ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/ontap-tools-vmware-vsphere-104/index.html on September 29, 2025. Always check docs.netapp.com for the latest.

목차

ONTAP tools for VMware vSphere . . . 1
릴리스 노트 . . . 2
릴리스 노트 . . . 2
ONTAP tools for VMware vSphere 의 새로운 기능 . . . 2
ONTAP tools for VMware vSphere 와 ONTAP tools for VMware vSphere 기능 비교 . . . 2
개념 . . . 4
ONTAP tools for VMware vSphere 개요 . . . 4
주요 개념 및 용어 . . . 4
역할 기반 액세스 제어 . . . 7
ONTAP tools for VMware vSphere 에 대해 알아보세요 . . . 7
VMware vSphere를 사용한 RBAC . . . 8
ONTAP 사용한 RBAC . . . 12
ONTAP tools for VMware vSphere 의 고가용성 . . . 14
ONTAP 도구 관리자 사용자 인터페이스 . . . 15
ONTAP tools for VMware vSphere 배포 . . . 17
ONTAP tools for VMware vSphere 에 대한 빠른 시작 . . . 17
고가용성(HA) 배포 워크플로 . . . 18
ONTAP tools for VMware vSphere . . . 19
시스템 요구 사항 . . . 19
최소 저장 및 적용 요구 사항 . . . 20
포트 요구 사항 . . . 20
ONTAP tools for VMware vSphere 배포를 위한 구성 제한 . . . 22
ONTAP tools for VMware vSphere - 스토리지 복제 어댑터(SRA) . . . 22
시작하기 전에… . . . 23
배포 워크시트 . . . 23
네트워크 방화벽 구성 . . . 24
ONTAP 스토리지 설정 . . . 25
ONTAP tools for VMware vSphere 배포 . . . 25
배포 오류 코드 . . . 30
ONTAP tools for VMware vSphere 구성 . . . 33
vCenter Server 인스턴스 추가 . . . 33
vCenter Server 인스턴스에 VASA 공급자 등록 . . . 33
NFS VAAI 플러그인을 설치하세요 . . . 34
ESXi 호스트 설정 구성 . . . 35
ESXi 서버 다중 경로 및 시간 초과 설정 구성 . . . 35
ESXi 호스트 값 설정 . . . 36
ONTAP 사용자 역할 및 권한 구성 . . . 37
SVM 집계 매핑 요구 사항 . . . 37
ONTAP 사용자 및 역할을 수동으로 생성 . . . 38

ONTAP tools for VMware vSphere 업그레이드 . . . 46
ONTAP tools for VMware vSphere 업그레이드 . . . 48
스토리지 백엔드 추가 . . . 48
vCenter Server 인스턴스와 스토리지 백엔드 연결 . . . 49
네트워크 액세스 구성 . . . 50
데이터 저장소 만들기 . . . 50
데이터 저장소 및 가상 머신 보호 . . . 55
호스트 클러스터 보호를 사용하여 보호 . . . 55
SRA 보호를 사용하여 보호하세요 . . . 56
데이터 저장소를 보호하기 위한 SRA 구성 . . . 56
SAN 및 NAS 환경에 대한 SRA 구성 . . . 56
확장성이 높은 환경에 맞게 SRA 구성 . . . 57
VMware Live Site Recovery 어플라이언스에서 SRA 구성 . . . 58
SRA 자격 증명 업데이트 . . . 59
보호 및 복구 사이트 구성 . . . 60
보호 및 복구 사이트 리소스 구성 . . . 61
복제된 스토리지 시스템 확인 . . . 65
팬아웃 보호 . . . 65
ONTAP tools for VMware vSphere 관리 . . . 69
ONTAP tools for VMware vSphere . . . 69
ONTAP 도구 관리자 사용자 인터페이스 . . . 70
ONTAP tools for VMware vSphere 에서 igroups 및 내보내기 정책 이해 . . . 72
수출 정책 . . . 75
ONTAP 도구 관리 igroups 이해 . . . 76
ONTAP tools for VMware vSphere 활성화 . . . 80
ONTAP tools for VMware vSphere 변경 . . . 80
데이터 저장소 관리 . . . 82
NFS 및 VMFS 데이터 저장소 마운트 . . . 82
NFS 및 VMFS 데이터 저장소 마운트 해제 . . . 82
vVols 데이터 저장소 마운트 . . . 83
NFS 및 VMFS 데이터 저장소 크기 조정 . . . 83
vVols 데이터 저장소 확장 . . . 83
vVols 데이터 저장소 축소 . . . 84
데이터 저장소 삭제 . . . 84
데이터 저장소에 대한 ONTAP 스토리지 뷰 . . . 85
가상 머신 스토리지 보기 . . . 86
저장 임계값 관리 . . . 86
스토리지 백엔드 관리 . . . 86
스토리지를 발견하세요 . . . 86
스토리지 백엔드 수정 . . . 87
스토리지 백엔드 제거 . . . 87

스토리지 백엔드의 드릴다운 보기 . . . 88
vCenter Server 인스턴스 관리 . . . 88
vCenter Server 인스턴스와 스토리지 백엔드 연결 해제 . . . 88
vCenter Server 인스턴스 수정 . . . 89
vCenter Server 인스턴스 제거 . . . 89
인증서 관리 . . . 89
ONTAP tools for VMware vSphere 에 액세스하세요 . . . 92
ONTAP tools for VMware vSphere 개요 . . . 92
원격 진단 액세스 구성 . . . 93
다른 노드에서 SSH 시작 . . . 93
vCenter Server 및 ONTAP 자격 증명 업데이트 . . . 94
ONTAP 도구 보고서 . . . 94
로그 파일을 수집합니다 . . . 95
가상 머신 관리 . . . 95
가상 머신을 마이그레이션하거나 복제할 때의 고려 사항 . . . 95
NFS 및 VMFS 데이터 저장소가 있는 가상 머신을 vVols 데이터 저장소로 마이그레이션 . . . 96
VASA 정리 . . . 97
가상 머신에서 데이터 디스크를 연결하거나 분리합니다. . . . 97
스토리지 시스템 및 호스트 검색 . . . 98
ONTAP 도구를 사용하여 ESXi 호스트 설정 수정 . . . 99
비밀번호 관리 . . . 99
ONTAP 도구 관리자 비밀번호 변경 . . . 99
ONTAP 도구 관리자 비밀번호 재설정 . . . 100
애플리케이션 사용자 비밀번호 재설정 . . . 100
유지 관리 콘솔 사용자 비밀번호 재설정 . . . 100
호스트 클러스터 보호 관리 . . . 102
보호된 호스트 클러스터 수정 . . . 102
호스트 클러스터 보호 제거 . . . 104
AutoSupport 비활성화 . . . 104
AutoSupport 프록시 URL 업데이트 . . . 105
NTP 서버 추가 . . . 105
백업을 생성하고 ONTAP 도구 설정을 복구합니다. . . . 105
백업을 생성하고 백업 파일을 다운로드합니다. . . . 106
다시 덮다 . . . 106
ONTAP tools for VMware vSphere 제거 . . . 107
FlexVol 볼륨 제거 . . . 107
ONTAP tools for VMware vSphere 업그레이드 . . . 109
ONTAP tools for VMware vSphere 에서 10.4로 업그레이드 . . . 109
업그레이드 오류 코드 . . . 112
ONTAP tools for VMware vSphere 10.4로 마이그레이션 . . . 116
ONTAP tools for VMware vSphere 에서 10.4로 마이그레이션 . . . 116

VASA 공급자를 마이그레이션하고 SRA를 업데이트합니다. 116
VASA 공급자를 마이그레이션하는 단계 116
스토리지 복제 어댑터(SRA)를 업데이트하는 단계 119
REST API를 사용하여 자동화 120
ONTAP tools for VMware vSphere 에 대해 알아보세요. 120
REST 웹 서비스 기반 120
ONTAP 도구 관리자 환경 120
ONTAP tools for VMware vSphere 에 대한 구현 세부 정보 121
REST API에 접근하는 방법 121
HTTP 세부 정보 121
입증 123
동기 및 비동기 요청 123
ONTAP tools for VMware vSphere 123
시작하기 전에 123
1단계: 액세스 토큰 획득 124
2단계: REST API 호출 실행 124
ONTAP tools for VMware vSphere 에 대한 API 참조 124
법적 고지 사항 126
저작권 126
상표 126
특허 126
개인정보 보호정책 126
오픈소스 126

ONTAP tools for VMware vSphere

릴리스 노트

릴리스 노트

ONTAP tools for VMware vSphere 에서 사용할 수 있는 새롭고 향상된 기능에 대해 알아보세요.

새로운 기능 및 향상된 기능의 전체 목록은 다음을 참조하세요.ONTAP tools for VMware vSphere 의 새로운 기능 .

ONTAP tools for VMware vSphere 에서 ONTAP 도구 10.4로 마이그레이션하는 것이 배포에 적합한지 자세히 알아보려면 다음을 참조하세요.ONTAP tools for VMware vSphere 와 ONTAP tools for VMware vSphere 기능 비교 . ONTAP tools for VMware vSphere 에서 ONTAP tools for VMware vSphere 로의 마이그레이션이 지원됩니다.

자세한 내용은 다음을 참조하세요. "ONTAP tools for VMware vSphere" . 릴리스 노트에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

ONTAP tools for VMware vSphere 의 새로운 기능

ONTAP tools for VMware vSphere 에서 사용할 수 있는 새로운 기능에 대해 알아보세요.

업데이트	설명
"클러스터당 12개 노드가 있는 ASA r2 시스템 지원"	ONTAP tools for VMware vSphere 클러스터당 최대 12개의 노드를 갖춘 ASA r2 스토리지 시스템의 워크플로를 지원하여 데이터 관리 효율성과 확장성을 개선합니다. iSCSI 및 FC 프로토콜을 사용하는 vVols 데이터스토어와 iSCSI, FC, NVMe 프로토콜을 사용하는 VMFS 데이터스토어를 지원하여 유연하고 향상된 스토리지 옵션을 제공합니다.
"ONTAP 도구 관리자 사용자 인터페이스 개선"	이제 ONTAP 도구 관리자 인터페이스에서 환경 전체에 걸쳐 정확한 시간 동기화를 위해 NTP 서버를 활성화하고 원격 측정 설정을 구성하여 시스템 성능을 모니터링하고 분석할 수 있습니다. 이러한 설정은 더 이상 유지 관리 콘솔에서 사용할 수 없습니다.
강화된 보안 기능	이제 보안 기능이 강화되어 업계 표준을 준수하고 보호 기능이 강화되어, 관리자가 VMware 환경을 보다 효과적으로 관리할 수 있도록 견고하고 사용자 친화적인 환경을 제공합니다.
"향상된 SRA 재해 복구 기능"	ONTAP tools for VMware vSphere 이제 SnapMirror 예약된 스냅샷 복사 외에도 사용자 정의 이름의 스냅샷을 사용하는 Site Recovery Appliance(SRA)를 사용하여 재해 복구 작업을 지원합니다.

ONTAP tools for VMware vSphere 와 ONTAP tools for VMware vSphere 기능 비교

ONTAP tools for VMware vSphere 에서 ONTAP tools for VMware vSphere 로 마이그레이션하는 것이 적합한지 알아보세요.

최신 호환성 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .

