



vSphere 8용 NFS 참조 가이드

NetApp Solutions

NetApp
August 24, 2024

목차

vSphere 8용 NFS 3.1 참조 가이드	1
vSphere 8 및 ONTAP 스토리지 시스템에서 NFS 3.1 사용	1
기술 개요	1
NetApp 및 VMware의 NFS nConnect 기능	8
ONTAP 툴 10 을 사용하여 vSphere 8용 NFS 데이터 저장소를 구성합니다	12
NFS 데이터 저장소의 재해 복구에 VMware Site Recovery Manager를 사용합니다	42
NFS 스토리지에 대한 자율적 랜섬웨어 방어	68

vSphere 8용 NFS 3.1 참조 가이드

VMware VF(vSphere Foundation)는 다양한 가상화 워크로드를 제공할 수 있는 엔터프라이즈급 플랫폼입니다. vSphere의 핵심은 VMware vCenter, ESXi 하이퍼바이저, 네트워킹 구성 요소 및 다양한 리소스 서비스입니다. ONTAP와 함께 사용할 경우 VMware 기반 가상화 인프라는 뛰어난 유연성, 확장성 및 기능을 제공합니다.

vSphere 8 및 ONTAP 스토리지 시스템에서 NFS 3.1 사용

이 문서에서는 NetApp All-Flash 스토리지를 사용하여 VMware Cloud vSphere Foundation에서 사용할 수 있는 스토리지 옵션에 대한 정보를 제공합니다. 지원되는 스토리지 옵션은 NFS 데이터 저장소 구축에 대한 특정 지침에서 다룹니다. 또한 NFS 데이터 저장소의 재해 복구를 위한 VMware Live Site Recovery도 시연됩니다. 마지막으로 NetApp의 NFS 스토리지에 대한 자율적 랜섬웨어 방어 기능이 검토되었습니다.

사용 사례

이 문서에서 다루는 사용 사례:

- 프라이빗 클라우드와 퍼블릭 클라우드 모두에서 동일한 환경을 원하는 고객에게 알맞은 스토리지 옵션 제공
- 워크로드를 위한 가상 인프라 구축
- 컴퓨팅 리소스 요구사항에 직접 부합하지 않는 경우에도 변화하는 요구사항에 맞춰 조정할 수 있는 확장 가능한 스토리지 솔루션입니다.
- VMware vSphere용 SnapCenter 플러그인을 사용하여 VM 및 데이터 저장소를 보호합니다.
- NFS 데이터 저장소의 재해 복구를 위한 VMware Live Site Recovery 사용
- ESXi 호스트 및 게스트 VM 레벨의 다중 보호 계층을 포함한 랜섬웨어 감지 전략

대상

이 솔루션은 다음과 같은 사용자를 대상으로 합니다.

- TCO 극대화를 위해 설계된 VMware 환경을 위한 더욱 유연한 스토리지 옵션을 찾는 솔루션 설계자
- 주요 클라우드 공급자와 데이터 보호 및 재해 복구 옵션을 제공하는 VVF 스토리지 옵션을 찾는 솔루션 설계자
- NFS 스토리지를 사용하여 VVF를 구성하는 방법에 대한 구체적인 지침을 원하는 스토리지 관리자
- ONTAP 스토리지에 상주하는 VM 및 데이터 저장소를 보호하는 방법에 대한 구체적인 지침을 원하는 스토리지 관리자

기술 개요

vSphere 8용 NFS 3.1 VCF 참조 가이드는 다음과 같은 주요 구성 요소로 이루어져 있습니다.

VMware vSphere 기반

vSphere Foundation의 핵심 구성 요소인 VMware vCenter는 vSphere 환경의 구성, 제어 및 관리를 제공하는 중앙 집중식 관리 플랫폼입니다. vCenter는 가상 인프라 관리를 위한 기반으로 활용되므로 관리자가 가상 환경 내에서 VM,

컨테이너 및 ESXi 호스트를 구축, 모니터링 및 관리할 수 있습니다.

VVF 솔루션은 기본 Kubernetes 및 가상 머신 기반 워크로드를 모두 지원합니다. 주요 구성 요소는 다음과 같습니다.

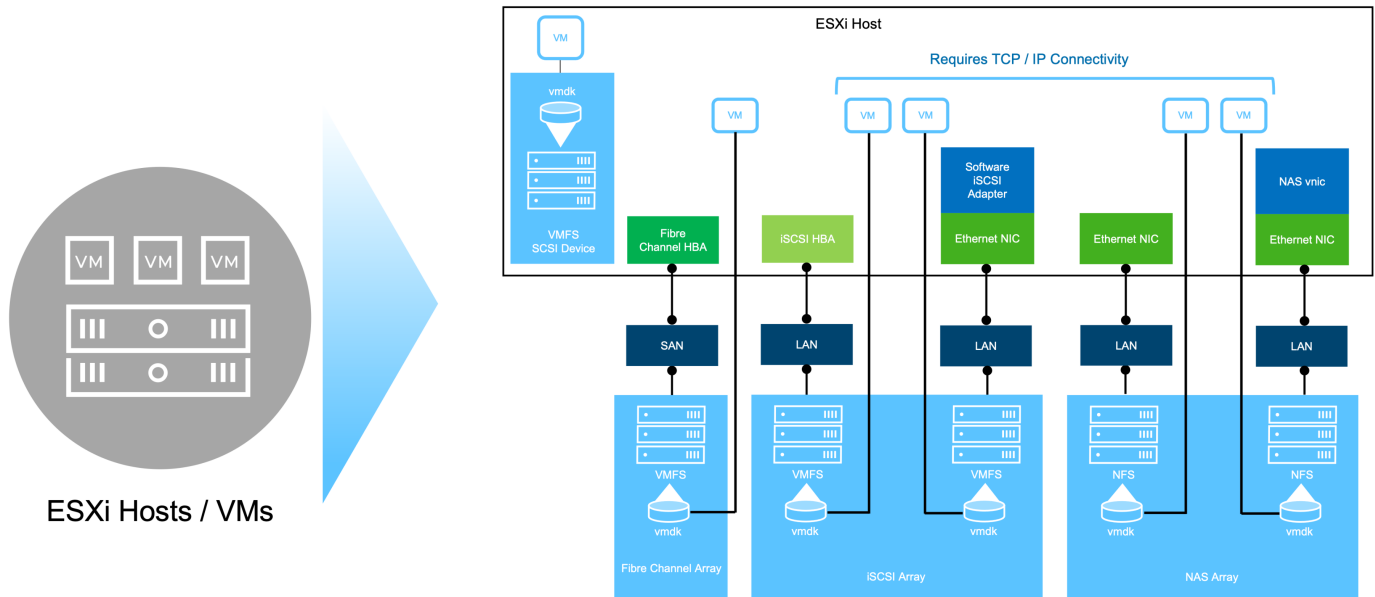
- VMware vSphere를 참조하십시오
- VMware vSAN을 선택합니다
- ARIA 표준
- vSphere용 VMware Tanzu Kubernetes Grid Service
- vSphere 분산 스위치

VF에 포함된 구성 요소에 대한 자세한 내용은 아키텍처 및 계획 을 참조하십시오. "[VMware vSphere 제품 실시간 비교](#)"

VVF 스토리지 옵션

성공적이고 강력한 가상 환경의 핵심은 스토리지입니다. VMware 데이터 저장소나 게스트 연결 활용 사례 중 어느 것을 사용하든 간에, 최상의 가치를 제공하는 GB당 가격을 선택할 수 있으므로 활용도가 낮을 수도 있습니다. ONTAP는 거의 20년 동안 VMware vSphere 환경을 위한 업계 최고의 스토리지 솔루션이며, 비용을 절감하면서 관리를 단순화하는 혁신적인 기능을 지속적으로 추가하고 있습니다.

VMware 스토리지 옵션은 일반적으로 기존 스토리지 및 소프트웨어 정의 스토리지 오퍼링으로 구성됩니다. 기존 스토리지 모델에는 로컬 및 네트워크 스토리지가 포함되며, 소프트웨어 정의 스토리지 모델에는 vSAN 및 VVol(VMware 가상 볼륨)이 포함됩니다.



<https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-storage/GUID-F602EB17-8D24-400A-9B05-196CEA66464F.html> ["vSphere 환경에서의 스토리지 소개"] VMware vSphere Foundation에서 지원되는 스토리지 유형에 대한 자세한 내용은 을 참조하십시오.

NetApp ONTAP를 참조하십시오

수많은 고객들이 vSphere의 운영 스토리지 솔루션으로 ONTAP을 선택한 데에는 수많은 이유가 있습니다. 여기에는 다음이 포함됩니다.

1. * 유니파이드 스토리지 시스템: * ONTAP는 SAN 및 NAS 프로토콜을 모두 지원하는 유니파이드 스토리지 시스템을 제공합니다. 이러한 다기능성을 통해 다양한 스토리지 기술을 단일 솔루션 내에 완벽하게 통합할 수 있습니다.
2. * 강력한 데이터 보호: * ONTAP는 공간 효율적인 스냅샷을 통해 강력한 데이터 보호 기능을 제공합니다. 이러한 스냅샷을 통해 백업 및 복구 프로세스를 효율적으로 수행할 수 있으므로 애플리케이션 데이터의 안전성과 무결성을 보장할 수 있습니다.
3. * 포괄적인 관리 도구: * ONTAP는 응용 프로그램 데이터를 효과적으로 관리할 수 있도록 설계된 다양한 도구를 제공합니다. 이러한 툴을 통해 스토리지 관리 작업이 간소화되므로 운영 효율성이 향상되고 관리가 단순화됩니다.
4. * 스토리지 효율성: * ONTAP에는 스토리지 활용도 최적화, 비용 절감 및 전체 시스템 성능 향상을 위해 기본적으로 지원되는 여러 가지 스토리지 효율성 기능이 포함되어 있습니다.

VMware와 함께 ONTAP를 사용하면 주어진 애플리케이션 요구 사항에 대해 뛰어난 유연성을 얻을 수 있습니다. 다음 프로토콜은 ONTAP * FCP * FCoE * NVMe/FC * NVMe/TCP * iSCSI * NFS v3 * NFS v4.1을 사용하는 VMware 데이터 저장소로 지원됩니다

하이퍼바이저와 별도로 스토리지 시스템을 사용하면 다양한 기능을 오프로드하고 vSphere 호스트 시스템에 대한 투자를 극대화할 수 있습니다. 이렇게 하면 호스트 리소스가 애플리케이션 워크로드에 집중되도록 할 뿐 아니라 스토리지 작업에서 애플리케이션에 미치는 랜덤 성능 영향을 방지할 수 있습니다.

ONTAP와 vSphere를 함께 사용하면 호스트 하드웨어 및 VMware 소프트웨어 비용을 절감할 수 있습니다. 또한 일관된 고성능을 통해 저렴한 비용으로 데이터를 보호할 수 있습니다. 가상화된 워크로드는 이동적이기 때문에 Storage vMotion을 사용하여 동일한 스토리지 시스템에서 VMFS, NFS 또는 VVol 데이터 저장소 간에 VM을 이동하는 다양한 접근 방식을 탐색할 수 있습니다.

NetApp All-Flash 어레이 를 참조하십시오

NetApp AFF(All Flash FAS)는 All-Flash 스토리지 어레이의 제품군입니다. 이 플랫폼은 엔터프라이즈 워크로드를 위한 고성능, 낮은 지연 시간의 스토리지 솔루션을 제공하도록 설계되었습니다. AFF 시리즈는 플래시 기술의 이점을 NetApp의 데이터 관리 기능과 결합하여 기업에 강력하고 효율적인 스토리지 플랫폼을 제공합니다.

AFF 제품군은 A-Series 모델과 C-Series 모델로 구성됩니다.

NetApp A-Series All-NVMe 플래시 어레이는 고성능 워크로드를 위해 설계되었으며, 매우 낮은 지연 시간과 높은 복원력을 제공하여 미션 크리티컬 애플리케이션에 적합합니다.

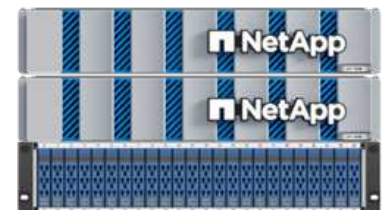
AFF A70



AFF A90



AFF A1K



C-Series QLC 플래시 어레이는 용량을 더 많이 사용하는 사례를 목표로 구축되었으며 하이브리드 플래시의 경제성과

플래시의 속도를 제공합니다.

AFF C250



AFF C400



AFF C800



스토리지 프로토콜 지원

AFF는 NFS, SMB, iSCSI, FC(파이버 채널), FCoE(Fibre Channel over Ethernet), NVMe over Fabrics, S3를 비롯한 가상화에 사용되는 모든 표준 프로토콜을 지원합니다. 고객은 워크로드 및 애플리케이션에 가장 적합한 항목을 자유롭게 선택할 수 있습니다.

- NFS * - NetApp AFF는 NFS를 지원하여 VMware 데이터 저장소의 파일 기반 액세스를 허용합니다. 여러 ESXi 호스트의 NFS 연결 데이터 저장소는 VMFS 파일 시스템에 적용되는 제한을 훨씬 초과합니다. vSphere와 함께 NFS를 사용하면 사용 편의성과 스토리지 효율성 측면에서 이점을 얻을 수 있습니다. ONTAP에는 NFS 프로토콜에 사용할 수 있는 파일 액세스 기능이 포함되어 있습니다. NFS 서버를 사용하도록 설정하고 볼륨 또는 qtree를 내보낼 수 있습니다.

NFS 구성에 대한 설계 지침은 ["NAS 스토리지 관리 설명서"](#) 참조하십시오.

- iSCSI * - NetApp AFF는 iSCSI에 대한 강력한 지원을 제공하여 IP 네트워크를 통해 스토리지 장치에 블록 수준 액세스를 허용합니다. iSCSI 이니시에이터와의 원활한 통합을 제공하여 iSCSI LUN의 효율적인 프로비저닝 및 관리를 지원합니다. 다중 경로, CHAP 인증 및 ALUA 지원과 같은 ONTAP의 고급 기능을 제공합니다.

iSCSI 구성에 대한 설계 지침은 ["SAN 구성 참조 설명서"](#) 참조하십시오.

- 파이버 채널 * - NetApp AFF는 SAN(Storage Area Network)에서 일반적으로 사용되는 고속 네트워크 기술인 파이버 채널(FC)에 대한 포괄적인 지원을 제공합니다. ONTAP는 FC 인프라와 원활하게 통합되어 스토리지 장치에 대한 안정적이고 효율적인 블록 레벨 액세스를 제공합니다. FC 환경에서 성능을 최적화하고 보안을 강화하고 원활한 연결을 보장하는 조닝, 다중 경로 지정 및 FLOGI(Fabric Login) 등의 기능을 제공합니다.

Fibre Channel 구성에 대한 설계 지침은 ["SAN 구성 참조 설명서"](#) 참조하십시오.

- NVMe over Fabrics * - NetApp ONTAP는 NVMe over Fabrics를 지원합니다. NVMe/FC를 사용하면 파이버 채널 인프라 및 스토리지 IP 네트워크를 통해 NVMe 스토리지 장치를 사용할 수 있습니다.

NVMe에 대한 설계 지침은 ["NVMe 구성, 지원 및 제한 사항"](#) 참조하십시오.

액티브-액티브 기술

NetApp All-Flash 어레이는 두 컨트롤러를 통해 액티브-액티브 경로를 허용하므로 호스트 운영 체제가 대체 경로를 활성화하기 전에 액티브 경로가 실패할 때까지 기다릴 필요가 없습니다. 즉, 호스트가 모든 컨트롤러에서 사용 가능한 경로를 모두 활용할 수 있으므로 시스템이 안정 상태에 있는지 또는 컨트롤러 페일오버 작업을 진행 중인지에 관계없이 활성 경로가 항상 존재하도록 보장합니다.

자세한 내용은 ["데이터 보호 및 재해 복구"](#) 설명서를 참조하십시오.

스토리지 보장

NetApp은 NetApp All-Flash Array에 고유한 스토리지 보장 세트를 제공합니다. 그 고유한 이점은 다음과 같습니다.

- 스토리지 효율성 보장: * 스토리지 효율성 보장으로 스토리지 비용을 최소화하면서 고성능을 달성하십시오. SAN 워크로드에서 4:1 * 랜섬웨어 복구 보장: * 랜섬웨어 공격 발생 시 데이터 복구를 보장합니다.

자세한 내용은 ["NetApp AFF 랜딩 페이지"](#) 참조하십시오.

VMware vSphere용 NetApp ONTAP 툴

vCenter의 강력한 구성 요소는 플러그인 또는 확장을 통합하여 기능을 더욱 강화하고 추가 기능을 제공하는 기능입니다. 이러한 플러그인을 사용하면 vCenter의 관리 기능이 확장되고 관리자가 타사 솔루션, 툴 및 서비스를 vSphere 환경에 통합할 수 있습니다.

NetApp ONTAP Tools for VMware는 vCenter 플러그인 아키텍처를 통해 VMware 환경 내에서 가상 머신 라이프사이클 관리를 용이하게 하도록 설계된 포괄적인 툴 제품군입니다. 이러한 툴은 VMware 에코시스템과 원활하게 통합되므로 데이터 저장소를 효율적으로 프로비저닝하고 가상 머신을 위한 필수 보호 기능을 제공할 수 있습니다. 관리자는 VMware vSphere용 ONTAP 툴을 사용하여 스토리지 라이프사이클 관리 작업을 간편하게 관리할 수 있습니다.

포괄적인 ONTAP 도구 10 리소스를 찾을 수 ["VMware vSphere용 ONTAP 툴 설명서 리소스"](#) 있습니다.

에서 ONTAP 툴 10 구축 솔루션을 확인하십시오 ["ONTAP 툴 10 을 사용하여 vSphere 8용 NFS 데이터 저장소를 구성합니다"](#)

VMware VAAI용 NetApp NFS 플러그인

NetApp NFS Plug-in for VAAI(vStorage API for Array Integration)는 특정 작업을 NetApp 스토리지 시스템으로 오프로드하여 스토리지 작업을 더욱 효율적으로 수행할 수 있도록 지원하기 때문에 성능 및 효율성이 향상됩니다. 여기에는 전체 복제, 블록 제로화 및 하드웨어 지원 잠금 등의 작업이 포함됩니다. 또한 VAAI 플러그인은 가상 머신 프로비저닝 및 클론 생성 작업 중에 네트워크를 통해 전송되는 데이터의 양을 줄여 스토리지 활용도를 최적화합니다.

VAAI용 NetApp NFS 플러그인은 NetApp 지원 사이트에서 다운로드할 수 있으며 VMware vSphere용 ONTAP 툴을 사용하여 ESXi 호스트에 업로드 및 설치됩니다.

자세한 내용은 ["VMware VAAI용 NetApp NFS 플러그인 설명서"](#) 참조하십시오.

VMware vSphere용 SnapCenter 플러그인

SCV(VMware vSphere)용 SnapCenter 플러그인은 VMware vSphere 환경에 포괄적인 데이터 보호를 제공하는 NetApp의 소프트웨어 솔루션입니다. 이 솔루션은 VM(가상 머신) 및 데이터 저장소를 보호하고 관리하는 프로세스를 간소화하고 간소화하도록 설계되었습니다. SCV는 저장소 기반 스냅샷 및 보조 스토리지에 대한 복제를 사용하여 복구 시간 목표를 줄입니다.

VMware vSphere용 SnapCenter 플러그인은 vSphere Client와 통합된 유니파이드 인터페이스에서 다음과 같은 기능을 제공합니다.

- 정책 기반 스냅샷 * - SnapCenter를 사용하면 VMware vSphere에서 가상 머신(VM)의 애플리케이션 정합성 보장 스냅샷을 생성하고 관리하기 위한 정책을 정의할 수 있습니다.
- 자동화 * - 정의된 정책에 기반한 자동 스냅샷 생성 및 관리는 일관되고 효율적인 데이터 보호를 보장합니다.

- VM 레벨 보호 * - VM 레벨의 세분화된 보호를 통해 개별 가상 머신을 효율적으로 관리하고 복구할 수 있습니다.
- 스토리지 효율성 기능 * - NetApp 스토리지 기술과의 통합은 스냅샷을 위한 중복 제거 및 압축과 같은 스토리지 효율성 기능을 제공하여 스토리지 요구 사항을 최소화합니다.

SnapCenter 플러그인은 NetApp 스토리지 시스템의 하드웨어 기반 스냅샷과 함께 가상 시스템의 정지를 조정합니다. SnapMirror 기술을 사용하여 백업 복사본을 클라우드를 포함한 2차 스토리지 시스템으로 복제합니다.

자세한 내용은 를 참조하십시오 "[VMware vSphere용 SnapCenter 플러그인 설명서](#)".

BlueXP 통합을 통해 데이터 복사본을 클라우드의 오브젝트 스토리지로 확장하는 3-2-1 백업 전략을 지원합니다.

BlueXP를 이용하는 3-2-1 백업 전략에 대한 자세한 내용은 를 참조하십시오 "[VM용 SnapCenter 플러그인 및 BlueXP 백업 및 복구를 통한 VMware용 3-2-1 데이터 보호](#)".

SnapCenter 플러그인의 단계별 배포 지침은 솔루션을 참조하십시오 "[VMware vSphere용 SnapCenter 플러그인을 사용하여 VCF 워크로드 도메인의 VM을 보호할 수 있습니다](#)".

스토리지 고려 사항

ONTAP NFS 데이터 저장소를 VMware vSphere와 함께 활용하면 블록 기반 스토리지 프로토콜에서 얻을 수 없는 VM-데이터 저장소 비율을 제공하는, 성능이 뛰어나고 관리가 용이하며 확장 가능한 환경을 구축할 수 있습니다. 이 아키텍처에서는 데이터 저장소 밀도가 10배 증가하는 동시에 데이터 저장소 수가 감소할 수 있습니다.

- nNFS용 연결: * nConnect * 기능을 활용할 수 있다는 또 다른 이점은 * nConnect * 기능을 활용하는 것입니다. nConnect는 NFS v3 데이터 저장소 볼륨에 대해 여러 TCP 연결을 지원하여 처리량을 증가시킵니다. 이렇게 하면 NFS 데이터 저장소의 병렬 처리 수를 늘릴 수 있습니다. NFS 버전 3을 사용하여 데이터 저장소를 구축하는 고객은 NFS 서버에 대한 연결 수를 늘려 고속 네트워크 인터페이스 카드의 활용도를 극대화할 수 있습니다.

nConnect에 대한 자세한 내용은 을 "[VMware 및 NetApp의 NFS nConnect 기능](#)"참조하십시오.

- NFS용 세션 트렁킹: * ONTAP 9.14.1부터 NFSv4.1을 사용하는 클라이언트는 세션 트렁킹을 활용하여 NFS 서버의 다양한 LIF에 대한 다중 연결을 설정할 수 있습니다. 이렇게 하면 다중 경로를 사용하여 데이터 전송 속도를 높이고 복원력을 향상시킬 수 있습니다. 트렁킹은 VMware 및 Linux 클라이언트와 같이 트렁킹을 지원하는 클라이언트로 FlexVol 볼륨을 내보내거나 RDMA, TCP 또는 pNFS 프로토콜을 통해 NFS를 사용할 때 특히 유용합니다.

자세한 내용은 을 "[NFS 트렁킹 개요](#)" 참조하십시오.

- FlexVol volumes: * NetApp는 대부분의 NFS 데이터 저장소에 * FlexVol * 볼륨을 사용할 것을 권장합니다. 데이터 저장소의 크기는 스토리지 효율성과 운영상의 이점을 강화할 수 있지만, 단일 ONTAP 컨트롤러에 VM을 저장하려면 4개 이상의 데이터 저장소(FlexVol 볼륨)를 사용하는 것이 좋습니다. 일반적으로 관리자는 4TB~8TB 용량의 FlexVol 볼륨을 지원하는 데이터 저장소를 구축합니다. 이 크기는 성능, 관리 용이성, 데이터 보호 간의 균형을 잘 유지합니다. 관리자는 작게 시작하여 필요에 따라 데이터 저장소를 확장할 수 있습니다(최대 100TB). 데이터 저장소가 작을수록 백업 또는 재해를 빠르게 복구할 수 있으며 클러스터 전체에서 민첩하게 이동할 수 있습니다. 이 방식을 사용하면 하드웨어 리소스의 성능 활용도를 극대화할 수 있고 복구 정책이 서로 다른 데이터 저장소를 사용할 수 있습니다.
- FlexGroup volumes: * 대용량 데이터 저장소가 필요한 경우에는 NetApp * FlexGroup * 볼륨을 사용하는 것이 좋습니다. FlexGroup 볼륨의 용량 또는 파일 수 제한이 거의 없으므로 관리자가 대규모 단일 네임스페이스를 쉽게 프로비저닝할 수 있습니다. FlexGroup 볼륨을 사용하더라도 추가적인 유지보수 또는 관리 오버헤드가 발생하지 않습니다. FlexGroup 볼륨의 성능에는 기본적으로 확장되므로 여러 데이터 저장소가 필요하지 않습니다. ONTAP 및 FlexGroup 볼륨을 VMware vSphere와 함께 활용하면 전체 ONTAP 클러스터의 성능을 최대한 활용하는, 간단하고 확장 가능한 데이터 저장소를 구축할 수 있습니다.

랜섬웨어 보호

NetApp ONTAP 데이터 관리 소프트웨어는 랜섬웨어 공격을 보호, 탐지 및 복구하는 데 도움이 되는 포괄적인 통합 기술 제품군을 갖추고 있습니다. ONTAP에 내장된 NetApp SnapLock Compliance 기능은 고급 데이터 보존과 함께 WORM(Write Once, Read Many) 기술을 사용하여 지원 볼륨에 저장된 데이터를 삭제하는 것을 방지합니다. 보존 기간이 설정되고 스냅샷 복사본이 잠긴 후에는 전체 시스템 Privileges를 사용하는 스토리지 관리자나 NetApp Support 팀의 구성원이 스냅샷 복사본을 삭제할 수 없습니다. 하지만 더 중요한 것은 손상된 자격 증명을 가진 해커가 데이터를 삭제할 수 없다는 것입니다.

NetApp은 적격 어레이에서 보호되는 NetApp® Snapshot™ 복사본을 복구할 수 있음을 보장하며, 그렇지 못할 경우 조직에 보상을 제공합니다.

랜섬웨어 복구 보장에 대한 자세한 내용은 다음을 "[Ransomware 복구 보증](#)" 참조하십시오.

<https://docs.netapp.com/us-en/ontap/anti-ransomware/> ["[자율 랜섬웨어 보호 개요](#)"] 자세한 내용은 를 참조하십시오.

NetApps 솔루션 설명서 센터에서 전체 솔루션을 참조하십시오. "[NFS 스토리지에 대한 자율적 랜섬웨어 방어](#)"

재해 복구 고려 사항

NetApp은 지구상에서 가장 안전한 스토리지를 제공합니다. NetApp을 사용하면 데이터 및 애플리케이션 인프라를 보호하고 온프레미스 스토리지와 클라우드 간에 데이터를 이동하며 클라우드 전반에서 데이터 가용성을 보장할 수 있습니다. ONTAP은 강력한 데이터 보호 및 보안 기술을 함께 제공하여 위협을 능동적으로 감지하고 데이터와 애플리케이션을 신속하게 복구하여 재해로부터 고객을 보호합니다.

- VMware Live Site Recovery * (이전 명칭: VMware Site Recovery Manager)는 vSphere 웹 클라이언트 내에서 가상 머신을 보호하기 위한 간소화된 정책 기반 자동화 기능을 제공합니다. 이 솔루션은 VMware용 ONTAP 툴의 일부로 스토리지 복제 어댑터를 통해 NetApp의 고급 데이터 관리 기술을 활용합니다. VMware 환경은 어레이 기반 복제를 위한 NetApp SnapMirror의 기능을 활용함으로써 ONTAP의 가장 안정적이고 성숙한 기술 중 하나를 활용할 수 있습니다. SnapMirror는 전체 VM 또는 데이터 저장소가 아닌 변경된 파일 시스템 블록만 복사하여 안전하고 효율적인 데이터 전송을 보장합니다. 또한 이러한 블록은 중복제거, 압축, 컴팩션과 같은 공간 절약 기술을 활용합니다. 최신 ONTAP 시스템에 버전에 상관없이 SnapMirror가 도입됨에 따라 소스 클러스터와 타겟 클러스터를 유연하게 선택할 수 있습니다. SnapMirror는 재해 복구를 위한 강력한 도구로 부각되었으며, 라이브 사이트 복구와 함께 사용할 경우 로컬 스토리지 대안에 비해 향상된 확장성, 성능 및 비용 절감 효과를 제공합니다.

자세한 내용은 를 "[VMware Site Recovery Manager 개요](#)" 참조하십시오.

