로 구축된 컨테이너 및 오케스트레이션 플랫폼을 사용하여 새로운 애플리케이션을 구축하는 고객이 크게 증가하고 있습니다. Red Hat OpenShift Container Platform은 많은 고객이 채택한 한 가지 예입니다.

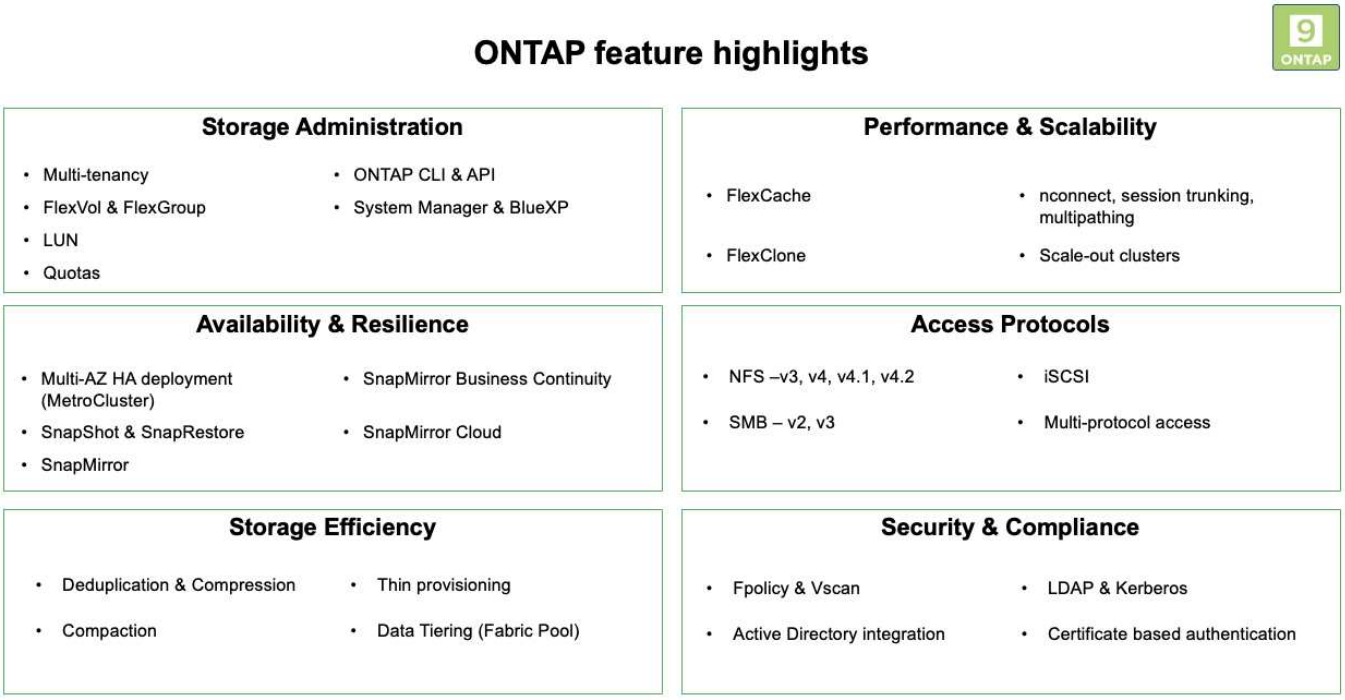
점점 더 많은 고객이 기업 내에 컨테이너를 채택하기 시작함에 따라 NetApp은 상태 저장 애플리케이션의 영구 스토리지 요구사항과 데이터 보호, 데이터 보안, 데이터 마이그레이션과 같은 기존의 데이터 관리 요구사항을 충족할 수 있는 완벽한 위치를 선점하고 있습니다. 그러나 이러한 요구 사항은 서로 다른 전략, 도구 및 방법을 사용하여 충족됩니다.

- NetApp ONTAP** 아래에 나열된 스토리지 옵션을 사용하여 컨테이너 및 Kubernetes 구축을 위한 보안, 데이터 보호, 안정성 및 유연성을 확보할 수 있습니다.
  - 사내 자가 관리형 스토리지:
- NetApp 패브릭 연결 스토리지(FAS), NetApp All Flash FAS 어레이(AFF), NetApp All SAN 어레이(ASA) 및

ONTAP Select

- 온프레미스에서 공급자 관리 스토리지:

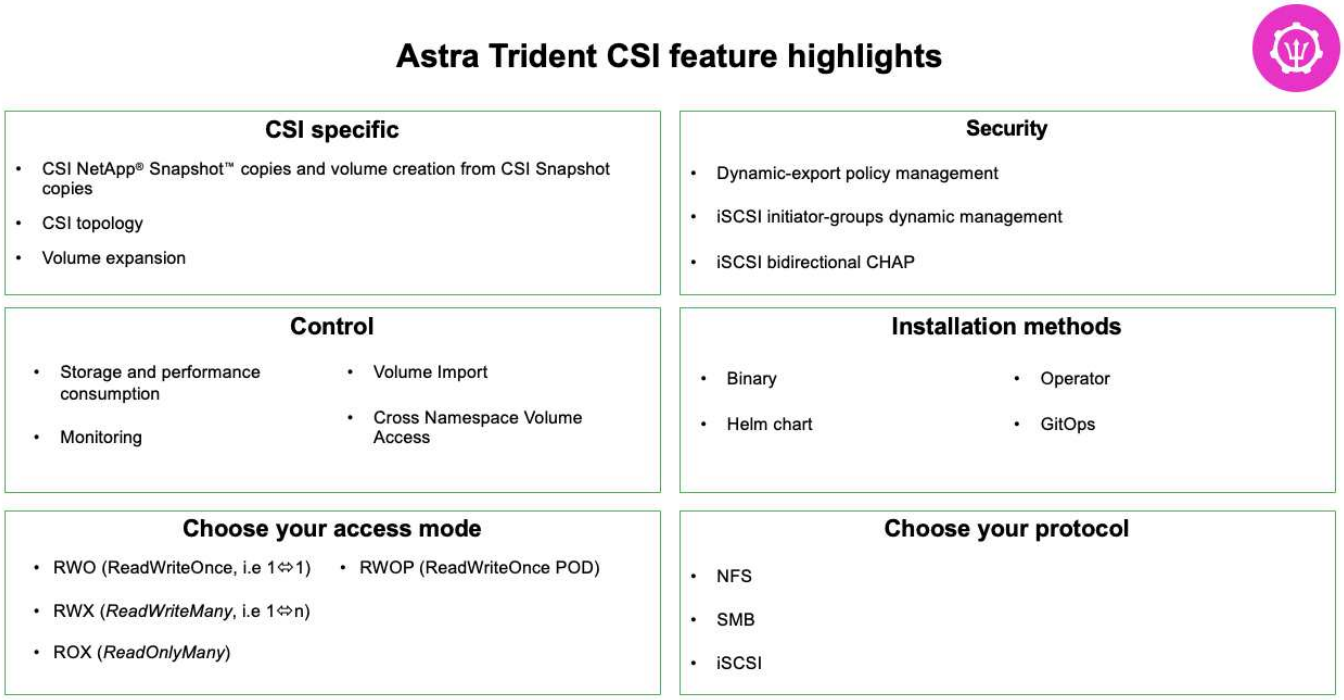
- NetApp Keystone, STaaS(서비스형 스토리지) 제공
  - 클라우드에서 자가 관리 스토리지:
- NetApp Cloud Volumes ONTAP(CVO)은 하이퍼스케일러에 자가 관리하는 스토리지를 제공합니다
  - 클라우드 내 공급자 관리 스토리지:
- Cloud Volumes Service for Google Cloud(CVS), Azure NetApp Files(ANF), Amazon FSx for NetApp ONTAP는 하이퍼스케일러에 완전 관리형 스토리지를 제공합니다



- NetApp BlueXP** - 단일 제어 플레인/인터페이스에서 모든 스토리지 및 데이터 자산을 관리할 수 있습니다.

BlueXP를 사용하여 클라우드 스토리지(예: Cloud Volumes ONTAP 및 Azure NetApp Files)를 생성 및 관리하고, 데이터를 이동, 보호 및 분석하며, 많은 사내 및 에지 스토리지 장치를 제어할 수 있습니다.

- NetApp Astra Trident**는 CSI 규정 준수 스토리지 오케스트레이터로서, 위에서 언급한 다양한 NetApp 스토리지 옵션을 통해 영구 스토리지를 빠르고 쉽게 사용할 수 있습니다. NetApp에서 관리 및 지원하는 오픈 소스 소프트웨어입니다.



비즈니스 크리티컬 컨테이너 워크로드에는 영구 볼륨 이상의 용량이 필요합니다. 이들의 데이터 관리 요구사항에 따라 애플리케이션 Kubernetes 객체의 보호 및 마이그레이션이 필요합니다.

애플리케이션 데이터에는 사용자 데이터 외에도 Kubernetes 객체가 포함됩니다. 몇 가지 예는 다음과 같습니다. POD 사양, PVC, 구축, 서비스 맞춤형 구성 개체(예: 구성 맵 및 암호), 스냅샷 복사본, 백업, CRS, CRD와 같은 클론 맞춤형 리소스 등의 영구 데이터)가 있습니다

- NetApp Astra Control**, 완전 관리형 및 자가 관리 소프트웨어로 모두 사용 가능하며, 강력한 애플리케이션 데이터 관리를 위한 오케스트레이션을 제공합니다. 을 참조하십시오 "Astra 문서" Astra 제품군에 대한 자세한 내용은

이 참조 문서는 NetApp Astra Control Center를 사용하여 RedHat OpenShift 컨테이너 플랫폼에 배포된 컨테이너 기반 애플리케이션의 마이그레이션 및 보호를 검증합니다. 또한 이 솔루션은 컨테이너 플랫폼 관리를 위한 Red Hat Advanced Cluster Management(ACM)의 배포 및 사용에 대한 자세한 정보를 제공합니다. 또한, Astra Trident CSI 프로비저닝을 사용하여 NetApp 스토리지를 Red Hat OpenShift 컨테이너 플랫폼과 통합하기 위한 세부 정보도 제공합니다. Astra Control Center는 허브 클러스터에 구축되며 컨테이너 애플리케이션 및 영구 스토리지 라이프사이클을 관리하는 데 사용됩니다. 마지막으로, NetApp FSx for NetApp ONTAP(FSxN)를 영구 스토리지로 사용하는 AWS(Rosa)의 관리되는 Red Hat OpenShift 클러스터에서 복제, 페일오버 및 컨테이너 워크로드에 대한 페일백용 솔루션을 제공합니다.