특징	**ONTAP** 도구 **9.13**	**ONTAP** 도구 **10.1**	**ONTAP** 도구 **10.2** 이상
핵심 가치 제안	향상된 보안, 규정 준수 및 자동화 기능으로 0일차부터 2일차까지의 운영을 간소화하고 단순화합니다.	고가용성, 성능 및 확장 한계를 확장하면서 ONTAP 도구 10.x를 9.xx 패리티로 발전시킵니다.	VMFS 및 vVols 에 대한 FC, VMFS에 대한 NVMe-oF/FC, NVMe-oF/TCP를 포함하도록 지원이 확대되었습니다. NetApp SnapMirror 의 사용 편의성, vSphere 메트로 스토리지 클러스터의 간단한 설정, 3개 사이트 VMware Live Site Recovery 지원
ONTAP 릴리스 자격	ONTAP 9.9.1에서 ONTAP 9.16.1로	ONTAP 9.12.1에서 ONTAP 9.14.1로	ONTAP 도구 10.2를 위한 ONTAP 9.12.1~ ONTAP 9.15.1. ONTAP 도구 10.3용 ONTAP 9.14.1, 9.15.1, 9.16.0 및 9.16.1. ONTAP 도구 10.4용 ONTAP 9.14.1, 9.15.1, 9.16.0 및 9.16.1. ASA r2 시스템을 사용하는 경우 ONTAP 도구 10.4에 ONTAP 9.16.1P3 이상이 필요합니다.
VMware 릴리스 지원	vSphere 7.x-8.x VMware Site Recovery Manager(SRM) 8.5에서 VMware Live Site Recovery 9.0으로	vSphere 7.x-8.x VMware Site Recovery Manager(SRM) 8.7에서 VMware Live Site Recovery 9.0으로	vSphere 7.x-8.x VMware Site Recovery Manager(SRM) 8.7에서 VMware Live Site Recovery 9.0으로
프로토콜 지원	NFS 및 VMFS 데이터 저장소: NFS(v3 및 v4.1), VMFS(iSCSI 및 FCP) vVols 데이터 저장소: iSCSI, FCP, NVMe/FC, NFS v3	NFS 및 VMFS 데이터 저장소: NFS(v3 및 v4.1), VMFS(iSCSI) vVols 데이터 저장소: iSCSI, NFS v3	NFS 및 VMFS 데이터 저장소: NFS(v3 및 v4.1), VMFS(iSCSI/FCP/NVMe-oF) vVols 데이터 저장소: iSCSI, FCP, NFS v3
확장성	호스트 및 VM: 300개 호스트, 최대 10,000개 VM 데이터 저장소: 600개 NFS, 최대 50개 VMFS, 최대 250개 vVols vVols: 최대 14,000개	호스트 및 VM: 600개 호스트 vVols: 최대 140,000개	호스트 및 VM: 600개 호스트 vVols: 최대 140,000개
관찰 가능성	성능, 용량 및 호스트 규정 준수 대시보드 동적 VM 및 데이터 저장소 보고서	업데이트된 성능, 용량 및 호스트 규정 준수 대시보드 동적 VM 및 데이터 저장소 보고서	업데이트된 성능, 용량 및 호스트 규정 준수 대시보드 동적 VM 및 데이터 저장소 보고서
데이터 보호	VMFS 및 NFS를 위한 SRA 복제 vVols SCV 통합을 위한 FlexVols 기반 복제 및 백업을 위한 상호 운용성	iSCSI VMFS 및 NFS v3 데이터 저장소에 대한 SRA 복제	SMAS와 VMware Live Site Recovery를 결합한 3개 사이트 보호, iSCSI VMFS 및 NFS v3 데이터 저장소를 위한 SRA 복제.
VASA 공급자 지원	VASA 4.0	VASA 3.0	VASA 3.0

개념

ONTAP tools for VMware vSphere 개요

ONTAP tools for VMware vSphere 가상 머신 수명 주기 관리를 위한 도구 세트입니다. VMware 에코시스템과 통합되어 데이터 저장소 프로비저닝을 지원하고 가상 머신에 대한 기본 보호 기능을 제공합니다. ONTAP tools for VMware vSphere OVA(Open Virtual Appliance)로 배포되는 수평 확장 가능한 이벤트 기반 마이크로서비스 모음입니다. 이 릴리스에서는 REST API가 ONTAP 과 통합되었습니다.

ONTAP tools for VMware vSphere 다음으로 구성됩니다.

- 기본 보호 및 재해 복구와 같은 가상 머신 기능
- VM 세부 관리를 위한 VASA 공급자
- 스토리지 정책 기반 관리
- 스토리지 복제 어댑터(SRA)

주요 개념 및 용어

다음 섹션에서는 문서에서 사용된 주요 개념과 용어를 설명합니다.

ASA r2 시스템

새로운 NetApp ASA r2 시스템은 SAN 전용 고객의 요구 사항에 맞춰 간소화된 환경을 만드는 통합 하드웨어 및 소프트웨어 솔루션을 제공합니다. "ASA r2 스토리지 시스템에 대해 알아보세요" .

인증 기관**(CA)**

CA는 SSL(Secure Sockets Layer) 인증서를 발급하는 신뢰할 수 있는 기관입니다.

일관성 그룹**(CG)**

일관성 그룹은 단일 단위로 관리되는 볼륨의 모음입니다. CG는 저장 장치와 볼륨 전체에서 데이터 일관성을 위해 동기화됩니다. ONTAP 에서는 여러 볼륨에 걸친 애플리케이션 작업 부하에 대한 쉬운 관리와 보호 보장을 제공합니다. 자세히 알아보세요 "일관성 그룹" .

듀얼 스택

듀얼 스택 네트워크는 IPv4와 IPv6 주소를 동시에 사용할 수 있는 네트워킹 환경입니다.

고가용성**(HA)**

클러스터 노드는 중단 없는 작업을 위해 HA 쌍으로 구성됩니다.

논리 단위 번호(LUN)

LUN은 SAN(Storage Area Network) 내의 논리적 단위를 식별하는 데 사용되는 번호입니다. 이러한 주소 지정 가능 장치는 일반적으로 SCSI(Small Computer System Interface) 프로토콜이나 캡슐화된 파생 프로토콜 중 하나를 통해 액세스하는 논리적 디스크입니다.

NVMe 네임스페이스 및 서브시스템

NVMe 네임스페이스는 논리 블록으로 포맷할 수 있는 비휘발성 메모리의 양입니다. 네임스페이스는 FC 및 iSCSI 프로토콜의 LUN과 동일하며, NVMe 하위 시스템은 igroup과 유사합니다. NVMe 하위 시스템은 이니시에이터와 연결될 수 있으므로 연관된 이니시에이터는 하위 시스템 내의 네임스페이스에 액세스할 수 있습니다.

ONTAP 도구 관리자

ONTAP 도구 관리자는 ONTAP tools for VMware vSphere 제어 기능을 더 많이 제공합니다. vCenter Server 인스턴스, 스토리지 백엔드, 인증서, 비밀번호 및 로그 번들 다운로드를 관리하는 데 도움이 됩니다.

오픈 가상 어플라이언스(OVA)

OVA는 가상 머신에서 실행되어야 하는 가상 어플라이언스나 소프트웨어를 패키징하고 배포하기 위한 개방형 표준입니다.

복구 지점 목표(RPO)

RPO는 데이터를 백업하거나 복제하는 빈도를 측정합니다. 이는 정전 후 비즈니스 운영을 재개하기 위해 데이터를 복원해야 하는 정확한 시점을 지정합니다. 예를 들어, 조직의 RPO가 4시간인 경우 재해 발생 시 최대 4시간 분량의 데이터 손실을 허용할 수 있습니다.

SnapMirror 액티브 싱크

SnapMirror 액티브 동기화를 사용하면 사이트 전체에 장애가 발생하더라도 비즈니스 서비스를 계속 운영할 수 있으며, 보조 복사본을 사용하여 애플리케이션이 투명하게 장애 조치되도록 지원합니다. SnapMirror Active Sync를 사용하면 장애 조치를 트리거하는 데 수동 개입이나 사용자 정의 스크립팅이 필요하지 않습니다. 자세히 알아보세요 "SnapMirror 액티브 싱크" .

스토리지 백엔드

스토리지 백엔드는 ESXi 호스트가 가상 머신 파일, 데이터 및 기타 리소스를 저장하는 데 사용하는 기본 스토리지 인프라입니다. ESXi 호스트가 영구 데이터에 액세스하고 관리할 수 있도록 하여 가상화된 환경에 필요한 저장 용량과 성능을 제공합니다.

글로벌 클러스터(스토리지 백엔드)

ONTAP 클러스터 자격 증명을 통해서만 사용할 수 있는 글로벌 스토리지 백엔드는 ONTAP 도구 관리자 인터페이스를 통해 온보딩됩니다. vVols 관리에 필요한 필수 클러스터 리소스를 검색할 수 있도록 최소한의 권한으로 추가할 수 있습니다. 글로벌 클러스터는 vVols 관리를 위해 SVM 사용자가 로컬로 추가되는 다중 테넌시 시나리오에 이상적입니다.

로컬 스토리지 백엔드

클러스터 또는 SVM 자격 증명이 있는 로컬 스토리지 백엔드는 ONTAP 도구 사용자 인터페이스를 통해 추가되며 vCenter로 제한됩니다. 로컬에서 클러스터 자격 증명을 사용하는 경우 연관된 SVM은 vCenter와 자동으로 매핑되어 vVols 또는 VMFS를 관리합니다. SRA를 포함한 VMFS 관리의 경우 ONTAP 도구는 글로벌 클러스터가 필요 없이 SVM 자격 증명을 지원합니다.

스토리지 복제 어댑터(**SRA**)

SRA는 VMware Live Site Recovery 어플라이언스 내부에 설치되는 스토리지 공급업체별 소프트웨어입니다. 어댑터는 SVM(Storage Virtual Machine) 수준과 클러스터 수준 구성에서 Site Recovery Manager와 스토리지 컨트롤러 간의 통신을 가능하게 합니다.

스토리지 가상 머신(**SVM**)

SVM은 ONTAP 의 멀티테넌시 단위입니다. 하이퍼바이저에서 실행되는 가상 머신과 마찬가지로 SVM은 물리적 리소스를 추상화하는 논리적 엔터티입니다. SVM은 데이터 볼륨과 하나 이상의 LIF를 포함하며, 이를 통해 클라이언트에 데이터를 제공합니다.

균일한 구성과 비균일한 구성

- *균일한 호스트 액세스*는 두 사이트의 호스트가 두 사이트의 스토리지 클러스터에 대한 모든 경로에 연결된다는 것을 의미합니다. 교차 사이트 경로는 거리에 따라 확장됩니다.
- *비균일 호스트 액세스*는 각 사이트의 호스트가 동일한 사이트의 클러스터에만 연결된다는 것을 의미합니다. 교차 사이트 경로와 늘어난 경로는 연결되지 않습니다.

> 모든 SnapMirror 활성 동기화 배포에 대해 균일한 호스트 액세스가 지원됩니다. 비균일한 호스트 액세스는 대칭적 활성/활성 배포에만 지원됩니다. 자세히 알아보세요 "ONTAP 의 SnapMirror Active Sync 개요" .

가상 머신 파일 시스템(**VMFS**)

VMFS는 VMware vSphere 환경에서 가상 머신 파일을 저장하도록 설계된 클러스터형 파일 시스템입니다.

가상 볼륨(**vVols**)

vVols 가상 머신에서 사용되는 저장소에 대한 볼륨 수준 추상화를 제공합니다. 이 방법에는 여러 가지 이점이 있으며 기존 LUN을 사용하는 것에 대한 대안을 제공합니다. vVol 데이터 저장소는 일반적으로 vVols 의 컨테이너 역할을 하는 단일 LUN과 연결됩니다.

VM 스토리지 정책

VM 스토리지 정책은 vCenter Server의 정책 및 프로필에서 생성됩니다. vVols 의 경우 NetApp vVols 스토리지 유형 공급자의 규칙을 사용하여 규칙 세트를 만듭니다.

VMware 라이브 사이트 복구

이전에 Site Recovery Manager(SRM)로 알려졌던 VMware Live Site Recovery는 VMware 가상 환경에 대한 비즈니스 연속성, 재해 복구, 사이트 마이그레이션 및 중단 없는 테스트 기능을 제공합니다.

스토리지 인식을 위한 **VMware vSphere API(VASA)**

VASA는 관리 및 운영을 위해 스토리지 어레이를 vCenter Server와 통합하는 API 세트입니다. 이 아키텍처는 VMware vSphere와 스토리지 시스템 간의 통신을 처리하는 VASA Provider를 포함한 여러 구성 요소를 기반으로 합니다.

VMware vSphere 스토리지 API - 어레이 통합(VAAI)

VAAI는 VMware vSphere ESXi 호스트와 스토리지 장치 간의 통신을 가능하게 하는 API 세트입니다. API에는 호스트가 스토리지 작업을 어레이로 오프로드하는 데 사용되는 기본 작업 세트가 포함되어 있습니다. VAAI는 저장 용량이 많은 작업에 대해 상당한 성능 향상을 제공할 수 있습니다.

vSphere Metro 스토리지 클러스터

vSphere Metro Storage Cluster(vMSC)는 확장된 클러스터 배포에서 vSphere를 활성화하고 지원하는 아키텍처입니다. vMSC 솔루션은 NetApp MetroCluster 및 SnapMirror Active Sync(이전 SMBC)에서 지원됩니다. 이러한 솔루션은 도메인 장애 발생 시 향상된 비즈니스 연속성을 제공합니다. 복원력 모델은 귀하의 특정 구성 선택에 따라 결정됩니다. 자세히 알아보세요 "VMware vSphere Metro 스토리지 클러스터" .

vVols 데이터 저장소

vVols 데이터 저장소는 VASA 공급자가 생성하고 유지 관리하는 vVols 컨테이너의 논리적 데이터 저장소 표현입니다.

제로 RPO

RPO는 복구 지점 목표를 의미하며, 특정 기간 동안 허용되는 데이터 손실량을 의미합니다. 0 RPO는 데이터 손실이 허용되지 않음을 의미합니다.