NetApps 솔루션 설명서 센터에서 전체 솔루션을 참조하십시오. "[NFS 스토리지에 대한 자율적 랜섬웨어 방어](#)"

- NFS용 BlueXP DRaaS * (서비스형 재해 복구)는 NFS 데이터 저장소가 있는 온프레미스 ONTAP 시스템에서 실행되는 VMware 워크로드를 위해 설계된 비용 효율적인 재해 복구 솔루션입니다. NetApp SnapMirror 복제를 활용하여 사이트 중단 및 랜섬웨어 공격과 같은 데이터 손상을 방지합니다. NetApp BlueXP 콘솔과 통합된 이 서비스를 통해 VMware vCenter 및 ONTAP 스토리지를 손쉽게 관리하고 자동으로 검색할 수 있습니다. 조직은 블록 레벨 복제를 통해 최대 5분 RPO(복구 시점 목표)를 달성하여 재해 복구 계획을 생성 및 테스트할 수 있습니다. BlueXP DRaaS는 프로덕션 리소스에 영향을 주지 않으면서 공간 효율적인 테스트를 위해 ONTAP의 FlexClone 기술을 활용합니다. 이 서비스는 장애 조치 및 장애 복구 프로세스를 조정하므로 최소한의 노력으로 보호된 가상 시스템을 지정된 재해 복구 사이트에 가져올 수 있습니다. BlueXP DRaaS는 널리 알려진 다른 대안과 비교하여 이러한 기능을 매우 적은 비용으로 제공하므로 조직에서 ONTAP 스토리지 시스템을 사용하여 VMware 환경의 재해 복구 작업을 설정, 테스트 및 실행할 수 있는 효율적인 솔루션입니다.

NetApps 솔루션 설명서 센터에서 전체 솔루션을 참조하십시오. ["NFS 데이터 저장소용 BlueXP DRaaS를 사용하는 DR"](#)

솔루션 개요

이 설명서에서 다루는 솔루션:

- * NetApp 및 VMware * 를 통한 NFS nConnect 기능 ["* 여기 *"](#) 배포 단계를 보려면 클릭하십시오.
 - * ONTAP 톨 10 을 사용하여 vSphere 8용 NFS 데이터 저장소를 구성합니다 . [" 여기 *"](#) 배포 단계를 보려면 클릭하십시오.
 - * VMware vSphere용 SnapCenter 플러그인을 구축 및 사용하여 VM 보호 및 복원 . [" 여기 *"](#) 배포 단계를 보려면 클릭하십시오.
 - * VMware Site Recovery Manager * 를 사용한 NFS 데이터 저장소 재해 복구 ["* 여기 *"](#) 배포 단계를 보려면 클릭하십시오.
 - * NFS 스토리지를 위한 자율적 랜섬웨어 방어 . [" 여기 *"](#) 배포 단계를 보려면 클릭하십시오.

NetApp 및 VMware의 NFS nConnect 기능

VMware vSphere 8.0 U1(Tech-preview)부터 nconnect 기능을 사용하면 NFS v3 데이터 저장소 볼륨에 대해 여러 TCP 연결을 활성화하여 처리량을 늘릴 수 있습니다. NFS 데이터 저장소를 사용하는 고객은 이제 NFS 서버에 대한 연결 수를 늘려 고속 네트워크 인터페이스 카드의 활용도를 극대화할 수 있습니다.



이 기능은 일반적으로 8.0 U2가 설치된 NFS v3에서 사용할 수 있습니다. 의 스토리지 섹션을 참조하십시오. ["VMware vSphere 8.0 Update 2 릴리즈 노트"](#) vSphere 8.0 U3에 NFS v4.1 지원이 추가되었습니다. 자세한 내용은 을 참조하십시오 ["vSphere 8.0 업데이트 3 릴리즈 노트"](#)

사용 사례

- 동일한 호스트에서 NFS 데이터 저장소당 더 많은 가상 머신을 호스팅합니다.
- NFS 데이터 저장소 성능 향상
- VM 및 컨테이너 기반 애플리케이션에 대해 상위 계층에서 서비스를 제공하는 옵션을 제공합니다.

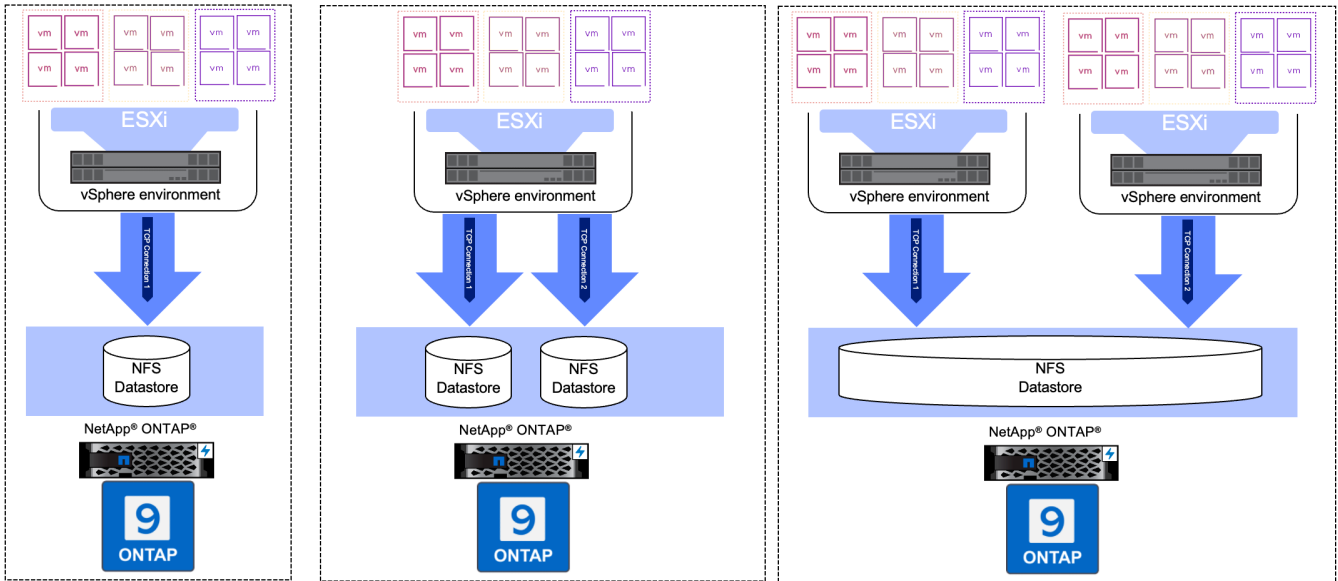
기술 세부 정보

nconnect의 목적은 vSphere 호스트의 NFS 데이터 저장소당 여러 TCP 연결을 제공하는 것입니다. 이렇게 하면 NFS 데이터 저장소의 병렬 처리 수와 성능을 높일 수 있습니다. ONTAP에서 NFS 마운트가 설정되면 CID(연결 ID)가 생성됩니다. 이 CID는 최대 128개의 동시 전송 작업을 제공합니다. 클라이언트에서 이 수를 초과하면 ONTAP는 다른 작업이 완료될 때 사용 가능한 일부 리소스를 확보할 수 있을 때까지 흐름 제어 형식을 실행합니다. 이러한 일시 중지는 일반적으로 몇 마이크로초일 뿐이지만, 수백만 번의 작업이 진행되는 동안 작동이 중지되면 그로 인해 성능 문제가 발생할 수 있습니다. nConnect는 128의 제한을 받고 이 제한에 클라이언트의 nconnect 세션 수를 곱할 수 있습니다. 그러면 CID당 더 많은 동시 작업이 제공되고 성능이 향상될 수 있습니다. 자세한 내용은 를 참조하십시오 ["NFS 모범 사례 및 구축 가이드"](#)

기본 NFS 데이터 저장소입니다

NFS 데이터 저장소의 단일 접속의 성능 제한을 해결하기 위해 추가 데이터 저장소가 마운트되거나 추가 호스트가 추가되어 연결이 증가합니다.

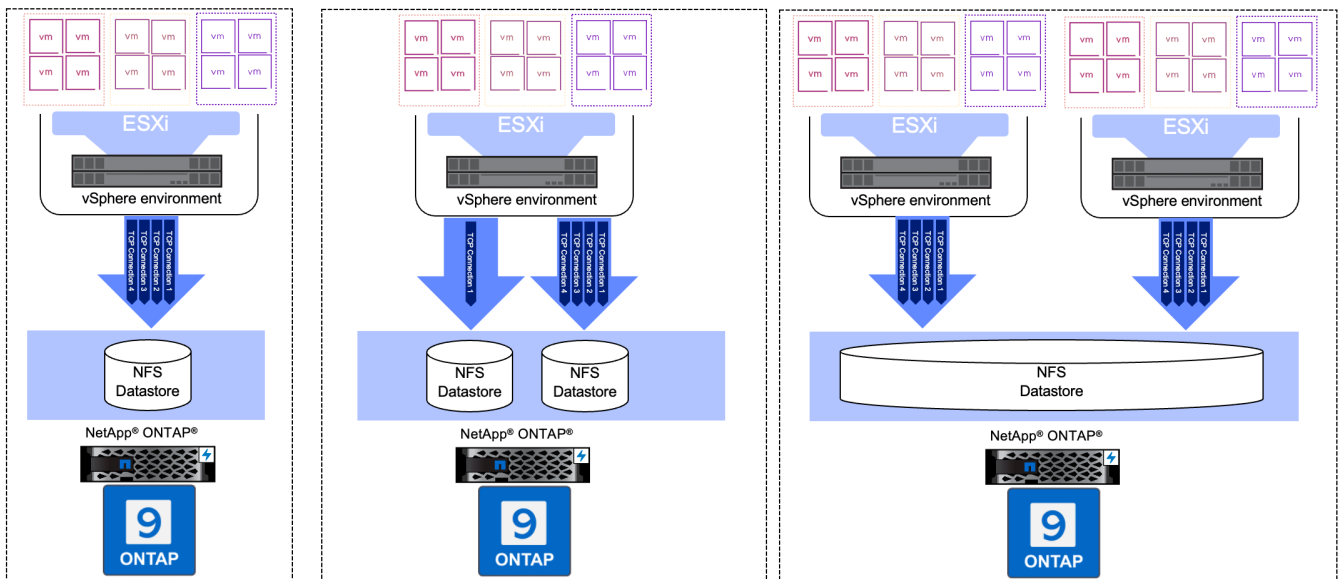
Without nConnect feature with NetApp and VMware



nConnect NFS 데이터 저장소 사용

ONTAP 툴 또는 다른 옵션을 사용하여 NFS 데이터 저장소를 생성한 후에는 vSphere CLI, PowerCLI, govc 툴 또는 기타 API 옵션을 사용하여 NFS 데이터 저장소당 연결 수를 수정할 수 있습니다. vMotion과 함께 성능 문제를 방지하려면 vSphere 클러스터에 포함된 모든 vSphere 호스트의 NFS 데이터 저장소에 대한 연결 수를 동일하게 유지해야 합니다.

With nConnect feature with NetApp and VMware



전제 조건

nconnect 기능을 사용하려면 다음 종속성을 충족해야 합니다.

ONTAP 버전	vSphere 버전	설명
9.8 이상	8 업데이트 1	연결 수를 늘리는 옵션이 있는 기술 미리 보기
9.8 이상	8 업데이트 2	일반적으로 연결 수를 늘리거나 줄이는 옵션과 함께 사용할 수 있습니다.
9.8 이상	8 업데이트 3	NFS 4.1 및 다중 경로 지원

NFS 데이터 저장소에 대한 연결 수를 업데이트합니다

단일 TCP 연결은 ONTAP 툴 또는 vCenter를 사용하여 NFS 데이터 저장소를 생성할 때 사용됩니다. 연결 수를 늘리기 위해 vSphere CLI를 사용할 수 있습니다. 참조 명령은 다음과 같습니다.

```
# Increase the number of connections while creating the NFS v3 datastore.
esxcli storage nfs add -H <NFS_Server_FQDN_or_IP> -v <datastore_name> -s
<remote_share> -c <number_of_connections>
# To specify the number of connections while mounting the NFS 4.1
datastore.
esxcli storage nfs41 add -H <NFS_Server_FQDN_or_IP> -v <datastore_name> -s
<remote_share> -c <number_of_connections>
# To utilize specific VMkernel adapters while mounting, use the -I switch
esxcli storage nfs41 add -I <NFS_Server_FQDN_or_IP>:vmk1 -I
<NFS_Server_FQDN_or_IP>:vmk2 -v <datastore_name> -s <remote_share> -c
<number_of_connections>
# To increase or decrease the number of connections for existing NFSv3
datastore.
esxcli storage nfs param set -v <datastore_name> -c
<number_of_connections>
# For NFSv4.1 datastore
esxcli storage nfs41 param set -v <datastore_name> -c
<number_of_connections>
# To set VMkernel adapter for an existing NFS 4.1 datastore
esxcli storage nfs41 param set -I <NFS_Server_FQDN_or_IP>:vmk2 -v
<datastore_name> -c <number_of_connections>
```

또는 아래 그림과 유사한 PowerCLI를 사용하십시오

```

$datastoreSys = Get-View (Get-VMHost host01.vsphere.local).ExtensionData
.ConfigManager.DatastoreSystem
$nfSpec = New-Object VMware.Vim.HostNasVolumeSpec
$nfSpec.RemoteHost = "nfs_server.ontap.local"
$nfSpec.RemotePath = "/DS01"
$nfSpec.LocalPath = "DS01"
$nfSpec.AccessMode = "readWrite"
$nfSpec.Type = "NFS"
$nfSpec.Connections = 4
$datastoreSys.CreateNasDatastore($nfSpec)

```

다음은 govc 도구에 대한 연결 수를 증가시키는 예입니다.

```

$env.GOVc_URL = 'vcenter.vsphere.local'
$env.GOVc_USERNAME = 'administrator@vsphere.local'
$env.GOVc_PASSWORD = 'XXXXXXXXXX'
$env.GOVc_Datastore = 'DS01'
# $env.GOVc_INSECURE = 1
$env.GOVc_HOST = 'host01.vsphere.local'
# Increase number of connections while creating the datastore.
govc host.esxcli storage nfs add -H nfs_server.ontap.local -v DS01 -s
/DS01 -c 2
# For NFS 4.1, replace nfs with nfs41
govc host.esxcli storage nfs41 add -H <NFS_Server_FQDN_or_IP> -v
<datastore_name> -s <remote_share> -c <number_of_connections>
# To utilize specific VMkernel adapters while mounting, use the -I switch
govc host.esxcli storage nfs41 add -I <NFS_Server_FQDN_or_IP>:vmk1 -I
<NFS_Server_FQDN_or_IP>:vmk2 -v <datastore_name> -s <remote_share> -c
<number_of_connections>
# To increase or decrease the connections for existing datastore.
govc host.esxcli storage nfs param set -v DS01 -c 4
# For NFSv4.1 datastore
govc host.esxcli storage nfs41 param set -v <datastore_name> -c
<number_of_connections>
# View the connection info
govc host.esxcli storage nfs list

```

을 참조하십시오 "VMware 기술 자료 문서 91497" 를 참조하십시오.

설계 고려 사항

ONTAP에서 지원되는 최대 연결 수는 스토리지 플랫폼 모델에 따라 다릅니다. 에서 Exec_CTX를 찾습니다 "NFS 모범 사례 및 구축 가이드" 를 참조하십시오.

NFSv3 데이터 저장소당 연결 수가 증가하면 해당 vSphere 호스트에 마운트할 수 있는 NFS 데이터 저장소의 수가 감소합니다. vSphere 호스트당 지원되는 총 연결 수는 256개입니다. 확인합니다 "[VMware 기술 자료 문서 91481](#)" vSphere 호스트당 데이터 저장소 제한이 있는 경우



VVOL 데이터 저장소는 nConnect 기능을 지원하지 않습니다. 그러나 프로토콜 엔드포인트는 연결 한도에 카운트됩니다. VVOL 데이터 저장소가 생성될 때 SVM의 각 데이터 lif에 대해 프로토콜 엔드포인트가 생성됩니다.

ONTAP 툴 10 을 사용하여 vSphere 8용 NFS 데이터 저장소를 구성합니다

ONTAP 툴 10 을 사용하여 vSphere 8용 NFS 데이터 저장소를 구성합니다

VMware vSphere 10용 ONTAP 툴은 VASA 공급자(iSCSI 및 NFS VVOL 지원)를 위한 기본 고가용성 및 확장성을 지원하는 차세대 아키텍처를 제공합니다. 따라서 여러 VMware vCenter Server 및 ONTAP 클러스터의 관리가 간소화됩니다.

이 시나리오에서는 VMware vSphere 10용 ONTAP 툴을 구축 및 사용하고 vSphere 8용 NFS 데이터 저장소를 구성하는 방법을 보여 줍니다.

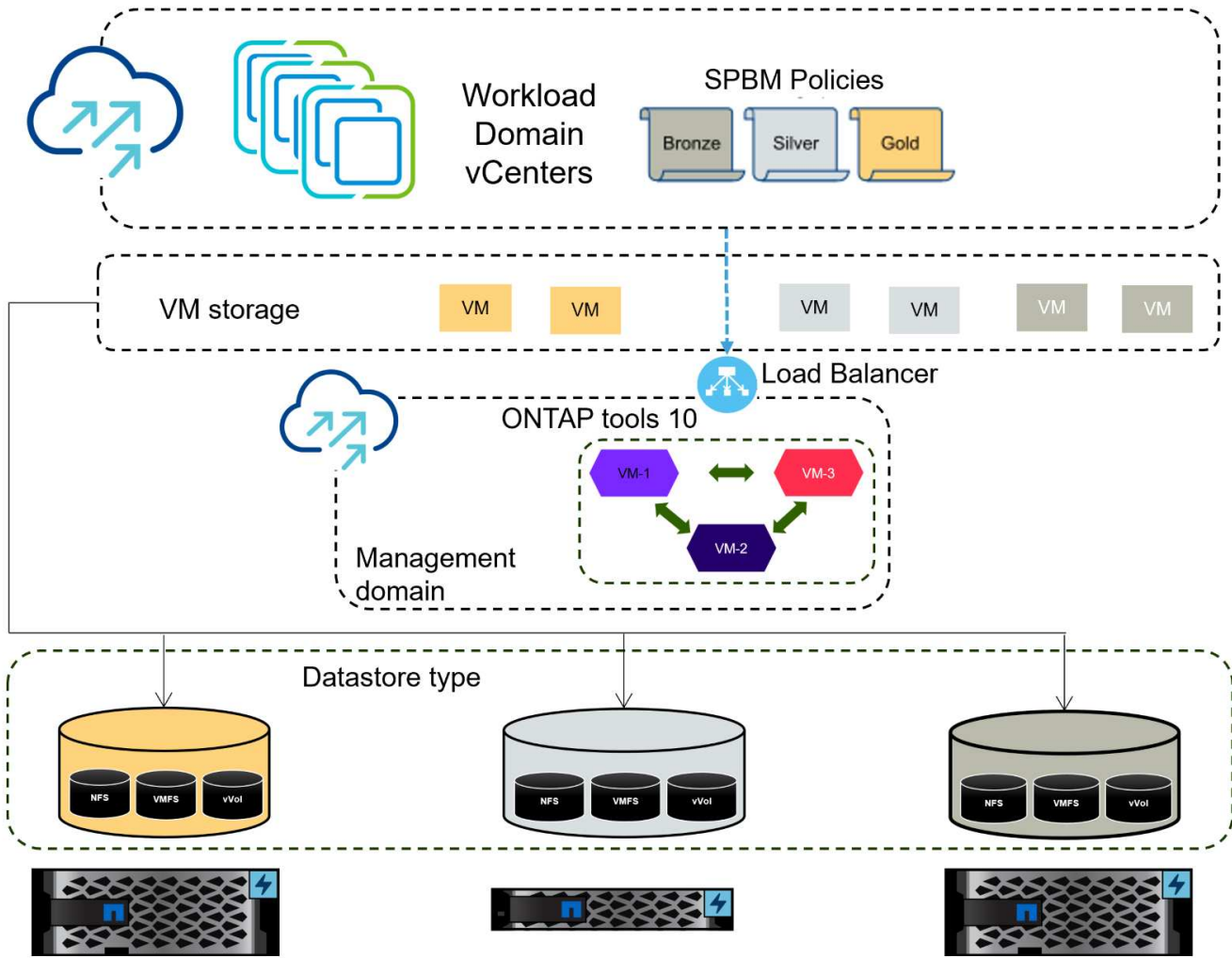
솔루션 개요

이 시나리오에서는 다음과 같은 상위 단계를 다룹니다.

- NFS 트래픽에 논리 인터페이스(LIF)를 사용하여 SVM(스토리지 가상 머신)을 생성합니다.
- vSphere 8 클러스터에서 NFS 네트워크에 대한 분산 포트 그룹을 생성합니다.
- vSphere 8 클러스터의 ESXi 호스트에서 NFS용 vmkernel 어댑터를 생성합니다.
- ONTAP 툴 10 을 구축하고 vSphere 8 클러스터에 등록합니다.
- vSphere 8 클러스터에 새 NFS 데이터 저장소를 생성합니다.

있습니다

다음 다이어그램은 VMware vSphere 10 구축용 ONTAP 툴의 아키텍처 구성 요소를 보여 줍니다.



필수 구성 요소

이 솔루션에는 다음과 같은 구성 요소 및 구성이 필요합니다.

- 스토리지 트래픽 전용 이더넷 스위치에 물리적 데이터 포트가 있는 ONTAP AFF 스토리지 시스템
- vSphere 8 클러스터 구축이 완료되었으며 vSphere Client에 액세스할 수 있습니다.
- VMware vSphere 10 OVA 템플릿용 ONTAP 툴이 NetApp 지원 사이트에서 다운로드되었습니다.

NetApp은 NFS에 대한 이중 네트워크 설계를 추천하여 스토리지 시스템, 스위치, 네트워크 어댑터 및 호스트 시스템에 대한 내결함성을 제공합니다. 아키텍처 요구 사항에 따라 단일 서브넷이나 여러 서브넷으로 NFS를 구축하는 것이 일반적입니다.

을 참조하십시오 ["VMware vSphere에서 NFS를 실행하는 모범 사례"](#) VMware vSphere에 대한 자세한 내용은

ONTAP를 VMware vSphere와 함께 사용하는 방법에 대한 네트워크 지침은 을 참조하십시오 ["네트워크 구성 - NFS"](#) 섹션을 NetApp 참조하십시오.

포괄적인 ONTAP 도구 10 리소스를 찾을 수 ["VMware vSphere용 ONTAP 툴 설명서 리소스"](#) 있습니다.

배포 단계

ONTAP 툴 10 을 구축하고 이 툴을 사용하여 VCF 관리 도메인에 NFS 데이터 저장소를 생성하려면 다음 단계를 완료합니다.

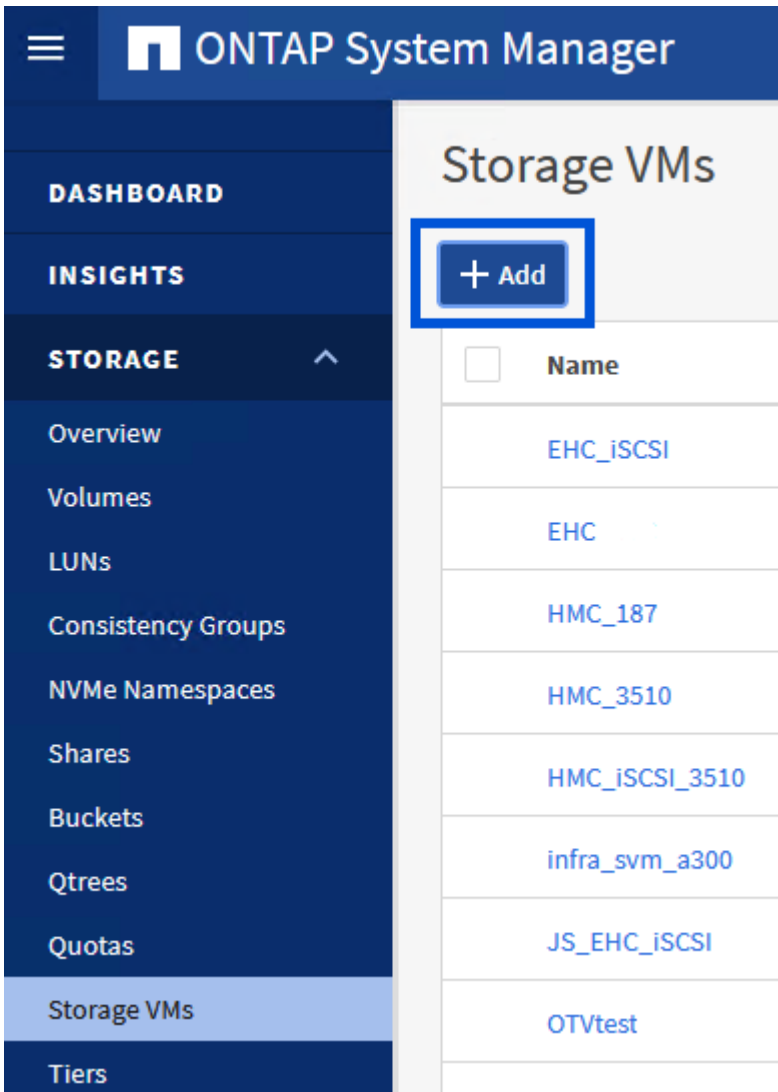
ONTAP 스토리지 시스템에서 **SVM** 및 **LIF**를 생성합니다

다음 단계는 ONTAP System Manager에서 수행합니다.

스토리지 VM 및 LIF를 생성합니다

NFS 트래픽용 여러 LIF와 함께 SVM을 생성하려면 다음 단계를 완료하십시오.

1. ONTAP 시스템 관리자에서 왼쪽 메뉴의 * 스토리지 VM * 으로 이동한 다음 * + 추가 * 를 클릭하여 시작합니다.



2. 스토리지 VM 추가 * 마법사에서 SVM에 * 이름 * 을 입력하고 * IP 공간 * 을 선택한 다음 * 액세스 프로토콜 * 에서 * SMB/CIFS, NFS, S3 * 탭을 클릭하고 * NFS * 활성화 확인란을 선택합니다.

Add Storage VM



STORAGE VM NAME

VCF_NFS

IPSPACE

Default

Access Protocol

SMB/CIFS, NFS, S3 iSCSI FC NVMe

Enable SMB/CIFS

Enable NFS

Allow NFS client access

Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

Enable S3

DEFAULT LANGUAGE [?](#)

c.utf_8



데이터 저장소 구축 프로세스를 자동화하는 데 VMware vSphere용 ONTAP 툴을 사용하므로 * Allow NFS client access * 버튼을 선택할 필요가 없습니다. 여기에는 ESXi 호스트에 대한 클라이언트 액세스 제공이 포함됩니다.

3. 네트워크 인터페이스 * 섹션에서 첫 번째 LIF에 대한 * IP 주소 *, * 서브넷 마스크 * 및 * 브로드캐스트 도메인 및 포트 * 를 입력합니다. 이후 LIF의 경우 나머지 모든 LIF에 공통 설정을 사용하거나 별도의 설정을 사용하도록 확인란을 설정할 수 있습니다.

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET

Without a subnet

IP ADDRESS

172.21.118.119

SUBNET MASK

24

GATEWAY

Add optional gateway

BROADCAST DOMAIN AND PORT

NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

ntaphci-a300-02

SUBNET

Without a subnet

IP ADDRESS

172.21.118.120

PORT

a0a-3374

4. 스토리지 VM 관리 계정(멀티 테넌시 환경의 경우)의 활성화 여부를 선택하고 * Save * 를 클릭하여 SVM을 생성합니다.