AWS 기반의 관리되는 Red Hat OpenShift Container 플랫폼 워크로드를 지원하는 NetApp 솔루션

AWS 기반의 관리되는 Red Hat OpenShift Container 플랫폼 워크로드를 지원하는 NetApp 솔루션

고객은 일부 특정 워크로드 또는 모든 워크로드를 데이터 센터에서 클라우드로 이동할 준비가 되었을 때 "클라우드에서 탄생됨" 또는 현대화 과정에서 일부가 될 수 있습니다. 고객은 클라우드에서 공급자 관리 OpenShift 컨테이너와 공급자 관리 NetApp 스토리지를 사용하여 워크로드를 실행할 수 있습니다. 컨테이너 워크로드를 위한 성공적인 프로덕션 준비 환경을 위해 클라우드에서 관리되는 Red Hat OpenShift 컨테이너 클러스터(Rosa)를 계획하고 배포해야 합니다. AWS 클라우드에 있는 고객은 스토리지 필요에 따라 NetApp ONTAP용 FSx를 구축할

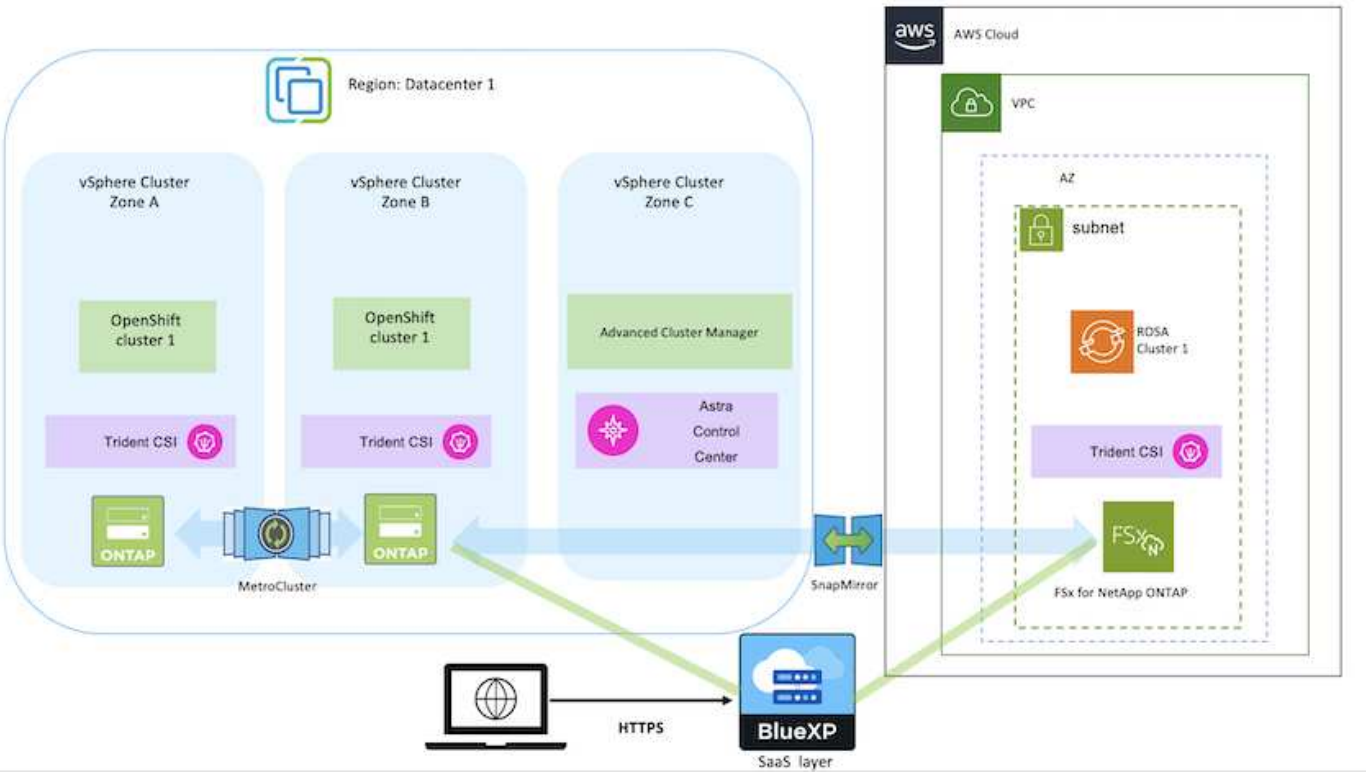
수 있습니다.

NetApp ONTAP용 FSX는 AWS의 컨테이너 구축을 위한 데이터 보호, 안정성 및 유연성을 제공합니다. Astra Trident는 고객의 상태 저장 애플리케이션에 영구 FSxN 스토리지를 사용하는 동적 스토리지 프로비저닝을 수행합니다.

여러 가용성 영역에 컨트롤 플레인 노드가 분산된 상태에서 HA 모드로 Rosa를 구축할 수 있으므로, FSx ONTAP는 고가용성을 제공하고 AZ 장애로부터 보호하는 Multi-AZ 옵션을 통해 구축할 수도 있습니다.

> 파일 시스템의 AZ(Preferred Availability Zone)에서 Amazon FSx 파일 시스템에 액세스할 때 데이터 전송 비용이 발생하지 않습니다. 가격에 대한 자세한 내용은 을 참조하십시오 "여기".

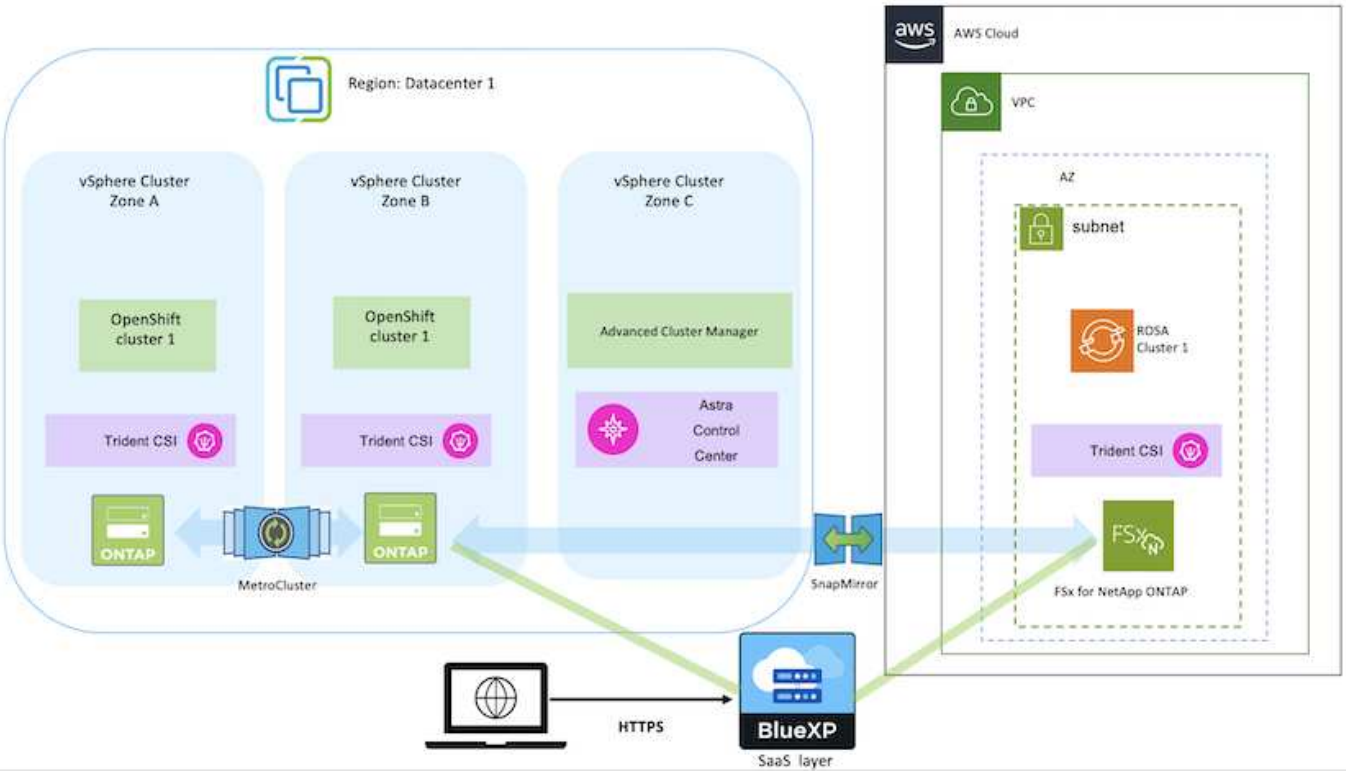
OpenShift Container 워크로드를 위한 데이터 보호 및 마이그레이션 솔루션



AWS에서 관리되는 **Red Hat OpenShift Container** 플랫폼을 배포하고 구성합니다

이 섹션에서는 AWS(Rosa)에서 관리되는 Red Hat OpenShift 클러스터를 설정하는 고급 워크플로우를 설명합니다. 또한 영구 볼륨을 제공하기 위해 Astra Trident가 NetApp FSx for NetApp ONTAP(FSxN)를 스토리지 백엔드로 사용하는 것을 보여 줍니다. BlueXP를 사용하는 AWS에서 FSxN을 배포하는 방법에 대한 자세한 정보가 제공됩니다. 또한 Rosa 클러스터의 상태 저장 애플리케이션에 대한 데이터 보호 및 마이그레이션 작업을 수행하기 위해 BlueXP 및 OpenShift GitOps(Argo CD)를 사용하는 방법에 대한 세부 정보도 제공됩니다.

다음은 AWS에 배포되고 FSxN을 백엔드 스토리지로 사용하는 Rosa 클러스터를 보여 주는 다이어그램입니다.



이 솔루션은 AWS의 두 대의 VPC에서 두 개의 Rosa 클러스터를 사용하여 검증되었습니다. 각 Rosa 클러스터는 Astra Trident를 사용하여 FSxN과 통합되었습니다. AWS에서 Rosa 클러스터와 FSxN을 구축하는 방법은 여러 가지가 있습니다. 설정에 대한 이 고급 설명은 사용된 특정 방법에 대한 설명서 링크를 제공합니다. 에 제공된 관련 링크에서 다른 방법을 참조할 수 있습니다 "리소스 섹션을 참조하십시오".

설치 프로세스는 다음 단계로 나눌 수 있습니다.

Rosa 클러스터를 설치합니다

- 2개의 VPC를 생성하고 VPC 간 VPC 피어링 연결을 설정합니다.
- 을 참조하십시오 "여기" Rosa 클러스터를 설치하는 지침은 를 참조하십시오.

FSxN을 설치합니다

- BlueXP에서 VPC에 FSxN을 설치합니다. 을 참조하십시오 "여기" BlueXP 계정 생성 및 시작 을 참조하십시오 "여기" FSxN 설치용. 을 참조하십시오 "여기" FSxN을 관리하기 위해 AWS에 커넥터를 생성하는 데 사용됩니다.
- AWS를 사용하여 FSxN을 구축합니다. 을 참조하십시오 "여기" AWS 콘솔을 사용하여 구축

Rosa 클러스터에 **Trident** 설치(제어 차트 사용)

- 제어 차트를 사용하여 Rosa 클러스터에 Trident를 설치합니다. 제어 차트 URL: https://netapp.github.io/trident-helm-chart

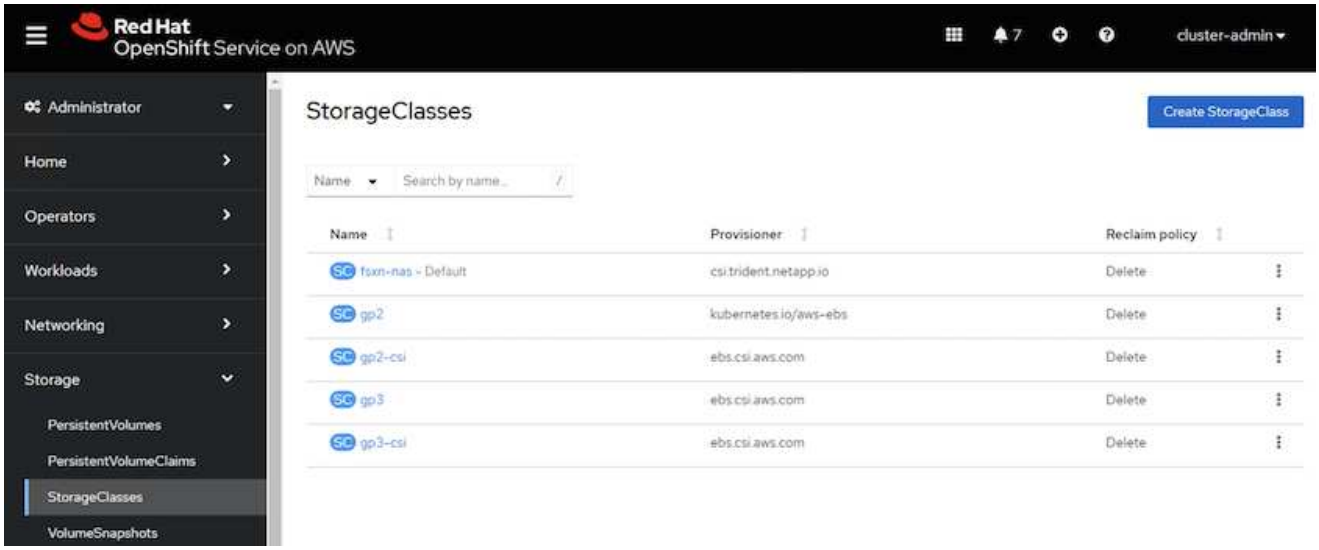
FSxN과 Astra Trident for Rosa 클러스터의 통합

OpenShift GitOps를 사용하면 ApplicationSet을 사용하여 ArgoCD에 등록될 때 모든 관리 클러스터에 Astra Trident CSI를 배포할 수 있습니다.

```
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: trident-operator
spec:
  generators:
  - clusters: {}
    # selector:
    #   matchLabels:
    #     tridentversion: '23.04.0'
  template:
    metadata:
      name: '{{nameNormalized}}-trident'
    spec:
      destination:
        namespace: trident
        server: '{{server}}'
      source:
        repoURL: 'https://netapp.github.io/trident-helm-chart'
        targetRevision: 23.04.0
        chart: trident-operator
      project: default
      syncPolicy:
        syncOptions:
          - CreateNamespace=true
```

Trident(FSxN용)를 사용하여 백엔드 및 스토리지 클래스 생성

- 을 참조하십시오 "여기" 백엔드 및 스토리지 클래스 생성에 대한 자세한 내용은 을 참조하십시오.
- OpenShift Console에서 Trident CSI로 FsxN에 대해 생성한 스토리지 클래스를 기본값으로 설정합니다. 아래 스크린샷을 참조하십시오.