역할 기반 액세스 제어

ONTAP tools for VMware vSphere 에 대해 알아보세요

역할 기반 접근 제어(RBAC)는 조직 내 리소스에 대한 접근을 제어하기 위한 보안 프레임워크입니다. RBAC는 개별 사용자에게 권한을 할당하는 대신, 작업을 수행하기 위한 특정 수준의 권한을 가진 역할을 정의하여 관리를 간소화합니다. 정의된 역할은 사용자에게 할당되므로 오류 위험을 줄이고 조직 전체의 액세스 제어 관리를 간소화하는 데 도움이 됩니다.

RBAC 표준 모델은 점점 더 복잡해지는 여러 구현 기술 또는 단계로 구성됩니다. 결과적으로 실제 RBAC 배포는 소프트웨어 공급업체와 고객의 요구 사항에 따라 다를 수 있으며 비교적 간단한 것부터 매우 복잡한 것까지 다양합니다.

RBAC 구성 요소

높은 수준에서 보면, 일반적으로 모든 RBAC 구현에는 여러 가지 구성 요소가 포함됩니다. 이러한 구성 요소는 승인 프로세스를 정의하는 일부로 다양한 방식으로 결합됩니다.

Privileges

_권한_은 허용되거나 거부될 수 있는 동작이나 기능입니다. 파일을 읽을 수 있는 권한처럼 간단한 것일 수도 있고, 특정 소프트웨어 시스템에 특화된 보다 추상적인 작업일 수도 있습니다. REST API 엔드포인트 및 CLI 명령에 대한 액세스를 제한하기 위해 Privileges 정의할 수도 있습니다. 모든 RBAC 구현에는 미리 정의된 권한이 포함되어 있으며, 관리자가 사용자 지정 권한을 생성할 수도 있습니다.

역할

_역할_은 하나 이상의 권한을 포함하는 컨테이너입니다. 역할은 일반적으로 특정 업무나 직무 기능에 따라 정의됩니다. 역할이 사용자에게 할당되면 해당 역할에 포함된 모든 권한이 사용자에게 부여됩니다. 권한과 마찬가지로 구현에는 미리 정의된 역할이 포함되며 일반적으로 사용자 정의 역할을 만들 수 있습니다.

사물

_객체_는 RBAC 환경 내에서 식별된 실제 또는 추상적인 리소스를 나타냅니다. 권한을 통해 정의된 작업은 연관된 개체에서 수행됩니다. 구현에 따라 권한은 객체 유형이나 특정 객체 인스턴스에 부여될 수 있습니다.

사용자 및 그룹

_사용자_는 인증 후 적용되는 역할에 할당되거나 연결됩니다. 일부 RBAC 구현에서는 사용자에게 하나의 역할만 할당하는 것을 허용하는 반면, 다른 구현에서는 사용자당 여러 역할을 허용하며, 한 번에 하나의 역할만 활성화될 수도 있습니다. _그룹_에 역할을 할당하면 보안 관리가 더욱 간소화될 수 있습니다.

권한

_권한_은 역할과 함께 사용자 또는 그룹을 개체에 연결하는 정의입니다. 권한은 계층적 개체 모델에서 유용할 수 있으며, 이 경우 권한은 계층 구조의 자식에게 선택적으로 상속될 수 있습니다.

두 가지 **RBAC** 환경

ONTAP tools for VMware vSphere 사용할 때 고려해야 할 두 가지 RBAC 환경이 있습니다.

VMware vCenter Server

VMware vCenter Server의 RBAC 구현은 vSphere Client 사용자 인터페이스를 통해 노출된 개체에 대한 액세스를 제한하는 데 사용됩니다. ONTAP tools for VMware vSphere 설치하는 과정에서 RBAC 환경이 확장되어 ONTAP 도구의 기능을 나타내는 추가 개체가 포함되었습니다. 이러한 객체에 대한 액세스는 원격 플러그인을 통해 제공됩니다 ."vCenter Server RBAC 환경" 자세한 내용은.

ONTAP 클러스터

ONTAP tools for VMware vSphere ONTAP REST API를 통해 ONTAP 클러스터에 연결하여 스토리지 관련 작업을 수행합니다. 저장 리소스에 대한 액세스는 인증 중에 제공된 ONTAP 사용자와 연관된 ONTAP 역할을 통해 제어됩니다. 보다 "ONTAP RBAC 환경" 자세한 내용은.

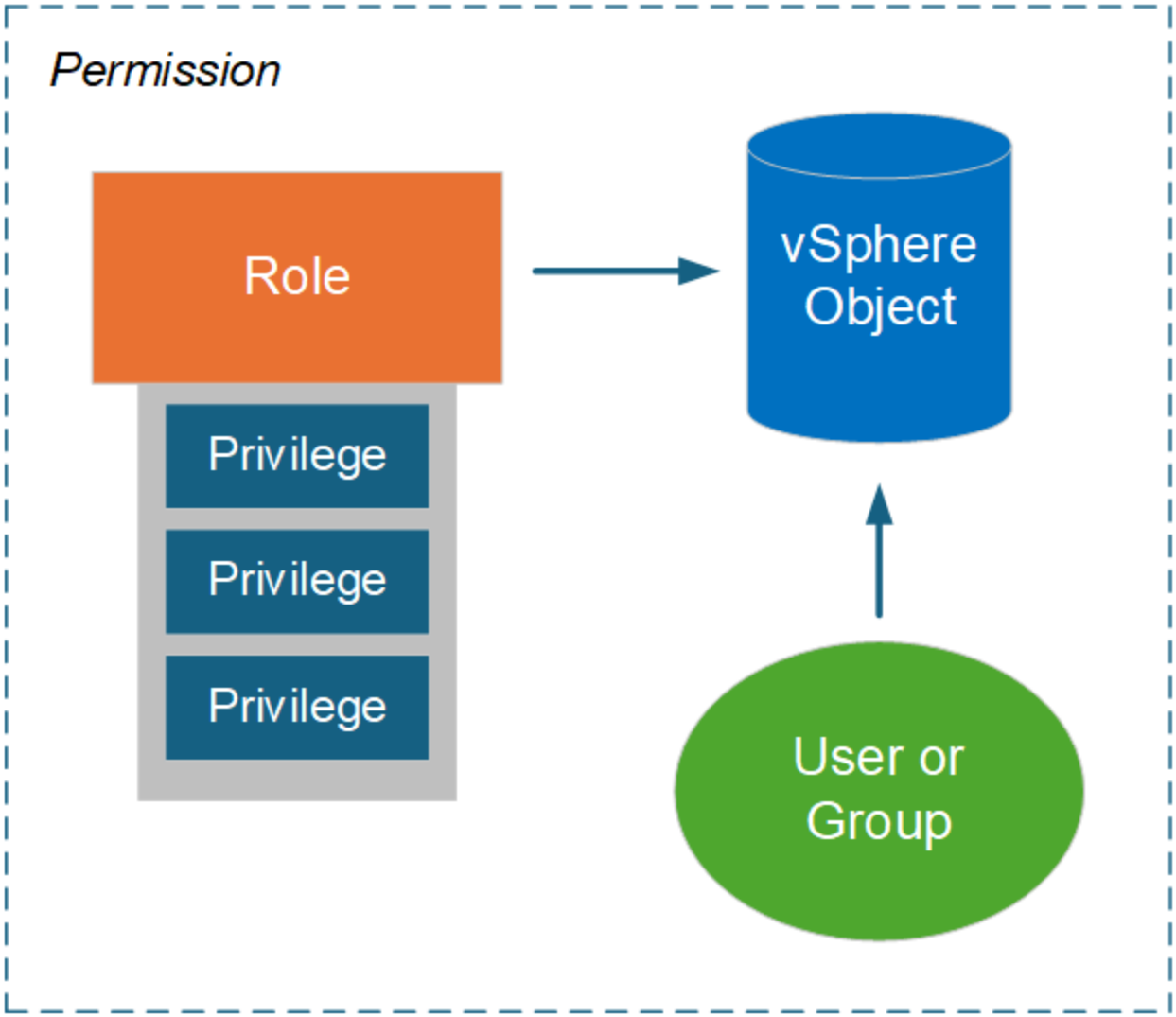
VMware vSphere를 사용한 RBAC

ONTAP tools for VMware vSphere 포함된 vCenter Server RBAC 환경

VMware vCenter Server는 vSphere 개체에 대한 액세스를 제어할 수 있는 RBAC 기능을 제공합니다. 이는 vCenter 중앙 인증 및 권한 부여 보안 서비스의 중요한 부분입니다.

vCenter Server 권한의 그림

권한은 vCenter Server 환경에서 액세스 제어를 시행하기 위한 기반입니다. 이는 권한 정의에 사용자 또는 그룹이 포함된 vSphere 개체에 적용됩니다. 아래 그림은 vCenter 권한에 대한 개략적인 설명을 보여줍니다.



vCenter Server 권한의 구성 요소

vCenter Server 권한은 권한이 생성될 때 함께 바인딩되는 여러 구성 요소의 패키지입니다.

vSphere 객체

권한은 vCenter Server, ESXi 호스트, 가상 머신, 데이터스토어, 데이터 센터, 폴더 등 vSphere 개체와 연결됩니다. vCenter Server는 개체에 할당된 권한에 따라 각 사용자 또는 그룹이 개체에서 수행할 수 있는 작업이나 태스크를 결정합니다. ONTAP tools for VMware vSphere 에 특정한 작업의 경우 모든 권한은 vCenter Server의 루트 또는 루트 폴더 수준에서 할당되고 검증됩니다. 보다 "vCenter Server와 함께 RBAC 사용" 자세한 내용은.

Privileges 및 역할

ONTAP tools for VMware vSphere 와 함께 사용되는 vSphere 권한에는 두 가지 유형이 있습니다. 이 환경에서 RBAC 작업을 간소화하기 위해 ONTAP 도구는 필수 기본 권한과 사용자 정의 권한이 포함된 역할을 제공합니다. 다음과 같은 특권이 있습니다.

- 기본 vCenter Server 권한

이는 vCenter Server에서 제공하는 권한입니다.

- ONTAP 도구별 권한

  이는 ONTAP tools for VMware vSphere 에만 적용되는 사용자 정의 권한입니다.

사용자 및 그룹

Active Directory 또는 로컬 vCenter Server 인스턴스를 사용하여 사용자와 그룹을 정의할 수 있습니다. 역할과 결합하여 vSphere 개체 계층 구조의 개체에 대한 권한을 생성할 수 있습니다. 이 권한은 연결된 역할의 권한을 기반으로 액세스 권한을 부여합니다. 역할은 사용자에게 개별적으로 직접 할당되지 않습니다. 대신, 사용자와 그룹은 더 큰 vCenter Server 권한의 일부인 역할 권한을 통해 개체에 액세스할 수 있습니다.

ONTAP tools for VMware vSphere 와 함께 **vCenter Server RBAC** 사용

vCenter Server를 사용하여 ONTAP tools for VMware vSphere 에는 프로덕션 환경에서 사용하기 전에 고려해야 할 여러 가지 측면이 있습니다.

vCenter 역할 및 관리자 계정

vSphere 개체 및 관련 관리 작업에 대한 액세스를 제한하려는 경우에만 사용자 지정 vCenter Server 역할을 정의하고 사용하면 됩니다. 접근 제한이 필요하지 않은 경우 대신 관리자 계정을 사용할 수 있습니다. 각 관리자 계정은 개체 계층의 최상위에 있는 관리자 역할로 정의됩니다. 이를 통해 ONTAP tools for VMware vSphere 에서 추가된 개체를 포함하여 vSphere 개체에 대한 전체 액세스가 제공됩니다.

vSphere 개체 계층 구조

vSphere 개체 인벤토리는 계층 구조로 구성됩니다. 예를 들어, 다음과 같이 계층 구조를 아래로 이동할 수 있습니다.

`vCenter Server` → `Datacenter` → `Cluster` → `ESXi host` → `Virtual Machine`

VAAI 플러그인 작업을 제외한 모든 권한은 vSphere 개체 계층에서 검증되며, 해당 작업은 대상 ESXi 호스트를 기준으로 검증됩니다.

ONTAP tools for VMware vSphere 에 포함된 역할

vCenter Server RBAC 작업을 간소화하기 위해 ONTAP tools for VMware vSphere 다양한 관리 작업에 맞게 미리 정의된 역할을 제공합니다.

> 필요한 경우 새로운 사용자 정의 역할을 만들 수 있습니다. 이 경우 기존 ONTAP 도구 역할 중 하나를 복제하고 필요에 따라 편집해야 합니다. 구성을 변경한 후에는 영향을 받는 vSphere 클라이언트 사용자는 로그아웃했다가 다시 로그인하여 변경 사항을 활성화해야 합니다.

ONTAP tools for VMware vSphere 보려면 vSphere Client 상단에서 *메뉴*를 선택하고 *관리*를 클릭한 다음 왼쪽에서 *역할*을 클릭합니다. 아래에 설명된 대로 미리 정의된 역할이 세 가지 있습니다.