Storage VM Administration

Manage administrator account

Save

Cancel

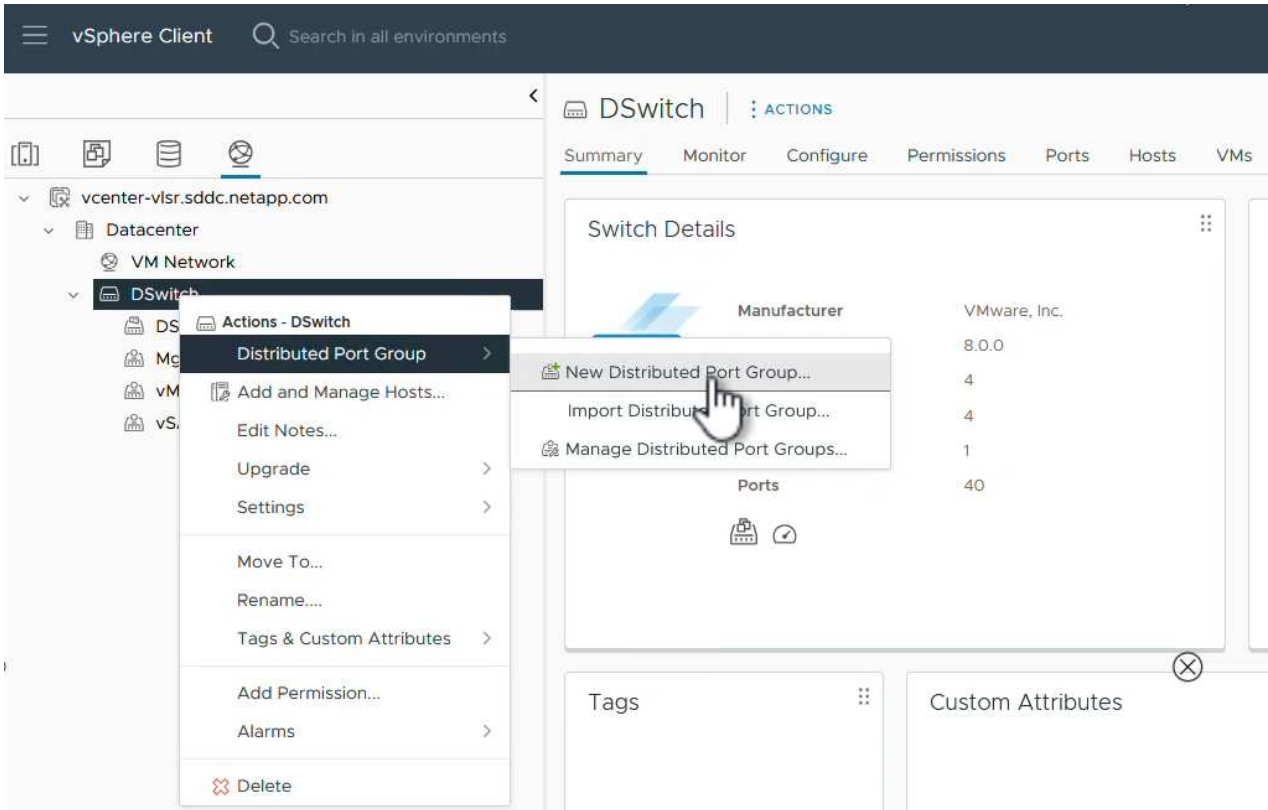
ESXi 호스트에서 NFS에 대한 네트워킹을 설정합니다

vSphere 클라이언트를 사용하여 VI 워크로드 도메인 클러스터에서 다음 단계를 수행합니다. 이 경우 vCenter Single Sign-On이 사용되므로 vSphere Client는 관리 및 워크로드 도메인 전체에서 공통적으로 사용됩니다.

NFS 트래픽에 대한 분산 포트 그룹을 생성합니다

NFS 트래픽을 전달하는 네트워크에 대한 새 분산 포트 그룹을 생성하려면 다음을 수행하십시오.

1. vSphere 클라이언트에서 워크로드 도메인에 대한 * Inventory > Networking * 으로 이동합니다. 기존 분산 스위치로 이동하여 * 새 분산 포트 그룹... * 을 만들 작업을 선택합니다.



2. 새 분산 포트 그룹* 마법사에서 새 포트 그룹의 이름을 입력하고 * 다음 * 을 클릭하여 계속합니다.
3. 설정 구성 * 페이지에서 모든 설정을 입력합니다. VLAN을 사용하는 경우 올바른 VLAN ID를 제공해야 합니다. 계속하려면 * 다음 * 을 클릭하십시오.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

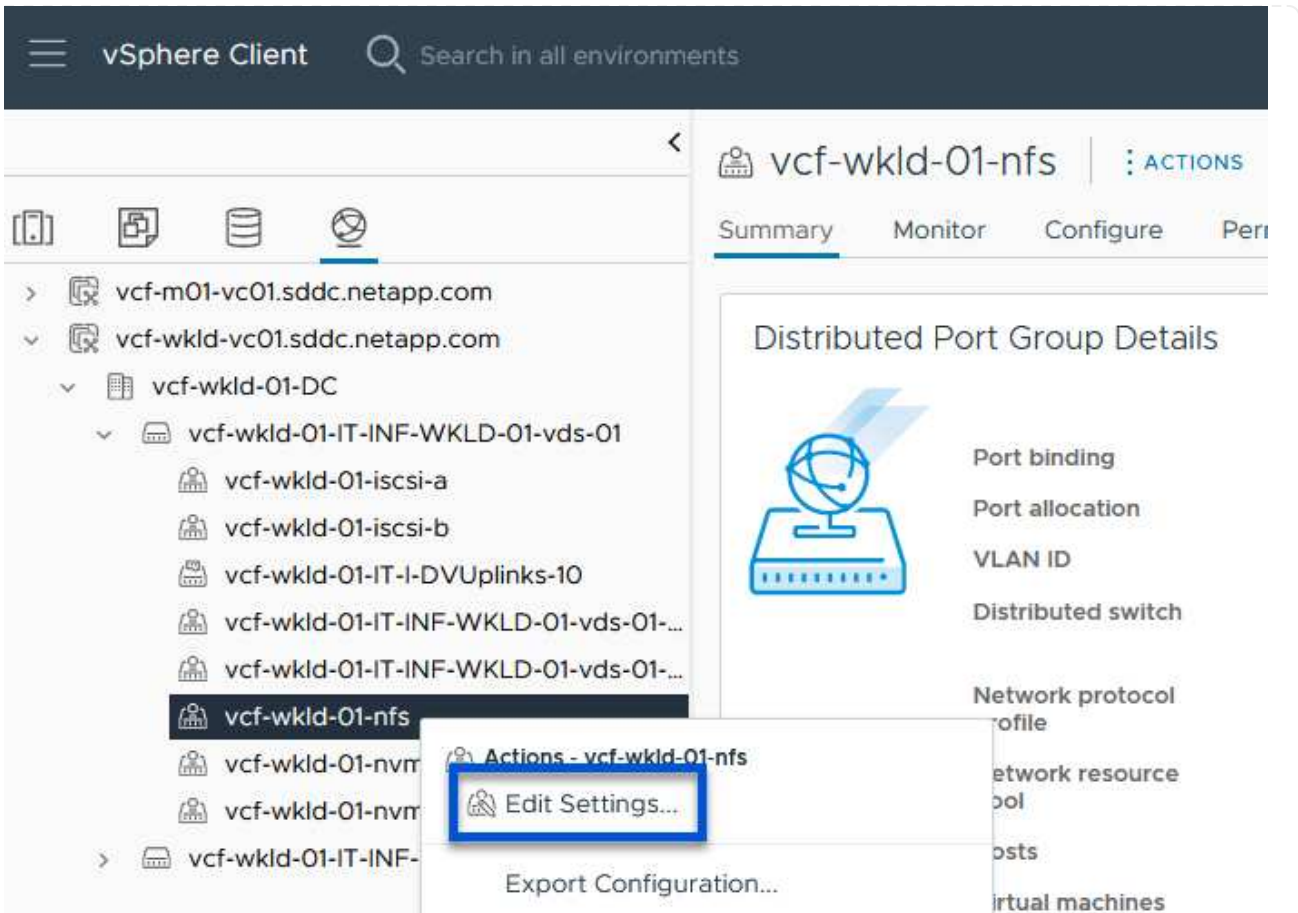
Port binding	Static binding
Port allocation	Elastic ⓘ
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

NEXT

- 완료 준비 * 페이지에서 변경 사항을 검토하고 * 마침 * 을 클릭하여 새 분산 포트 그룹을 생성합니다.
- 포트 그룹이 생성되면 포트 그룹으로 이동하고 * 설정 편집... * 작업을 선택합니다.



6. Distributed Port Group - Edit Settings * 페이지에서 왼쪽 메뉴의 * Teaming and Failover * 로 이동합니다. 활성 업링크 * 영역에서 함께 구성되어 있는지 확인하여 NFS 트래픽에 사용할 업링크에 대한 팀 구성을 활성화합니다. 사용하지 않는 업링크를 * 사용되지 않은 업링크 * 로 아래로 이동합니다.

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual port ▾

Network failure detection

Link status only ▾

Notify switches

Yes ▾

Failback

Yes ▾

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

Uplink 1

Uplink 2

Standby uplinks

Unused uplinks

CANCEL

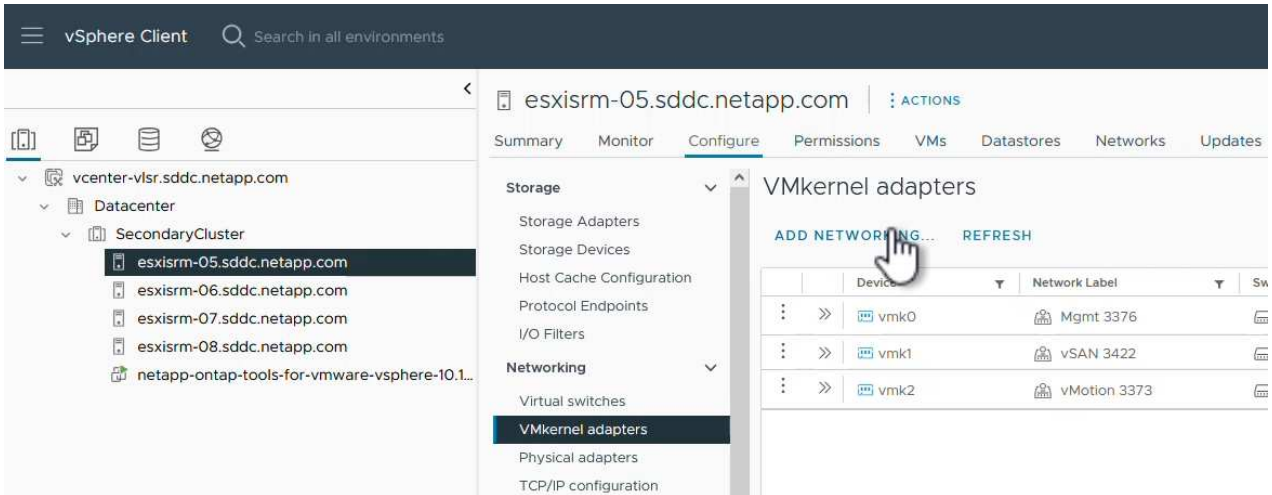
OK

7. 클러스터의 각 ESXi 호스트에 대해 이 프로세스를 반복합니다.

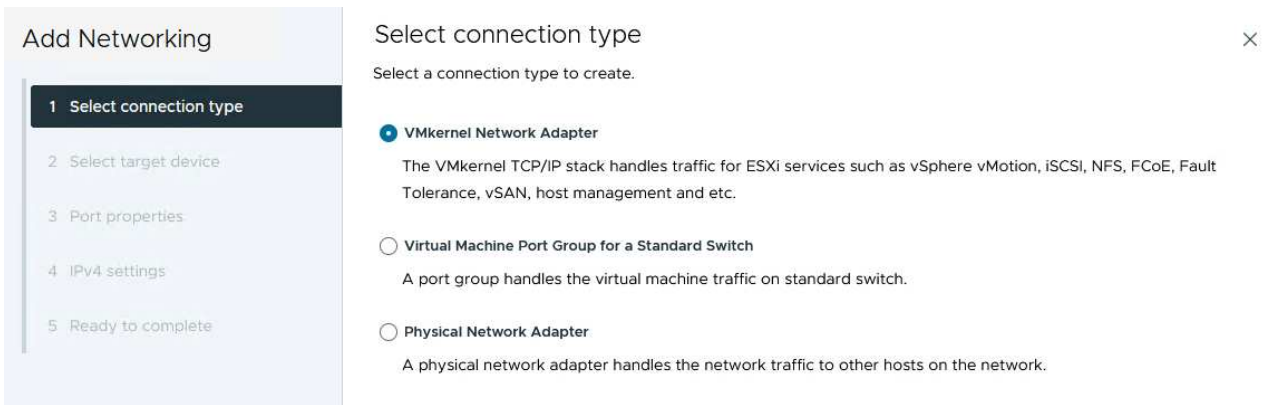
각 ESXi 호스트에 VMkernel 어댑터를 생성합니다

워크로드 도메인의 각 ESXi 호스트에서 이 프로세스를 반복합니다.

1. vSphere Client에서 워크로드 도메인 인벤토리에 있는 ESXi 호스트 중 하나로 이동합니다. Configure * 탭에서 * VMkernel Adapters * 를 선택하고 * Add Networking... * 을 클릭하여 시작합니다.



2. Select connection type * 창에서 * VMkernel Network Adapter * 를 선택하고 * Next * 를 클릭하여 계속합니다.



3. Select target device * 페이지에서 이전에 생성된 NFS에 대한 분산 포트 그룹 중 하나를 선택합니다.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	Mgmt 3376	--	DSwitch
<input checked="" type="radio"/>	NFS 3374	--	DSwitch
<input type="radio"/>	vMotion 3373	--	DSwitch
<input type="radio"/>	vSAN 3422	--	DSwitch

Manage Columns 4 items

CANCEL

BACK

NEXT

4. Port properties * 페이지에서 기본값(활성화된 서비스 없음)을 유지하고 * Next * 를 클릭하여 계속합니다.
5. IPv4 설정 * 페이지에서 * IP 주소 *, * 서브넷 마스크 * 를 입력하고 새 게이트웨이 IP 주소를 입력합니다 (필요한 경우에만 해당). 계속하려면 * 다음 * 을 클릭하십시오.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings**
- 5 Ready to complete

IPv4 settings



Specify VMkernel IPv4 settings.

- Obtain IPv4 settings automatically
 Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway Override default gateway for this adapter

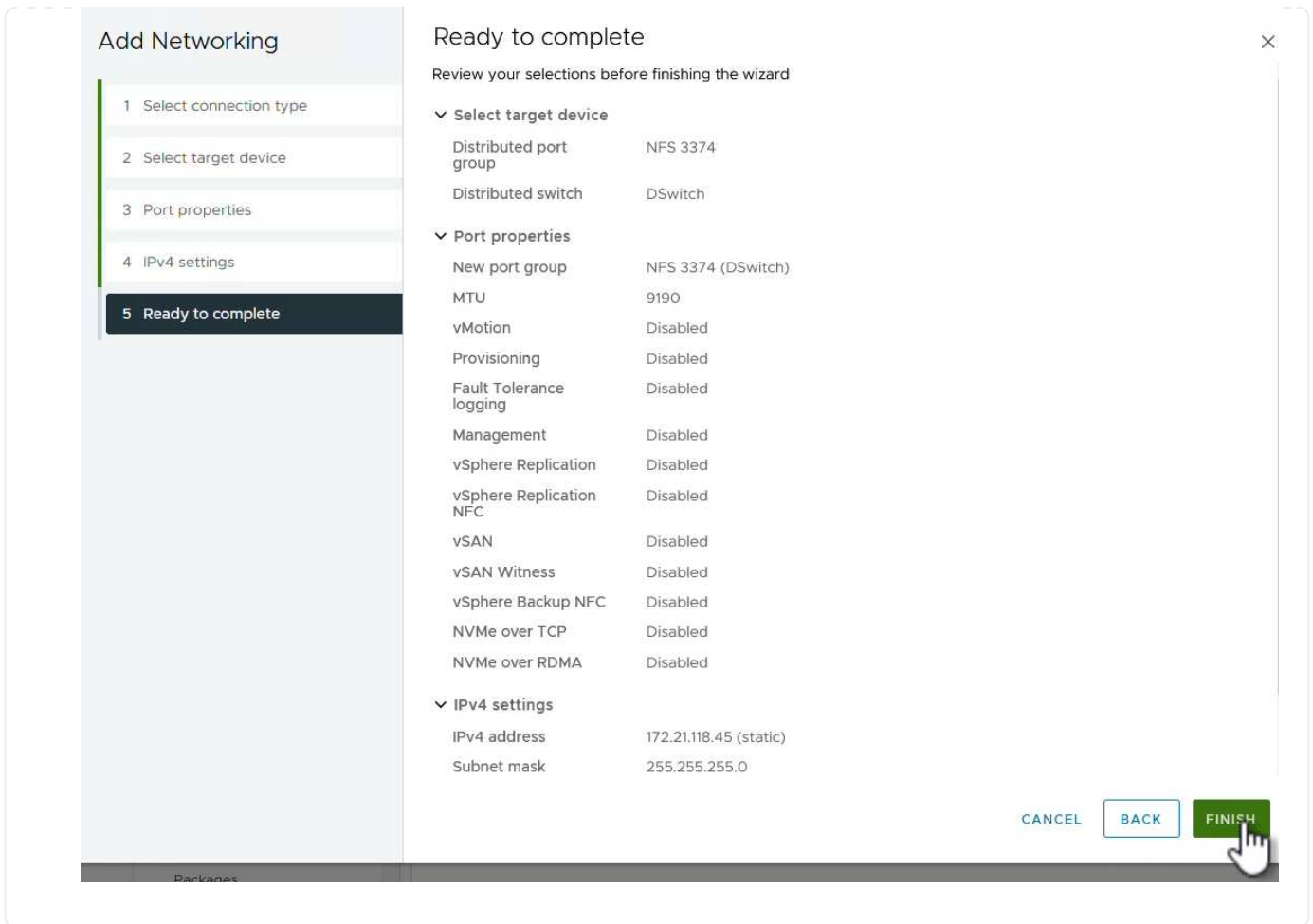
DNS server addresses

CANCEL

BACK

NEXT

6. Ready to Complete * 페이지에서 선택 사항을 검토하고 * Finish * 를 클릭하여 VMkernel 어댑터를 생성합니다.



ONTAP 톨 10 을 구축 및 사용하여 스토리지를 구성합니다

다음 단계는 vSphere Client를 사용하는 vSphere 8 클러스터에서 수행되며 OTV 구축, ONTAP Tools Manager 구성, VVol NFS 데이터 저장소 생성과 관련됩니다.

VMware vSphere 10용 ONTAP 톨 구축 및 사용에 대한 전체 설명서는 ["VMware vSphere용 ONTAP 톨을 구축할 준비를 합니다"](#)참조하십시오.

VMware vSphere 10용 ONTAP 툴을 구축합니다

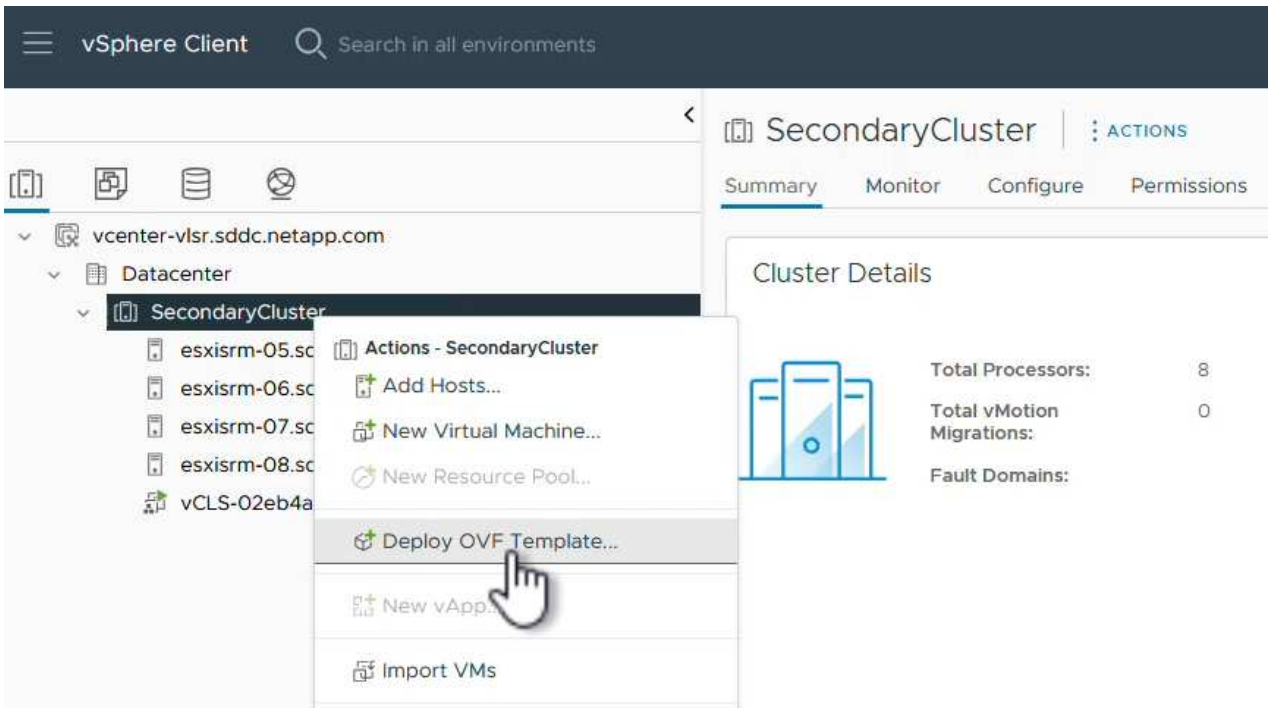
VMware vSphere 10용 ONTAP 툴은 VM 어플라이언스로 구축되며 ONTAP 스토리지 관리를 위한 통합 vCenter UI를 제공합니다. ONTAP Tools 10에는 여러 vCenter 서버 및 ONTAP 스토리지 백엔드에 대한 연결을 관리할 수 있는 새로운 글로벌 관리 포털이 있습니다.



HA가 아닌 배포 시나리오에서는 3개의 사용 가능한 IP 주소가 필요합니다. 한 IP 주소는 로드 밸런서에 할당되고, 다른 주소는 Kubernetes 컨트롤 플레인에 할당되며, 나머지 주소는 노드에 할당됩니다. HA 구축에서는 처음 3개 노드에 2개의 추가 IP 주소 외에 2개의 추가 IP 주소가 필요합니다. 할당하기 전에 호스트 이름이 DNS의 IP 주소에 연결되어 있어야 합니다. 5개의 IP 주소 모두 동일한 VLAN에 있어야 하며, 이 VLAN은 배포용으로 선택됩니다.

VMware vSphere용 ONTAP 툴을 구축하려면 다음을 완료하십시오.

1. 에서 ONTAP 도구 OVA 이미지를 가져와서 "[NetApp Support 사이트](#)"로컬 폴더로 다운로드합니다.
2. vSphere 8 클러스터용 vCenter 어플라이언스에 로그인합니다.
3. vCenter 어플라이언스 인터페이스에서 관리 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * Deploy OVF Template를 선택합니다



4. Deploy OVF Template * 마법사에서 * Local file * 라디오 버튼을 클릭하고 이전 단계에서 다운로드한 ONTAP tools OVA 파일을 선택합니다.

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. 마법사의 2-5단계에서 VM의 이름과 폴더를 선택하고 컴퓨팅 리소스를 선택하고 세부 정보를 검토한 후 라이선스 계약에 동의합니다.

6. 구성 및 디스크 파일의 스토리지 위치로 로컬 데이터 저장소 또는 vSAN 데이터 저장소를 선택합니다.

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Configuration
- 7 Select storage**
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format

VM Storage Policy

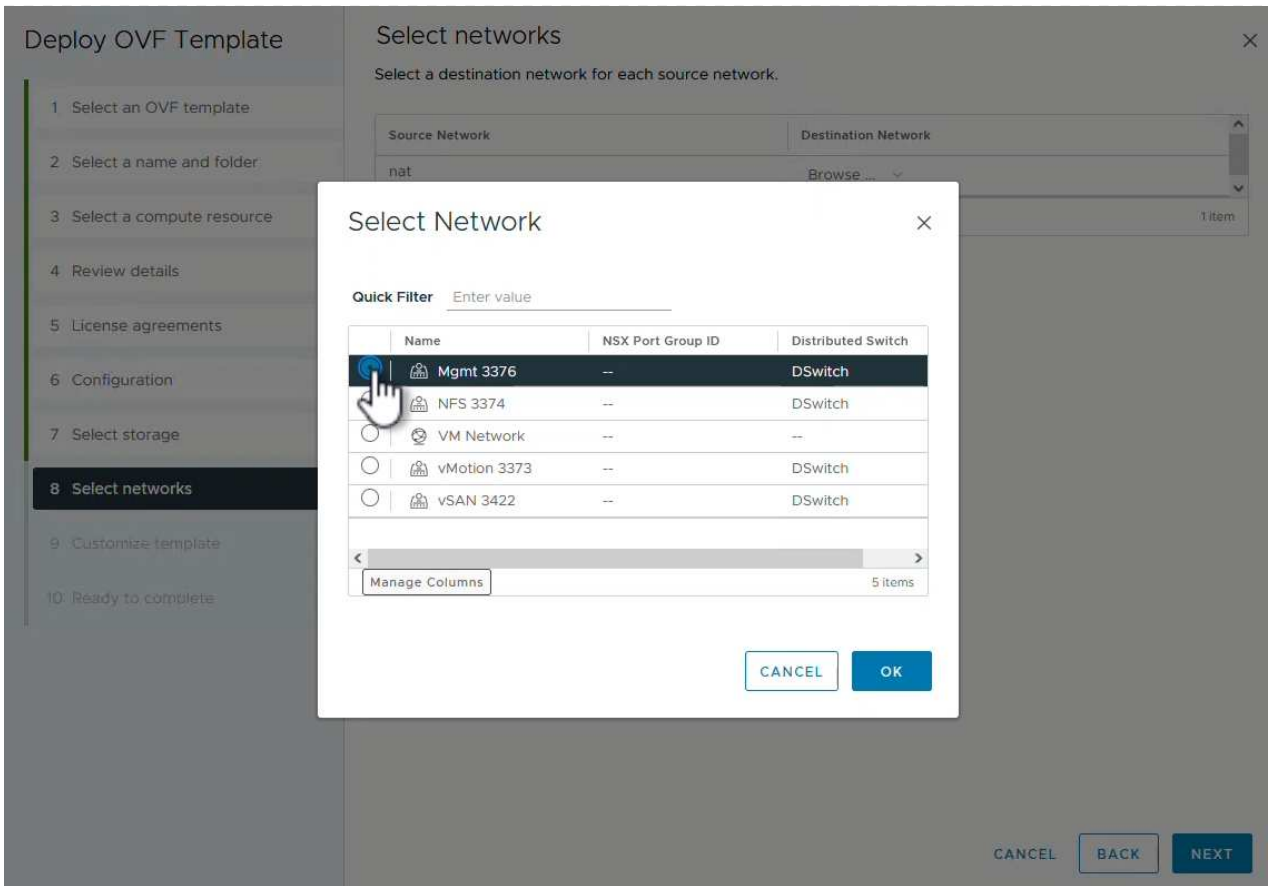
Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	T
vsanDatastore	--	799.97 GB	26.05 GB	783.98 GB	v

Manage Columns Items per page 10 1 item

Compatibility

7. 네트워크 선택 페이지에서 관리 트래픽에 사용되는 네트워크를 선택합니다.



8. 구성 페이지에서 사용할 배포 구성을 선택합니다. 이 시나리오에서는 쉬운 배포 방법을 사용합니다.



ONTAP 툴 10은 다중 노드를 사용한고가용성 구축을 포함하여 다양한 구축 구성을 제공합니다. 모든 배포 구성에 대한 설명은 ["VMware vSphere용 ONTAP 툴을 구축할 준비를 합니다"](#)참조하십시오.

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Configuration**
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Configuration

Select a deployment configuration

	Description	
<input checked="" type="radio"/> Easy deployment (S)	Deploy local provisioner Non-HA Small single node instance of ONTAP tools	
<input type="radio"/> Easy deployment (M)		
<input type="radio"/> Advanced deployment (S)		
<input type="radio"/> Advanced deployment (M)		
<input type="radio"/> High-Availability deployment (S)		
<input type="radio"/> High-Availability deployment (M)		
<input type="radio"/> High-Availability deployment (L)		
<input type="radio"/> Recovery		
8 Items		

CANCEL

BACK

NEXT

9. 템플릿 사용자 지정 페이지에서 필요한 모든 정보를 입력합니다.

- vCenter Server에 VASA 공급자 및 SRA를 등록하는 데 사용할 애플리케이션 사용자 이름입니다.
- 자동화된 지원을 위해 ASUP 사용
- 필요한 경우 ASUP 프록시 URL입니다.
- 관리자 사용자 이름 및 암호
- NTP 서버
- 콘솔에서 관리 기능에 액세스하기 위한 유지 관리 사용자 암호입니다.
- 로드 밸런서 IP
- K8 컨트롤 플레인에 대한 가상 IP
- 기본 VM - 현재 VM을 기본 VM으로 선택합니다(HA 구성의 경우).
- VM의 호스트 이름입니다
- 필수 네트워크 속성 필드를 입력합니다.

계속하려면 * 다음 * 을 클릭하십시오.

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template**
- 10 Ready to complete

Customize template

Customize the deployment properties of this software solution.