OpenShift GitOps(Argo CD)를 사용하여 애플리케이션 배포

- 클러스터에 OpenShift GitOps 운영자를 설치합니다. 지침을 참조하십시오 "여기".
- 클러스터에 대한 새 Argo CD 인스턴스를 설정합니다. 지침을 참조하십시오 "여기".

Argo CD 콘솔을 열고 앱을 배포합니다. 예를 들어, Argo CD와 H제어 차트를 사용하여 Jenkins 앱을 배포할 수 있습니다. 응용 프로그램을 생성할 때 다음과 같은 세부 정보가 제공됩니다. Project: 기본 클러스터: https://kubernetes.default.svc네임스페이스: Jenkins 제어 차트의 URL: https://charts.bitnami.com/bitnami

Helm Parameters:global.storageClass:fsxn-nas

데이터 보호

이 페이지에는 Astra Control Service를 사용하는 AWS(ROSA) 관리형 Red Hat OpenShift 클러스터에 대한 데이터 보호 옵션이 나와 있습니다. Astra Control Service(ACS)는 사용이 간편한 그래픽 사용자 인터페이스를 제공하여 클러스터를 추가하고, 클러스터에서 실행되는 애플리케이션을 정의하고, 애플리케이션 인식 데이터 관리 활동을 수행할 수 있습니다. ACS 기능은 워크플로우 자동화를 지원하는 API를 사용하여 액세스할 수도 있습니다.

Astra Control(ACS 또는 ACC)은 NetApp Astra Trident입니다. Astra Trident는 Red Hat OpenShift, EKS, AKS, SUSE Rancher, Anthos 등과 같은 다양한 유형의 Kubernetes 클러스터를 통합합니다. FAS/AFF, ONTAP Select, CVO, Google Cloud Volumes Service, Azure NetApp Files 및 Amazon FSx for NetApp ONTAP 같은 다양한 유형의 NetApp ONTAP 스토리지를 활용할 수 있습니다.

이 섹션에서는 ACS를 사용하는 다음 데이터 보호 옵션에 대해 자세히 설명합니다.

- 한 지역에서 실행 중인 Rosa 애플리케이션의 백업 및 복원과 다른 지역으로 복원한 비디오를 보여 줍니다.
- Rosa 애플리케이션의 스냅샷 및 복원을 보여주는 비디오
- Rosa 클러스터, Amazon FSx for NetApp ONTAP 설치, NetApp Astra Trident를 사용하여 스토리지 백엔드와 통합, Rosa 클러스터에 PostgreSQL 애플리케이션 설치, ACS를 사용하여 애플리케이션 스냅샷을 생성하고 애플리케이션을 복원하는 방법에 대한 단계별 세부 정보입니다.
- ACS를 사용하는 FSx for ONTAP가 포함된 ROSA 클러스터의 MySQL 애플리케이션에 대한 스냅샷을 생성하고 복원하는 방법에 대한 단계별 세부 정보를 보여주는 블로그

백업에서 백업/복원

다음 비디오에서는 한 지역에서 실행되고 다른 지역으로 복원되는 Rosa 응용 프로그램의 백업을 보여 줍니다.

AWS 기반 FSx NetApp ONTAP for Red Hat OpenShift Service

스냅샷/스냅샷에서 복구

다음 비디오는 Rosa 응용 프로그램의 스냅샷 촬영 및 이후 스냅샷에서 복원하는 방법을 보여 줍니다.

Amazon FSx for NetApp ONTAP 스토리지를 사용하는 AWS(ROSA) 기반 Red Hat OpenShift Service의 애플리케이션을 위한 스냅샷/복원

블로그

- "Amazon FSx 스토리지가 탑재된 Rosa 클러스터에서 앱의 데이터를 관리하는 데 Astra Control Service를 사용합니다"

스냅샷을 생성하고 이 스냅샷에서 복구하는 단계별 세부 정보입니다

사전 요구 사항 설정

- "설치하 고 있습니다"
- "Red Hat OpenShift 계정"
- IAM 사용자 "적절한 사용 권한" Rosa 클러스터를 생성하고 액세스합니다
- "AWS CLI를 참조하십시오"
- "로사 CLI"
- "OpenShift CLI를 참조하십시오"(OC)
- VPC와 서브넷, 적절한 게이트웨이 및 라우트
- "ROSA 클러스터가 설치되었습니다" VPC로 이동합니다
- "NetApp ONTAP용 Amazon FSx" 동일한 VPC에서 생성됨
- 에서 Rosa 클러스터에 액세스합니다 "OpenShift 하이브리드 클라우드 콘솔"

다음 단계

1. admin 사용자를 생성하고 클러스터에 로그인합니다.
2. 클러스터에 대한 kubeconfig 파일을 생성합니다.

3. 클러스터에 Astra Trident를 설치합니다.
4. Trident CSI Provisioner를 사용하여 백엔드, 스토리지 클래스 및 스냅샷 클래스 구성을 생성합니다.
5. 클러스터에 PostgreSQL 애플리케이션을 구축합니다.
6. 데이터베이스를 만들고 레코드를 추가합니다.
7. 클러스터를 ACS에 추가합니다.
8. ACS에서 애플리케이션을 정의합니다.
9. ACS를 사용하여 스냅샷을 생성합니다.
10. PostgreSQL 애플리케이션에서 데이터베이스를 삭제합니다.
11. ACS를 사용하여 스냅샷에서 복원합니다.
12. 앱이 스냅숏에서 복원되었는지 확인합니다.

1. 관리자 사용자를 생성하고 클러스터에 로그인합니다

다음 명령을 사용하여 admin 사용자를 생성하여 Rosa 클러스터에 액세스합니다(설치 시 admin 사용자를 생성하지 않은 경우에만 생성 필요).

```
rosa create admin --cluster=<cluster-name>
```

명령은 다음과 같은 출력을 제공합니다. 를 사용하여 클러스터에 로그인합니다 `oc login` 출력에 제공된 명령입니다.

```
W: It is recommended to add an identity provider to login to this cluster.
See 'rosa create idp --help' for more information.
I: Admin account has been added to cluster 'my-rosa-cluster'. It may take up
to a minute for the account to become active.
I: To login, run the following command:
oc login https://api.my-rosa-cluster.abcd.p1.openshiftapps.com:6443 \
--username cluster-admin \
--password FWGYL-2mkJI-00000-00000
```

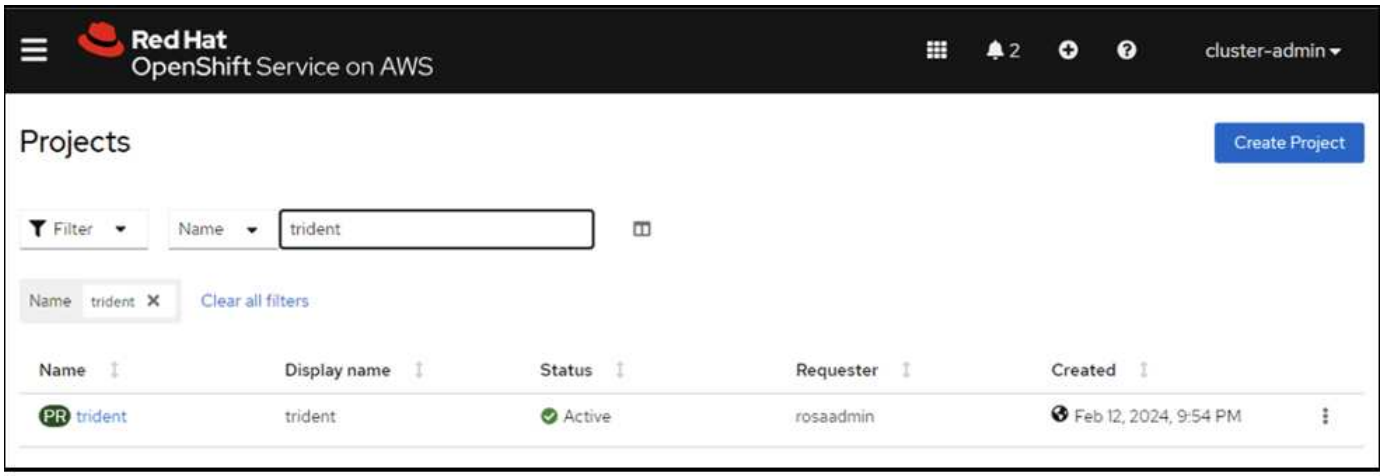
토큰을 사용하여 클러스터에 로그인할 수도 있습니다. 클러스터 생성 시 이미 관리자 사용자를 생성한 경우 Red Hat OpenShift Hybrid Cloud 콘솔에서 관리자 자격 증명을 사용하여 클러스터에 로그인할 수 있습니다. 그런 다음, 로그인한 사용자의 이름을 표시하는 오른쪽 상단 모서리를 클릭하여 를 얻을 수 있습니다 `oc login` 명령줄에 대한 명령(토큰 로그인)입니다.

2. 클러스터에 대한 **kubeconfig** 파일을 생성합니다

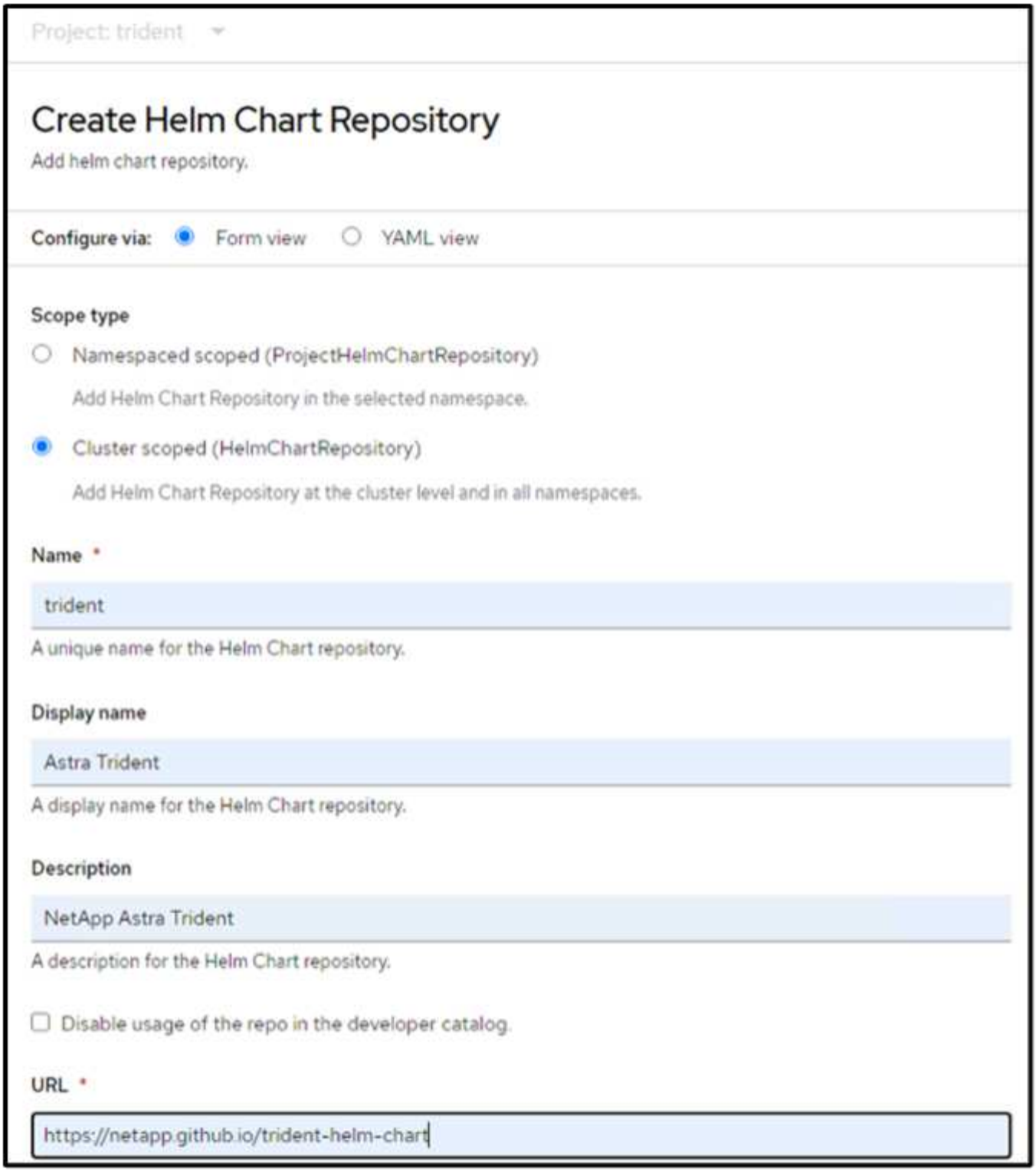
절차를 따르십시오 "여기" Rosa 클러스터에 대한 kubeconfig 파일을 생성합니다. 이 kubeconfig 파일은 ACS에 클러스터를 추가할 때 나중에 사용됩니다.