VMware vSphere 관리자를 위한 **NetApp ONTAP tools for VMware vSphere**

ONTAP tools for VMware vSphere 수행하는 데 필요한 모든 기본 vCenter Server 권한과 ONTAP 도구 관련 권한을 제공합니다.

ONTAP tools for VMware vSphere NetApp ONTAP 도구**(**읽기 전용**)**

ONTAP 도구에 대한 읽기 전용 액세스를 제공합니다. 이러한 사용자는 액세스가 제어되는 ONTAP tools for VMware vSphere 수행할 수 없습니다.

VMware vSphere Provision을 위한 **NetApp ONTAP tools for VMware vSphere**

스토리지 프로비저닝에 필요한 일부 기본 vCenter Server 권한과 ONTAP 도구 관련 권한을 제공합니다. 다음 작업을 수행할 수 있습니다.

- 새로운 데이터 저장소 만들기
- 데이터 저장소 관리

vSphere 객체 및 **ONTAP** 스토리지 백엔드

두 RBAC 환경은 함께 작동합니다. vSphere 클라이언트 인터페이스에서 작업을 수행할 때 vCenter Server에 정의된 ONTAP 도구 역할이 먼저 확인됩니다. vSphere에서 작업이 허용되는 경우 ONTAP 역할 권한이 검사됩니다. 두 번째 단계는 스토리지 백엔드가 생성되고 구성될 때 사용자에게 할당된 ONTAP 역할에 따라 수행됩니다.

vCenter Server RBAC 작업

vCenter Server 권한 및 사용 권한을 사용할 때 고려해야 할 몇 가지 사항이 있습니다.

필수 권한

ONTAP tools for VMware vSphere 에 액세스하려면 ONTAP 도구 관련 *View* 권한이 필요합니다. 이 권한 없이 vSphere에 로그인하고 NetApp 아이콘을 클릭하면 ONTAP tools for VMware vSphere 오류 메시지가 표시되고 사용자 인터페이스에 액세스할 수 없습니다.

vSphere 개체 계층의 할당 수준에 따라 사용자 인터페이스의 어떤 부분에 액세스할 수 있는지가 결정됩니다. 루트 개체에 보기 권한을 할당하면 NetApp 아이콘을 클릭하여 ONTAP tools for VMware vSphere 액세스할 수 있습니다.

대신 보기 권한을 다른 하위 vSphere 개체 수준에 할당할 수 있습니다. 하지만 이렇게 하면 액세스하고 사용할 수 있는 ONTAP tools for VMware vSphere 제한됩니다.

권한 할당

vSphere 개체 및 작업에 대한 액세스를 제한하려면 vCenter Server 권한을 사용해야 합니다. vSphere 개체 계층에서 권한을 할당하는 위치에 따라 ONTAP tools for VMware vSphere 사용자가 수행할 수 있는 작업이 결정됩니다.

> 더 제한적인 액세스를 정의할 필요가 없는 한 일반적으로 루트 개체나 루트 폴더 수준에서 권한을 할당하는 것이 좋습니다.

ONTAP tools for VMware vSphere 에서 제공하는 권한은 스토리지 시스템과 같은 사용자 지정 비 vSphere 개체에 적용됩니다. 가능하다면 ONTAP tools for VMware vSphere 에 이러한 권한을 할당해야 합니다. 할당할 수 있는 vSphere 개체가 없기 때문입니다. 예를 들어, ONTAP tools for VMware vSphere "스토리지 시스템 추가/수정/제거" 권한이 포함된 모든 권한은 루트 개체 수준에서 할당되어야 합니다.

개체 계층 구조에서 상위 레벨의 권한을 정의할 때 해당 권한이 하위 개체에 전달되고 상속되도록 구성할 수 있습니다. 필요한 경우 부모로부터 상속받은 권한을 재정의하는 추가 권한을 자식 개체에 할당할 수 있습니다.

언제든지 권한을 수정할 수 있습니다. 권한 내의 권한을 변경하는 경우 해당 권한과 연결된 사용자는 vSphere에서 로그아웃했다가 다시 로그인하여 변경 사항을 적용해야 합니다.

ONTAP 사용한 RBAC

ONTAP tools for VMware vSphere 사용한 ONTAP RBAC 환경

ONTAP 견고하고 확장 가능한 RBAC 환경을 제공합니다. RBAC 기능을 사용하면 REST API와 CLI를 통해 노출된 스토리지 및 시스템 작업에 대한 액세스를 제어할 수 있습니다. ONTAP tools for VMware vSphere 사용하기 전에 해당 환경에 익숙해지는 것이 좋습니다.

관리 옵션 개요

환경과 목표에 따라 ONTAP RBAC를 사용할 때 사용할 수 있는 여러 가지 옵션이 있습니다. 주요 행정 결정에 대한 개요는 아래와 같습니다. 또한 참조 "ONTAP 자동화: RBAC 보안 개요" 자세한 내용은.

> ONTAP RBAC는 스토리지 환경에 맞춰 설계되었으며 vCenter Server에서 제공하는 RBAC 구현보다 간단합니다. ONTAP 사용하면 사용자에게 직접 역할을 할당할 수 있습니다. ONTAP RBAC에서는 vCenter Server에서 사용되는 것과 같은 명시적 권한을 구성할 필요가 없습니다.

역할 및 권한 유형

ONTAP 사용자를 정의하려면 ONTAP 역할이 필요합니다. ONTAP 역할에는 두 가지 유형이 있습니다.

- 나머지

  REST 역할은 ONTAP 9.6에서 도입되었으며 일반적으로 REST API를 통해 ONTAP 에 액세스하는 사용자에게 적용됩니다. 이러한 역할에 포함된 권한은 ONTAP REST API 엔드포인트와 관련 작업에 대한 액세스 측면에서 정의됩니다.

- 전통적인

  이는 ONTAP 9.6 이전에 포함된 레거시 역할입니다. 그것들은 RBAC의 기초적인 측면으로 계속 유지됩니다. 권한은 ONTAP CLI 명령에 대한 액세스 측면에서 정의됩니다.

REST 역할은 최근에 도입되었지만, 기존 역할에도 몇 가지 장점이 있습니다. 예를 들어, 추가 쿼리 매개변수를 선택적으로 포함시켜 권한이 적용되는 개체를 보다 정확하게 정의할 수 있습니다.

범위

ONTAP 역할은 두 가지 범위 중 하나로 정의할 수 있습니다. 이러한 기능은 특정 데이터 SVM(SVM 수준)이나 전체 ONTAP 클러스터(클러스터 수준)에 적용될 수 있습니다.

역할 정의

ONTAP 클러스터와 SVM 수준 모두에서 미리 정의된 역할 세트를 제공합니다. 사용자 정의 역할을 정의할 수도 있습니다.

ONTAP REST 역할 작업

ONTAP tools for VMware vSphere 에 포함된 ONTAP REST 역할을 사용할 때는 몇 가지 고려 사항이 있습니다.

역할 매핑

기존 역할이나 REST 역할을 사용하든 모든 ONTAP 액세스 결정은 기본 CLI 명령을 기반으로 내려집니다. 하지만 REST 역할의 권한은 REST API 엔드포인트에 따라 정의되므로 ONTAP 각 REST 역할에 대해 매핑된 기존 역할을 만들어야 합니다. 따라서 각 REST 역할은 기본적인 기존 역할에 매핑됩니다. 이를 통해 ONTAP 역할 유형에 관계없이

일관된 방식으로 액세스 제어 결정을 내릴 수 있습니다. 병렬 매핑된 역할은 수정할 수 없습니다.

CLI 권한을 사용하여 REST 역할 정의

ONTAP 항상 CLI 명령을 사용하여 기본 수준에서 액세스를 결정하므로 REST 엔드포인트 대신 CLI 명령 권한을 사용하여 REST 역할을 표현할 수 있습니다. 이 접근 방식의 장점 중 하나는 기존 역할에서 사용할 수 있는 추가적인 세분성입니다.

ONTAP 역할 정의 시 관리 인터페이스

ONTAP CLI와 REST API를 사용하여 사용자와 역할을 생성할 수 있습니다. 하지만 ONTAP 도구 관리자를 통해 제공되는 JSON 파일과 함께 시스템 관리자 인터페이스를 사용하는 것이 더 편리합니다. 보다 "ONTAP tools for VMware vSphere 와 함께 ONTAP RBAC 사용" 자세한 내용은.

ONTAP tools for VMware vSphere 와 함께 ONTAP RBAC 사용

ONTAP 사용하여 ONTAP tools for VMware vSphere 에는 프로덕션 환경에서 사용하기 전에 고려해야 할 여러 가지 측면이 있습니다.

구성 프로세스 개요

ONTAP tools for VMware vSphere 사용자 정의 역할이 있는 ONTAP 사용자를 만드는 기능이 포함되어 있습니다. 정의는 ONTAP 클러스터에 업로드할 수 있는 JSON 파일에 패키징됩니다. 사용자를 만들고 해당 환경과 보안 요구 사항에 맞게 역할을 조정할 수 있습니다.

주요 구성 단계는 아래에 자세히 설명되어 있습니다. 참조하다"ONTAP 사용자 역할 및 권한 구성" 자세한 내용은.

1. 준비하다

ONTAP 도구 관리자와 ONTAP 클러스터 모두에 대한 관리 자격 증명이 필요합니다.

2. JSON 정의 파일을 다운로드하세요

ONTAP 도구 관리자 사용자 인터페이스에 로그인하면 RBAC 정의가 포함된 JSON 파일을 다운로드할 수 있습니다.

3. 역할이 있는 ONTAP 사용자 생성

시스템 관리자에 로그인한 후 사용자와 역할을 생성할 수 있습니다.

1. 왼쪽에서 *클러스터*를 선택한 다음 *설정*을 선택합니다.
2. *사용자 및 역할*까지 아래로 스크롤하여 클릭하세요. −→ .
3. *사용자*에서 *추가*를 선택하고 *가상화 제품*을 선택합니다.
4. 로컬 워크스테이션에서 JSON 파일을 선택하여 업로드합니다.

4. 역할 구성

역할을 정의하는 과정에서 몇 가지 관리적 결정을 내려야 합니다. 보다시스템 관리자를 사용하여 역할 구성 자세한 내용은.

시스템 관리자를 사용하여 역할 구성

System Manager에서 새로운 사용자와 역할을 만들고 JSON 파일을 업로드한 후에는 환경과 요구 사항에 맞게 역할을 사용자 정의할 수 있습니다.

핵심 사용자 및 역할 구성

RBAC 정의는 VSC, VASA Provider, SRA의 조합을 포함한 여러 제품 기능으로 패키지화되어 있습니다. RBAC 지원이 필요한 환경을 선택해야 합니다. 예를 들어, 원격 플러그인 기능을 지원하는 역할을 원하는 경우 VSC를 선택합니다. 또한 사용자 이름과 관련 비밀번호를 선택해야 합니다.

Privileges

역할 권한은 ONTAP 저장소에 필요한 액세스 수준에 따라 4개 세트로 구성됩니다. 역할의 기반이 되는 권한은 다음과 같습니다.

- 발견

  이 역할을 사용하면 스토리지 시스템을 추가할 수 있습니다.

- 저장소 만들기

  이 역할을 통해 저장소를 만들 수 있습니다. 여기에는 검색 역할과 관련된 모든 권한도 포함됩니다.

- 저장소 수정

  이 역할을 사용하면 저장소를 수정할 수 있습니다. 여기에는 검색 및 저장소 역할 생성과 관련된 모든 권한도 포함됩니다.

- 저장소 파괴

  이 역할을 사용하면 저장소를 파괴할 수 있습니다. 여기에는 검색, 저장소 생성, 저장소 역할 수정과 관련된 모든 권한이 포함됩니다.

역할이 있는 사용자 생성

환경에 대한 구성 옵션을 선택한 후 *추가*를 클릭하면 ONTAP 에서 사용자와 역할을 생성합니다. 생성된 역할의 이름은 다음 값을 연결한 것입니다.

- JSON 파일에 정의된 상수 접두사 값(예: "OTV_10")
- 선택한 제품 기능
- 권한 집합 목록입니다.

예

```
OTV_10_VSC_Discovery_Create
```

새로운 사용자는 "사용자 및 역할" 페이지의 목록에 추가됩니다. HTTP와 ONTAPI 사용자 로그인 방법이 모두 지원됩니다.

ONTAP tools for VMware vSphere 의 고가용성

ONTAP tools for VMware vSphere 장애 발생 시에도 ONTAP tools for VMware vSphere 의 중단 없는 기능을 제공하는 데 도움이 되는 고가용성(HA) 구성을 지원합니다.

고가용성(HA) 솔루션은 다음으로 인한 중단으로부터 빠른 복구를 제공합니다.

- 호스트 실패

> 단일 노드 장애만 지원됩니다.