10 properties have invalid values

System Configuration 8 settings

Application username(*) Username to assign to the Application
vsphere-services

Application password(*) Password to assign to the Application

Password

Confirm Password

Enable ASUP Select this checkbox to enable ASUP

ASUP Proxy URL Proxy url (in case if egress is blocked in datacenter side), through which we can push the asup bundle.

Administrator username(*) Username to assign to the Administrator. Please use only a letter as the beginning. And only '@', '_', '.', ':', '-' special characters are supported

Administrator password(*) Password to assign to the Administrator

CANCEL BACK NEXT

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template**
- 10 Ready to complete

Customize template

Maintenance user password(*) Password to assign to maint user account

Password

Confirm Password

Deployment Configuration 3 settings

Load balancer IP(*) Load balancer IP (*)
172.21.120.57

Virtual IP for K8s control plane(*) Provide the virtual IP address for K8s control plane
172.21.120.58

Primary VM Maintain this field as selected to set the current VM as primary and install the ONTAP tools.

Node Configuration 10 settings

HostName(*) Specify the hostname for the VM

IP Address(*) Specify the IP address for the appliance

IPv6 Address Specify the IPv6 address on the deployed network only when you need dual stack

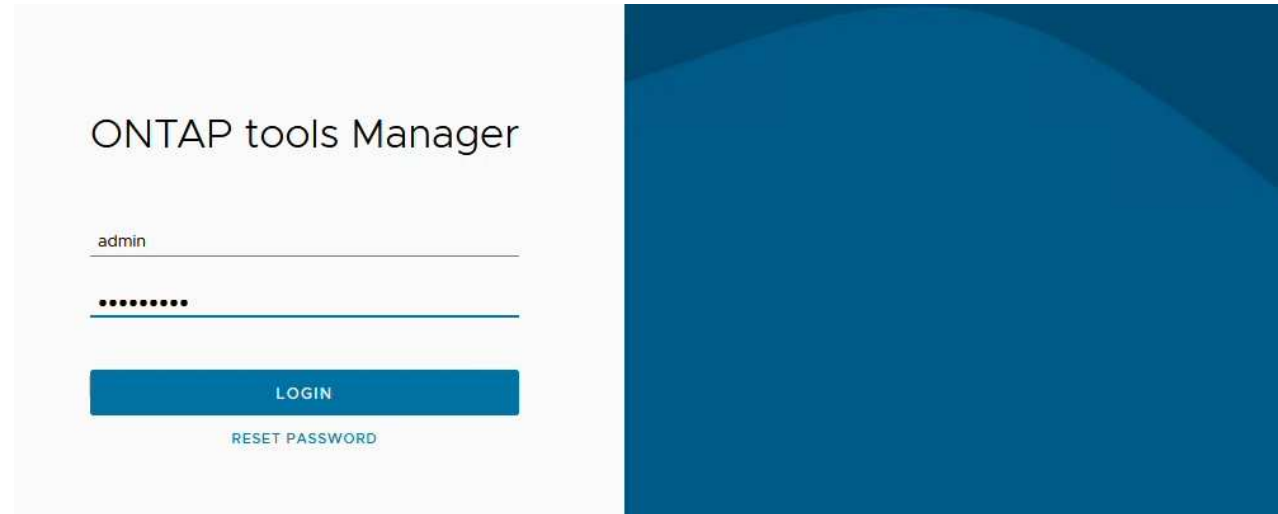
CANCEL BACK NEXT

10. 완료 준비 페이지에서 모든 정보를 검토하고 마침 을 클릭하여 ONTAP 도구 어플라이언스 배포를 시작합니다.

스토리지 백엔드 및 vCenter Server를 ONTAP 툴에 연결합니다. 10.

ONTAP 도구 관리자는 ONTAP 도구 10의 전역 설정을 구성하는 데 사용됩니다.

1. <https://loadBalanceIP:8443/virtualization/ui/> 웹 브라우저에서 로 이동하고 배포 중에 제공된 관리 자격 증명으로 로그인하여 ONTAP 도구 관리자에 액세스합니다.



2. 시작하기 * 페이지에서 * 스토리지 백엔드로 이동 * 을 클릭합니다.

Getting Started



ONTAP tools Manager allows you to manage ONTAP Storage Backends and associate them with vCenters. You can also download support log bundles.



Storage Backends

Add, modify, and remove storage backends.

[Go to Storage Backends](#)



vCenters

Add, modify, and remove vCenters and associate storage backends with them.

[Go to vCenters](#)



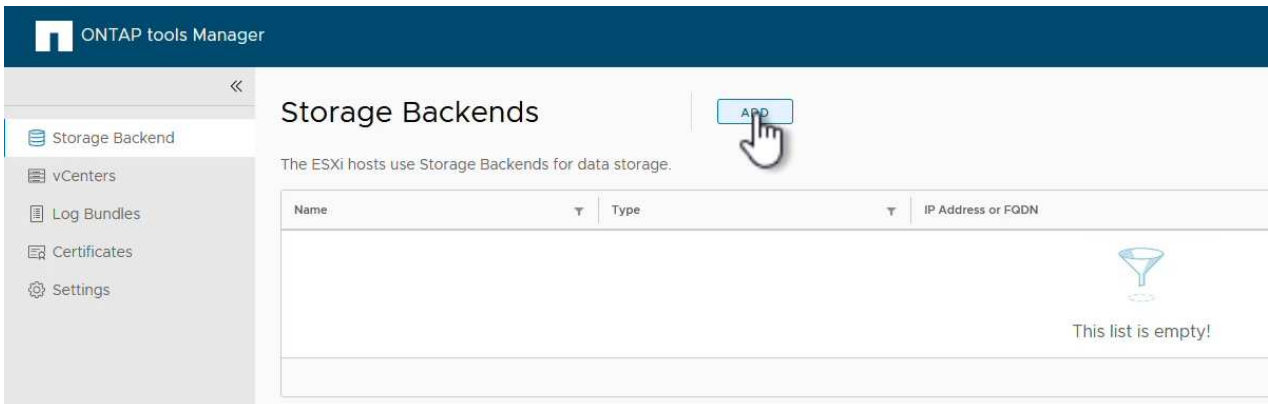
Log Bundles

Generate and download log bundles for support purposes.

[Go to Log Bundles](#)

Don't show again

3. 스토리지 백엔드 * 페이지에서 * 추가 * 를 클릭하여 ONTAP 툴에 등록할 ONTAP 스토리지 시스템의 자격 증명을 입력합니다 10.




4. 스토리지 백엔드 추가 * 상자에서 ONTAP 스토리지 시스템에 대한 자격 증명을 입력합니다.

Add Storage Backend

Hostname: * 172.16.9.25

Username: * admin

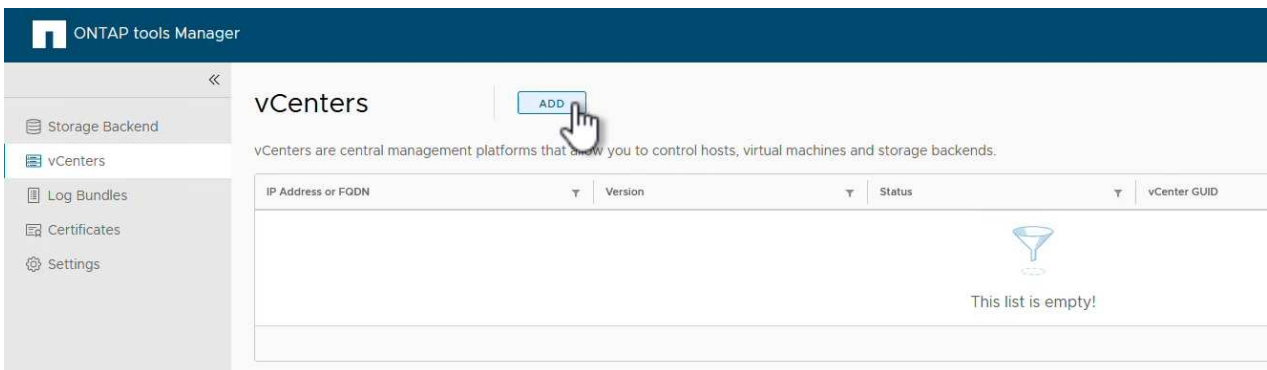
Password: * ●●●●●●●● 

Port: * 443

CANCEL

ADD 

5. 왼쪽 메뉴에서 * vCenters * 를 클릭한 다음 * add * 를 클릭하여 ONTAP 툴 10 에 등록할 vCenter 서버의 자격 증명을 입력합니다.



The screenshot shows the ONTAP tools Manager interface. The left sidebar contains a menu with items: Storage Backend, vCenters (highlighted), Log Bundles, Certificates, and Settings. The main content area is titled 'vCenters' and features an 'ADD' button with a hand cursor pointing to it. Below the button, there is a table with columns: IP Address or FQDN, Version, Status, and vCenter GUID. The table is currently empty, with a message 'This list is empty!' and a funnel icon centered below it.

6. vCenter 추가 * 상자에서 ONTAP 스토리지 시스템에 대한 자격 증명을 입력합니다.

Add vCenter

Server IP Address or FQDN: *

Username: *

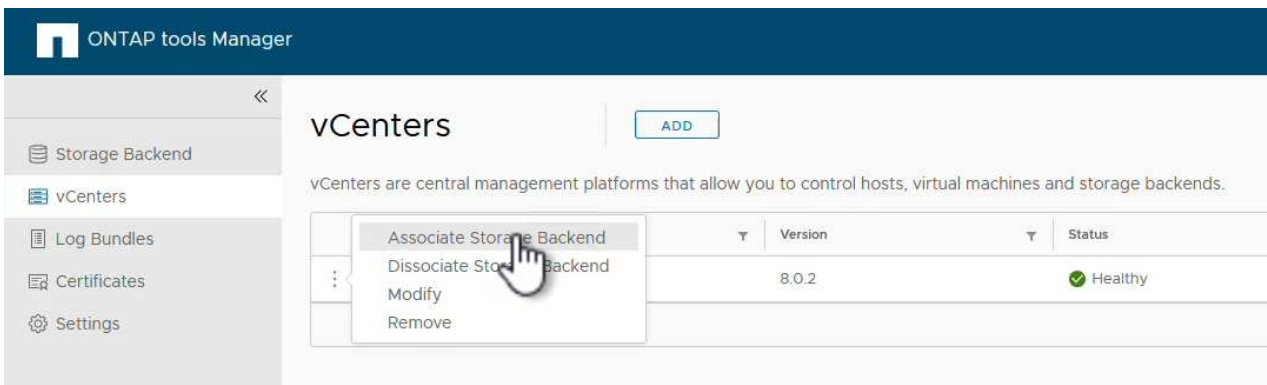
Password: * 

Port: *

CANCEL

ADD 


7. 새로 검색된 vCenter 서버의 세로 3점 메뉴에서 * Associate Storage Backend * 를 선택합니다.



ONTAP tools Manager

vCenters

vCenters are central management platforms that allow you to control hosts, virtual machines and storage backends.

	Version	Status
 Associate Storage Backend Dissociate Storage Backend Modify Remove	8.0.2	Healthy

8. 스토리지 백엔드 연결 * 상자에서 vCenter 서버와 연결할 ONTAP 스토리지 시스템을 선택하고 * 연결 * 을 클릭하여 작업을 완료합니다.

Associate Storage Backend

vcenter-vlsr.sddc.netapp.com



Storage Backend

ntaphci-a300e9u25

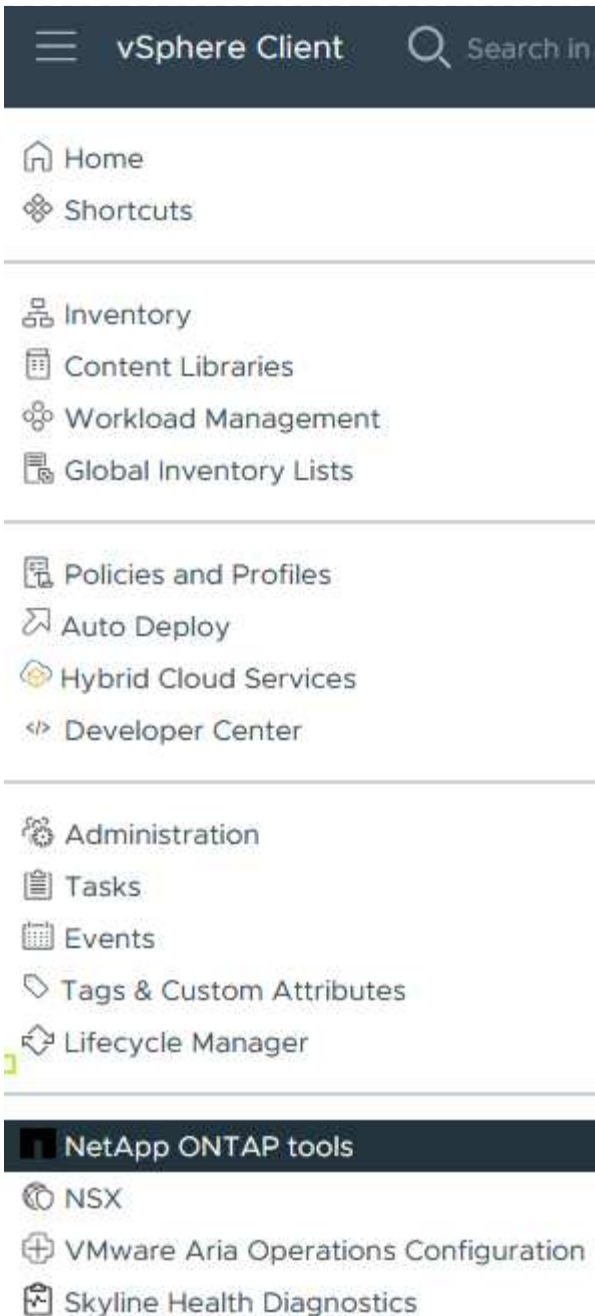


CANCEL

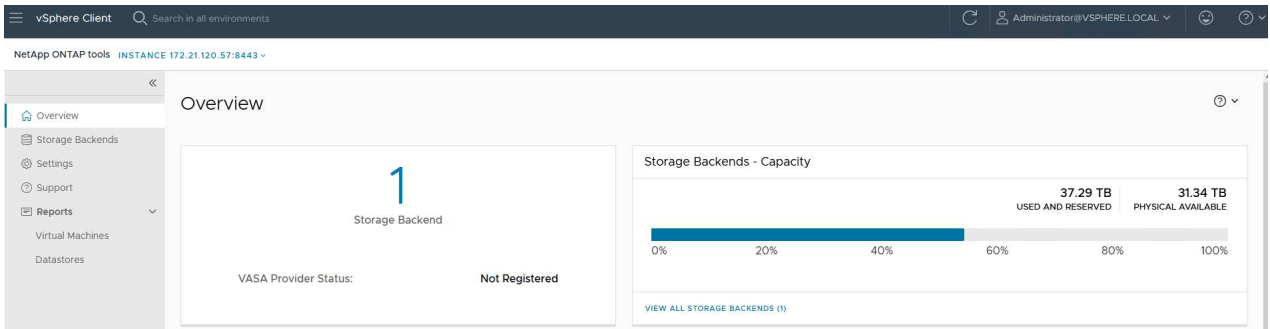
ASSOCIATE



9. 설치를 확인하려면 vSphere Client에 로그인하고 왼쪽 메뉴에서 * NetApp ONTAP tools * 를 선택합니다.



10. ONTAP 툴 대시보드에서 스토리지 백엔드가 vCenter Server와 연결되어 있음을 확인할 수 있습니다.

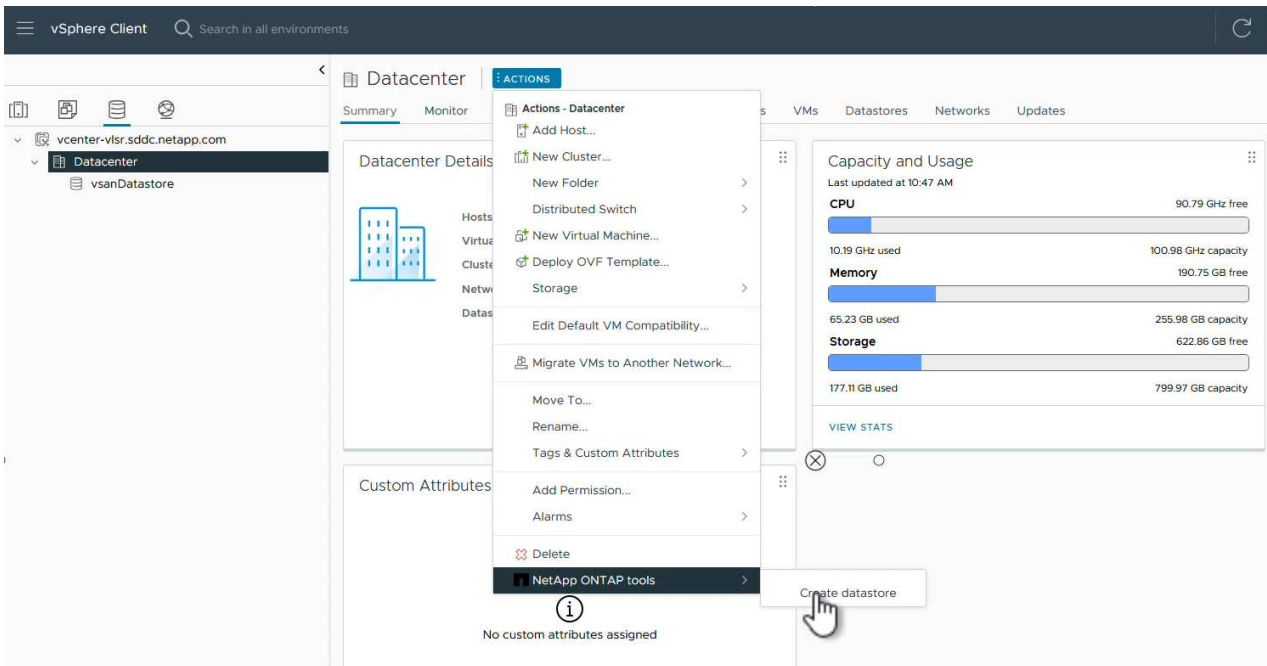




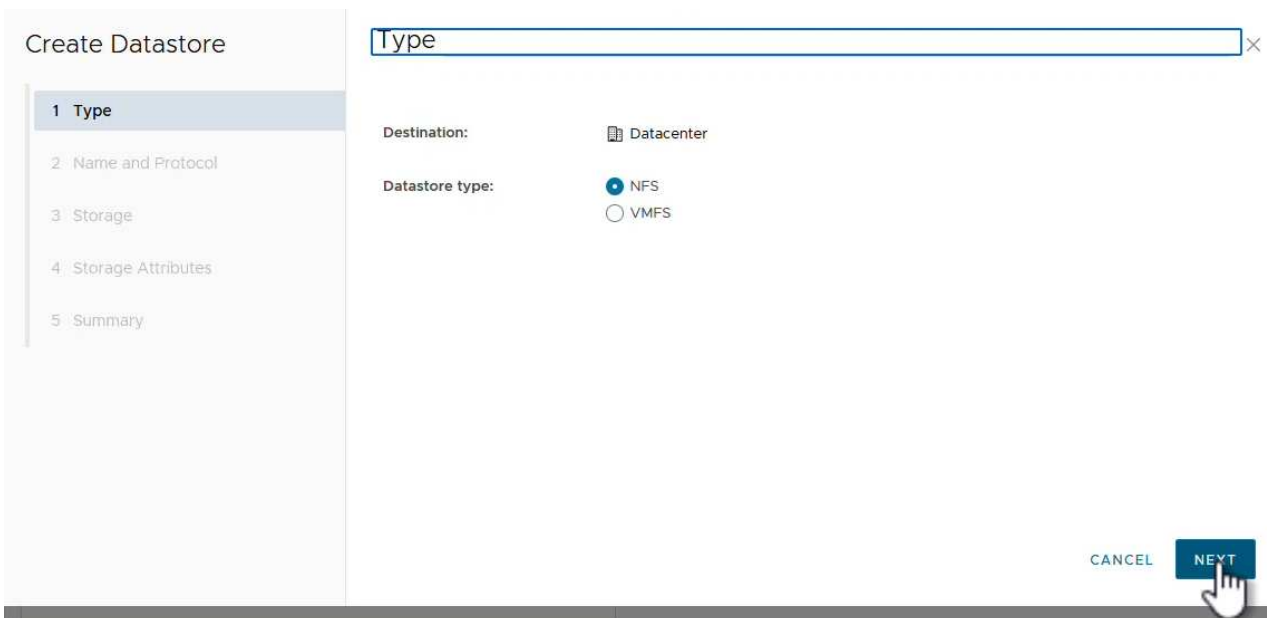
ONTAP 툴을 사용하여 NFS 데이터 저장소를 생성합니다 10

ONTAP 툴 10 을 사용하여 NFS에서 실행되는 ONTAP 데이터 저장소를 구축하려면 다음 단계를 완료하십시오.

1. vSphere Client에서 스토리지 인벤토리로 이동합니다. Actions * 메뉴에서 * NetApp ONTAP tools > DataStore 생성 * 을 선택합니다.



2. Create Datastore 마법사의 * Type * 페이지에서 NFS 라디오 버튼을 클릭한 후 * Next * 를 클릭하여 계속합니다.



3. 이름 및 프로토콜 * 페이지에서 데이터 저장소의 이름, 크기 및 프로토콜을 입력합니다. 계속하려면 * 다음 * 을

클릭하십시오.

The screenshot shows the 'Create Datastore' wizard with the 'Name and Protocol' step selected. The left sidebar lists the steps: 1 Type, 2 Name and Protocol, 3 Storage, 4 Storage Attributes, and 5 Summary. The main content area is titled 'Name and Protocol' and contains the following fields:

- Datastore name:** NFS_DS1
- Size:** 2 TB (with a note: Minimum supported size is 1 GB)
- Protocol:** NFS 3
- Advanced Options:** (expanded)
- Datastore Cluster:** (empty dropdown)

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT. A mouse cursor is pointing at the NEXT button.

- 스토리지 * 페이지에서 플랫폼(유형별로 스토리지 시스템 필터링)과 볼륨의 스토리지 VM을 선택합니다. 필요한 경우 사용자 지정 익스포트 정책을 선택합니다. 계속하려면 * 다음 * 을 클릭하십시오.

The screenshot shows the 'Create Datastore' wizard with the 'Storage' step selected. The left sidebar lists the steps: 1 Type, 2 Name and Protocol, 3 Storage, 4 Storage Attributes, and 5 Summary. The main content area is titled 'Storage' and contains the following fields:

- Platform: *** Performance (A)
- Storage VM: *** VCF_NFS (with a note: ntaphci-a300e9u25 (172.16.9.25))
- Advanced Options:** (expanded)
- Custom Export Policy:** Search or specify policy name (with a note: Choose an existing policy or give a new name to the default policy.)

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT. A mouse cursor is pointing at the NEXT button.

- 스토리지 속성 * 페이지에서 사용할 스토리지 집계를 선택하고 선택적으로 공간 예약 및 서비스 품질과 같은 고급 옵션을 선택합니다. 계속하려면 * 다음 * 을 클릭하십시오.

Create Datastore

- 1 Type
- 2 Name and Protocol
- 3 Storage
- 4 **Storage Attributes**
- 5 Summary

Storage Attributes

Specify the storage details for provisioning the datastore.

Aggregate: * EHCaggr02 (16.61 TB Free) ▾

Volume: A new volume will be created automatically.

^ Advanced Options

Space Reserve: * Thin ▾

Enable QoS

CANCEL

BACK

NEXT

6. 마지막으로 * Summary * 를 검토하고 Finish를 클릭하여 NFS 데이터 저장소 생성을 시작합니다.

Create Datastore

- 1 Type
- 2 Name and Protocol
- 3 Storage
- 4 Storage Attributes
- 5 **Summary**

Summary

A new datastore will be created with these settings.

Type

Destination: Datacenter
Datastore type: NFS

Name and Protocol

Datastore name: NFS_DS1
Size: 2 TB
Protocol: NFS 3

Storage

Platform: Performance (A)
Storage VM: VCF_NFS

CANCEL

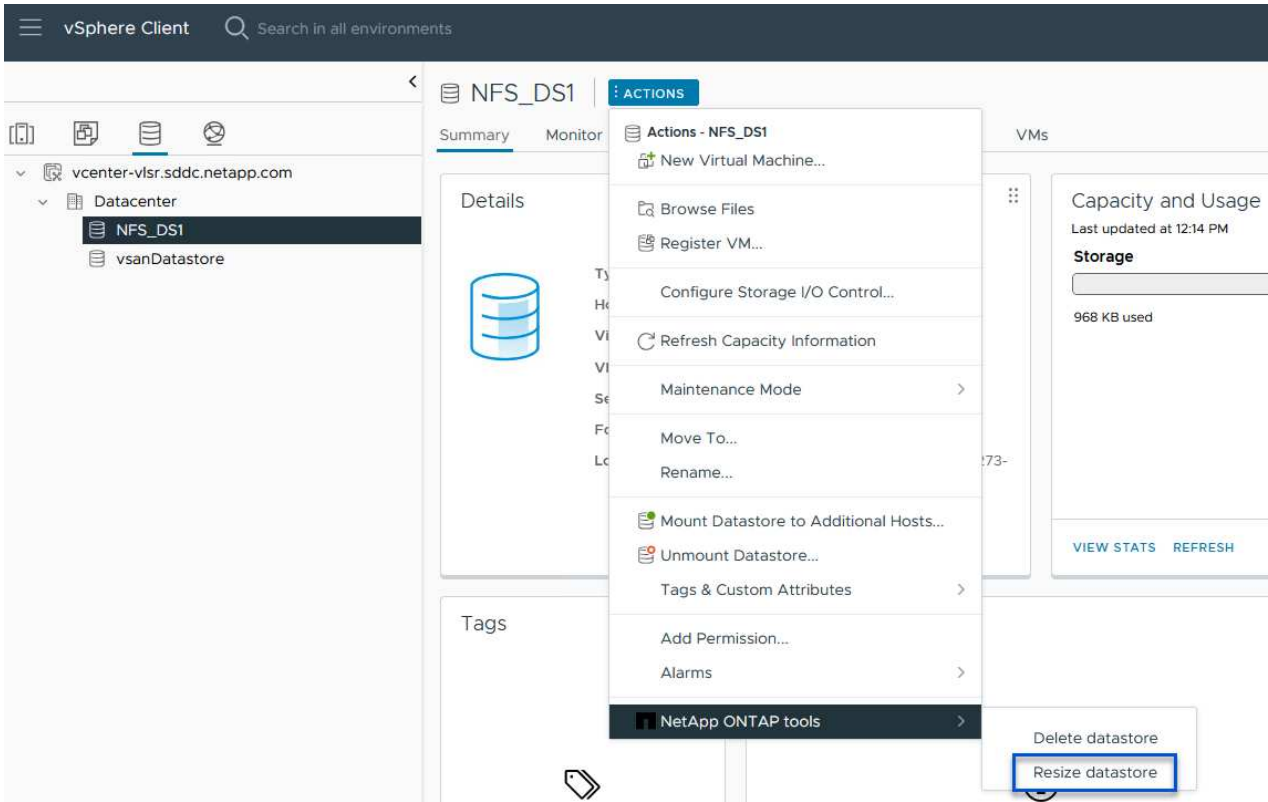
BACK

FINISH

ONTAP 툴을 사용하여 NFS 데이터 저장소 크기 조정 10

ONTAP 툴 10 을 사용하여 기존 NFS 데이터 저장소의 크기를 조정하려면 다음 단계를 완료하십시오.

1. vSphere Client에서 스토리지 인벤토리로 이동합니다. actions * 메뉴에서 * NetApp ONTAP tools > Resize datastore * 를 선택합니다.



2. 데이터 저장소 크기 조정 * 마법사에서 데이터 저장소의 새 크기를 GB 단위로 입력하고 * 크기 조정 * 을 클릭하여 계속합니다.

Resize Datastore | NFS_DS1

Volume Details

Volume Name:	NFS_DS1
Total Size:	2.1 TB
Used Size:	968 KB
Snapshot Reserve (%):	5
Thin Provisioned:	Yes

Size

Current Datastore Size:	2 TB
New Datastore Size (GB): *	3000 <input type="text"/>

CANCEL

RESIZE

3. 최근 작업 * 창에서 크기 조정 작업의 진행 상황을 모니터링합니다.

Task Name	Target	Status	Details
Expand Datastore	vcenter-vlsr.sddc.net app.com	100% <input checked="" type="checkbox"/>	Expand datastore initiated with job id 2807

추가 정보

VMware vSphere 10용 ONTAP 툴 리소스의 전체 목록은 을 참조하십시오 "[VMware vSphere용 ONTAP 툴 설명서 리소스](#)".