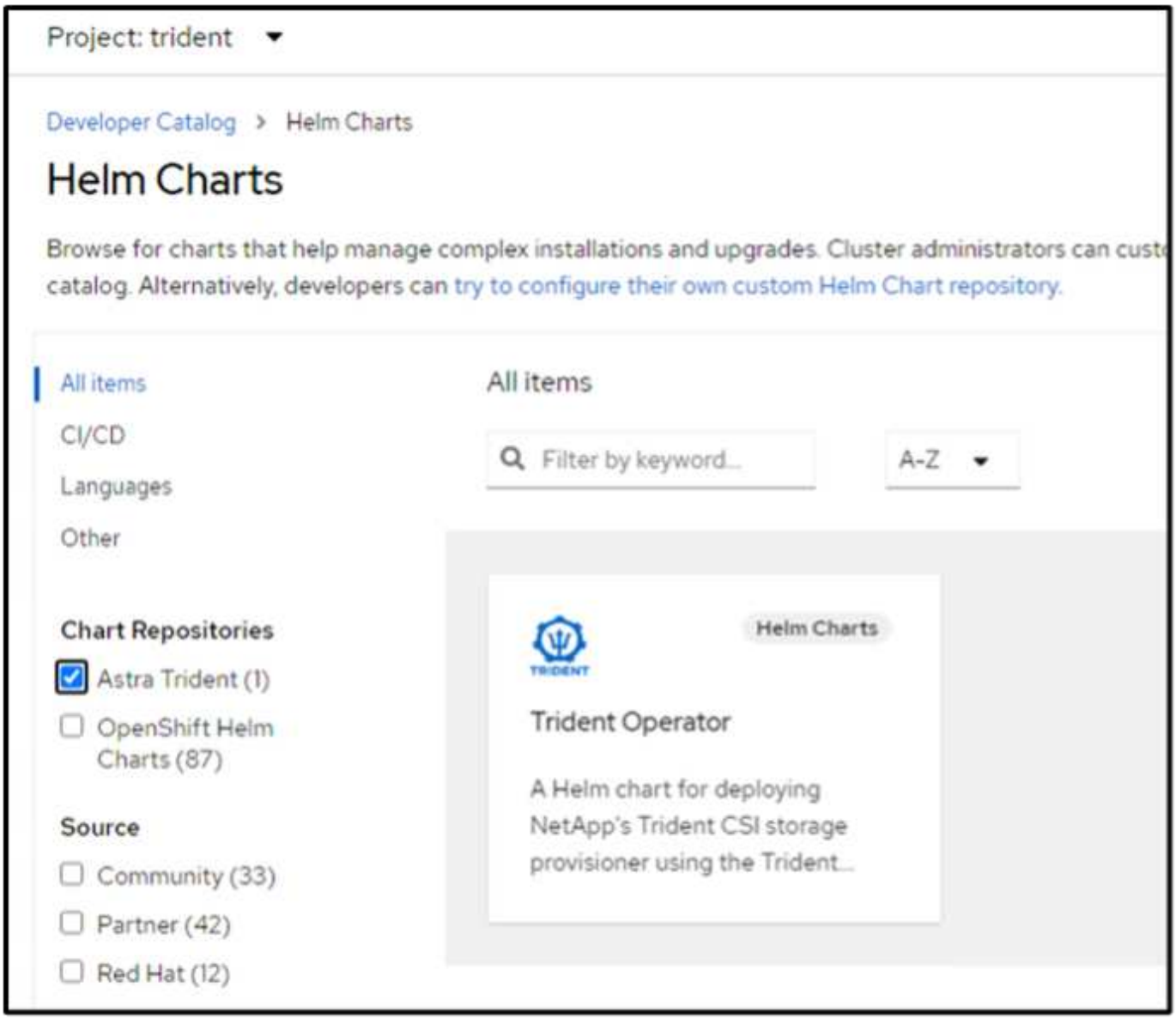
3. 클러스터에 **Astra Trident**를 설치합니다

Rosa 클러스터에 Astra Trident(최신 버전)를 설치합니다. 이렇게 하려면 주어진 절차 중 하나를 따를 수 있습니다 " 여기". 클러스터 콘솔에서 Helm을 사용하여 Trident를 설치하려면 먼저 Trident라는 프로젝트를 생성합니다.

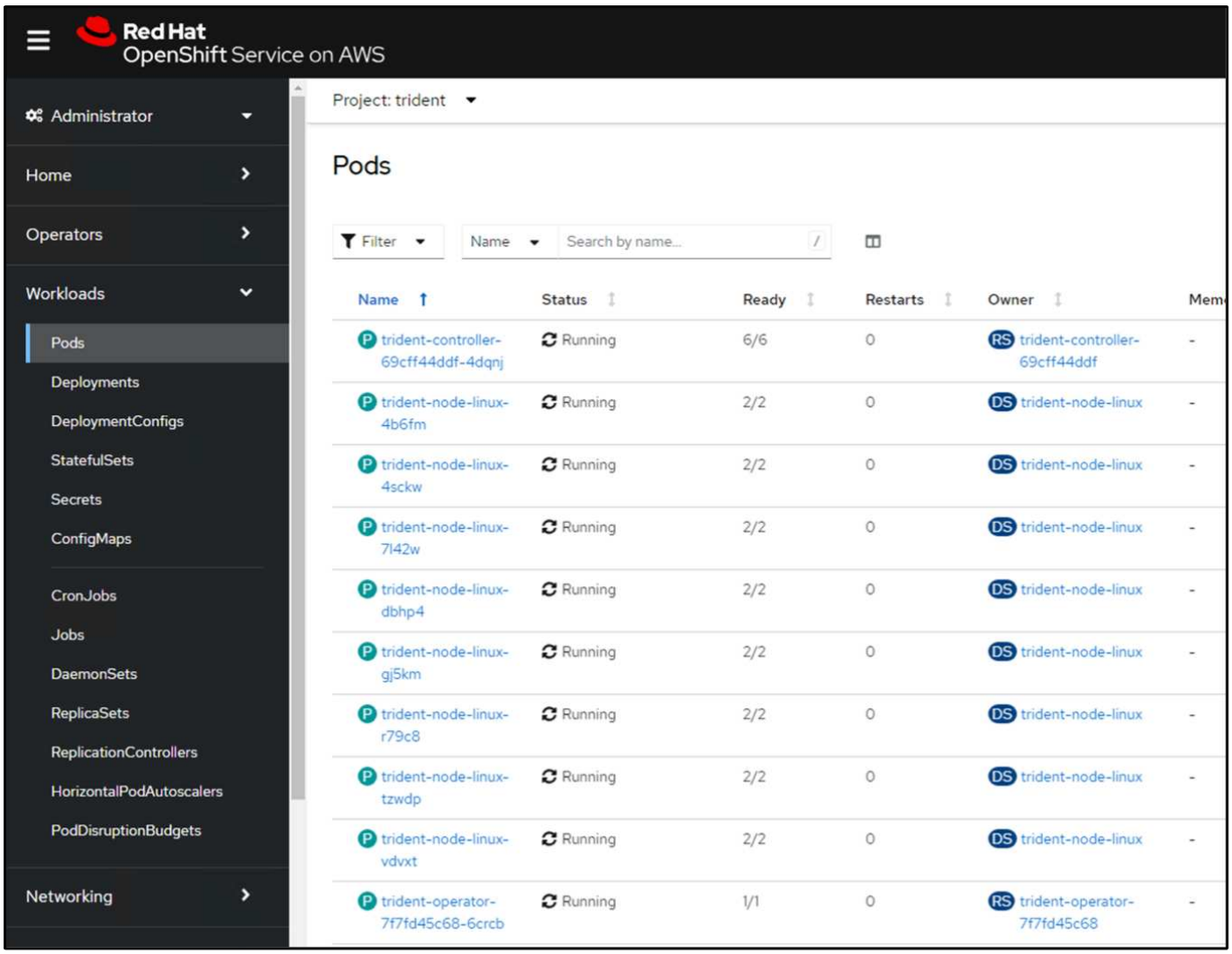


그런 다음 개발자 보기에서 Helm 차트 리포지토리를 만듭니다. URL 필드에 을 사용합니다 `'https://netapp.github.io/trident-helm-chart'`. 그런 다음 Trident 운영자에 대한 Helm 릴리즈를 작성합니다.


Project: trident
Create Helm Chart Repository
Add helm chart repository.
Configure via:
Form view
YAML view
Scope type
Namespaced scoped (ProjectHelmChartRepository)
Add Helm Chart Repository in the selected namespace.
Cluster scoped (HelmChartRepository)
Add Helm Chart Repository at the cluster level and in all namespaces.
Name *
trident
A unique name for the Helm Chart repository.
Display name
Astra Trident
A display name for the Helm Chart repository.
Description
NetApp Astra Trident
A description for the Helm Chart repository.
Disable usage of the repo in the developer catalog.
URL *
https://netapp.github.io/trident-helm-chart