- 네트워크 장애
- 가상 머신 장애(게스트 OS 장애)
- 애플리케이션(ONTAP 도구) 충돌

ONTAP tools for VMware vSphere 는 고가용성(HA)을 제공하기 위해 추가 구성이 필요하지 않습니다.

> ONTAP tools for VMware vSphere vCenter HA를 지원하지 않습니다.

HA 기능을 활성화하려면 배포 중 또는 나중에 ONTAP tools for VMware vSphere 에서 CPU 핫 애드 및 메모리 핫 플러그를 활성화해야 합니다.

ONTAP 도구 관리자 사용자 인터페이스

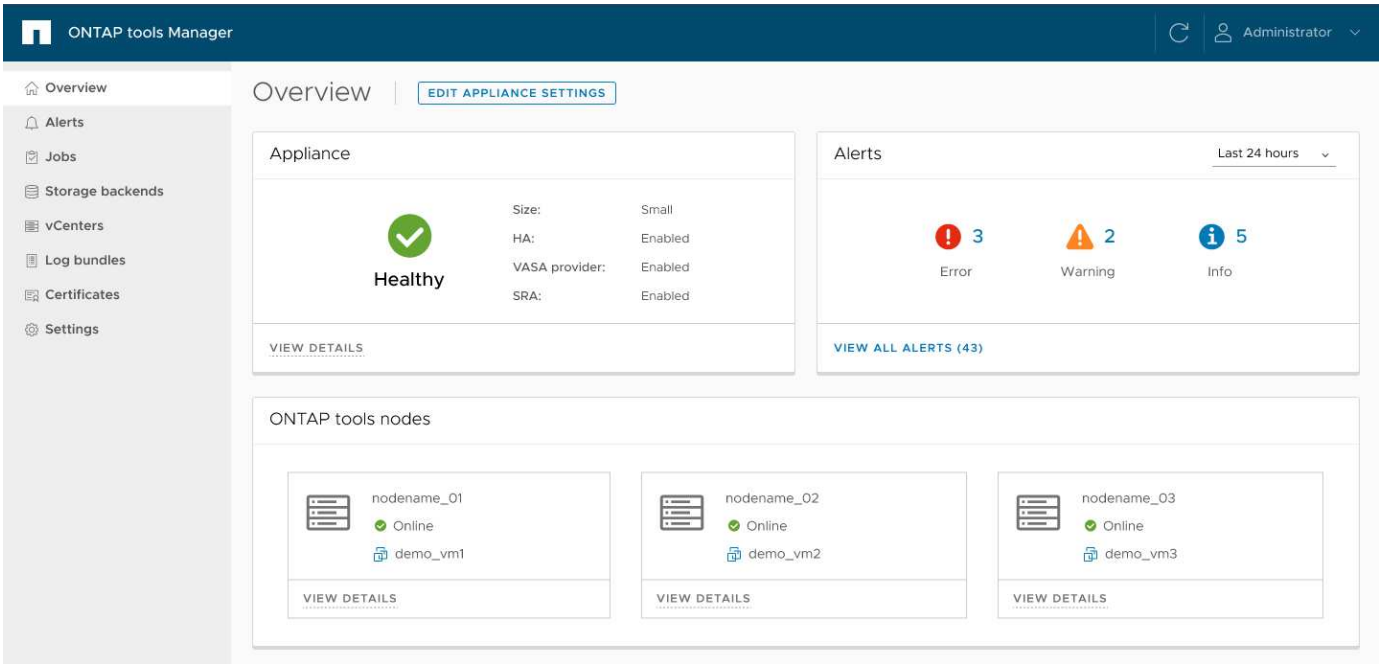
ONTAP tools for VMware vSphere 여러 vCenter Server 인스턴스를 관리할 수 있는 멀티 테넌트 시스템입니다. ONTAP 도구 관리자는 관리되는 vCenter Server 인스턴스와 온보딩된 스토리지 백엔드에 대한 ONTAP tools for VMware vSphere 에 대한 더 많은 제어 기능을 제공합니다.

ONTAP 도구 관리자는 다음과 같은 데 도움이 됩니다.

- vCenter Server 인스턴스 관리 - ONTAP 도구에 vCenter Server 인스턴스를 추가하고 관리합니다.
- 스토리지 백엔드 관리 - ONTAP tools for VMware vSphere 에 ONTAP 스토리지 클러스터를 추가하고 관리하고 이를 전역적으로 온보딩된 vCenter Server 인스턴스에 매핑합니다.
- 로그 번들 다운로드 - ONTAP tools for VMware vSphere 에 대한 로그 파일을 수집합니다.
- 인증서 관리 - 자체 서명된 인증서를 사용자 정의 CA 인증서로 변경하고 VASA Provider 및 ONTAP 도구의 모든 인증서를 갱신하거나 새로 고칩니다.
- 비밀번호 관리 - 사용자의 OVA 애플리케이션 비밀번호를 재설정합니다.

ONTAP 도구 관리자에 액세스하려면 다음을 실행하세요.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/` 브라우저에서 ONTAP tools for VMware vSphere 로그인합니다.

ONTAP 도구 관리자 개요 섹션은 서비스 관리, 노드 크기 확장, 고가용성(HA) 활성화 등의 어플라이언스 구성을 관리하는 데 도움이 됩니다. 또한 노드와 관련된 ONTAP 도구의 전반적인 정보(상태, 네트워크 세부 정보, 알림 등)를 모니터링할 수 있습니다.



카드	설명
가전제품 카드	어플라이언스 카드는 ONTAP 도구 어플라이언스의 전반적인 상태를 제공합니다. 여기에는 기기 구성 세부 정보와 활성화된 서비스 상태가 표시됩니다. ONTAP 도구 어플라이언스에 대한 추가 정보를 보려면 세부 정보 보기 링크를 선택하세요. 편집 기기 설정 작업 작업이 진행 중일 때, 기기 포틀릿에 작업의 상태와 세부 정보가 표시됩니다.
알림 카드	알림 카드에는 HA 노드 수준 알림을 포함하여 유형별로 ONTAP 도구 알림이 나열됩니다. 알림 목록을 보려면 개수 텍스트(하이퍼링크)를 선택하세요. 링크를 클릭하면 선택한 유형으로 필터링된 알림 보기 페이지로 이동합니다.
vCenter	vCenter 카드는 시스템의 vCenter 상태를 보여줍니다.
스토리지 백엔드	스토리지 백엔드 카드는 시스템의 스토리지 백엔드 상태를 보여줍니다.
ONTAP 도구 노드 카드	ONTAP 도구 노드 카드는 노드 이름, 노드 VM 이름, 상태 및 모든 네트워크 관련 데이터가 포함된 노드 목록을 보여줍니다. *세부정보 보기*를 선택하면 선택한 노드와 관련된 추가 세부정보를 볼 수 있습니다. [참고] HA가 아닌 설정에서는 노드가 하나만 표시됩니다. HA 설정에서는 세 개의 노드가 표시됩니다.

ONTAP tools for VMware vSphere 배포

ONTAP tools for VMware vSphere 에 대한 빠른 시작

이 빠른 시작 섹션을 통해 ONTAP tools for VMware vSphere 설정하세요.

처음에는 NFS 및 VMFS 데이터 저장소를 지원하는 핵심 서비스를 제공하는 소규모 단일 노드 구성으로 ONTAP tools for VMware vSphere 배포합니다. vVols 데이터 저장소와 고가용성(HA)을 사용하기 위해 구성을 확장해야 하는 경우 이 워크플로를 완료한 후에 해당 작업을 수행하게 됩니다. 자세한 내용은 다음을 참조하세요. "HA 배포 워크플로" .

1 배포 계획

vSphere, ONTAP 및 ESXi 호스트 버전이 ONTAP 도구 버전과 호환되는지 확인하세요. 충분한 CPU, 메모리 및 디스크 공간을 할당하세요. 보안 규칙에 따라 네트워크 트래픽을 허용하기 위해 방화벽이나 기타 보안 도구를 설정해야 할 수도 있습니다.

vCenter Server가 설치되어 있고 접근 가능한지 확인하세요.

- "상호 운용성 매트릭스 도구"
- "ONTAP tools for VMware vSphere"
- "시작하기 전에"

2 **ONTAP tools for VMware vSphere** 배포

처음에는 ONTAP tools for VMware vSphere NFS 및 VMFS 데이터 저장소를 지원하는 핵심 서비스를 제공하는 소규모 단일 노드 구성으로 배포합니다. vVols 데이터 저장소와 고가용성(HA)을 사용하도록 구성을 확장하려면 이 워크플로를 완료한 후에 확장해야 합니다. HA 설정으로 확장하려면 CPU 핫 애드 및 메모리 핫 플러그가 활성화되어 있는지 확인하십시오.

- "ONTAP tools for VMware vSphere 배포"

3 **vCenter Server** 인스턴스 추가

vCenter Server 환경에서 가상 데이터스토어를 구성, 관리 및 보호하기 위해 ONTAP tools for VMware vSphere 에 vCenter Server 인스턴스를 추가합니다.

- "vCenter Server 인스턴스 추가"

4 **ONTAP** 사용자 역할 및 권한 구성

ONTAP tools for VMware vSphere 와 함께 제공되는 JSON 파일을 사용하여 스토리지 백엔드를 관리하기 위한 새로운 사용자 역할과 권한을 구성합니다.

- "ONTAP 사용자 역할 및 권한 구성"

5 스토리지 백엔드 구성

ONTAP 클러스터에 스토리지 백엔드를 추가합니다. vCenter가 연관된 SVM이 있는 테넌트 역할을 하는 다중 테넌시 설정의 경우 ONTAP 도구 관리자를 사용하여 클러스터를 추가합니다. 스토리지 백엔드를 vCenter Server와 연결하여 온보딩된 vCenter Server 인스턴스에 전역적으로 매핑합니다.

ONTAP 도구 사용자 인터페이스를 사용하여 클러스터 또는 SVM 자격 증명으로 로컬 스토리지 백엔드를 추가합니다. 이러한 스토리지 백엔드는 단일 vCenter로 제한됩니다. 로컬에서 클러스터 자격 증명을 사용하는 경우 연관된 SVM은 자동으로 vCenter에 매핑되어 vVols 또는 VMFS를 관리합니다. SRA를 포함한 VMFS 관리의 경우 ONTAP 도구는 글로벌 클러스터가 필요 없이 SVM 자격 증명을 지원합니다.

- "스토리지 백엔드 추가"
- "스토리지 백엔드를 vCenter Server 인스턴스와 연결합니다."

6 여러 **vCenter Server** 인스턴스로 작업하는 경우 인증서를 업그레이드하세요.

여러 vCenter Server 인스턴스로 작업하는 경우 자체 서명된 인증서를 인증 기관(CA) 서명 인증서로 업그레이드합니다.

- "인증서 관리"

7 (선택 사항) **SRA** 보호 구성

SRA 기능을 활성화하여 재해 복구를 구성하고 NFS 또는 VMFS 데이터 저장소를 보호합니다.

- "ONTAP tools for VMware vSphere 활성화"
- "VMware Live Site Recovery 어플라이언스에서 SRA 구성"

8 (선택 사항) **SnapMirror** 활성 동기화 보호 활성화

SnapMirror 활성 동기화에 대한 호스트 클러스터 보호를 관리하기 위해 ONTAP tools for VMware vSphere 구성합니다. ONTAP 시스템에서 ONTAP 클러스터 및 SVM 피어링을 수행하여 SnapMirror 활성 동기화를 사용합니다. 이는 VMFS 데이터 저장소에만 적용됩니다.

- "호스트 클러스터 보호를 사용하여 보호"

9 **ONTAP tools for VMware vSphere** 에 대한 백업 및 복구 설정

장애 발생 시 설정을 복구하는 데 사용할 수 있는 ONTAP tools for VMware vSphere 의 백업을 예약합니다.

- "백업을 생성하고 ONTAP 도구 설정을 복구합니다."

고가용성(HA) 배포 워크플로

vVols 데이터 저장소를 사용하는 경우 ONTAP 도구의 초기 배포를 고가용성(HA) 구성으로 확장하고 VASA 공급자 서비스를 활성화해야 합니다.

1 배포 확장

배포에서 노드 수를 늘리고 구성을 HA 설정으로 변경하기 위해 ONTAP tools for VMware vSphere 확장할 수 있습니다.

- "ONTAP tools for VMware vSphere 변경"

2 서비스 활성화

vVols 데이터 저장소를 구성하려면 VASA Provider 서비스를 활성화해야 합니다. vCenter에 VASA 공급자를 등록하고 적절한 네트워크 및 스토리지 구성을 비롯하여 스토리지 정책이 HA 요구 사항을 충족하는지 확인하세요.

VMware Site Recovery Manager(SRM) 또는 VMware Live Site Recovery(VLSR)를 위해 ONTAP 도구 Storage Replication Adapter(SRA)를 사용하도록 SRA 서비스를 활성화합니다.