ONTAP 스토리지 시스템 구성에 대한 자세한 "[ONTAP 10 설명서](#)"내용은 센터를 참조하십시오.

NFS 데이터 저장소의 재해 복구에 VMware Site Recovery Manager를 사용합니다

NFS 데이터 저장소의 재해 복구에 **VMware Site Recovery Manager**를 사용합니다

VMware SRM(Site Recovery Manager)과 함께 VMware vSphere 10용 ONTAP 툴 및 SRA(Site Replication Adapter)를 활용하면 재해 복구 작업에 큰 가치를 제공할 수 있습니다. ONTAP 툴 10은 VASA Provider를 위한 기본 고가용성 및 확장성을 포함하여 강력한 스토리지 기능을 제공하며, iSCSI 및 NFS VVOL을 지원합니다. 따라서 데이터 가용성이 보장되고 여러

VMware vCenter Server 및 ONTAP 클러스터의 관리가 간소화됩니다. VMware Site Recovery Manager와 함께 SRA를 사용하면 사이트 간에 가상 시스템과 데이터를 원활하게 복제 및 장애 조치할 수 있으므로 효율적인 재해 복구 프로세스를 구현할 수 있습니다. ONTAP 툴과 SRA를 함께 사용하면 기업이 중요한 워크로드를 보호하고 다운타임을 최소화하며 예기치 못한 사건이나 재해가 발생해도 비즈니스 연속성을 유지할 수 있습니다.

ONTAP 툴 10을 사용하면 스토리지 관리 및 효율성 기능을 간소화하고, 가용성을 개선하고, SAN 또는 NAS를 사용하는 경우 스토리지 비용 및 운영 오버헤드를 줄일 수 있습니다. Best Practice를 사용하여 데이터 저장소를 프로비저닝하고 NFS 및 블록 스토리지 환경에 대한 ESXi 호스트 설정을 최적화합니다. 이러한 모든 이점을 누리게 하려면 ONTAP 소프트웨어를 실행하는 시스템에서 vSphere를 사용할 때 이 플러그인을 사용하는 것이 좋습니다.

SRA는 SRM과 함께 사용되어 기존 VMFS 및 NFS 데이터 저장소의 프로덕션 및 재해 복구 사이트 간에 VM 데이터 복제를 관리하고 DR 복제본의 무중단 테스트를 수행합니다. 검색, 복구 및 재보호 작업을 자동화할 수 있습니다.

이 시나리오에서는 데이터 저장소를 보호하고 보조 사이트에 대한 테스트 및 최종 페일오버를 실행하는 VMware Site Recovery Manager를 배포 및 사용하는 방법을 보여 줍니다. 재보호 및 장애 복구에 대해서도 설명합니다.

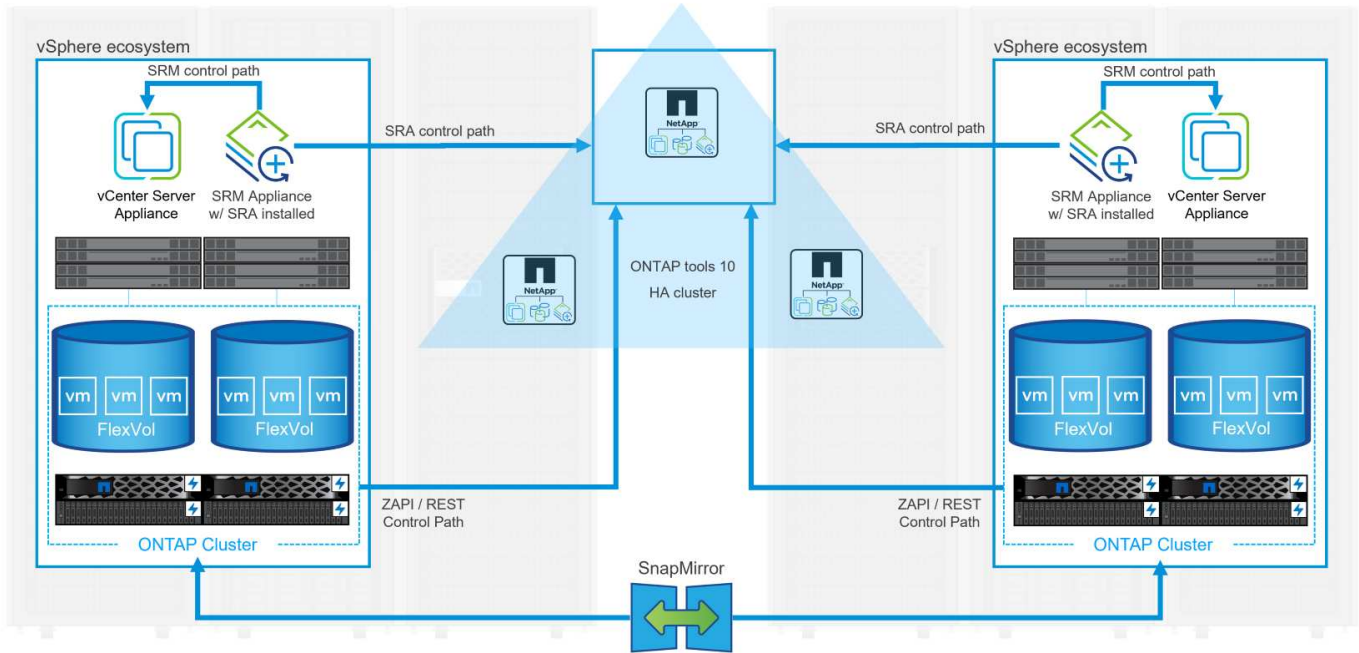
시나리오 개요

이 시나리오에서는 다음과 같은 상위 단계를 다룹니다.

- 기본 및 보조 사이트에서 vCenter Server를 사용하여 SRM을 구성합니다.
- VMware vSphere 10용 ONTAP 툴용 SRA 어댑터를 설치하고 vCenter에 등록합니다.
- 소스 및 대상 ONTAP 스토리지 시스템 간에 SnapMirror 관계 생성
- SRM에 대한 사이트 복구를 구성합니다.
- 테스트 및 최종 페일오버를 수행합니다.
- 재보호 및 페일백에 대해 논의합니다.

있습니다

다음 다이어그램은 3노드 고가용성 구성으로 구성된 VMware vSphere 10용 ONTAP 툴을 사용하는 일반적인 VMware 사이트 복구 아키텍처를 보여 줍니다.



필수 구성 요소

이 시나리오에는 다음과 같은 구성 요소 및 구성이 필요합니다.

- vSphere 8 클러스터는 운영 및 보조 위치 모두에 설치되며 환경 간 통신을 위한 적절한 네트워킹을 제공합니다.
- 운영 및 2차 위치에 ONTAP 스토리지 시스템이 있으며, NFS 스토리지 트래픽 전용 이더넷 스위치의 물리적 데이터 포트가 있습니다.
- VMware vSphere 10용 ONTAP 툴이 설치되어 있고 두 vCenter 서버가 모두 등록되어 있습니다.
- 운영 및 보조 사이트용으로 VMware Site Replication Manager 어플라이언스가 설치되어 있습니다.
 - 인벤토리 매핑(네트워크, 폴더, 리소스, 스토리지 정책)이 SRM에 대해 구성되었습니다.

NetApp은 NFS에 대한 이중 네트워크 설계를 추천하여 스토리지 시스템, 스위치, 네트워크 어댑터 및 호스트 시스템에 대한 내결함성을 제공합니다. 아키텍처 요구 사항에 따라 단일 서브넷이나 여러 서브넷으로 NFS를 구축하는 것이 일반적입니다.

을 참조하십시오 ["VMware vSphere에서 NFS를 실행하는 모범 사례"](#) VMware vSphere에 대한 자세한 내용은

ONTAP를 VMware vSphere와 함께 사용하는 방법에 대한 네트워크 지침은 을 참조하십시오 ["네트워크 구성 - NFS"](#) 섹션을 NetApp 참조하십시오.

VMware SRM에서 ONTAP 스토리지를 사용하는 방법에 대한 NetApp 설명서는 을 참조하십시오 ["ONTAP를 사용하는 VMware 사이트 복구 관리자"](#)

배포 단계

다음 섹션에서는 ONTAP 스토리지 시스템을 사용하여 VMware Site Recovery Manager 구성을 구현하고 테스트하는 구축 단계를 간략히 설명합니다.

ONTAP 스토리지 시스템 간에 **SnapMirror** 관계를 생성합니다

데이터 저장소 볼륨을 보호하려면 소스 및 대상 **ONTAP** 스토리지 시스템 간에 **SnapMirror** 관계를 설정해야 합니다.

<https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-replication-workflow-concept.html> ["여기를 클릭하십시오"] **ONTAP** 볼륨에 대한 **SnapMirror** 관계를 생성하는 방법에 대한 자세한 내용은 **ONTAP** 설명서를 참조하십시오.

단계별 지침은 다음 문서의 개요를 참조하십시오. "[여기를 클릭하십시오](#)" 이 단계에서는 클러스터 피어 및 SVM 피어 관계를 생성한 다음 각 볼륨의 **SnapMirror** 관계를 생성하는 방법을 개략적으로 설명합니다. 이러한 단계는 **ONTAP System Manager** 또는 **ONTAP CLI**를 사용하여 수행할 수 있습니다.

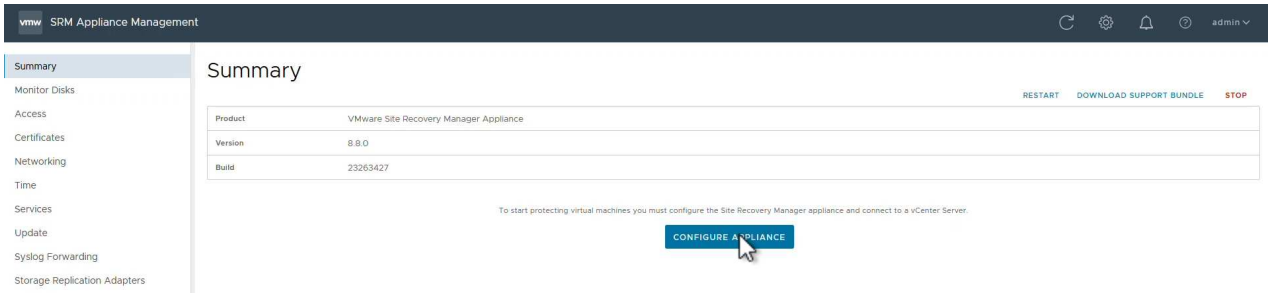
SRM 어플라이언스를 구성합니다

SRM 어플라이언스 및 **SRA** 어댑터를 구성하려면 다음 단계를 완료하십시오.

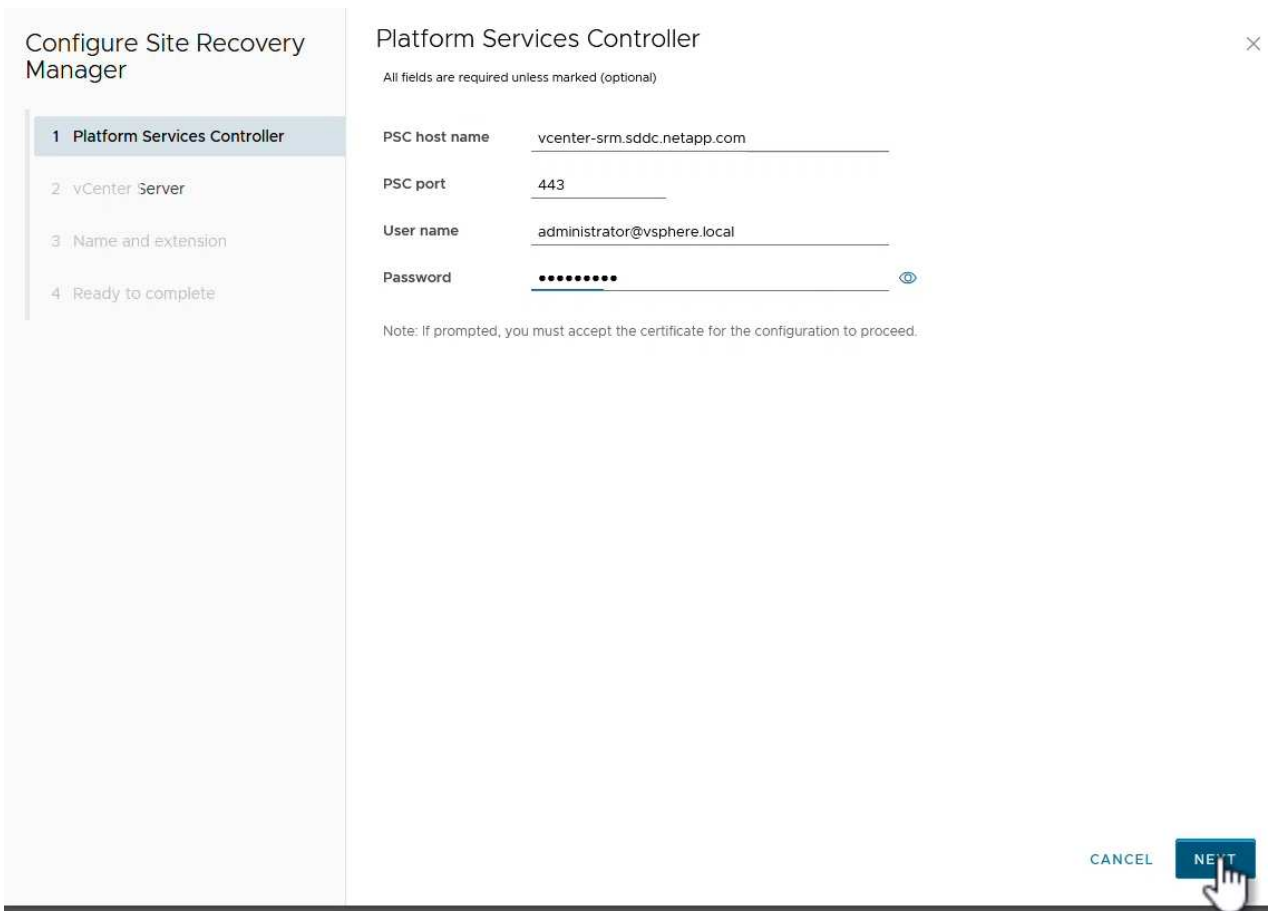
기본 및 보조 사이트의 SRM 어플라이언스를 연결합니다

운영 사이트와 보조 사이트 모두에 대해 다음 단계를 완료해야 합니다.

1. 웹 브라우저에서 로 이동하고 https://<SRM_appliance_IP>:5480 로그인합니다. * Configure Appliance * 를 클릭하여 시작합니다.



2. 사이트 복구 관리자 구성 마법사의 * 플랫폼 서비스 컨트롤러 * 페이지에서 SRM이 등록될 vCenter 서버의 자격 증명을 입력합니다. 계속하려면 * 다음 * 을 클릭하십시오.



3. vCenter Server * 페이지에서 연결된 가상 서버를 확인하고 * Next * 를 클릭하여 계속합니다.
4. 이름 및 확장자 * 페이지에서 SRM 사이트의 이름, 관리자 이메일 주소 및 SRM에서 사용할 로컬 호스트를 입력합니다. 계속하려면 * 다음 * 을 클릭하십시오.

Configure Site Recovery Manager

- 1 Platform Services Controller
- 2 vCenter Server
- 3 Name and extension**
- 4 Ready to complete

Name and extension

All fields are required unless marked (optional)

Enter name and extension for Site Recovery Manager

Site name

A unique display name for this Site Recovery Manager site.

Administrator email

An email address to use for system notifications.

Local host

The address on the local host to be used by Site Recovery Manager.

Extension ID Default extension ID (com.vmware.vcDr)

Custom extension ID

The default extension ID is recommended for most configurations. For shared recovery site installations, in which multiple sites connect to a shared recovery site, use a unique custom extension ID for each SRM pair.

Extension ID

Organization

Description

CANCEL

BACK

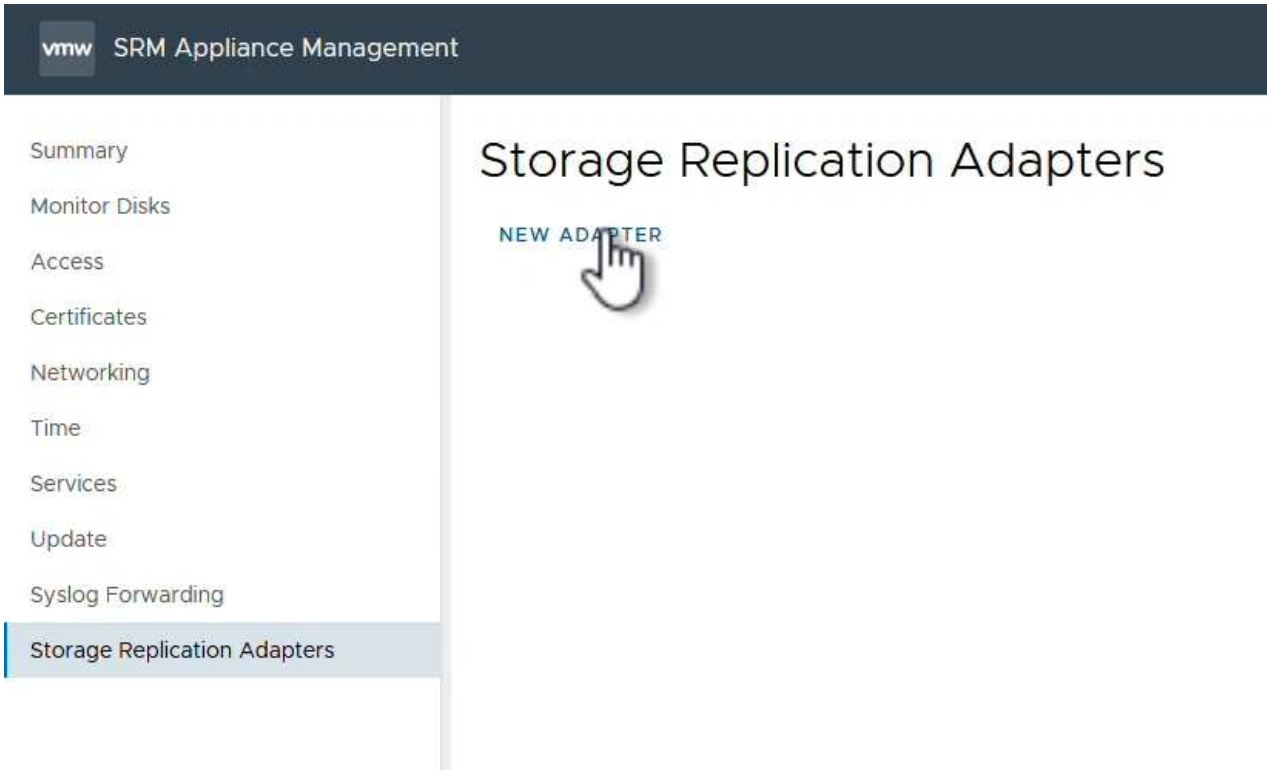
NEXT

5. 완료 준비 * 페이지에서 변경 사항 요약을 검토합니다

SRM 어플라이언스에 SRA를 구성합니다

SRM 어플라이언스에 SRA를 구성하려면 다음 단계를 수행하십시오.

1. 에서 ONTAP용 SRA 도구 10 을 "[NetApp Support 사이트](#)" 다운로드하고 tar.gz 파일을 로컬 폴더에 저장합니다.
2. SRM 관리 어플라이언스의 왼쪽 메뉴에서 * Storage Replication Adapters * 를 클릭한 다음 * New Adapter * 를 클릭합니다.



3. ONTAP tools 10 설명서 사이트()에 설명된 단계를 따릅니다 "[SRM 어플라이언스에 SRA를 구성합니다](#)". 완료되면 SRA는 vCenter 서버의 제공된 IP 주소 및 자격 증명을 사용하여 SRA와 통신할 수 있습니다.

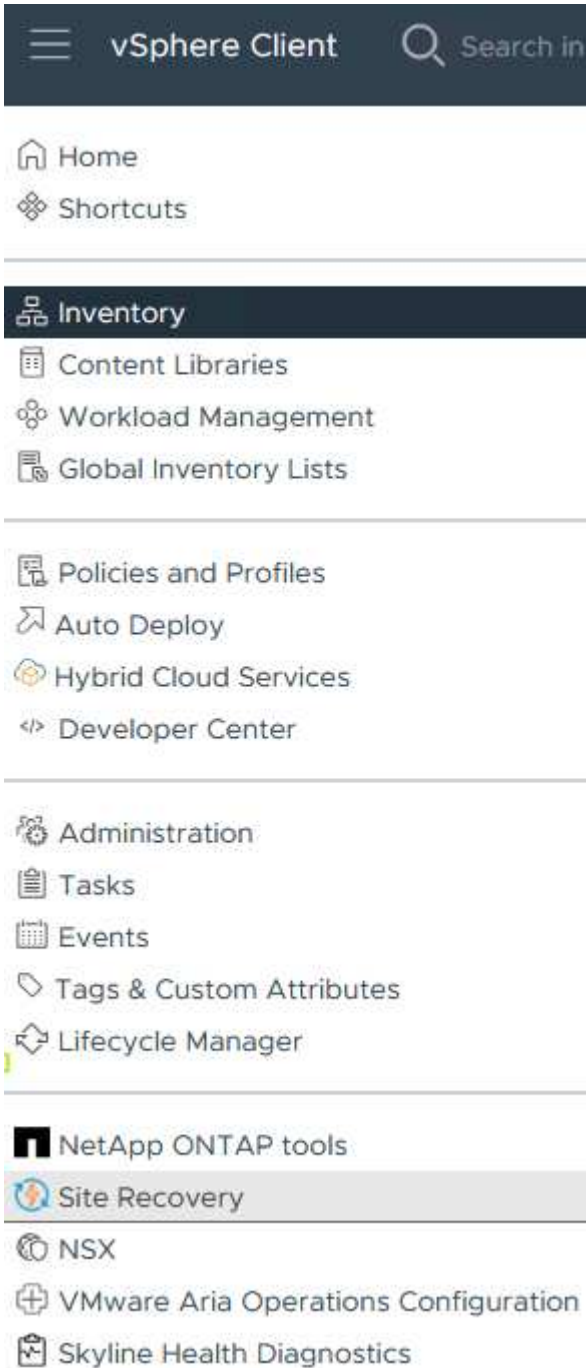
SRM에 대한 사이트 복구를 구성합니다

사이트 페어링을 구성하고 보호 그룹을 생성하려면 다음 단계를 완료하십시오.

SRM에 대한 사이트 페어링을 구성합니다

다음 단계는 운영 사이트의 vCenter 클라이언트에서 완료됩니다.

1. vSphere Client의 왼쪽 메뉴에서 * Site Recovery * 를 클릭합니다. 기본 사이트의 SRM 관리 UI에 대한 새 브라우저 창이 열립니다.



2. 사이트 복구 * 페이지에서 * 새 사이트 쌍 * 을 클릭합니다.

Before you can use Site Recovery, you must configure the connection between the Site Recovery Manager server and vSphere Replication server instances on the protected and recovery sites. This is known as a site pair.

NEW SITE PAIR

[Learn More](#)

3. 새 쌍 마법사 * 의 * 쌍 유형 * 페이지에서 로컬 vCenter 서버가 선택되었는지 확인하고 * 쌍 유형 * 을 선택합니다. 계속하려면 * 다음 * 을 클릭하십시오.


New Pair

- 1 Pair type
- 2 Peer vCenter Server
- 3 Services
- 4 Ready to complete

Pair type

Select a local vCenter Server.

vCenter Server

-  vcenter-vlsr.sddc.netapp.com

Pair type

Pair with a peer vCenter Server located in a different SSO domain

Pair with a peer vCenter Server located in the same SSO domain

CANCEL **NEXT**

4. 피어 vCenter * 페이지에서 보조 사이트의 vCenter 자격 증명을 입력하고 * vCenter 인스턴스 찾기 * 를 클릭합니다. vCenter 인스턴스가 검색되었는지 확인하고 * Next * 를 클릭하여 계속합니다.

New Pair

1 Pair type

2 Peer vCenter Server

3 Services

4 Ready to complete

Peer vCenter Server



All fields are required unless marked (optional)

Enter the Platform Services Controller details for the peer vCenter Server.

PSC host name

PSC port

User name

Password

FIND VCENTER SERVER INSTANCES

Select a vCenter Server you want to pair.

vCenter Server

- vcenter-srm.sddc.netapp.com

CANCEL

BACK

NEXT

- 서비스 * 페이지에서 제안된 사이트 페어링 옆에 있는 확인란을 선택합니다. 계속하려면 * 다음 * 을 클릭하십시오.

New Pair

- 1 Pair type
- 2 Peer vCenter Server
- 3 Services
- 4 Ready to complete

Services

The following services were identified on the selected vCenter Server instances. Select the ones you want to pair.

Service	vcenter-vlsr.sddc.netapp.com	vcenter-srm.sddc.netapp.com
<input checked="" type="checkbox"/> Site Recovery Manager (com.vmware.vc...	Site 1	Site 2

CANCEL

BACK

NEXT

6. 완료 준비 * 페이지에서 제안된 구성을 검토한 후 * 마침 * 버튼을 클릭하여 사이트 페어링을 생성합니다
7. 새 사이트 쌍과 요약 정보는 요약 페이지에서 볼 수 있습니다.

Summary

RECONNECT

BREAK SITE PAIR



vCenter Server: [vcenter-vlsr.sddc.netapp.com](#) [vcenter-srm.sddc.netapp.com](#)
vCenter Version: 8.0.2, 22385739 8.0.2, 22385739
vCenter Host Name: vcenter-vlsr.sddc.netapp.com:443 vcenter-srm.sddc.netapp.com:443
Platform Services Controller: vcenter-vlsr.sddc.netapp.com:443 vcenter-srm.sddc.netapp.com:443

Site Recovery Manager

EXPORT/IMPORT SRM CONFIGURATION

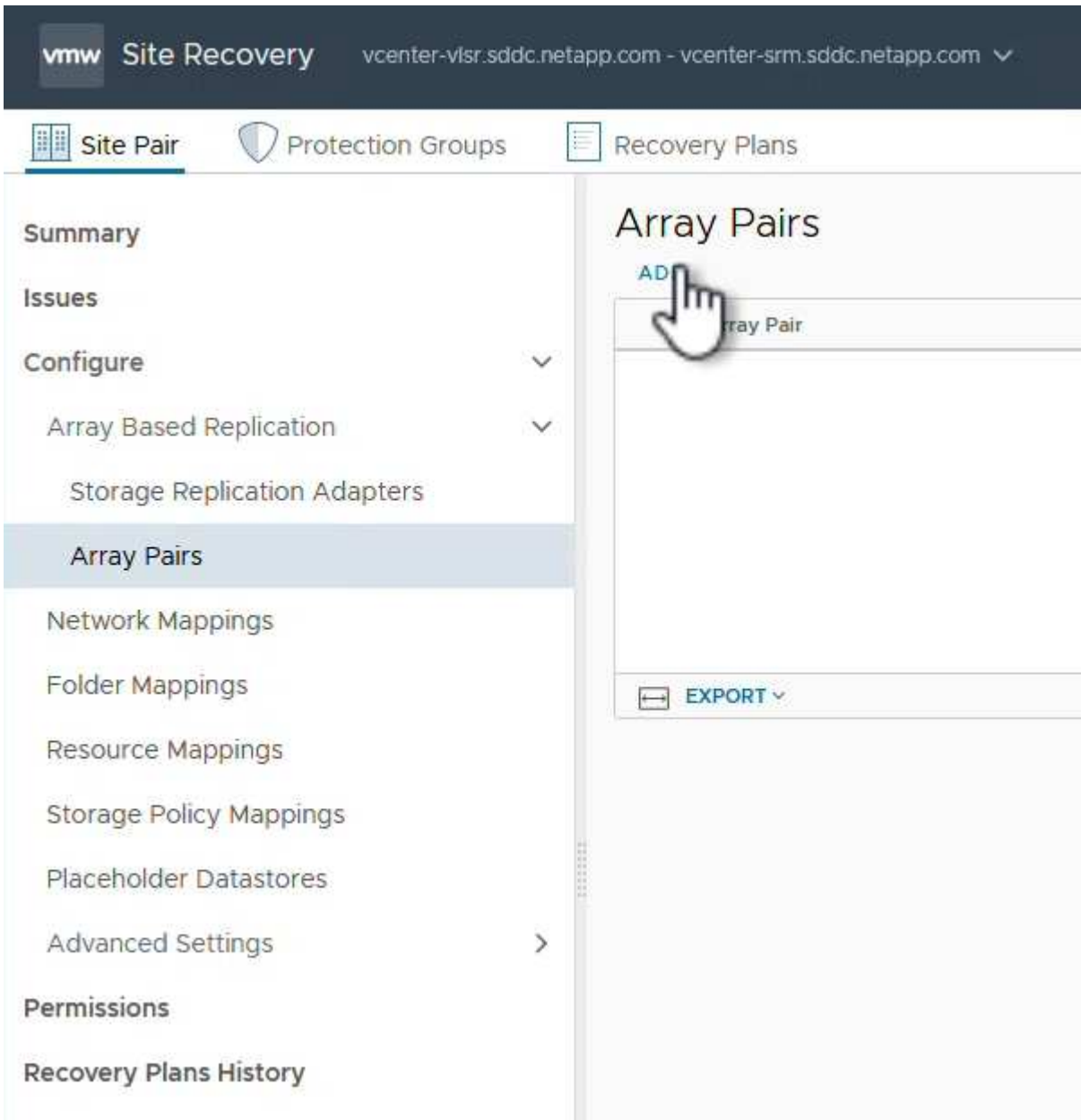
Protection Groups:0 Recovery Plans:0

Name	Site 1 RENAME	Site 2 RENAME
Server	srm-site1.sddc.netapp.com:443 ACTIONS	srm-site2.sddc.netapp.com:443 ACTIONS
Version	8.8.0, 23263429	8.8.0, 23263429
ID	com.vmware.vcDr	com.vmware.vcDr
Logged in as	VSPHERE.LOCAL\Administrator	VSPHERE.LOCAL\Administrator
Remote SRM connection	✓ Connected	✓ Connected

SRM용 어레이 쌍을 추가합니다

다음 단계는 기본 사이트의 사이트 복구 인터페이스에서 완료됩니다.