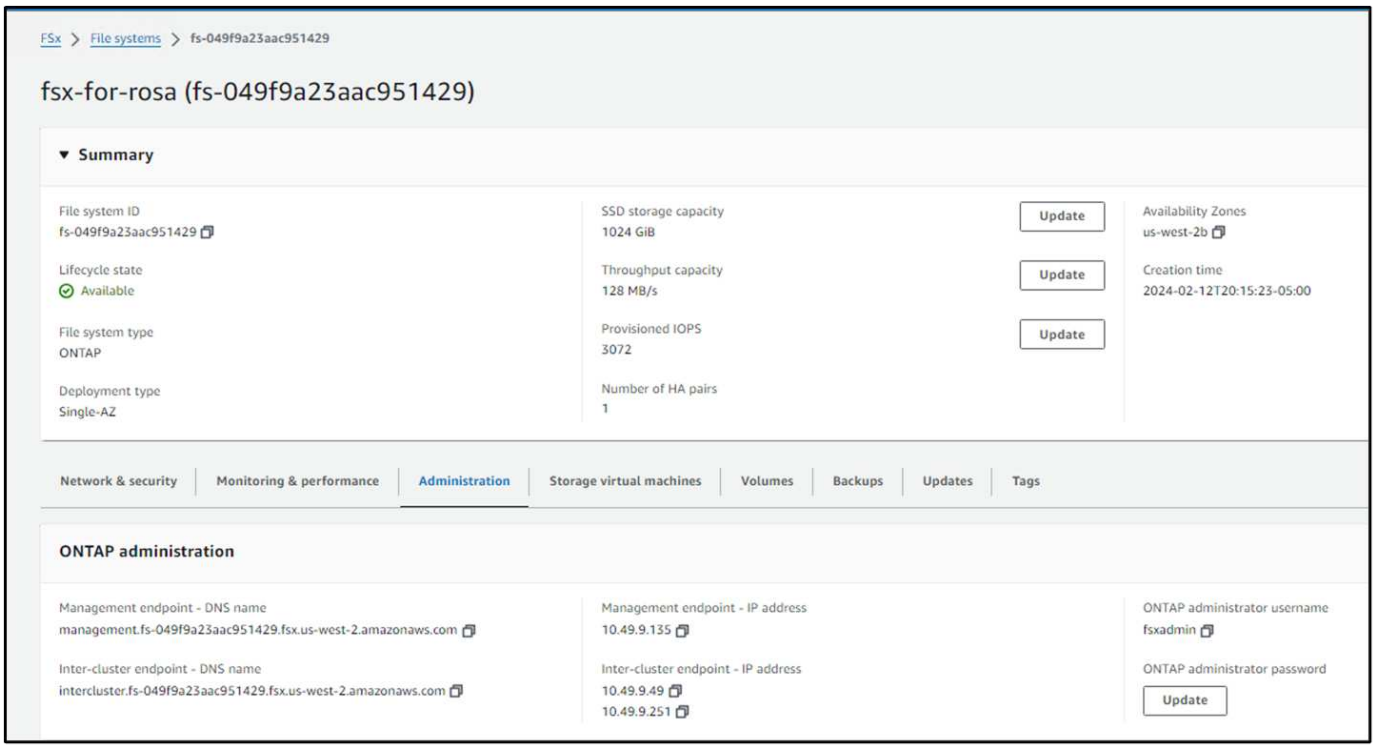
콘솔의 관리자 보기로 돌아가 트라이덴트 프로젝트에서 Pod를 선택하여 모든 트라이덴트 포드가 실행 중인지 확인합니다.



4. Trident CSI Provisioner 를 사용하여 백엔드, 스토리지 클래스 및 스냅샷 클래스 구성을 생성합니다

아래 표시된 YAML 파일을 사용하여 트리덴트 백엔드 객체, 스토리지 클래스 객체 및 Volumesnapshot 객체를 생성합니다. 생성한 Amazon FSx for NetApp ONTAP 파일 시스템에 대한 자격 증명, 백엔드의 YAML 구성에서 파일 시스템의 관리 LIF 및 가상 서버 이름을 제공해야 합니다. 이러한 세부 정보를 보려면 Amazon FSx용 AWS 콘솔로 이동하여 파일 시스템을 선택하고 관리 탭으로 이동합니다. 또한 UPDATE(업데이트)를 클릭하여 의 암호를 설정합니다 `fsxadmin` 사용자.

명령줄을 사용하여 개체를 만들거나 하이브리드 클라우드 콘솔에서 YAML 파일을 사용하여 개체를 만들 수 있습니다.



- Trident 백엔드 구성**

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-nas-secret
type: Opaque
stringData:
  username: fsxadmin
  password: <password>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: <management lif>
  backendName: ontap-nas
  svm: fsx
  credentials:
    name: backend-tbc-ontap-nas-secret
```

- 저장소 클래스**

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
allowVolumeExpansion: true
```

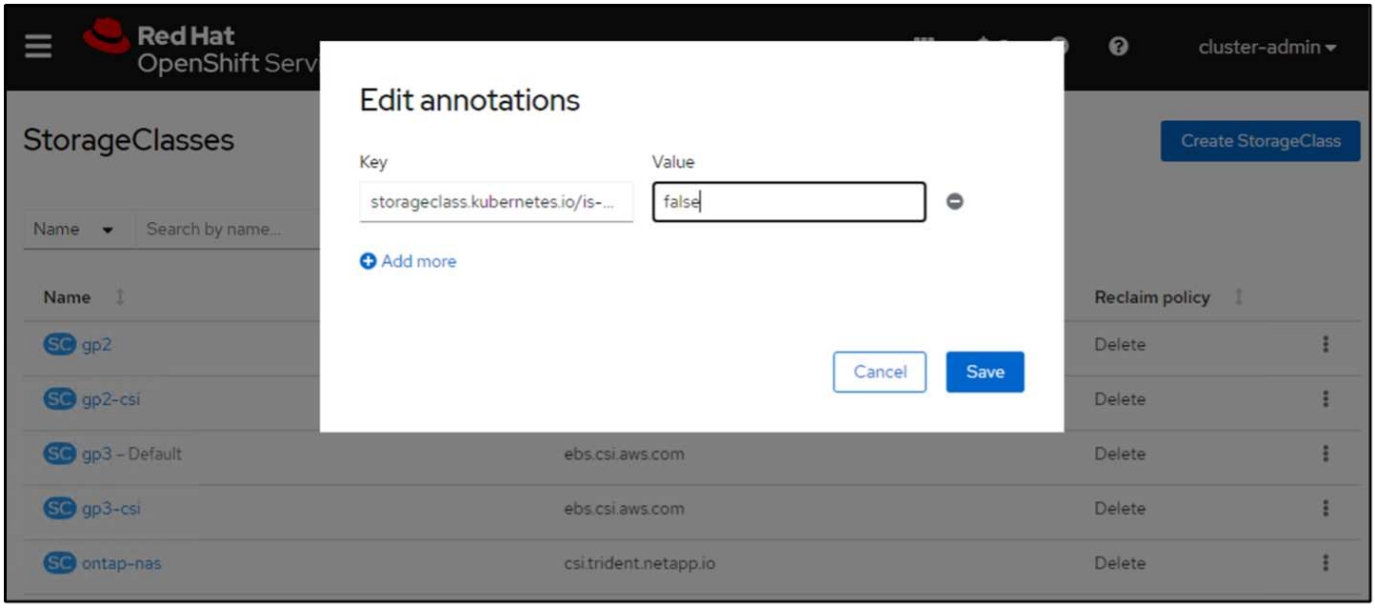
- 스냅샷 클래스**

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

아래 표시된 명령을 실행하여 백엔드, 스토리지 클래스 및 trident-snapshotclass 객체가 생성되었는지 확인합니다.

```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get tbc -n trident
NAME        BACKEND NAME   BACKEND UUID                           PHASE   STATUS
ontap-nas   ontap-nas      8a5e4583-2dac-46bb-b01e-fa7c3816f121   Bound   Success
[ec2-user@ip-10-49-11-132 storage]$ kubectl get sc
NAME            PROVISIONER             RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE
gp2             kubernetes.io/aws-ebs   Delete          WaitForFirstConsumer   true                   3h23m
gp2-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
gp3 (default)   ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h23m
gp3-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
ontap-nas       csi.trident.netapp.io   Delete          Immediate              true                   141m
[ec2-user@ip-10-49-11-132 storage]$ kubectl get Volumesnapshotclass
NAME                    DRIVER                  DELETIONPOLICY   AGE
csi-aws-vsc             ebs.csi.aws.com         Delete           3h19m
trident-snapshotclass   csi.trident.netapp.io   Delete           6m56s
[ec2-user@ip-10-49-11-132 storage]$
```

현재 중요한 수정 사항은 나중에 구축하는 PostgreSQL 앱에서 기본 스토리지 클래스를 사용할 수 있도록 ONTAP-NAS를 GP3이 아닌 기본 스토리지 클래스로 설정하는 것입니다. 클러스터의 OpenShift 콘솔의 Storage에서 StorageClasses를 선택합니다. 현재 기본 클래스의 주석을 false로 편집하고 ONTAP-NAS 스토리지 클래스에 대해 주석 storageclass.cubernetes/is-default-class 세트를 true로 추가하십시오.



5. 클러스터에 **PostgreSQL** 애플리케이션을 구축합니다

다음과 같이 명령줄에서 응용 프로그램을 배포할 수 있습니다.

```
helm install postgresql bitnami/postgresql -n postgresql --create-namespace
```

```
[ec2-user@ip-10-49-11-132 astra]$ helm install postgresql bitnami/postgresql -n postgresql --create-namespace
NAME: postgresql
LAST DEPLOYED: Tue Feb 13 14:46:16 2024
NAMESPACE: postgresql
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
CHART NAME: postgresql
CHART VERSION: 14.0.4
APP VERSION: 16.2.0

** Please be patient while the chart is being deployed **

PostgreSQL can be accessed via port 5432 on the following DNS names from within your cluster:

    postgresql.postgresql.svc.cluster.local - Read/Write connection

To get the password for "postgres" run:

    export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="{.data.postgres-password}" | base64 -d)

To connect to your database run the following command:

    kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PG
PASSWORD=$POSTGRES_PASSWORD" \
      --command -- psql --host postgresql -U postgres -d postgres -p 5432

    > NOTE: If you access the container using bash, make sure that you execute "/opt/bitnami/scripts/postgresql/entrypoint.sh /bin/bash" in order to avoid
the error "psql: local user with ID 1001} does not exist"

To connect to your database from outside the cluster execute the following commands:

    kubectl port-forward --namespace postgresql svc/postgresql 5432:5432 &
    PGPASSWORD="$POSTGRES_PASSWORD" psql --host 127.0.0.1 -U postgres -d postgres -p 5432

WARNING: The configured password will be ignored on new installation in case when previous PostgreSQL release was deleted through the helm command. In that
 case, old PVC will have an old password, and setting it through helm won't take effect. Deleting persistent volumes (PVs) will solve the issue.
[ec2-user@ip-10-49-11-132 astra]$
```

응용 프로그램 포드가 실행되고 있지 않으면 보안 컨텍스트 제약 때문에 발생한 오류가 있을 수 있습니다.

```
[ec2-user@ip-10-49-11-132 astra]$ kubectl get all -n postgresql
NAME                     TYPE        CLUSTER-IP     EXTERNAL-IP   PORT(S)    AGE
service/postgresql       ClusterIP   172.30.245.50  <none>        5432/TCP   12m
service/postgresql-hl    ClusterIP   None           <none>        5432/TCP   12m

NAME                          READY   AGE
statefulset.apps/postgresql   0/1     12m
[ec2-user@ip-10-49-11-132 astra]$ kubectl get events -n postgresql
LAST SEEN   TYPE      REASON                OBJECT                                  MESSAGE
2m39s       Normal    WaitForFirstConsumer  persistentvolumeclaim/data-postgresql-0  waiting for first consumer to be created before binding
12m         Normal    SuccessfulCreate      statefulset/postgresql                  create Claim data-postgresql-0 Pod postgresql-0 in StatefulSet postg
resql success
107s        Warning   FailedCreate          statefulset/postgresql                  create Pod postgresql-0 in StatefulSet postgresql failed error: pods
 "postgresql-0" is forbidden: unable to validate against any security context constraint: [provider "trident-controller": Forbidden: not usable by user or
serviceaccount, provider "anyuid": Forbidden: not usable by user or serviceaccount, provider restricted-v2: .spec.securityContext.fsGroup: Invalid value: [
]int64{1001}: 1001 is not an allowed group, provider restricted-v2: .containers[0].runAsUser: Invalid value: 1001: must be in the ranges: [1001010000, 1001
019999], provider "restricted": Forbidden: not usable by user or serviceaccount, provider "nonroot-v2": Forbidden: not usable by user or serviceaccount, pr
ovider "nonroot": Forbidden: not usable by user or serviceaccount, provider "pcap-dedicated-admins": Forbidden: not usable by user or serviceaccount, provi
der "hostmount-anyuid": Forbidden: not usable by user or serviceaccount, provider "machine-api-termination-handler": Forbidden: not usable by user or servi
ceaccount, provider "hostnetwork-v2": Forbidden: not usable by user or serviceaccount, provider "hostnetwork": Forbidden: not usable by user or serviceacco
unt, provider "hostaccess": Forbidden: not usable by user or serviceaccount, provider "splunkforwarder": Forbidden: not usable by user or serviceaccount, p
rovider "trident-node-linux": Forbidden: not usable by user or serviceaccount, provider "node-exporter": Forbidden: not usable by user or serviceaccount, p
rovider "privileged": Forbidden: not usable by user or serviceaccount]
[ec2-user@ip-10-49-11-132 astra]$
```