- "VASA 공급자 및 SRA 서비스 활성화"

3 인증서 업그레이드

여러 vCenter Server 인스턴스와 함께 vVol 데이터스토어를 사용하는 경우 자체 서명된 인증서를 인증 기관(CA) 서명 인증서로 업그레이드합니다.

- "인증서 관리"

ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 배포하기 전에 배포 패키지의 공간 요구 사항과 몇 가지 기본 호스트 시스템 요구 사항을 숙지해야 합니다.

VMware vCenter Server Virtual Appliance(vCSA)와 함께 ONTAP tools for VMware vSphere 사용할 수 있습니다. ESXi 시스템을 포함하는 지원되는 vSphere 클라이언트에 ONTAP tools for VMware vSphere 배포해야 합니다.

시스템 요구 사항

- 노드당 설치 패키지 공간 요구 사항
  - 씬 프로비저닝 설치의 경우 15GB
  - 두꺼운 프로비저닝 설치의 경우 348GB
- 호스트 시스템 크기 요구 사항 배포 크기에 따른 권장 메모리는 아래 표와 같습니다. 고가용성(HA)을 구축하려면 표에 명시된 어플라이언스 크기의 3배가 필요합니다.

배치 유형	노드당 **CPU**	노드당 메모리**(GB)**	노드당 두꺼운 프로비저닝 디스크 공간**(GB)**
작은	9	18	350
중간	13	26	350

대규모 참고: 대규모 배포는 HA 구성에만 적용됩니다.	17	34	350

백업이 활성화되면 각 ONTAP 도구 클러스터에는 VM이 배포된 데이터 저장소에 50GB의 추가 공간이 필요합니다. 따라서 non-HA는 400GB가 필요하고, HA는 총 1100GB의 공간이 필요합니다.

최소 저장 및 적용 요구 사항

저장소, 호스트 및 애플리케이션	버전 요구 사항
ONTAP	9.14.1, 9.15.1, 9.16.0, 9.16.1 및 9.16.1P3 FAS, ASA A-시리즈, ASA C-시리즈, AFF A-시리즈, AFF C-시리즈 및 ASA r2.
ONTAP 도구는 ESXi 호스트를 지원합니다.	7.0.3부터
ONTAP 도구 지원 vCenter Server	7.0U3 이상
VASA 제공자	3.0
OVA 애플리케이션	10.4
ONTAP 도구 가상 머신을 배포하기 위한 ESXi 호스트	7.0U3 및 8.0U3
ONTAP 도구 가상 머신을 배포하기 위한 vCenter Server	7.0과 8.0

ONTAP tools for VMware vSphere 부터 가상 머신 하드웨어가 버전 10에서 17로 변경되었습니다.

상호 운용성 매트릭스 도구(IMT)에는 지원되는 ONTAP, vCenter Server, ESXi 호스트 및 플러그인 애플리케이션 버전에 대한 최신 정보가 포함되어 있습니다.

"상호 운용성 매트릭스 도구"

포트 요구 사항

다음 표는 NetApp 에서 사용하는 네트워크 포트와 그 용도를 간략하게 설명합니다. 시스템 내에서 원활한 작동 및 통신을 위해 이러한 포트가 열려 있고 접근 가능한지 확인하십시오. 관련 서비스가 정상적으로 작동하려면 이러한 포트에서 트래픽을 허용하는 데 필요한 네트워크 구성이 제대로 되어 있는지 확인하십시오. 보안 정책에 따라 네트워크 내에서 이러한 트래픽을 허용하도록 방화벽이나 기타 보안 어플라이언스를 구성해야 할 수도 있습니다.

포트	규약	설명
8143	TCP	ONTAP 도구에 대한 HTTP/HTTPS 연결.
8043	TCP	ONTAP 도구에 대한 HTTP/HTTPS 연결.
9060	TCP	ONTAP 도구에 대한 HTTP/HTTPS 연결.

22	TCP	Ansible은 클러스터 프로비저닝 중 통신을 위해 이 SSH 포트를 사용합니다. 이 포트는 HA 구성의 경우 유지 관리 사용자 비밀번호, 상태 메시지를 변경하고 세 노드 모두의 값을 업데이트하는 등의 기능에 필요합니다.
443	TCP	이는 VASA 공급자 서비스에 대한 수신 통신을 위한 통과 포트입니다. VASA 공급자 자체 서명 인증서와 사용자 정의 CA 인증서가 이 포트에 호스팅됩니다.
8443	TCP	이 포트는 swagger와 Manager 사용자 인터페이스 애플리케이션을 통해 API 문서를 호스팅합니다.
2379	TCP	이는 etcd 키 값 저장소에서 키를 가져오거나, 넣거나, 삭제하거나, 감시하는 것과 같은 클라이언트 요청에 대한 기본 포트입니다.
2380	TCP	이는 etcd가 데이터 복제 및 일관성을 위해 사용하는 Raft 합의 알고리즘에 사용되는 etcd 클러스터의 서버 간 통신을 위한 기본 포트입니다.
7472	TCP/UDP	이것은 프로메테우스 메트릭 서비스 포트입니다.
7946	TCP/UDP	이 포트는 Docker의 컨테이너 네트워크 검색에 사용됩니다.
9083	TCP	이 포트는 VASA Provider 서비스를 위한 내부적으로 사용되는 서비스 포트입니다.
1162	UDP	이것은 SNMP 트랩 패킷 포트입니다.
6443	TCP	출처: RKE2 에이전트 노드. 대상: REK2 서버 노드. 설명: Kubernetes API
9345	TCP	출처: RKE2 에이전트 노드. 대상: REK2 서버 노드. 설명: REK2 관리자 API
8472	TCP+UDP	플란넬 VXLAN을 사용하는 경우 모든 노드는 UDP 포트 8472를 통해 다른 노드에 접속할 수 있어야 합니다. 출처: 모든 RKE2 노드. 대상지: 모든 REK2 노드. 설명: VXLAN을 사용한 Canal CNI
10250	TCP	출처: 모든 RKE2 노드. 대상지: 모든 REK2 노드. 설명: Kubelet 메트릭

30000-32767	TCP	출처: 모든 RKE2 노드. 대상지: 모든 REK2 노드. 설명: NodePort 포트 범위
123	TCP	Ntpd는 이 포트를 사용하여 NTP 서버의 유효성 검사를 수행합니다.
137-139	TCP/UDP	SMB/Windows 공유 패킷.
6789	TCP	세프 모니터(MON)
3300	TCP	세프 모니터(MON)
6800-7300	TCP	Ceph 관리자, OSD 및 파일 시스템(MDS).
80	TCP	Ceph RADOS 게이트웨이(RGW)
9080	TCP	VP HTTP/HTTPS 연결(IPv4의 경우 127.0.0.0/8에서만 가능, IPv6의 경우 ::1/128에서만 가능).

ONTAP tools for VMware vSphere 배포를 위한 구성 제한

다음 표를 가이드로 사용하여 ONTAP tools for VMware vSphere 구성할 수 있습니다.

전개	유형	* vVols 수 *	호스트 수
비HA	소형(S)	~12K	32
비HA	중간(M)	~24K	64
고가용성	소형(S)	~24K	64
고가용성	중간(M)	~5만	128
고가용성	대형(L)	~10만	256 [참고] 표의 호스트 수는 여러 vCenter의 총 호스트 수를 보여줍니다.

ONTAP tools for VMware vSphere - 스토리지 복제 어댑터(SRA)

다음 표는 ONTAP tools for VMware vSphere 사용하여 VMware Live Site Recovery 인스턴스당 지원되는 숫자를 보여줍니다.

vCenter 배포 크기	작은	중간
어레이 기반 복제를 사용하여 보호를 위해 구성된 총 가상 머신 수	2000	5000
어레이 기반 복제 보호 그룹의 총 수	250	250
복구 계획당 보호 그룹의 총 수	50	50
복제된 데이터 저장소 수	255	255
VM 수	4000	7000

다음 표는 ONTAP tools for VMware vSphere 보여줍니다.

VMware Live Site Recovery 인스턴스 수	* ONTAP 도구 배포 크기*
최대 4개	작은
4에서 8까지	중간
8개 이상	크기가 큰

자세한 내용은 다음을 참조하세요. "VMware Live Site Recovery의 운영 한계" .

시작하기 전에...

배포를 진행하기 전에 다음 요구 사항이 충족되는지 확인하세요.

요구 사항	귀하의 상태
vSphere 버전, ONTAP 버전, ESXi 호스트 버전은 ONTP 도구 버전과 호환됩니다.	□ 예 □ 아니오
vCenter Server 환경이 설정 및 구성되었습니다.	□ 예 □ 아니오
브라우저 캐시가 삭제되었습니다	□ 예 □ 아니오
부모 vCenter Server 자격 증명이 있습니다.	□ 예 □ 아니오
ONTAP tools for VMware vSphere 등록을 위해 배포 후 연결할 vCenter Server 인스턴스에 대한 로그인 자격 증명이 있습니다.	□ 예 □ 아니오
인증서가 발급된 도메인 이름은 사용자 지정 CA 인증서가 필수인 다중 vCenter 배포 환경에서 가상 IP 주소에 매핑됩니다.	□ 예 □ 아니오
도메인 이름에 대해 nslookup 검사를 실행하여 도메인이 의도한 IP 주소로 확인되는지 확인했습니다.	□ 예 □ 아니오
인증서는 도메인 이름과 ONTAP 도구 IP 주소로 생성됩니다.	□ 예 □ 아니오
ONTAP 도구 애플리케이션과 내부 서비스는 vCenter Server에서 접근할 수 있습니다.	□ 예 □ 아니오
멀티 테넌트 SVM을 사용하는 경우 각 SVM에 SVM 관리 LIF가 있습니다.	□ 예 □ 아니오

배포 워크시트

단일 노드 배포의 경우

다음 워크시트를 사용하여 ONTAP tools for VMware vSphere 에 필요한 정보를 수집하세요.

요구 사항	당신의 가치
ONTAP 도구 애플리케이션의 IP 주소입니다. 이는 ONTAP 도구 웹 인터페이스에 액세스하기 위한 IP 주소입니다.	

요구 사항	당신의 가치
ONTAP 도구는 내부 통신을 위한 가상 IP 주소를 제공합니다. 이 IP 주소는 여러 ONTAP 도구 인스턴스가 있는 설정에서 내부 통신에 사용됩니다. 이 IP 주소는 ONTAP 도구 애플리케이션의 IP 주소와 동일해서는 안 됩니다.	
첫 번째 노드의 DNS 호스트 이름	
기본 DNS 서버	
보조 DNS 서버	
DNS 검색 도메인	
첫 번째 노드의 IPv4 주소입니다. 이는 관리 네트워크의 노드 관리 인터페이스를 위한 고유한 IPv4 주소입니다.	
IPv4 주소에 대한 서브넷 마스크	
IPv4 주소에 대한 기본 게이트웨이	
IPv6 주소(선택 사항)	
IPv6 접두사 길이(선택 사항)	
IPv6 주소에 대한 게이트웨이(선택 사항)	

위의 모든 IP 주소에 대한 DNS 레코드를 만듭니다. 호스트 이름을 할당하기 전에 DNS의 사용 가능한 IP 주소에 매핑하세요. 모든 IP 주소는 배포를 위해 선택된 동일한 VLAN에 있어야 합니다.

고가용성**(HA)** 배포를 위해

단일 노드 배포 요구 사항 외에도 HA 배포를 위해 다음 정보가 필요합니다.

요구 사항	당신의 가치
기본 DNS 서버	
보조 DNS 서버	
DNS 검색 도메인	
두 번째 노드의 DNS 호스트 이름	
두 번째 노드의 IP 주소	
세 번째 노드의 DNS 호스트 이름	
세 번째 노드의 IP 주소	

네트워크 방화벽 구성

네트워크 방화벽에서 IP 주소에 필요한 포트를 엽니다. ONTAP 도구는 포트 443을 통해 이 LIF에 도달할 수 있어야 합니다. 참조하다"포트 요구 사항" 최신 업데이트를 확인하세요.

ONTAP 스토리지 설정

ONTAP tools for VMware vSphere ONTAP 도구와 ONTAP 스토리지의 원활한 통합을 보장하려면 다음 설정을 고려하세요.

- 스토리지 연결에 파이버 채널(FC)을 사용하는 경우 FC 스위치의 구역 설정을 구성하여 ESXi 호스트를 SVM의 FC LIF에 연결합니다. "ONTAP 시스템을 사용한 FC 및 FCoE 구역 지정에 대해 알아보세요"
- ONTAP 도구 관리 SnapMirror 복제를 사용하려면 ONTAP 스토리지 관리자가 다음을 생성해야 합니다. "ONTAP 클러스터 피어 관계" 그리고 "ONTAP 클러스터 간 SVM 피어 관계" SnapMirror 사용하기 전에 ONTAP 에서.