1. 사이트 복구 인터페이스의 왼쪽 메뉴에서 * 구성 > 어레이 기반 복제 > 어레이 쌍 * 으로 이동합니다. 시작하려면 * ADD * 를 클릭하십시오.



2. 어레이 쌍 추가 * 마법사의 * 스토리지 복제 어댑터 * 페이지에서 기본 사이트에 대한 SRA 어댑터가 있는지 확인하고 * 다음 * 을 클릭하여 계속합니다.

Add Array Pair

1 Storage replication adapter

2 Local array manager

3 Remote array manager

4 Array pairs

5 Ready to complete

Storage replication adapter

Select a storage replication adapter (SRA):

	Storage Replication Adapter	Status	Vendor	Version	Stretched Storage
>	NetApp Storage Replication Ada...	OK	NetApp	10.1	Not Support...

Items per page AUTO 1 items

CANCEL

NEXT

3. Local Array Manager * 페이지에서 운영 사이트의 어레이 이름, 스토리지 시스템의 FQDN, NFS를 지원하는 SVM IP 주소, 검색할 특정 볼륨의 이름을 입력합니다. 계속하려면 * 다음 * 을 클릭하십시오.

Add Array Pair

1 Storage replication adapter

2 Local array manager

3 Remote array manager

4 Array pairs

5 Ready to complete

Local array manager

×

Array managers allow Site Recovery Manager to communicate with array based replication storage systems.

Enter a name for the array manager on "vcenter-vlsr.sddc.netapp.com":

Array_1

Storage Array Parameters

Storage System connection parameters

Storage Management IP Address or Hostname ontap-source.sddc.netapp.com

Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.

NFS Hostnames or IP Addresses 172.21.118.49

Comma separated list of Hostnames or IP addresses that serve NFS to ESX hosts. Leave blank for SAN only.

Storage Virtual Machine(SVM) Name SQL_NFS

Provide Storage Virtual Machine(SVM) name. Leave blank if connecting directly to an SVM.

Volume include list SQL_NFS

Comma separated list of strings in volume names to discover. Leave blank to discover all. Example: srm,sql,win.

Volume exclude list

Comma separated list of strings in volume names to exclude. Leave blank to exclude none. Example: home,dept,tmp.

CANCEL

BACK

NEXT

4. 원격 스토리지 관리자 * 에서 보조 사이트의 ONTAP 스토리지 시스템에 대한 마지막 단계와 동일한 정보를 입력합니다.

Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs
- 5 Ready to complete

Remote array manager

Do not create a remote array manager now.

Enter a name for the array manager on "vcenter-srm.sddc.netapp.com":

Array_2

Storage Array Parameters

Storage System connection parameters

Storage Management IP Address or Hostname ontap-destination.sddc.netapp.com

Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.

NFS Hostnames or IP Addresses 172.21.118.51

Comma separated list of Hostnames or IP addresses that serve NFS to ESX hosts. Leave blank for SAN only.

Storage Virtual Machine(SVM) Name SRM_NFS

Provide Storage Virtual Machine(SVM) name. Leave blank if connecting directly to an SVM.

Volume include list |

Comma separated list of strings in volume names to discover. Leave blank to discover all. Example: srm,sql,win.

Volume exclude list |

Comma separated list of strings in volume names to exclude. Leave blank to exclude none. Example: home,dept,tmp.

CANCEL

BACK

NEXT

5. Array Pairs * 페이지에서 활성화할 어레이 쌍을 선택하고 * Next * 를 클릭하여 계속합니다.

Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs**
- 5 Ready to complete

Array pairs

Select the array pairs to enable:

<input checked="" type="checkbox"/>	vcenter-vlsr.sddc.netapp.com	vcenter-srm.sddc.netapp.com	Status
<input checked="" type="checkbox"/>	ontap-source:SQL_NFS (Array_1)	ontap-destination:SRM_NFS (Array_2)	Ready to be enabled

1 1 items

CANCEL

BACK

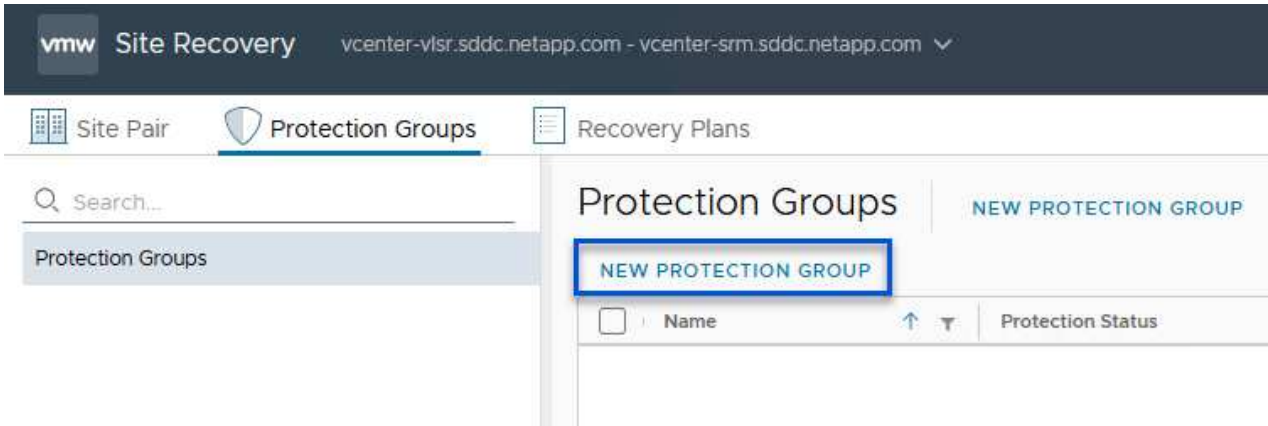
NEXT

6. 완료 준비 * 페이지에서 정보를 검토하고 * 마침 * 을 클릭하여 어레이 쌍을 생성합니다.

SRM에 대한 보호 그룹을 구성합니다

다음 단계는 기본 사이트의 사이트 복구 인터페이스에서 완료됩니다.

1. Site Recovery 인터페이스에서 * Protection Groups * 탭을 클릭한 다음 * New Protection Group * 을 클릭하여 시작합니다.



2. 새 보호 그룹 * 마법사의 * 이름 및 방향 * 페이지에서 그룹 이름을 입력하고 데이터 보호를 위한 사이트 방향을 선택합니다.

The screenshot shows the 'New Protection Group' wizard in the Site Recovery console. The wizard has five steps: 1. Name and direction (selected), 2. Type, 3. Datastore groups, 4. Recovery plan, and 5. Ready to complete. The 'Name and direction' step is active and contains the following fields:

- Name:** A text input field containing 'SQL_Datastore' with a character count of '67 characters remaining'.
- Description:** An optional text input field with a character count of '4096 characters remaining'.
- Direction:** Two radio button options: 'Site 1 -> Site 2' (selected) and 'Site 2 -> Site 1'.
- Location:** A search input field with a dropdown menu showing 'Protection Groups'.

At the bottom right of the wizard, there are 'CANCEL' and 'NEXT' buttons.

3. Type * 페이지에서 보호 그룹 유형(데이터 저장소, VM 또는 VVol)을 선택하고 어레이 쌍을 선택합니다. 계속하려면 * 다음 * 을 클릭하십시오.

New Protection Group

- 1 Name and direction
- 2 Type**
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete

Type

Select the type of protection group you want to create:

- Datastore groups (array-based replication)**
Protect all virtual machines which are on specific datastores.
- Individual VMs (vSphere Replication)
Protect specific virtual machines, regardless of the datastores.
- Virtual Volumes (vVol replication)
Protect virtual machines which are on replicated vVol storage.

Select array pair

Array Pair	Array Manager Pair
<input checked="" type="radio"/> ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2	nfs_array1 ↔ nfs_Array2
<input type="radio"/> ontap-source:SQL_NFS ↔ ontap-destination:SRM_NFS	Array_1 ↔ Array_2

Items per page: AUTO 2 array pairs

[CANCEL](#) [BACK](#) [NEXT](#)

4. Datastore groups * 페이지에서 보호 그룹에 포함할 데이터 저장소를 선택합니다. 선택한 각 데이터 저장소에 대해 현재 데이터 저장소에 상주하는 VM이 표시됩니다. 계속하려면 * 다음 * 을 클릭하십시오.

New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete

Datastore groups

Select the datastore groups to be part of this protection group. Datastore groups contain datastores which must be recovered together.

SELECT ALL CLEAR SELECTION

<input checked="" type="checkbox"/>	Datastore Group	Status
<input checked="" type="checkbox"/>	NFS_DS1	Add to this protection group

1 Items per page AUTO ^ 1 datastore groups

The following virtual machines are in the selected datastore groups:

Virtual Machine	Datastore	Status
SQLSRV-01	NFS_DS1	Add to this protection group
SQLSRV-03	NFS_DS1	Add to this protection group
SQLSRV-02	NFS_DS1	Add to this protection group

CANCEL BACK NEXT

5. 복구 계획 * 페이지에서 필요에 따라 복구 계획에 보호 그룹을 추가하도록 선택합니다. 이 경우 복구 계획이 아직 생성되지 않았으므로 * 복구 계획에 추가하지 마십시오 * 가 선택됩니다. 계속하려면 * 다음 * 을 클릭하십시오.

New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete

Recovery plan

You can optionally add this protection group to a recovery plan.

- Add to existing recovery plan
- Add to new recovery plan
- Do not add to recovery plan now

 The protection group cannot be recovered unless it is added to a recovery plan.

CANCEL

BACK

NEXT

6. 완료 준비 * 페이지에서 새 보호 그룹 매개 변수를 검토하고 * 마침 * 을 클릭하여 그룹을 생성합니다.

New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete**

Ready to complete



Review your selected settings.

Name	SQL_Datastore
Description	
Protected site	Site 1
Recovery site	Site 2
Location	Protection Groups
Protection group type	Datastore groups (array-based replication)
Array pair	ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2 (nfs_array1 ↔ nfs_array2)
Datastore groups	NFS_DS1
Total virtual machines	3
Recovery plan	none

CANCEL

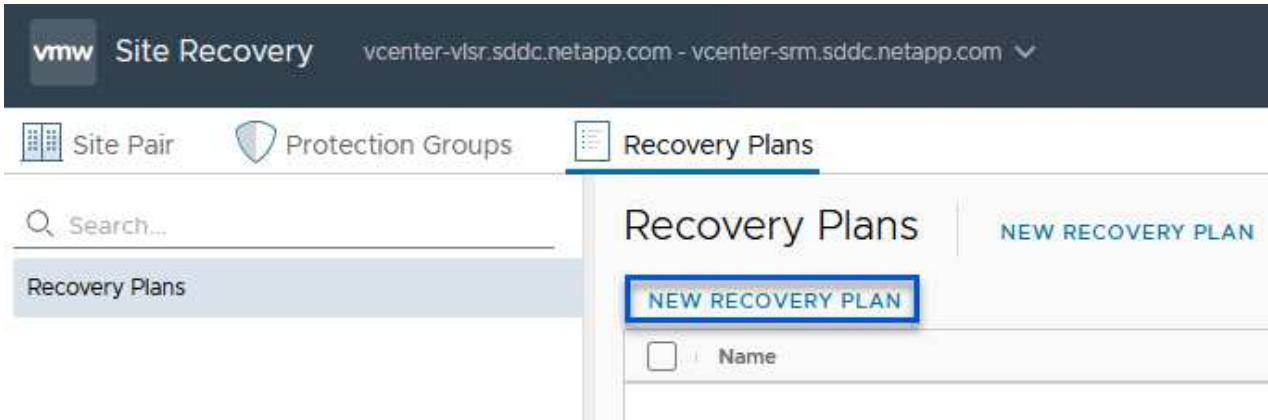
BACK

FINISH

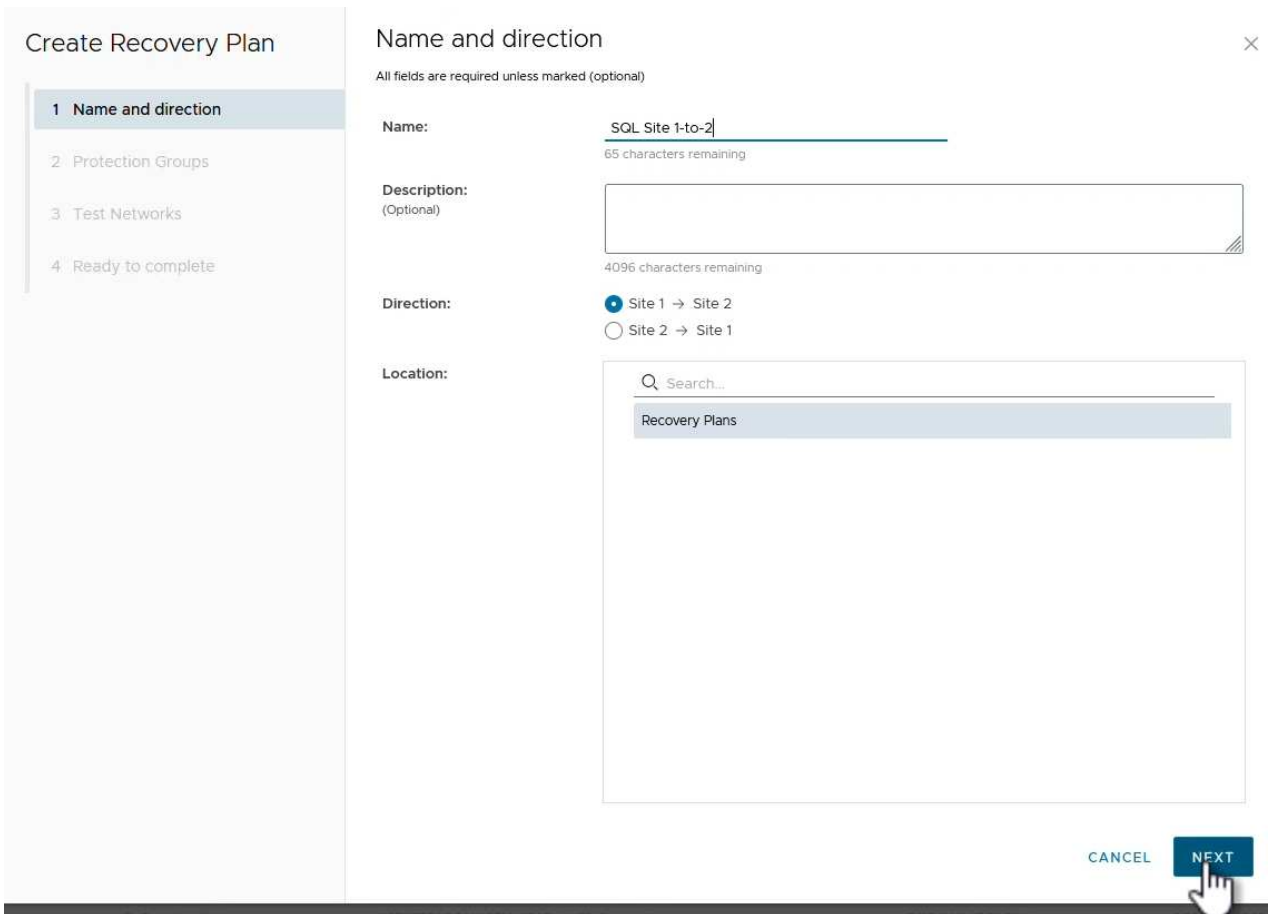
SRM에 대한 복구 계획을 구성합니다

다음 단계는 기본 사이트의 사이트 복구 인터페이스에서 완료됩니다.

1. Site Recovery 인터페이스에서 * Recovery plan * 탭을 클릭한 다음 * New Recovery Plan * 을 클릭하여 시작합니다.



2. 복구 계획 생성 * 마법사의 * 이름 및 방향 * 페이지에서 복구 계획의 이름을 입력하고 소스 사이트와 대상 사이트 간의 방향을 선택합니다. 계속하려면 * 다음 * 을 클릭하십시오.



3. 보호 그룹 * 페이지에서 이전에 생성한 보호 그룹을 복구 계획에 포함시킵니다. 계속하려면 * 다음 * 을 클릭하십시오.

The screenshot shows the 'Create Recovery Plan' wizard in step 2, 'Protection Groups'. The left sidebar shows the progress: 1. Name and direction, 2. Protection Groups (current), 3. Test Networks, 4. Ready to complete. The main area is titled 'Protection Groups' and shows a table with columns 'Name' and 'Description'. One row is visible: 'SQL_Datastore'. The table has a 'Selected (1)' filter and a '1' icon in the bottom left. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'. A mouse cursor is pointing at the 'NEXT' button.

4. 테스트 네트워크*에서 계획 테스트 중에 사용할 특정 네트워크를 구성합니다. 매핑이 없거나 네트워크를 선택하지 않으면 격리된 테스트 네트워크가 생성됩니다. 계속하려면 * 다음 * 을 클릭하십시오.

Create Recovery Plan

- 1 Name and direction
- 2 Protection Groups
- 3 Test Networks
- 4 Ready to complete

Test Networks ×

Select the networks to use while running tests of this plan.

i If "Use site-level mapping" is selected and no such mapping exists, an isolated test network will be created.

Recovery Network	↑ ↓	Test Network	
Datacenter > DPortGroup	☰	Use site-level mapping	CHANGE
Datacenter > Mgmt 3376	☰	Mgmt 3376	☰ CHANGE
Datacenter > NFS 3374	☰	NFS 3374	☰ CHANGE
Datacenter > VLAN 181	☰	Use site-level mapping	CHANGE
Datacenter > VM Network	☰	Use site-level mapping	CHANGE
Datacenter > vMotion 3373	☰	Use site-level mapping	CHANGE
Datacenter > vSAN 3422	☰	Use site-level mapping	CHANGE

7 network(s)

CANCEL
BACK
NEXT

5. 완료 준비 * 페이지에서 선택한 매개 변수를 검토한 후 * 마침 * 을 클릭하여 복구 계획을 생성합니다.

SRM을 사용한 재해 복구 작업

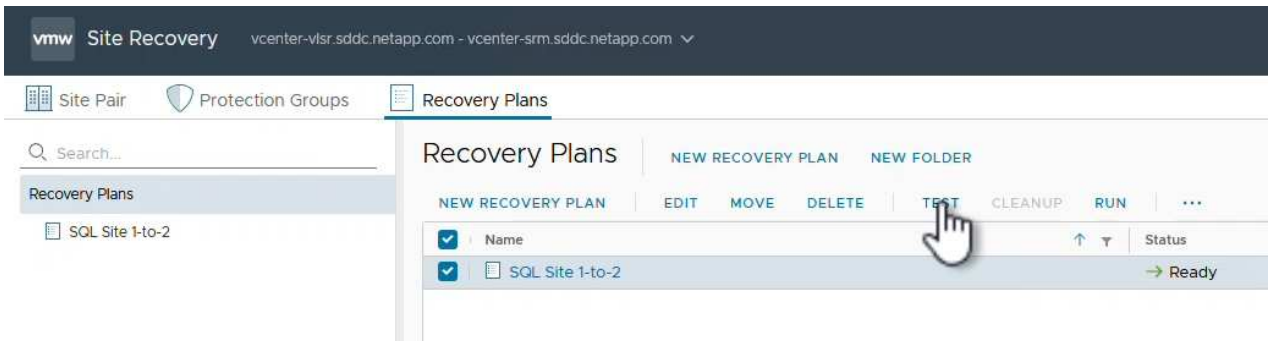
이 섹션에서는 장애 조치 테스트, 장애 조치 수행, 재보호 수행 및 장애 복구를 비롯하여 SRM에서 재해 복구를 사용하는 다양한 기능에 대해 설명합니다.

https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-srm-operational_best_practices.html ["운영 모범 사례"] SRM 재해 복구 작업에 ONTAP 스토리지를 사용하는 방법에 대한 자세한 내용은 을 참조하십시오.

SRM을 사용한 장애 조치 테스트

다음 단계는 사이트 복구 인터페이스에서 완료됩니다.

1. 사이트 복구 인터페이스에서 * 복구 계획 * 탭을 클릭한 다음 복구 계획을 선택합니다. 테스트 * 버튼을 클릭하여 보조 사이트에 대한 장애 조치 테스트를 시작합니다.

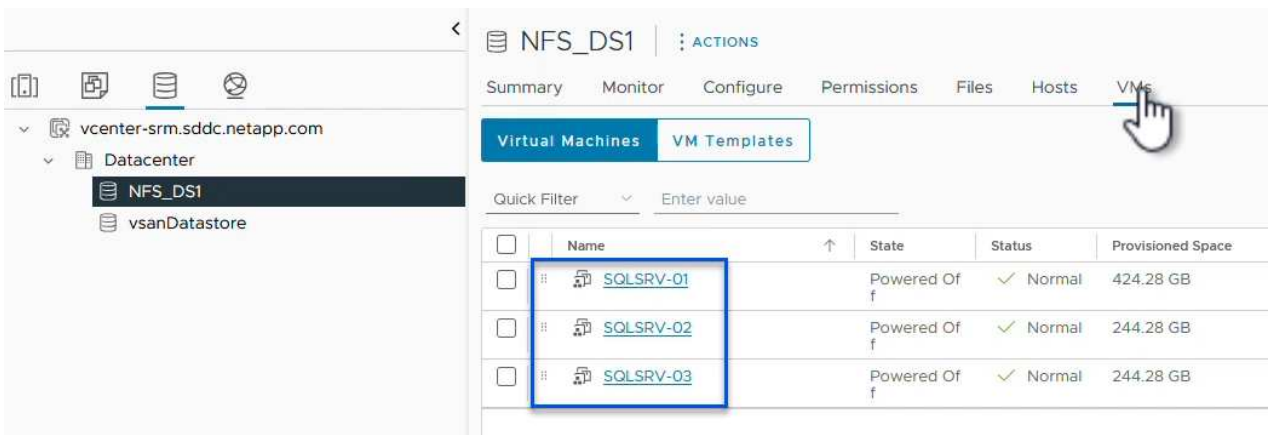


2. Site Recovery 작업창과 vCenter 작업창에서 테스트 진행률을 볼 수 있습니다.

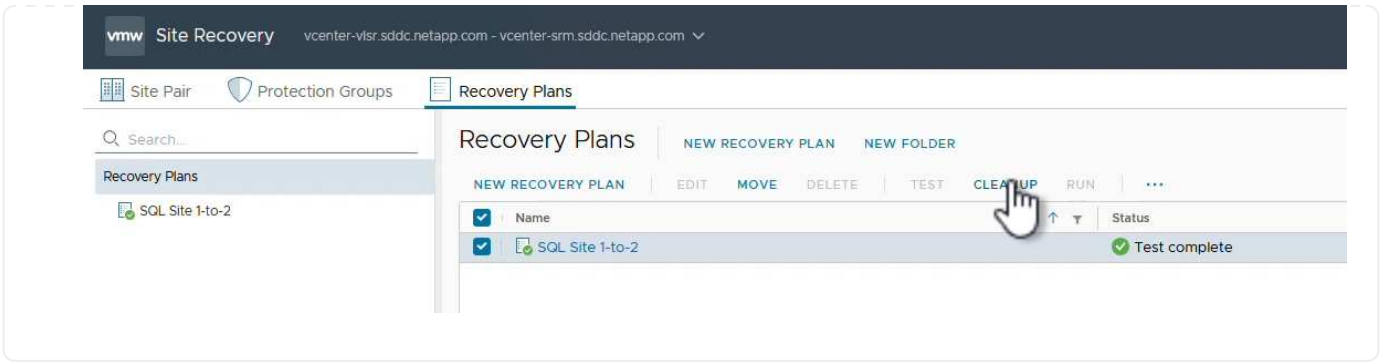
The screenshot shows the 'Recent Tasks' table in the vCenter console. The table has columns for Task Name, Target, Status, Initiator, and Queued For. The first task, 'Test Recovery Plan', is highlighted with a progress bar showing 6% completion.

Task Name	Target	Status	Initiator	Queued For
Test Recovery Plan	vcenter-vlsr.sddc.netapp.com	6 %	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	11 ms
Create Recovery Plan	vcenter-vlsr.sddc.netapp.com	Completed	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	10 ms
Set virtual machine custom value	SQLSRV-02	Completed	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	4 ms
Set virtual machine custom value	SQLSRV-01	Completed	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	3 ms

3. SRM은 SRA를 통해 보조 ONTAP 스토리지 시스템으로 명령을 전송합니다. 최신 스냅샷의 FlexClone가 생성되고 보조 vSphere 클러스터에 마운트됩니다. 새로 마운트된 데이터 저장소는 스토리지 인벤토리에서 볼 수 있습니다.



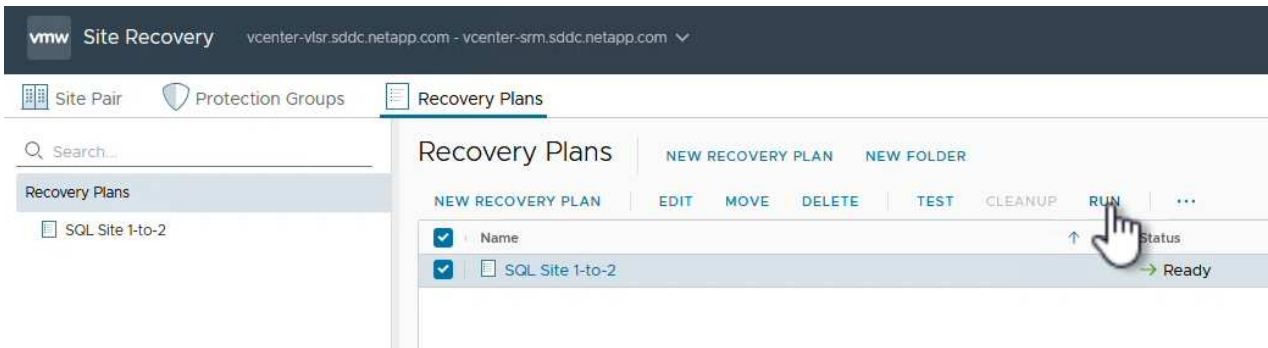
4. 테스트가 완료되면 * Cleanup * 을 클릭하여 데이터 저장소를 마운트 해제하고 원래 환경으로 되돌립니다.



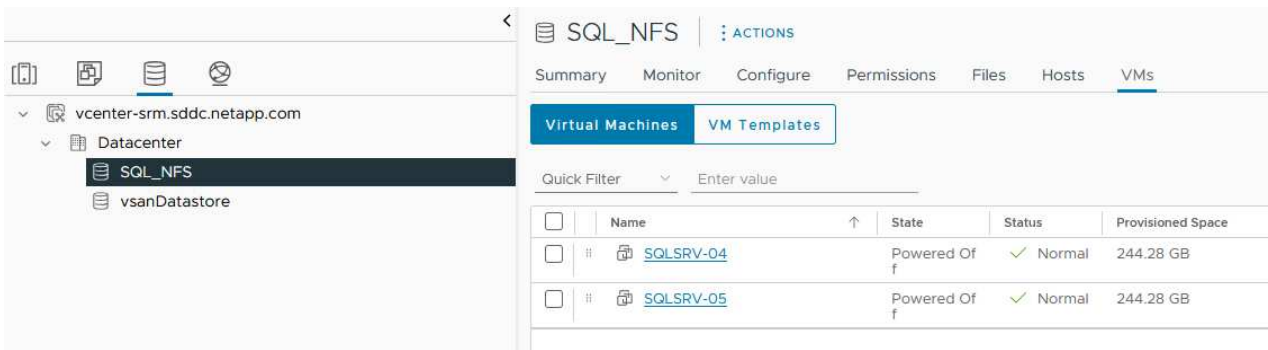
SRM에서 복구 계획을 실행합니다

보조 사이트에 대한 전체 복구 및 장애 조치를 수행합니다.