을 편집하여 오류를 수정하십시오 `runAsUser` 및 `fsGroup` 의 필드 `statefuleset.apps/postgresql` 의 출력에 있는 uid 를 가진 개체입니다 `oc get project` 명령을 사용합니다.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get project postgresql -o yaml | grep uid-range
    openshift.io/sa.scc.uid-range: 1001010000/10000
[ec2-user@ip-10-49-11-132 astra]$ oc edit -n postgresql statefulset.apps/postgresql
statefulset.apps/postgresql edited
[ec2-user@ip-10-49-11-132 astra]$
```

PostgreSQL 앱은 Amazon FSx for NetApp ONTAP 스토리지에서 지원하는 영구 볼륨을 실행하고 사용해야 합니다.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          2m46s
[ec2-user@ip-10-49-11-132 astra]$
```

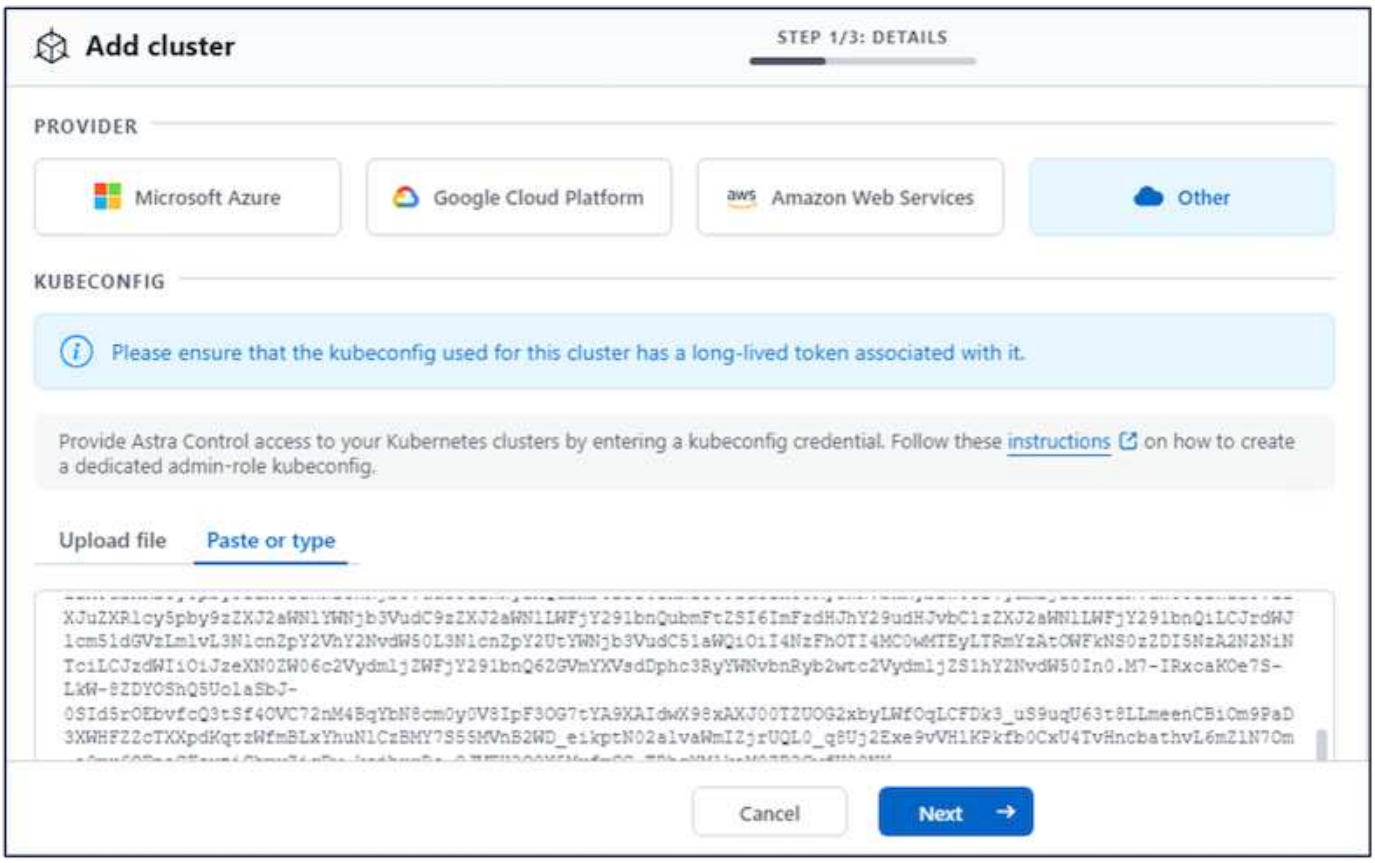
```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get pvc -n postgresql
NAME                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-dd09524a-de75-4825-9424-03a9b91195ca   8Gi        RWO            ontap-nas      4m2s
[ec2-user@ip-10-49-11-132 storage]$
```