ONTAP tools for VMware vSphere 배포

ONTAP tools for VMware vSphere NFS 및 VMFS 데이터 저장소를 지원하는 핵심 서비스를 갖춘 소규모 단일 노드로 배포됩니다. ONTAP 도구 배포 프로세스는 최대 45분이 소요될 수 있습니다.

시작하기 전에

VMware의 콘텐츠 라이브러리는 VM 템플릿, vApp 템플릿 및 기타 유형의 파일을 저장하는 컨테이너 객체입니다. 콘텐츠 라이브러리를 사용한 배포는 네트워크 연결에 의존하지 않으므로 원활한 환경을 제공합니다.

> 클러스터 내의 모든 호스트가 액세스할 수 있도록 콘텐츠 라이브러리를 공유 데이터 저장소에 저장해야 합니다. HA 구성으로 어플라이언스를 구성하기 전에 OVA를 저장할 콘텐츠 라이브러리를 만듭니다. 배포 후에는 콘텐츠 라이브러리 템플릿을 삭제하지 마세요.

> 나중에 HA 배포를 활성화하려면 ONTAP 도구를 호스팅하는 가상 머신을 ESXi 호스트에 직접 배포하지 마세요. 대신 클러스터나 리소스 풀에 배포하세요.

콘텐츠 라이브러리가 없는 경우 다음 단계에 따라 라이브러리를 만드세요.

콘텐츠 라이브러리 만들기 소규모 단일 노드 배포만 사용하려는 경우 콘텐츠 라이브러리를 만들 필요가 없습니다.

1. ONTAP tools for VMware vSphere 의 바이너리(*.ova*)와 서명된 인증서가 포함된 파일을 다운로드하세요. "NetApp 지원 사이트" .
2. vSphere 클라이언트에 로그인합니다
3. vSphere 클라이언트 메뉴를 선택하고 *콘텐츠 라이브러리*를 선택합니다.
4. 페이지 오른쪽에서 *만들기*를 선택하세요.
5. 라이브러리 이름을 지정하고 콘텐츠 라이브러리를 만듭니다.
6. 생성한 콘텐츠 라이브러리로 이동합니다.
7. 페이지 오른쪽에서 *작업*을 선택하고 *항목 가져오기*를 선택하여 OVA 파일을 가져옵니다.

> 자세한 내용은 다음을 참조하세요. "콘텐츠 라이브러리 만들기 및 사용" 블로그.

> 배포를 진행하기 전에 인벤토리의 클러스터 분산 리소스 스케줄러(DRS)를 '보수적'으로 설정합니다. 이렇게 하면 설치 중에 VM이 마이그레이션되지 않습니다.

ONTAP tools for VMware vSphere 처음에는 비 HA 설정으로 배포됩니다. HA 배포로 확장하려면 CPU 핫 플러그와 메모리 핫 플러그인을 활성화해야 합니다. 이 단계는 배포 프로세스의 일부로 수행하거나 배포 후 VM 설정을 편집할 수 있습니다.

단계

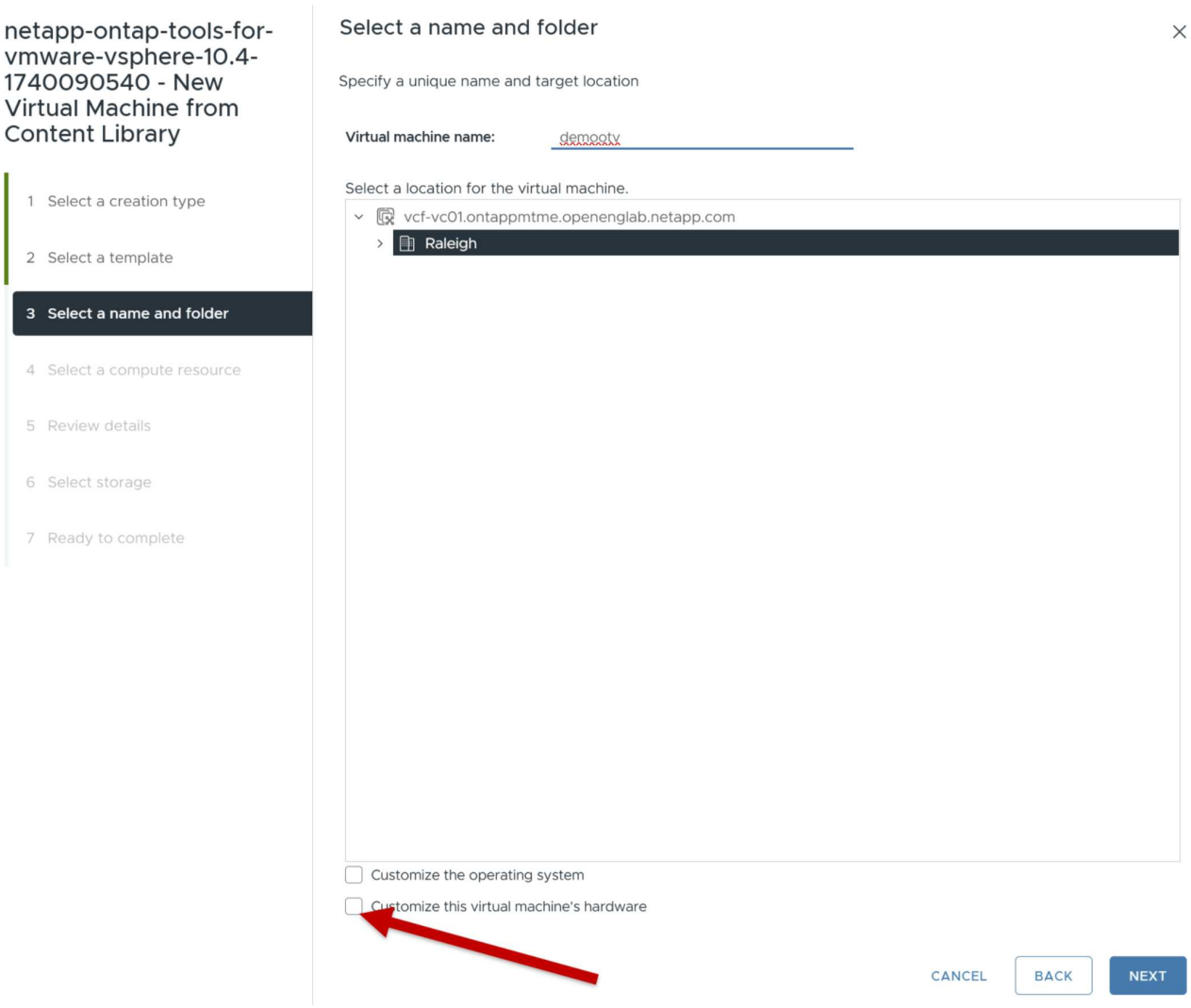
1. 에서 ONTAP tools for VMware vSphere에 대한 바이너리(*.ova*) 및 서명된 인증서가 포함된 파일을 다운로드합니다 "NetApp 지원 사이트" OVA를 콘텐츠 라이브러리로 가져온 경우 이 단계를 건너뛰고 다음 단계로 진행할 수 있습니다
2. vSphere 서버에 로그인합니다.
3. OVA를 배포하려는 리소스 풀, 클러스터 또는 호스트로 이동합니다.

   ONTAP tools for VMware vSphere 해당 가상 머신이 관리하는 vVols 데이터 저장소에 저장하지 마세요.

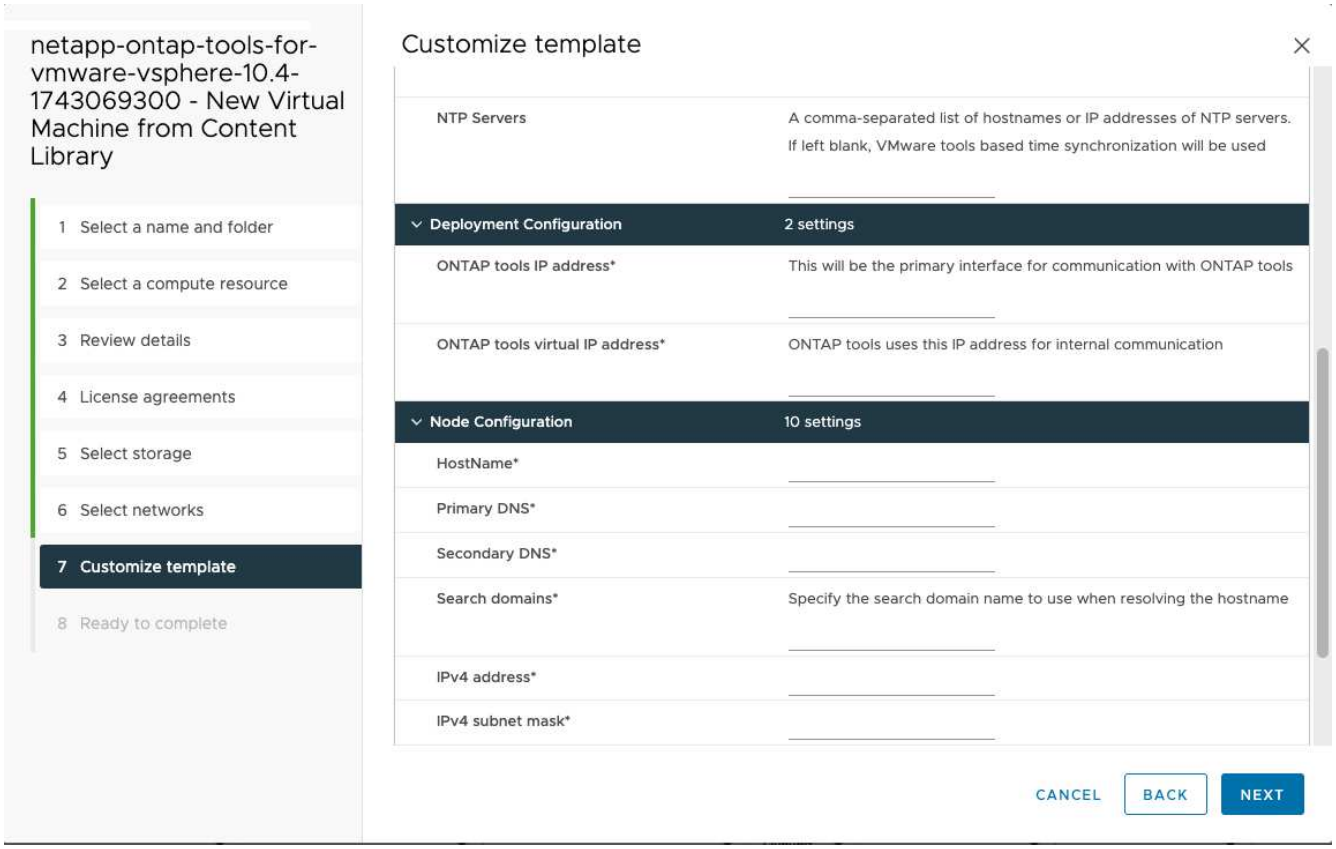
4. 콘텐츠 라이브러리나 로컬 시스템에서 OVA를 배포할 수 있습니다.

로컬 시스템에서	콘텐츠 라이브러리에서
a. 마우스 오른쪽 버튼을 클릭하고 *OVF 템플릿 배포…*를 선택합니다. b. URL에서 OVA 파일을 선택하거나 해당 위치를 찾은 후 *다음*을 선택합니다.	a. 콘텐츠 라이브러리로 이동하여 배포할 라이브러리 항목을 선택합니다. b. 작업 > *이 템플릿에서 새 VM*을 선택합니다.

5. 이름 및 폴더 선택 필드에 가상 머신 이름을 입력하고 위치를 선택합니다.
   - vCenter Server 8.0.3 버전을 사용하는 경우 이 가상 머신의 하드웨어 사용자 지정 옵션을 선택하면 완료 준비 창으로 넘어가기 전에 *하드웨어 사용자 지정*이라는 추가 단계가 활성화됩니다.
   - vCenter Server 7.0.3 버전을 사용하는 경우 배포 마지막 부분의 다음 단계는 무엇입니까**?** 섹션의 단계를 따르세요.



6. 컴퓨터 리소스를 선택하고 다음*을 선택합니다. 선택적으로, *배포된 **VM**을 자동으로 켜기 상자를 선택합니다.
7. 템플릿의 세부 정보를 검토하고 *다음*을 선택하세요.
8. 라이센스 계약을 읽고 동의한 후 *다음*을 선택하세요.
9. 구성을 위한 저장소와 디스크 형식을 선택하고 *다음*을 선택합니다.
10. 각 소스 네트워크에 대한 대상 네트워크를 선택하고 *다음*을 선택합니다.
11. 템플릿 사용자 지정 창에서 필수 필드를 입력하고 *다음*을 선택합니다
.