1. 사이트 복구 인터페이스에서 * 복구 계획 * 탭을 클릭한 다음 복구 계획을 선택합니다. Run * 버튼을 클릭하여 보조 사이트로 장애 조치를 시작합니다.



2. 파일오버가 완료되면 데이터 저장소가 마운트되고 보조 사이트에 등록된 VM이 표시됩니다.



파일오버가 완료되면 SRM에서 추가 기능을 사용할 수 있습니다.

- 재보호 *: 복구 프로세스가 완료되면 이전에 지정된 복구 사이트가 새 운영 사이트의 역할을 맡습니다. 그러나 복구 작업 중에 SnapMirror 복제가 중단되어 새 운영 사이트가 향후 재해에 취약하다는 점에 유의해야 합니다. 지속적인 보호를 위해 새 프로덕션 사이트를 다른 사이트로 복제하여 새 프로덕션 사이트에 대한 새로운 보호 기능을 설정하는 것이 좋습니다. 원래 운영 사이트가 계속 작동하는 경우 VMware 관리자는 해당 사이트를 새 복구 사이트로 재활용하여 보호 방향을 효과적으로 전환할 수 있습니다. 재보호는 심각한 장애가 아닌 경우에만 실현 가능하여 원래 vCenter Server, ESXi 서버, SRM 서버 및 해당 데이터베이스의 최종 복구 기능이 필요하다는 점을

강조하는 것이 중요합니다. 이러한 구성 요소를 사용할 수 없는 경우 새 보호 그룹 및 새 복구 계획을 생성해야 합니다.

페일백: 장애 복구 작업은 역방향 장애 조치로, 작업을 원래 사이트로 되돌립니다. 장애 복구 프로세스를 시작하기 전에 원래 사이트의 기능이 다시 활성화되었는지 확인하는 것이 중요합니다. 원활한 페일백을 위해 재보호 프로세스를 완료한 후 최종 페일백을 실행하기 전에 테스트 페일오버를 수행하는 것이 좋습니다. 이 방법은 원래 사이트의 시스템에서 작업을 완벽하게 처리할 수 있음을 확인하는 확인 단계 역할을 합니다. 이러한 접근 방식을 따르면 위험을 최소화하고 원래 운영 환경으로 보다 안정적으로 전환할 수 있습니다.

추가 정보

VMware SRM에서 ONTAP 스토리지를 사용하는 방법에 대한 NetApp 설명서는 [을 참조하십시오 "ONTAP를 사용하는 VMware 사이트 복구 관리자"](#)

ONTAP 스토리지 시스템 구성에 대한 자세한 내용은 [을 참조하십시오 "ONTAP 9 설명서"](#) 가운데.

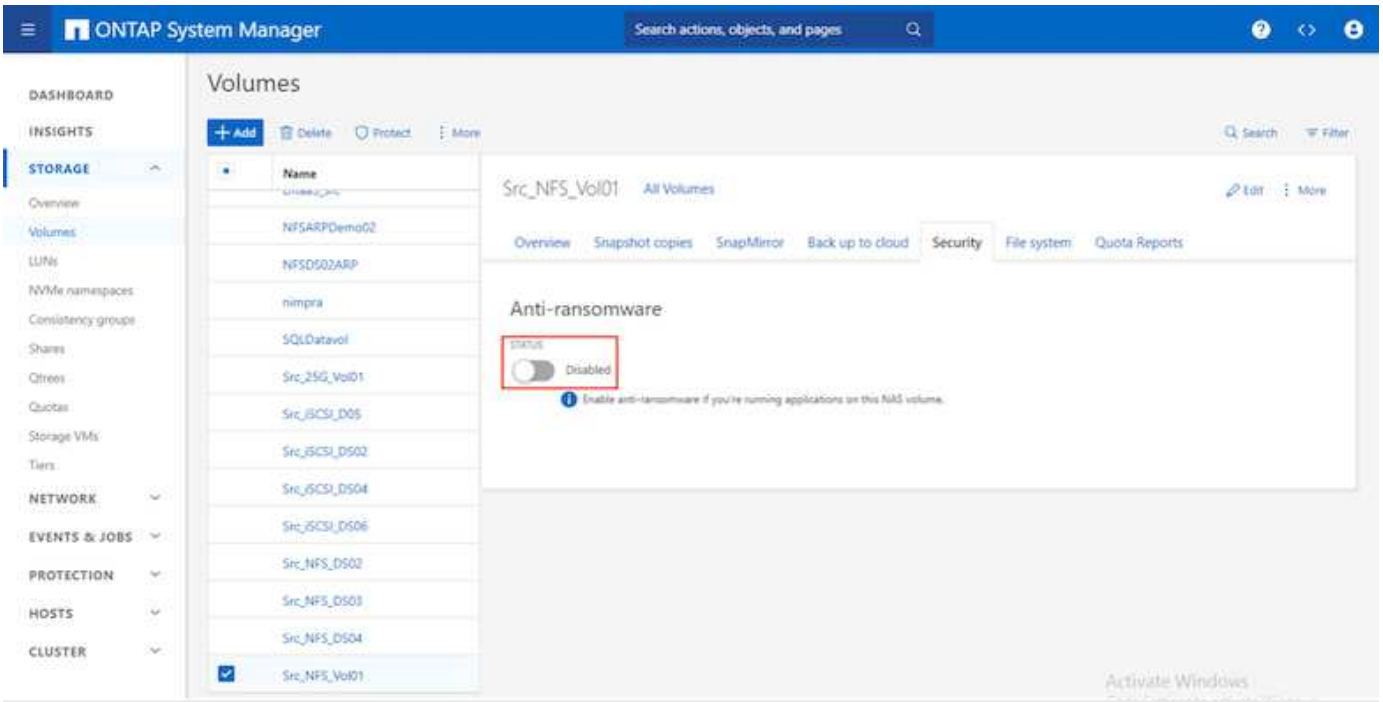
VCF 구성에 대한 자세한 내용은 [을 참조하십시오 "VMware Cloud Foundation 설명서"](#).

NFS 스토리지에 대한 자율적 랜섬웨어 방어

NFS 스토리지에 대한 자율적 랜섬웨어 방어

랜섬웨어를 최대한 빨리 감지하는 것은 확산을 방지하고 비용이 많이 드는 다운타임을 방지하는 데 매우 중요합니다. 효과적인 랜섬웨어 감지 전략에서는 ESXi 호스트 및 게스트 VM 레벨에 여러 계층의 보호를 통합해야 합니다. 랜섬웨어 공격에 대한 포괄적인 방어 체계를 구축하기 위해 여러 보안 수단을 구현하지만, ONTAP를 사용하면 전체 방어 방식에 보호 계층을 더 추가할 수 있습니다. 몇 가지 기능을 소개하려면 Snapshots, 자율적 랜섬웨어 Protection, 무단 변경 방지 스냅샷 등으로 시작합니다.

위에서 언급한 기능이 VMware와 함께 작동하여 랜섬웨어로부터 데이터를 보호하고 복구하는 방법을 살펴보겠습니다. 공격으로부터 vSphere 및 게스트 VM을 보호하려면 엔드포인트에 대한 EDR/XDR/SIEM 분리, 보안 업데이트 설치, 적절한 강화 지침 준수 등 여러 가지 조치를 취해야 합니다. 데이터 저장소에 상주하는 각 가상 머신도 표준 운영 체제를 호스팅합니다. 엔터프라이즈 서버 맬웨어 방지 제품군이 설치되어 있고 정기적으로 업데이트되도록 하십시오. 이는 다계층 랜섬웨어 방어 전략의 필수 구성 요소입니다. 이와 함께 데이터 저장소를 지원하는 NFS 볼륨에서 ARP(Autonomous Ransomware Protection)를 활성화하십시오. ARP는 볼륨 워크로드 활동과 데이터 엔트로피를 조사하여 랜섬웨어를 자동으로 탐지하는 온박스 ML을 활용합니다. ARP는 ONTAP 내장 관리 인터페이스 또는 시스템 관리자를 통해 구성할 수 있으며 볼륨별로 활성화됩니다.

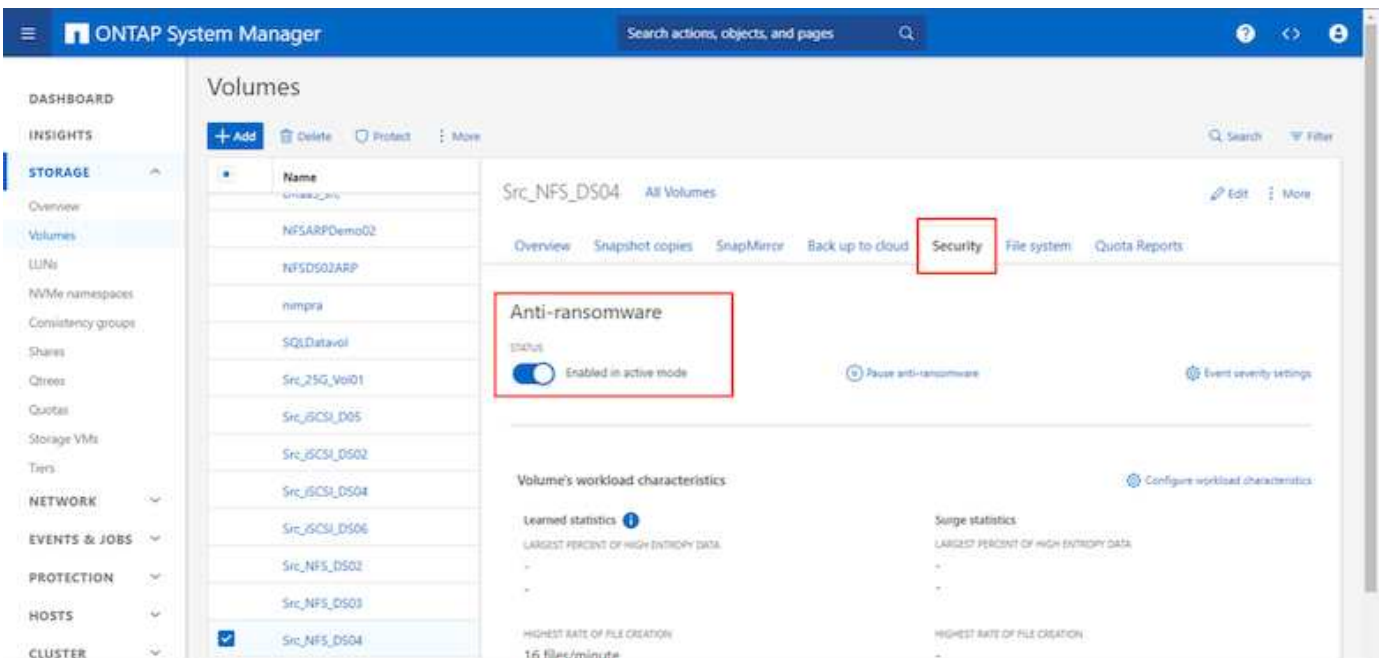


현재 기술 미리 보기에 있는 새로운 NetApp ARP/AI를 사용하면 학습 모드가 필요하지 않습니다. 대신 AI 기반 랜섬웨어 감지 기능을 통해 바로 액티브 모드로 전환할 수 있습니다.



ONTAP One을 사용하면 이러한 모든 기능 세트가 완전히 무료입니다. 라이선스 장벽에 대한 걱정 없이 NetApp의 강력한 데이터 보호, 보안 및 ONTAP가 제공하는 모든 기능을 이용할 수 있습니다.

활성 모드로 전환하면 랜섬웨어가 될 수 있는 비정상적인 볼륨 활동을 찾아내기 시작합니다. 비정상적인 활동이 감지되면 스냅샷 자동 복사본이 즉시 생성되고, 파일 감염에 가장 가까운 복원 지점을 제공합니다. ARP는 암호화된 볼륨에 새 확장자가 추가되거나 파일 확장자가 수정될 때 VM 외부에 있는 NFS 볼륨에서 VM별 파일 확장자의 변경을 감지할 수 있습니다.

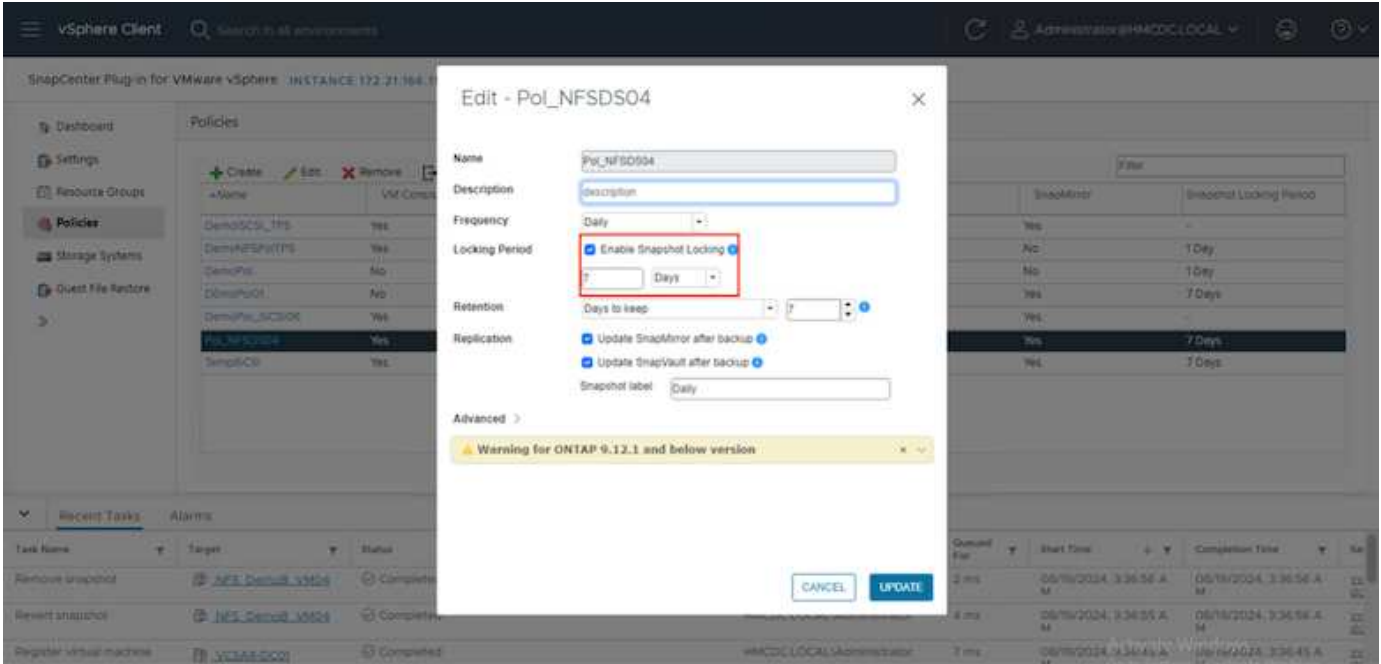


랜섬웨어 공격이 가상 머신(VM)을 대상으로 하고 VM 외부에서 변경하지 않고 VM 내의 파일을 변경하는 경우, VM의

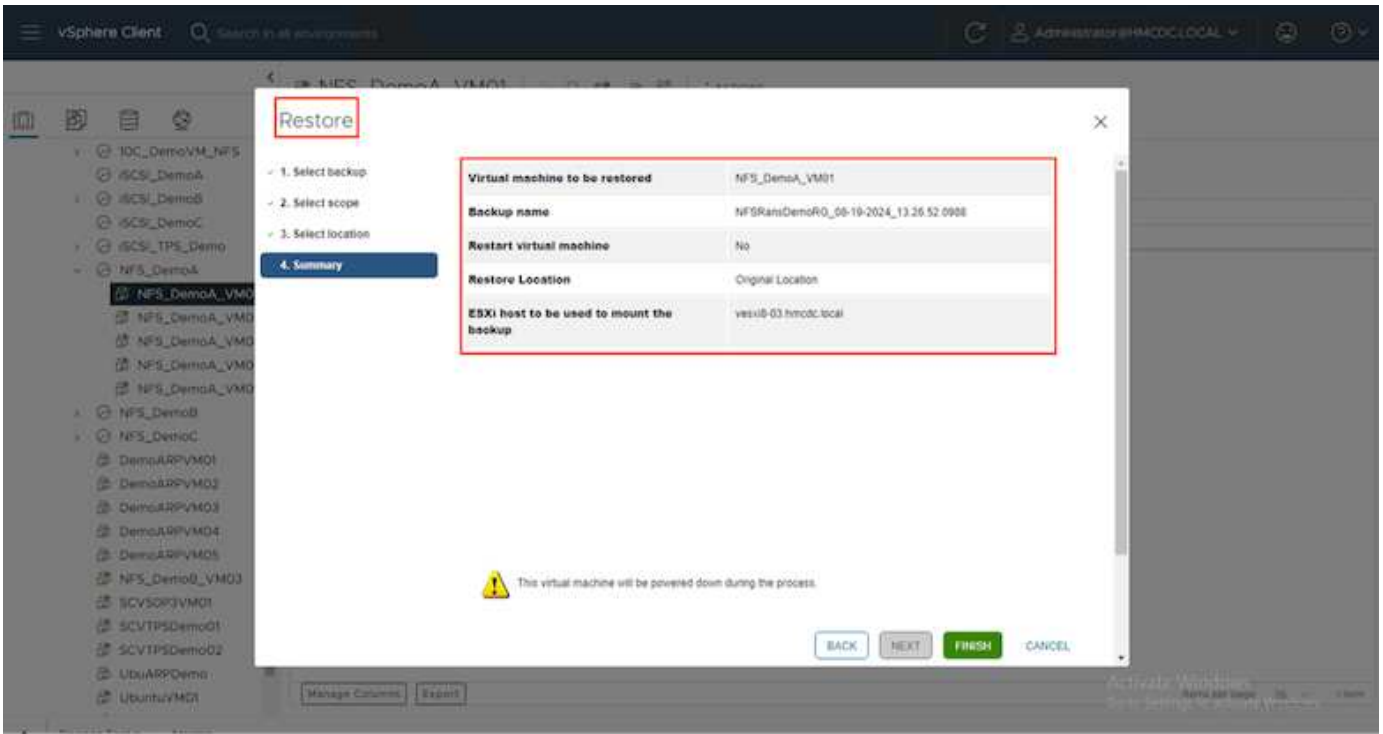
기본 엔트로피(예: .txt, .docx 또는 .mp4 파일)가 낮은 경우에도 ARP(Advanced Ransomware Protection)가 위협을 감지합니다. ARP는 이 시나리오에서 보호 스냅샷을 생성하지만 VM 외부의 파일 확장자가 변조되지 않았기 때문에 위협 경고를 생성하지 않습니다. 이러한 시나리오에서는 초기 방어 계층이 이상 현상을 식별하지만 ARP는 엔트로피를 기반으로 스냅샷을 생성하는 데 도움이 됩니다.

자세한 내용은 의 "ARP 및 가상 머신" 섹션을 "ARP 사용 및 고려 사항"참조하십시오.

파일에서 백업 데이터로 이동하는 랜섬웨어 공격은 파일 암호화를 시작하기 전에 삭제를 시도하여 백업 및 스냅샷 복구 지점을 점점 더 많이 타겟으로 삼습니다. 그러나 ONTAP를 사용하면 를 사용하여 기본 또는 보조 시스템에서 변조 방지 스냅샷을 생성하여 이 문제를 방지할 수 "NetApp Snapshot™ 복사본 잠금"있습니다.



이러한 스냅샷 복사본은 랜섬웨어 공격자나 악성 관리자가 삭제하거나 변경할 수 없으므로 공격 후에도 사용할 수 있습니다. 데이터 저장소 또는 특정 가상 머신이 영향을 받는 경우 SnapCenter는 몇 초 만에 가상 머신 데이터를 복구하여 조직의 다운타임을 최소화할 수 있습니다.



위의 내용은 ONTAP 스토리지가 기존 기술에 레이어를 추가하여 환경의 미래 대비를 강화하는 방법을 보여줍니다.

자세한 내용은 의 지침을 "[바로 랜섬웨어용 NetApp 솔루션입니다](#)" 참조하십시오.

이제 이 모든 것을 오케스트레이션하여 SIEM 툴과 통합해야 한다면 BlueXP 랜섬웨어 보호와 같은 OFFTAP 서비스를 사용할 수 있습니다. 랜섬웨어로부터 데이터를 보호하도록 설계된 서비스입니다. 이 서비스는 온프레미스 NFS 스토리지의 Oracle, MySQL, VM 데이터 저장소 및 파일 공유와 같은 애플리케이션 기반 워크로드에 대한 보호를 제공합니다.

이 예에서는 NFS 데이터 저장소 "SRC_NFS_DS04"가 BlueXP 랜섬웨어 보호를 사용하여 보호됩니다.

NetApp BlueXP

BlueXP Search

Ransomware protection Dashboard Protection Alerts Recovery Reports Free trial (55 days left) - view details

Workloads (10)

Workload	Type	Connector	Importance	Protection st...	Detection sta...	Detection pol...	Snapshot an...	Backup destina...	
Src_nfs_ds02	VM datastore	GISABXPConn	Critical	Protected	Learning mode	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Draas_src_test_3130	VM file share	GISABXPConn	Standard	At risk	None	None	None	n/a	Protect
Nfsds02zrp_804	VM file share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection
Draas_src_7027	VM file share	GISABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	Protect
Src_nfs_vsi01_7948	VM file share	GISABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	Protect
Src_nfs_ds03	VM datastore	GISABXPConn	Standard	At risk	None	None	SnapCenter for VMw...	netapp-backup-add...	Protect
Src_nfs_ds04	VM datastore	GISABXPConn	Standard	Protected	Active	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Src_nfs_ds04	File share	GISABXPConn	Critical	Protected	Active	rps-policy-primary	BlueXP backup and ...	netapp-backup-ba3...	Edit protection
Testvol_1787	File share	GISABXPConn	Standard	Protected	Learning mode	rps-policy-primary	None	netapp-backup-ba3...	Edit protection
Nfsrpdemo02_3419	File share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection

NetApp BlueXP

BlueXP Search

Ransomware protection Dashboard Protection Alerts Recovery

Datastore protected and No Alerts reported

Standard Importance

Protected Protection health Alerts 0

Not marked for recovery Recovery

Protection

These policies managed by SnapCenter for VMware will not be modified by applying a detection policy to this workload.

- Pol_NFSD504 Snapshot policy
- 1 Year Daily LTR Backup policy

VM datastore

Location urn:scv:scvmUI:Resou...

vCenter server vccsa8-01.hmcdc.local

Connector GISABXPConn

Storage

Cluster id add38626-348c-11ef-6...