6. 데이터베이스를 만들고 레코드를 추가합니다

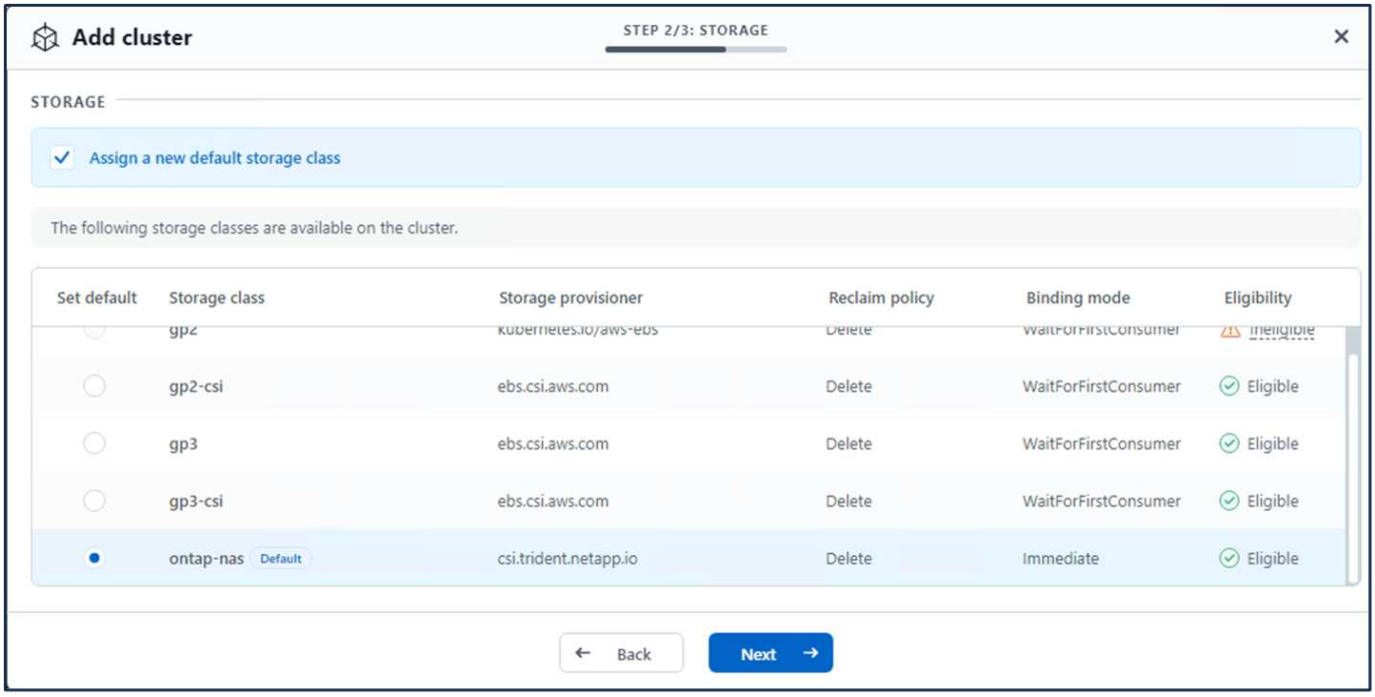
```
[ec2-user@ip-10-49-11-132 astra]$ export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="
{.data.postgres-password}" | base64 -d)
[ec2-user@ip-10-49-11-132 astra]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image
docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" \
> --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must se
t securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityCo
ntext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "postgresql-client" must set securityContext.runAsNonR
oot=true), seccompProfile (pod or container "postgresql-client" must set securityContext.seccompProfile.type to "RuntimeDefault
" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# CREATE DATABASE erp;
CREATE DATABASE
postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# CREATE TABLE PERSONS(ID INT PRIMARY KEY NOT NULL, FIRSTNAME TEXT NOT NULL, LASTNAME TEXT NOT NULL);
CREATE TABLE
erp=# INSERT INTO PERSONS VALUES(1,'John','Doe');
INSERT 0 1
erp=# \dt
         List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * FROM persons;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```

7. ACS에 클러스터를 추가합니다

ACS에 로그인합니다. 클러스터를 선택하고 Add를 클릭합니다. 기타 를 선택하고 kubeconfig 파일을 업로드하거나 붙여 넣습니다.



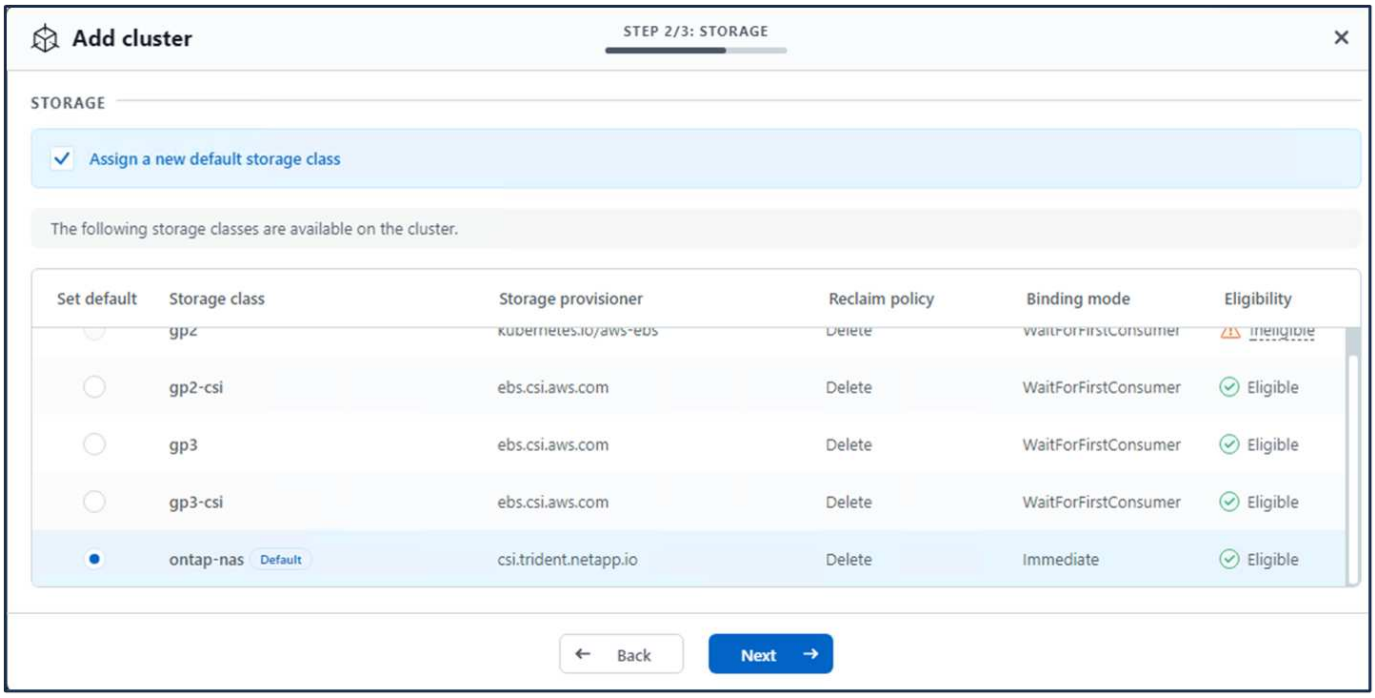
Next * 를 클릭하고 ACS의 기본 스토리지 클래스로 ONTAP-NAS 를 선택합니다. Next * 를 클릭하고 세부 정보를 검토한 후 * Add * the cluster를 클릭합니다.



8. ACS에서 응용 프로그램을 정의합니다

ACS에서 PostgreSQL 애플리케이션을 정의합니다. 시작 페이지에서 * 응용 프로그램 *, * 정의 * 를 선택하고 적절한 세부 정보를 입력합니다. 다음 * 을 두 번 클릭하고 세부 정보를 검토한 후 * 정의 * 를 클릭합니다. 응용 프로그램이

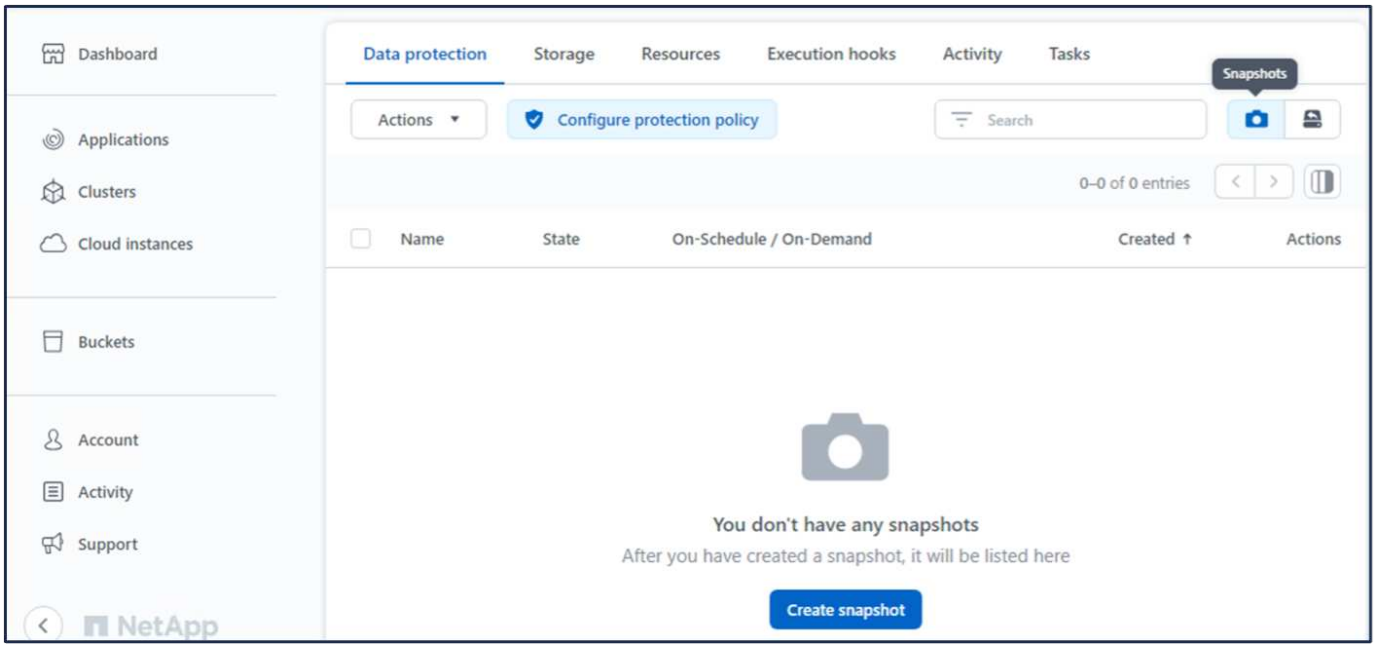
ACS에 추가됩니다.

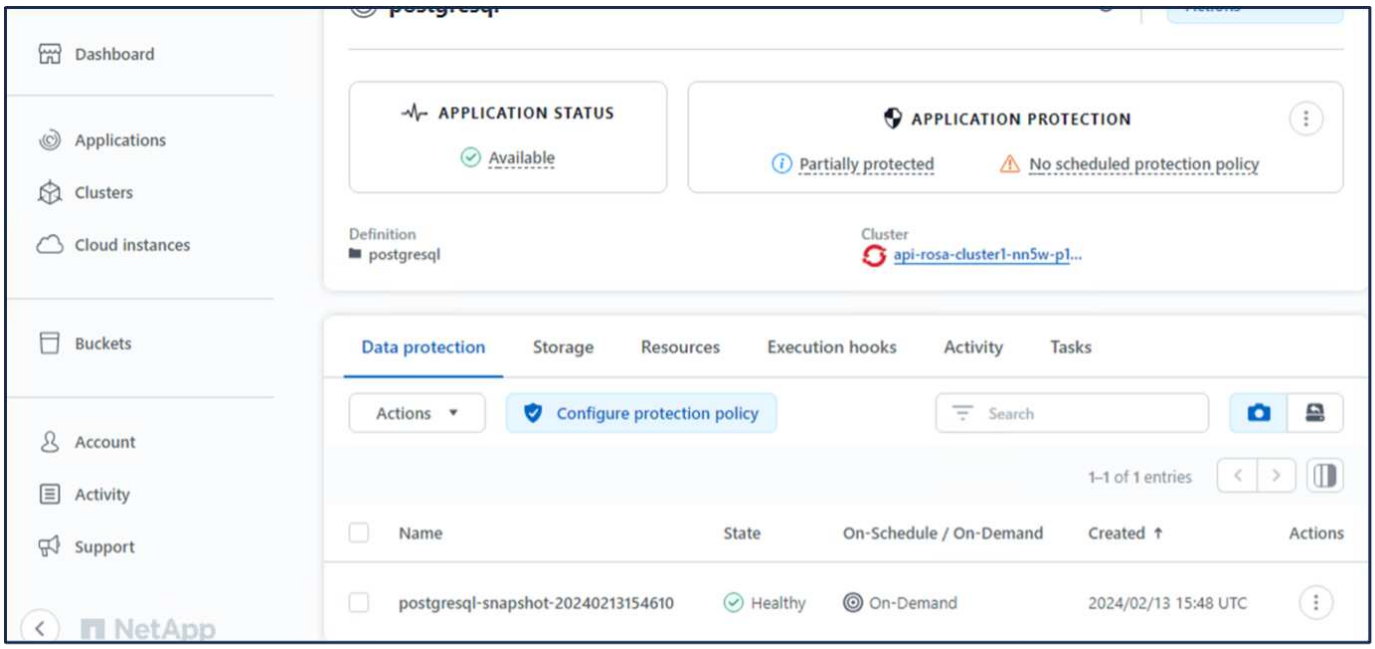


9. ACS를 사용하여 스냅샷을 생성합니다

ACS에서 스냅샷을 생성하는 방법은 여러 가지가 있습니다. 응용 프로그램을 선택하고 페이지에서 응용 프로그램의 세부 정보를 보여 주는 스냅샷을 만들 수 있습니다. 스냅샷 생성 을 클릭하여 필요 시 스냅샷을 생성하거나 보호 정책을 구성할 수 있습니다.

스냅샷 생성 * 을 클릭하고 이름을 입력하고 세부 정보를 검토한 후 * 스냅샷 * 을 클릭하여 주문형 스냅샷을 생성합니다. 작업이 완료되면 스냅샷 상태가 정상으로 변경됩니다.





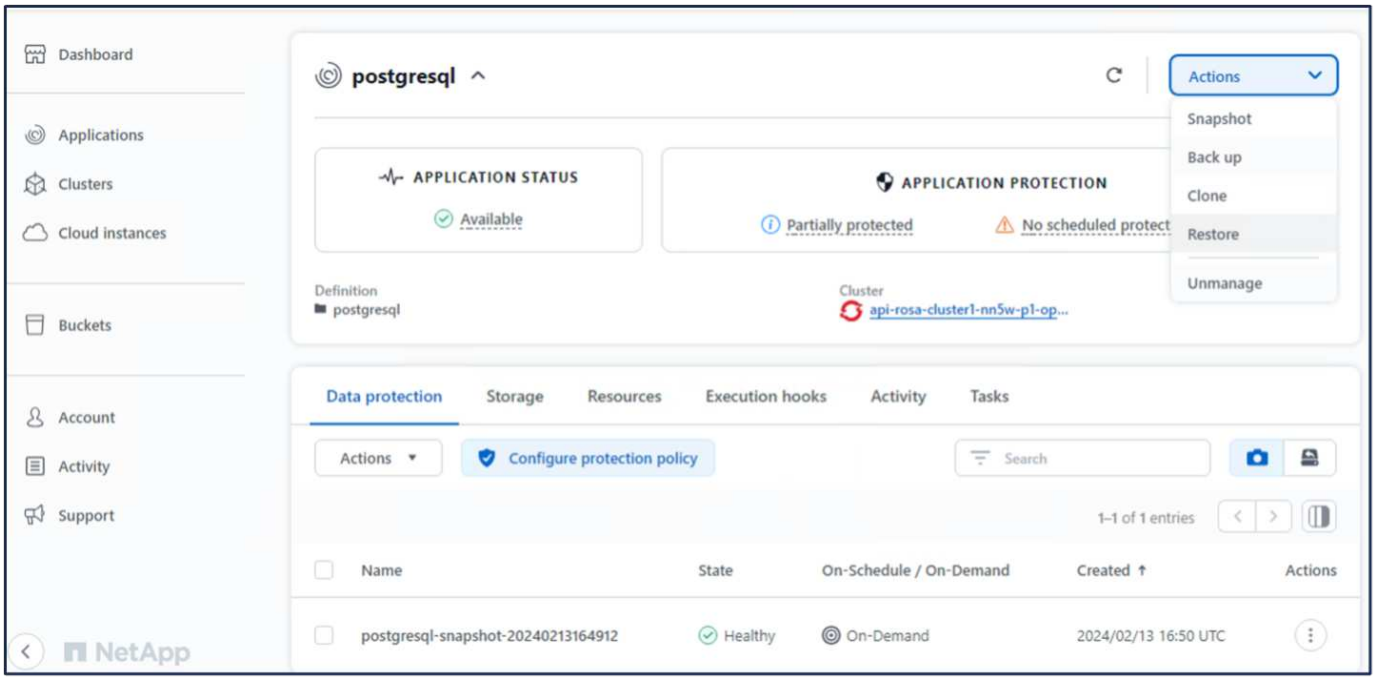
10. PostgreSQL 응용 프로그램에서 데이터베이스를 삭제합니다

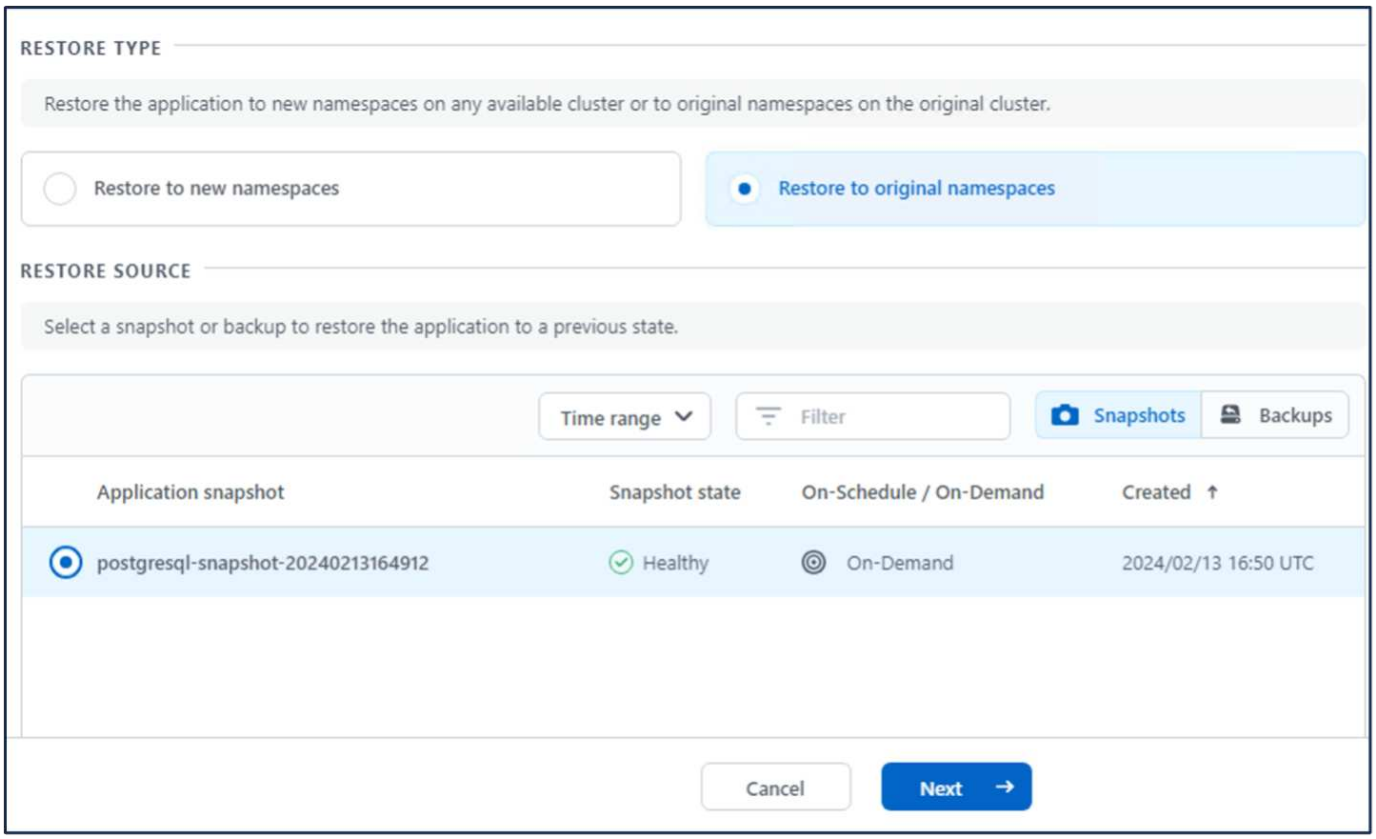
PostgreSQL에 다시 로그인하고 사용 가능한 데이터베이스를 나열한 다음 이전에 만든 데이터베이스를 삭제하고 다시 나열하여 데이터베이스가 삭제되었는지 확인합니다.

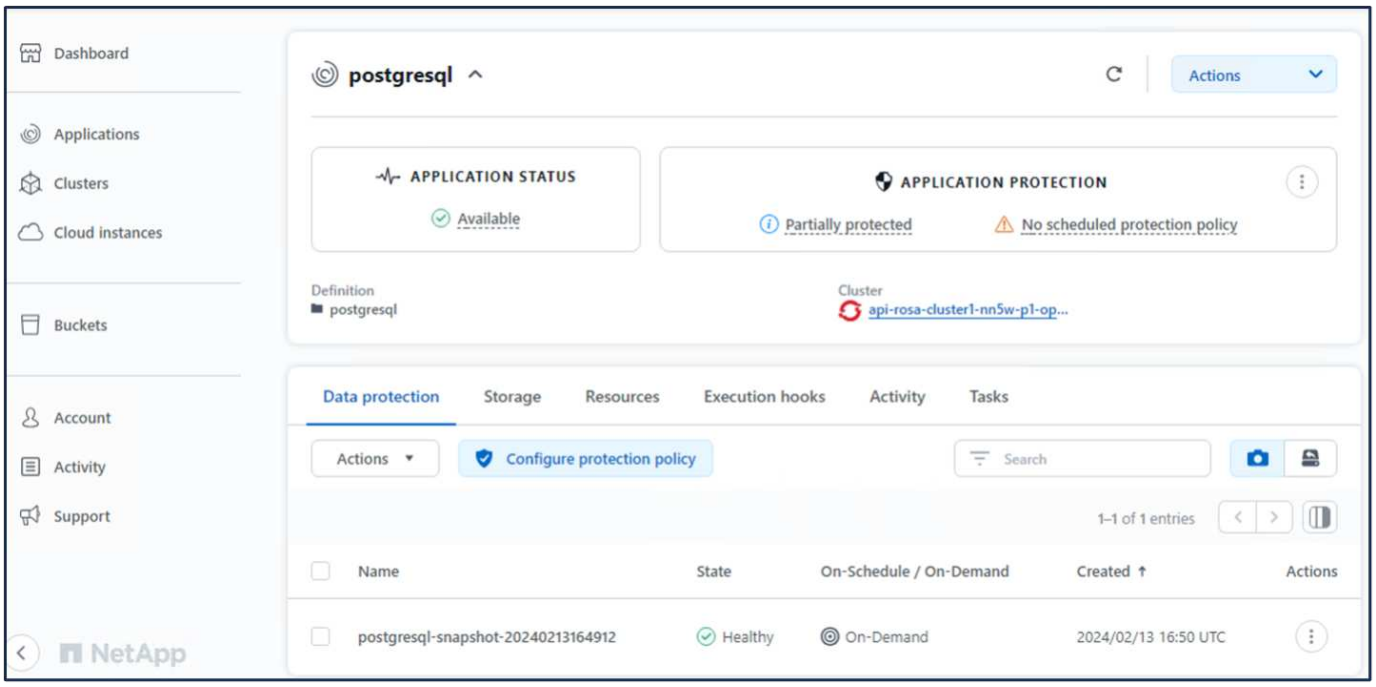
```
postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
-
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(4 rows)

postgres=# DROP DATABASE erp;
DROP DATABASE
postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
-
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(3 rows)
```

11. ACS를 사용하여 스냅샷에서 복원합니다

스냅샷에서 애플리케이션을 복원하려면 ACS UI 시작 페이지로 이동하여 애플리케이션을 선택하고 Restore(복원) 를 선택합니다. 복원할 스냅샷 또는 백업을 선택해야 합니다. (일반적으로 구성한 정책에 따라 여러 개의 를 생성할 수 있습니다.) 다음 두 화면에서 적절한 항목을 선택한 다음 * Restore * 를 클릭합니다. 스냅샷에서 복구된 후 애플리케이션 상태가 복원 중 에서 사용 가능 으로 이동합니다.







12. 앱이 스냅샷에서 복원되었는지 확인합니다

PostgreSQL 클라이언트에 로그인하면 이전에 사용했던 테이블과 레코드가 테이블에 표시됩니다. 이상입니다. 버튼을 클릭하기만 하면 프로그램이 이전 상태로 복원됩니다. Astra Control을 사용하는 고객은 이렇게 손쉽게 이용할 수 있습니다.

```
[ec2-user@ip-10-49-11-132 ~]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.
2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must set securityContext.allowPrivi
legeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (
pod or container "postgresql-client" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "postgresql-client" must set securityCon
text.seccompProfile.type to "RuntimeDefault" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access privileges
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-----------------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
(4 rows)

postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# \dt
         List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * from PERSONS;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```

Activate Windows

데이터 마이그레이션

이 페이지에는 영구 스토리지용 NetApp ONTAP용 FSx를 사용하는 관리형 Red Hat OpenShift 클러스터의 컨테이너 워크로드에 대한 데이터 마이그레이션 옵션이 나와 있습니다.

AWS의 Red Hat OpenShift 서비스와 NetApp FSxN(ONTAP)용 FSx는 AWS의 서비스 포트폴리오에 포함됩니다. FSxN은 단일 AZ 또는 Multi-AZ 옵션에서 사용할 수 있습니다. Multi-AZ 옵션은 가용성 영역 장애로부터 데이터를 보호합니다. FSxN을 Astra Trident와 통합하여 Rosa 클러스터의 애플리케이션에 영구 스토리지를 제공할 수 있습니다.

제어 차트를 사용하여 **FSxN**과 **Trident** 통합

Amazon FSx for ONTAP와 Rosa Cluster 통합

컨테이너 애플리케이션 마이그레이션에는 다음이 포함됩니다.

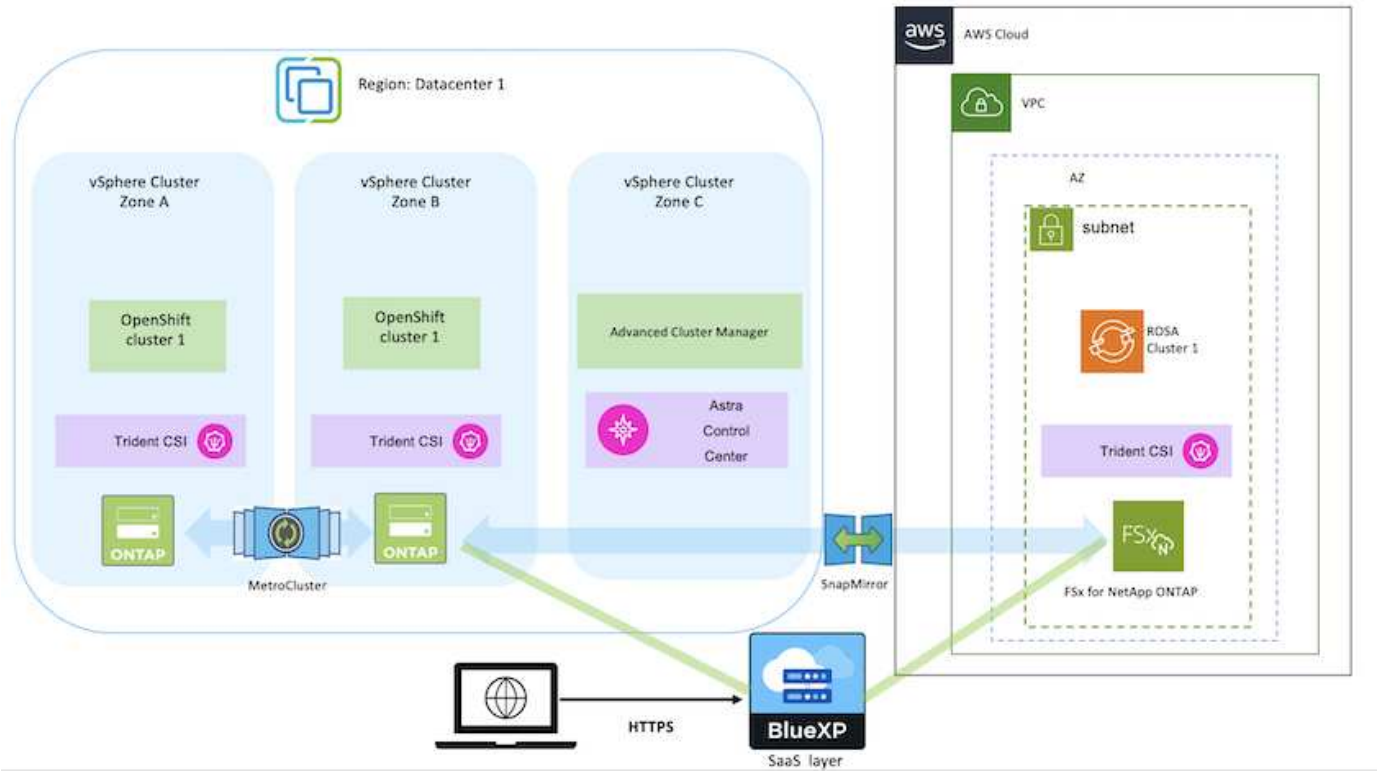
- 영구 볼륨: BlueXP를 사용하여 이 작업을 수행할 수 있습니다. 또 다른 옵션은 Astra Control Center를 사용하여 사내에서 클라우드 환경으로 컨테이너 애플리케이션 마이그레이션을 처리하는 것입니다. 자동화는 같은 용도로 사용할 수 있습니다.
- 애플리케이션 메타데이터: OpenShift GitOps(Argo CD)를 사용하여 이 작업을 수행할 수 있습니다.

영구 스토리지에 **FSxN**을 사용하여 **Rosa** 클러스터에서 애플리케이션의 페일오버 및 페일백

다음 비디오에서는 BlueXP 및 Argo CD를 사용한 애플리케이션 장애 조치 및 장애 복구 시나리오에 대해 설명합니다.

ROSA 클러스터에서 애플리케이션의 장애 조치 및 장애 복구

OpenShift Container 워크로드를 위한 데이터 보호 및 마이그레이션 솔루션



저작권 정보

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

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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