Working Env name NTAP915_Src

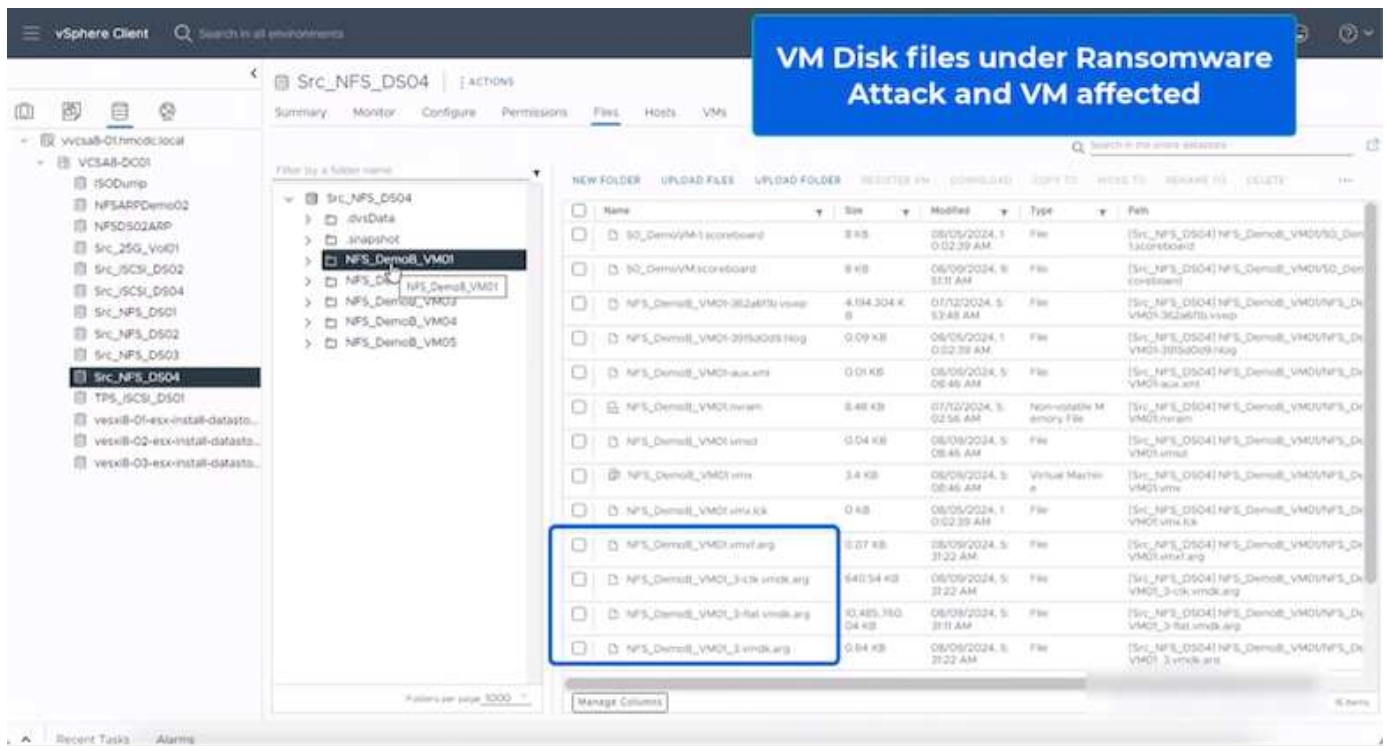
Storage VM name svm_nfs

Volume name Src_NFS_DS04

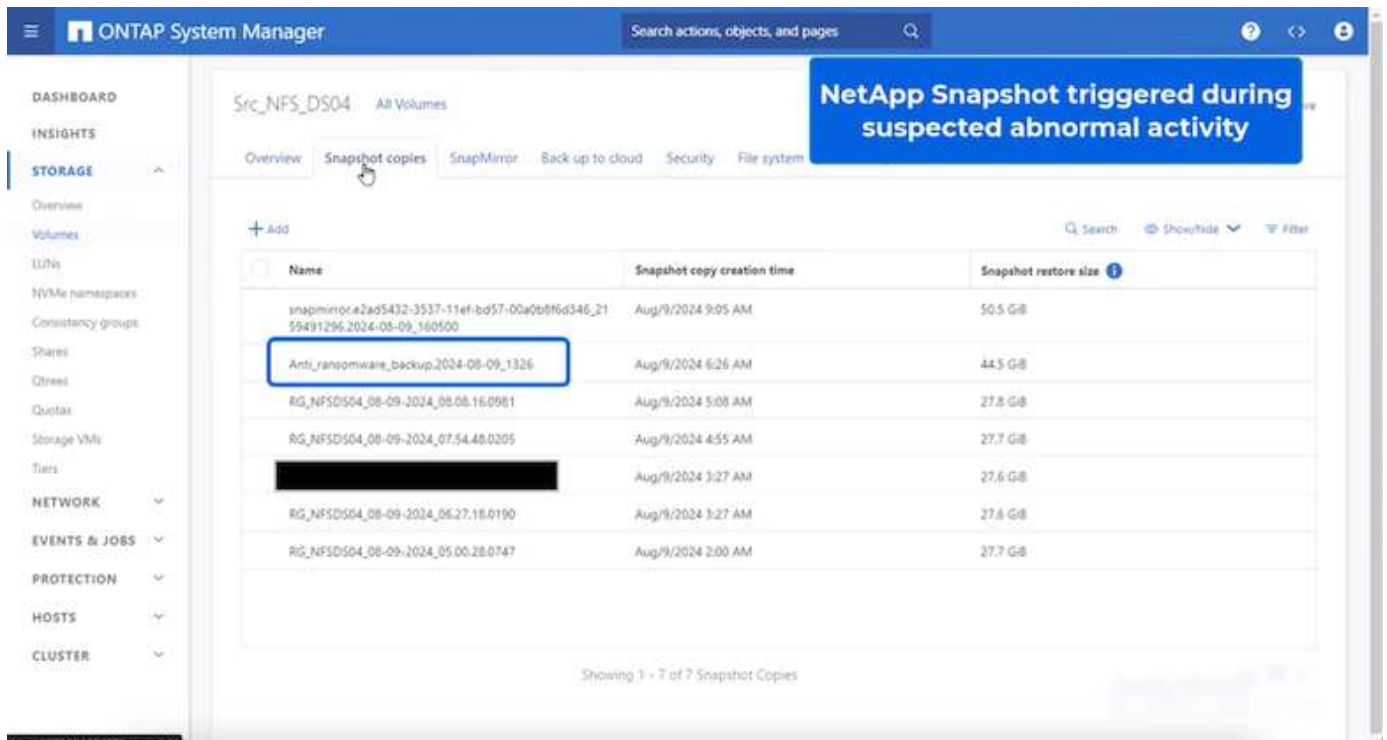
Used size 29 GiB

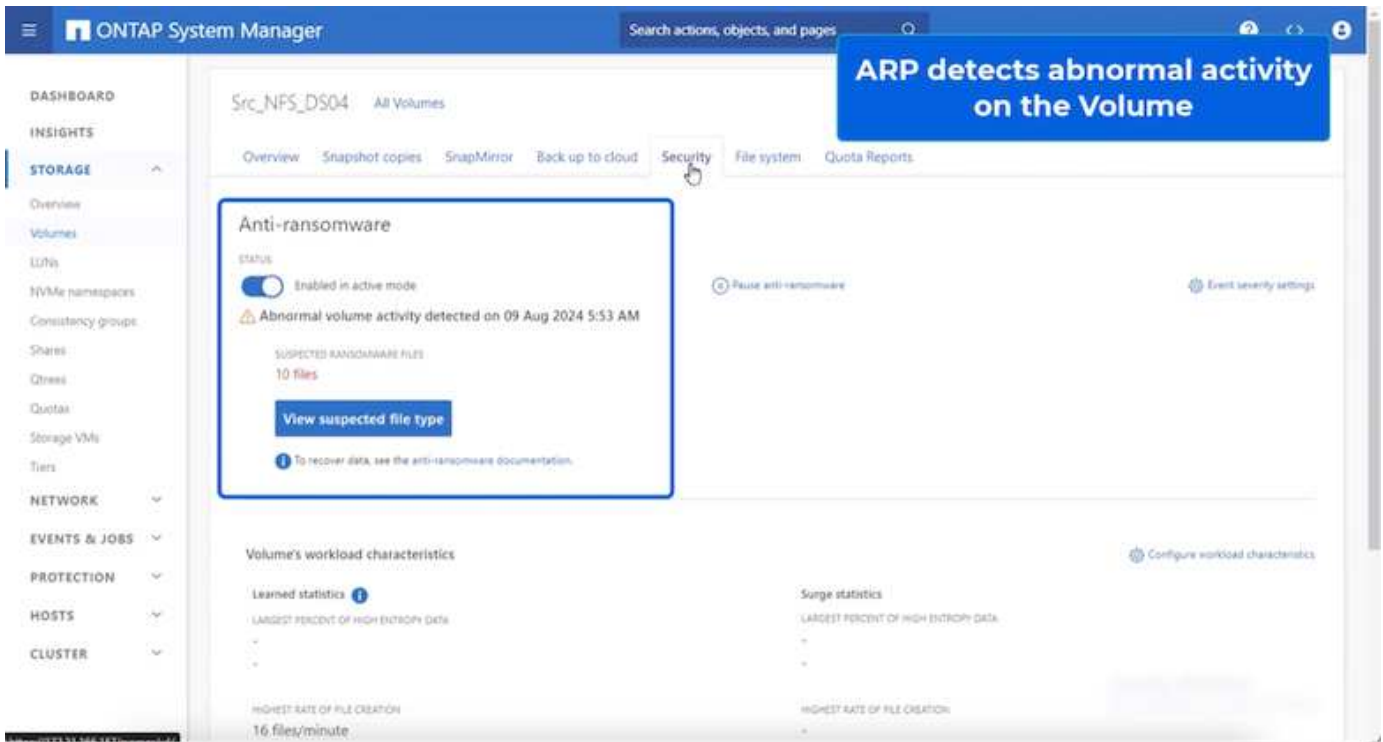
BlueXP 랜섬웨어 보호를 구성하는 방법에 대한 자세한 내용은 "BlueXP 랜섬웨어 방어 설정" 및 를 참조하십시오 "BlueXP 랜섬웨어 보호 설정을 구성합니다".

예를 들어 살펴보겠습니다. 이 연습에서는 데이터 저장소 "SRC_NFS_DS04"가 영향을 받습니다.

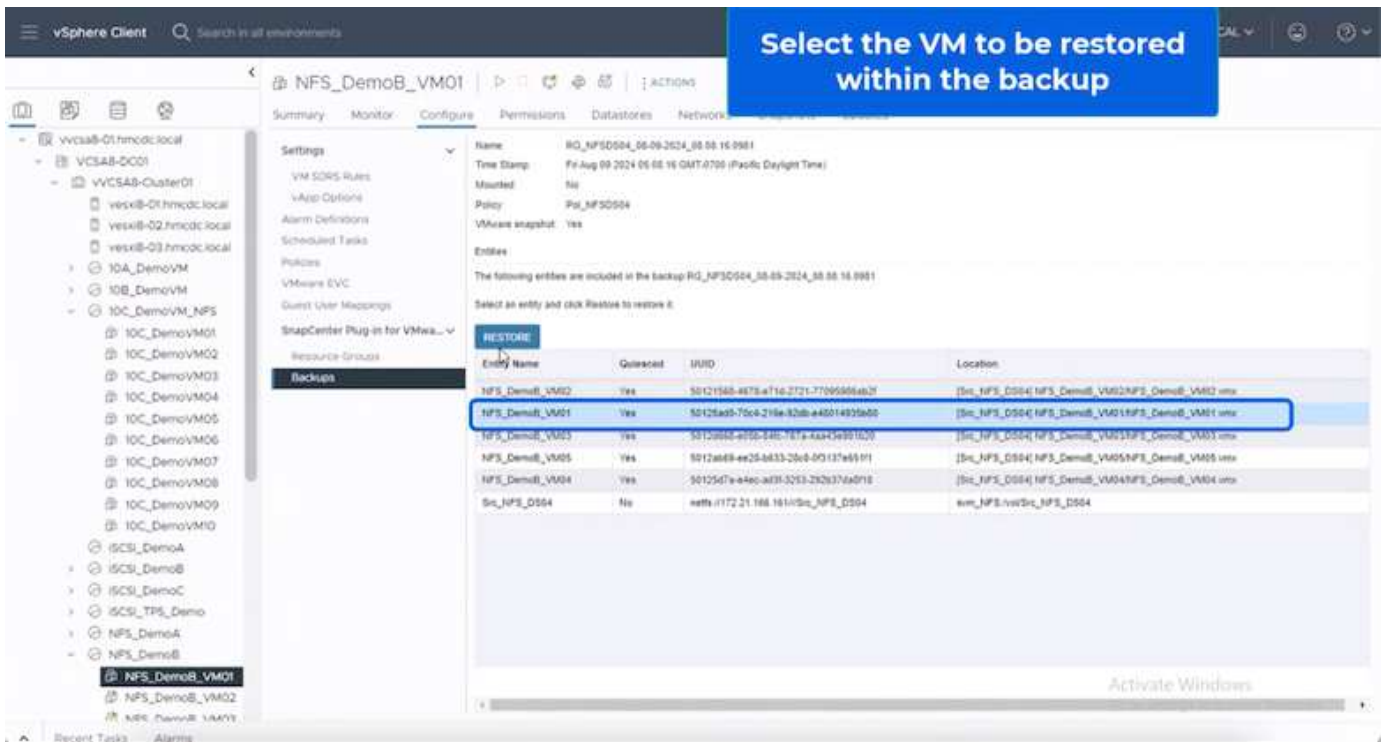


ARP가 감지될 때 즉시 불륨에 대한 스냅샷을 트리거했습니다.





포렌식 분석이 완료되면 SnapCenter 또는 BlueXP 랜섬웨어 보호를 사용하여 복원을 빠르고 원활하게 수행할 수 있습니다. SnapCenter를 사용하여 영향을 받는 가상 머신으로 이동하고 복구할 적절한 스냅샷을 선택합니다.



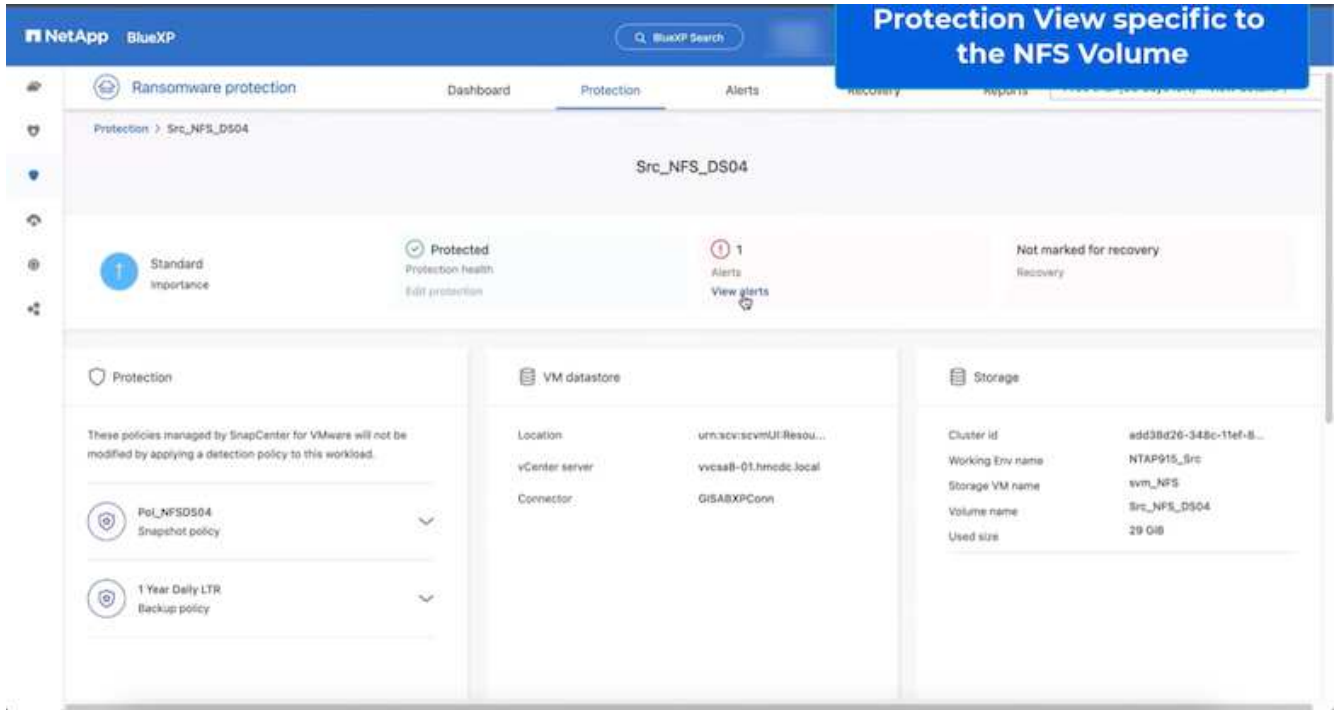
이 섹션에서는 BlueXP 랜섬웨어 방어가 VM 파일이 암호화된 랜섬웨어 인시던트에서 복구를 오케스트레이션하는 방법에 대해 알아봅니다.



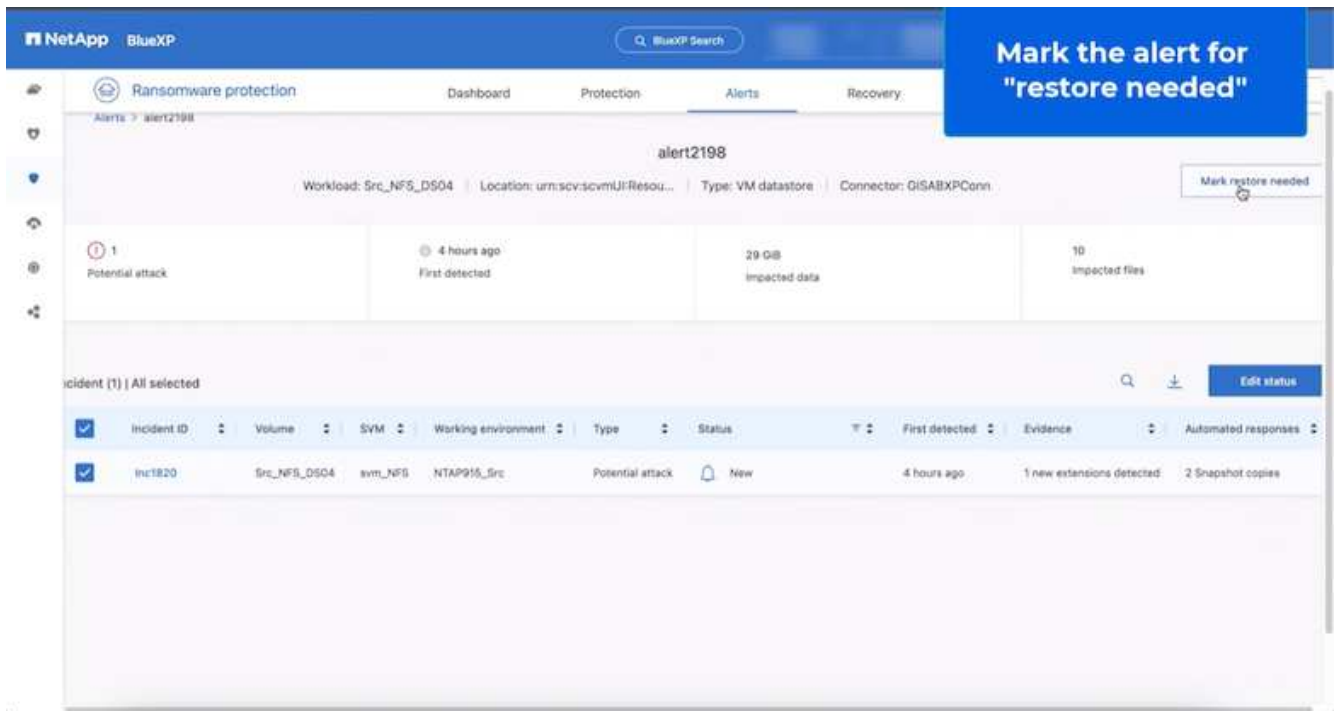
VM이 SnapCenter에 의해 관리되는 경우 BlueXP 랜섬웨어 방어는 VM 정합성 보장 프로세스를 사용하여 VM을 이전 상태로 복원합니다.


1. BlueXP 랜섬웨어 방어에 액세스하면 BlueXP 랜섬웨어 보호 대시보드에 경고가 표시됩니다.

2. 경고를 클릭하여 생성된 경고에 대한 특정 볼륨의 인시던트를 검토합니다

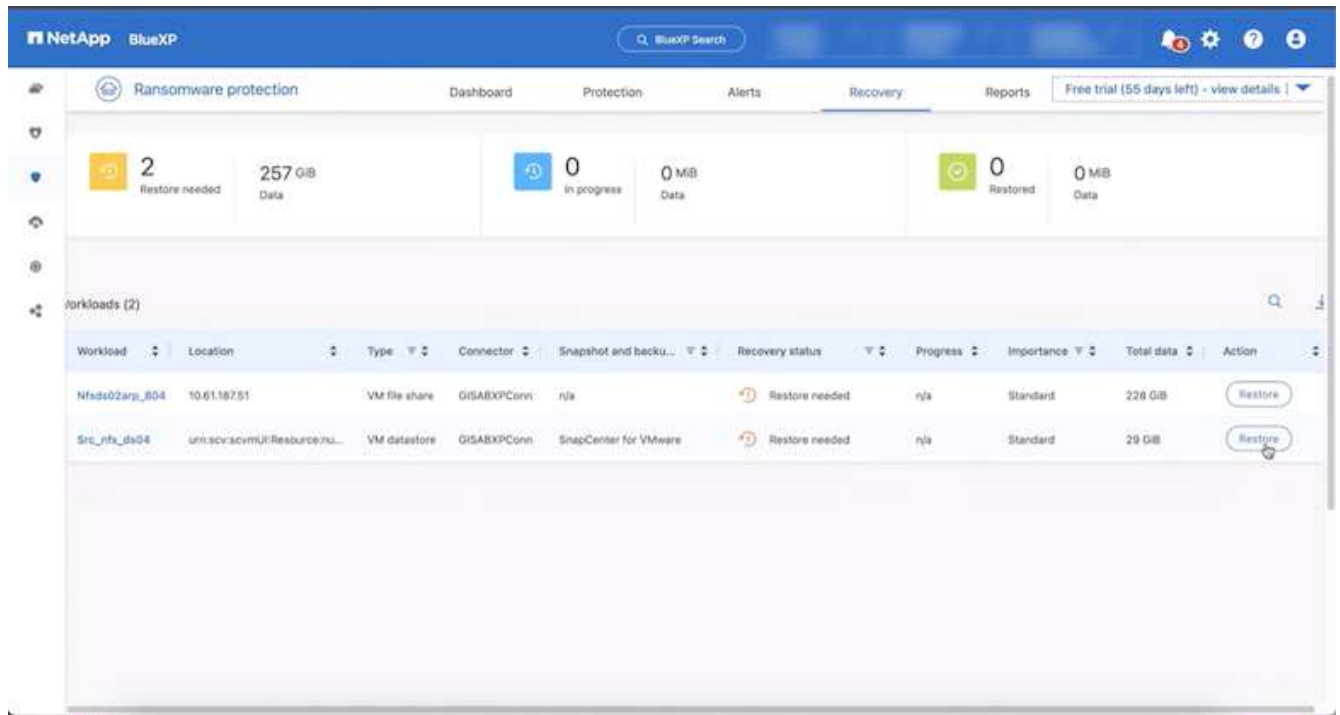


3. "복원 필요함"을 선택하여 랜섬웨어 인시던트를 복구 준비(인시던트가 해소된 후)로 표시합니다.

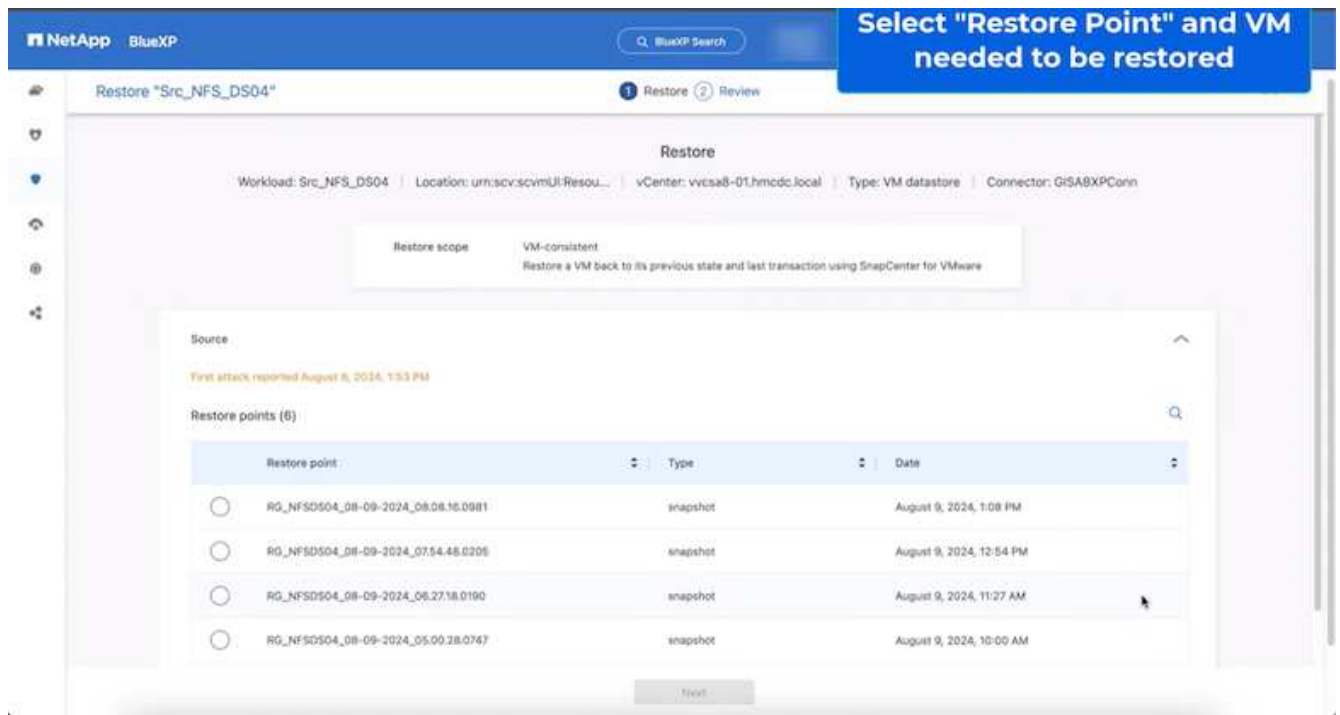


 사고가 거짓 긍정인 것으로 판명되면 경고를 무시할 수 있습니다.

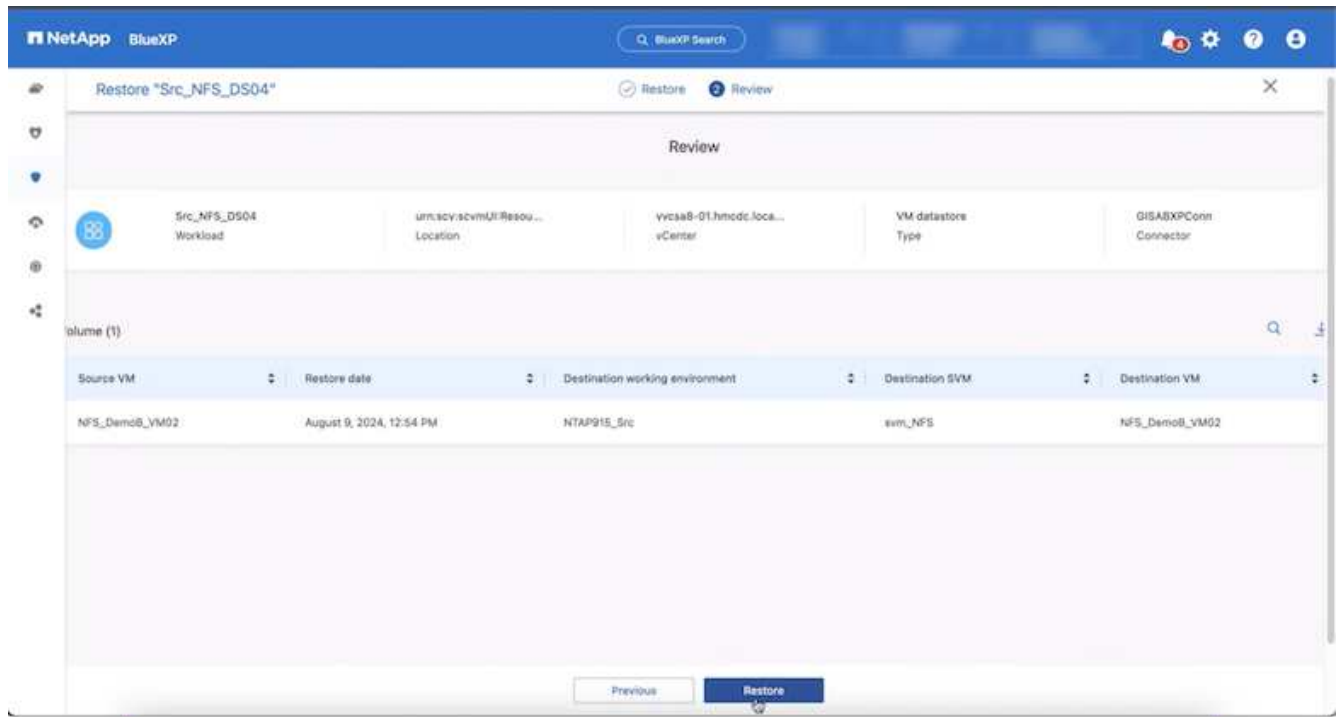
4. 복구 탭으로 이동하여 복구 페이지에서 워크로드 정보를 검토하고 "복구 필요" 상태의 데이터 저장소 볼륨을 선택하고 복구를 선택합니다.



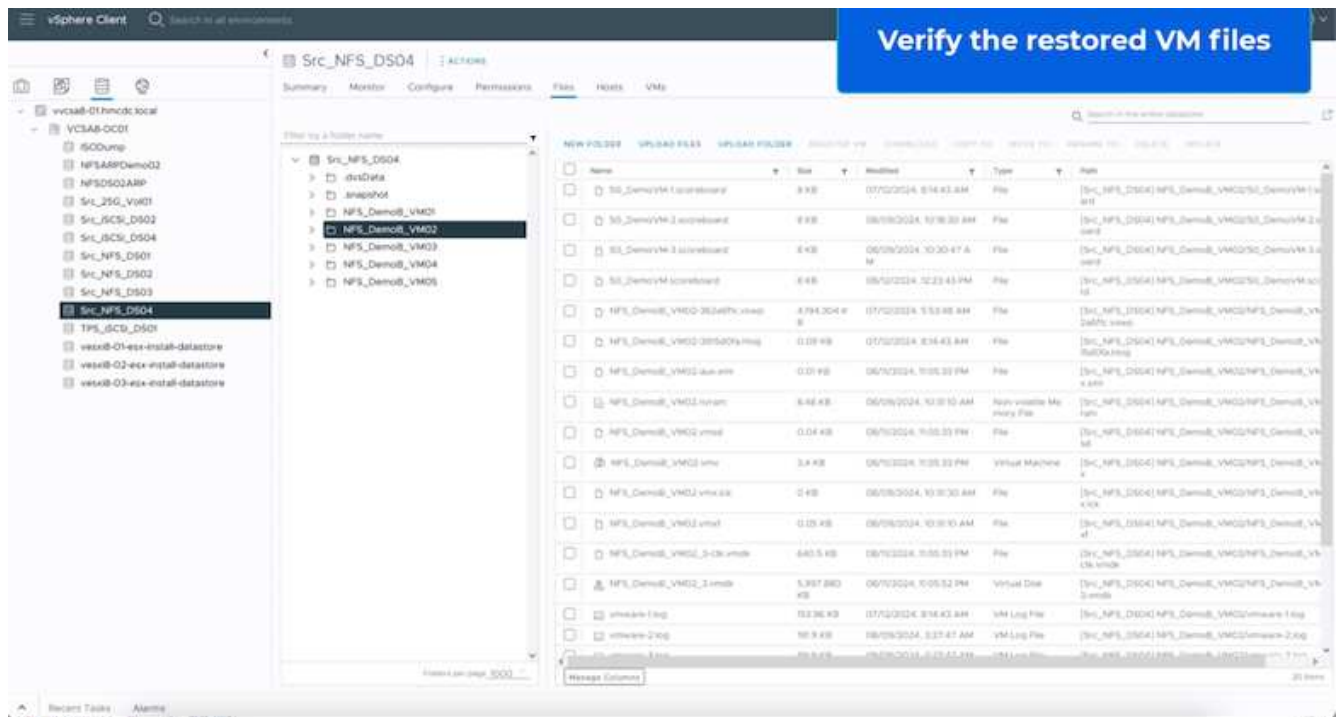
5. 이 경우 복구 범위는 "VM별"입니다(VM용 SnapCenter의 경우 복구 범위는 "VM별"임).



6. 데이터를 복원하는 데 사용할 복원 지점을 선택하고 대상을 선택한 다음 복원을 클릭합니다.



7. 상단 메뉴에서 복구를 선택하여 작업 상태가 상태로 이동하는 복구 페이지에서 작업 부하를 검토합니다. 복원이 완료되면 VM 파일이 아래와 같이 복원됩니다.



애플리케이션에 따라 SnapCenter for VMware 또는 SnapCenter 플러그인에서 복구를 수행할 수 있습니다.

NetApp 솔루션은 가시성, 감지, 해결을 위한 다양한 효과적인 툴을 제공하므로 랜섬웨어를 조기에 탐지하고 확산을 방지하며 필요한 경우 신속하게 복구하여 비용이 많이 드는 다운타임을 방지할 수 있습니다. 기존의 계층화된 방어 솔루션은 가시성과 감지를 위한 타사 및 파트너 솔루션처럼 널리 사용되고 있습니다. 효과적인 치료는 위협에 대한 대응의 중요한 부분입니다.

저작권 정보

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

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 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 라이선스도 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 라이선스를 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 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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