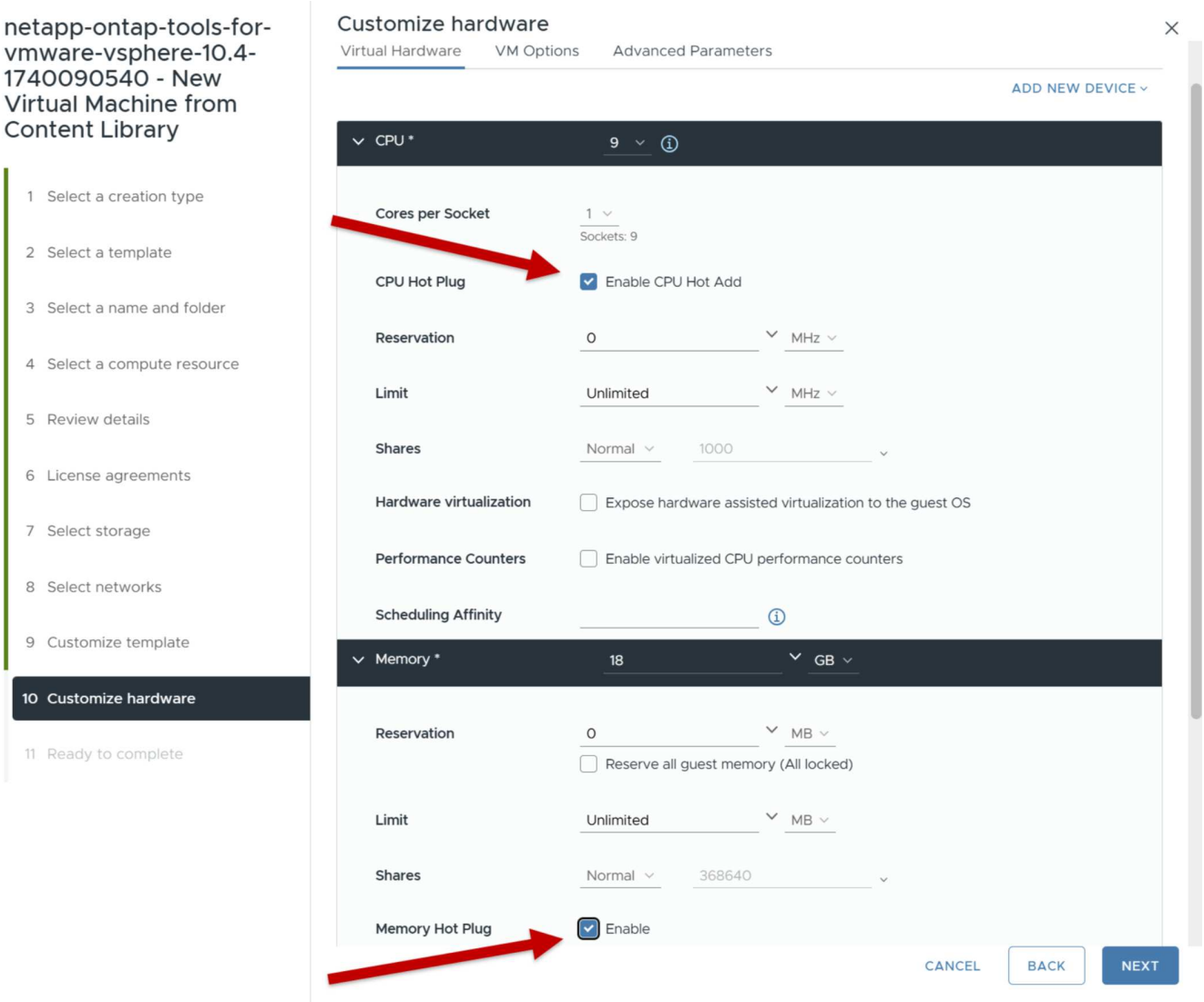


- 정보는 설치 중에 검증됩니다. 불일치가 있는 경우 웹 콘솔에 오류 메시지가 나타나고 이를 수정하라는 메시지가 표시됩니다.
- 호스트 이름에는 문자(AZ, az), 숫자(0-9), 하이픈(-)이 포함되어야 합니다. 듀얼 스택을 구성하려면 IPv6 주소에 매핑된 호스트 이름을 지정합니다.

> 순수 IPv6는 지원되지 않습니다. 혼합 모드는 IPv6 및 IPv4 주소를 모두 포함하는 VLAN에서 지원됩니다.

- ONTAP 도구 IP 주소는 ONTAP 도구와 통신하기 위한 기본 인터페이스입니다.
- IPv4는 노드 구성의 IP 주소 구성 요소로, 디버깅 및 유지 관리를 위해 노드에서 진단 셸과 SSH 액세스를 활성화하는 데 활용할 수 있습니다.

12. vCenter Server 8.0.3 버전을 사용하는 경우, 하드웨어 사용자 지정 창에서 **CPU** 핫 추가 및 메모리 핫 플러그 옵션을 활성화하여 HA 기능을 허용합니다
.



13. 완료 준비 창에서 세부 정보를 검토하고 *마침*을 선택하세요.

    배포 작업이 생성되면 vSphere 작업 표시줄에 진행률이 표시됩니다.

14. VM을 자동으로 켜는 옵션이 선택되지 않은 경우, 작업을 완료한 후 VM의 전원을 켭니다.

VM의 웹 콘솔에서 설치 진행 상황을 추적할 수 있습니다.

OVF 양식에 불일치 사항이 있는 경우 대화 상자가 나타나 수정 조치를 취하도록 안내합니다. 탭 버튼을 사용하여 탐색하고, 필요한 변경 사항을 적용한 후 *확인*을 선택하세요. 문제를 해결하려면 세 번의 시도가 있습니다. 3번 시도 후에도 문제가 지속되면 설치 프로세스가 중지되므로 새 가상 머신에서 설치를 다시 시도하는 것이 좋습니다.

다음은 무엇인가요**?**

vCenter Server 7.0.3이 포함된 ONTAP tools for VMware vSphere 있는 경우 배포 후 다음 단계를 따르세요.

1. vCenter 클라이언트에 로그인합니다.
2. ONTAP 도구 노드의 전원을 끕니다.
3. 인벤토리*에서 **ONTAP tools for VMware vSphere** 로 이동하여 *설정 편집 옵션을 선택합니다.
4. **CPU** 옵션에서 **CPU** 핫 추가 사용 확인란을 선택합니다.

5. 메모리 옵션에서 메모리 핫 플러그*에 대한 *활성화 확인란을 선택합니다.

배포 오류 코드

ONTAP tools for VMware vSphere 사용 중 오류 코드가 발생할 수 있습니다. 오류 코드는 5자리 숫자로, 처음 두 자리는 문제가 발생한 스크립트를 나타내고, 마지막 세 자리는 해당 스크립트 내의 특정 워크플로를 나타냅니다.

모든 오류 로그는 ansible-perl-errors.log 파일에 기록되어 문제를 쉽게 추적하고 해결할 수 있습니다. 이 로그 파일에는 오류 코드와 실패한 Ansible 작업이 포함되어 있습니다.

> 이 페이지에 제공된 오류 코드는 참조용일 뿐입니다. 오류가 지속되거나 해결 방법이 언급되지 않으면 지원팀에 문의하세요.

다음 표에는 오류 코드와 해당 파일 이름이 나열되어 있습니다.

오류 코드	스크립트 이름
00	firstboot-network-config.pl, 배포 모드
01	firstboot-network-config.pl, 모드 업그레이드
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, 배포, HA
04	firstboot-deploy-otv-ng.pl, 배포, 비HA
05	firstboot-deploy-otv-ng.pl, 재부팅
06	firstboot-deploy-otv-ng.pl, 업그레이드, HA
07	firstboot-deploy-otv-ng.pl, 업그레이드, 비 HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

오류 코드의 마지막 세 자리는 스크립트 내의 특정 워크플로 오류를 나타냅니다.

배포 오류 코드	작업 흐름	해결
049	네트워크 및 검증을 위해 Perl 스크립트도 곧 할당됩니다.	-
050	SSH 키 생성에 실패했습니다	기본 가상 머신(VM)을 다시 시작합니다.
053	RKE2 설치에 실패했습니다	다음을 실행하고 기본 VM을 다시 시작하거나 다시 배포합니다. sudo rke2-killall.sh(모든 VM) sudo rke2-uninstall.sh(모든 VM).
054	kubeconfig 설정에 실패했습니다.	재배치

055	레지스트리 배포에 실패했습니다.	레지스트리 포드가 있는 경우 포드가 준비될 때까지 기다린 다음 기본 VM을 다시 시작하거나 그렇지 않은 경우 다시 배포합니다.
059	KubeVip 배포에 실패했습니다.	Kubernetes 제어 평면과 ONTAP 도구에 대한 가상 IP 주소를 확인하세요. 배포 중에 제공된 IP 주소는 동일한 VLAN에 속하며 사용 가능한 IP 주소입니다. 이전 사항이 모두 정확하다면 다시 시작하세요. 그렇지 않으면 재배치하세요.
060	운영자 배포에 실패했습니다	다시 시작
061	서비스 배포에 실패했습니다	ntv-system 네임스페이스에서 get pods, get rs, get svc 등과 같은 기본 Kubernetes 디버깅을 수행하여 자세한 내용과 오류 로그를 /var/log/ansible-perl-errors.log 및 /var/log/ansible-run.log에 기록하고 다시 배포합니다.
062	ONTAP 도구 서비스 배포에 실패했습니다.	자세한 내용은 /var/log/ansible-perl-errors.log의 오류 로그를 참조하고 다시 배포하세요.
065	Swagger 페이지 URL에 접근할 수 없습니다.	재배치
066	게이트웨이 인증서에 대한 배포 후 단계가 실패했습니다.	업그레이드를 복구/완료하려면 다음을 수행하세요. * 진단 셸을 활성화합니다. * 'sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy' 명령을 실행합니다. * /var/log/post-deploy-upgrade.log에서 로그를 확인하세요.
088	journald에 대한 로그 회전 구성에 실패했습니다.	VM이 호스팅되는 호스트와 호환되는 VM 네트워크 설정을 확인하세요. 다른 호스트로 마이그레이션하고 VM을 다시 시작해 보세요.
089	요약 로그 회전 구성 파일의 소유권을 변경하는 데 실패했습니다.	기본 VM을 다시 시작합니다.
096	동적 스토리지 프로비저너 설치	-
108	시드 스크립트가 실패했습니다	-

재부팅 오류 코드	작업 흐름	해결
067	rke2-server 대기 시간이 초과되었습니다.	-
101	Maint/Console 사용자 비밀번호를 재설정하지 못했습니다.	-

102	Maint/Console 사용자 비밀번호를 재설정하는 동안 비밀번호 파일을 삭제하지 못했습니다.	-
103	볼트에서 새로운 Maint/Console 사용자 비밀번호를 업데이트하지 못했습니다.	-
088	journald에 대한 로그 회전 구성에 실패했습니다.	VM이 호스팅되는 호스트와 호환되는 VM 네트워크 설정을 확인하세요. 다른 호스트로 마이그레이션하고 VM을 다시 시작해 보세요.
089	요약 로그 회전 구성 파일의 소유권을 변경하는 데 실패했습니다.	VM을 다시 시작합니다.

ONTAP tools for VMware vSphere 구성

vCenter Server 인스턴스 추가

vCenter Server 환경에서 가상 데이터스토어를 구성, 관리 및 보호하기 위해 ONTAP tools for VMware vSphere 에 vCenter Server 인스턴스를 추가합니다. 여러 vCenter Server 인스턴스를 추가하는 경우 ONTAP 도구와 각 vCenter Server 간의 보안 통신을 위해 사용자 지정 CA 인증서가 필요합니다.

이 작업에 관하여

ONTAP 도구를 vCenter와 통합하면 프로비저닝, 스냅샷, 데이터 보호와 같은 스토리지 작업을 vSphere 클라이언트에서 직접 수행할 수 있으므로 별도의 스토리지 관리 콘솔로 전환할 필요가 없습니다.

단계

1. 웹 브라우저를 열고 다음 URL로 이동하세요. `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. **vCenters** > *Add*를 선택하여 vCenter Server 인스턴스를 온보딩합니다. vCenter IP 주소 또는 호스트 이름, 사용자 이름, 비밀번호 및 포트 세부 정보를 제공하세요.

> ONTAP 도구에 vCenter 인스턴스를 추가하는 데 관리자 계정은 필요하지 않습니다. 관리자 계정 없이도 제한된 권한으로 사용자 정의 역할을 만들 수 있습니다. 참조하다"ONTAP tools for VMware vSphere 와 함께 vCenter Server RBAC 사용" 자세한 내용은.

ONTAP 도구에 vCenter Server 인스턴스를 추가하면 다음 작업이 자동으로 트리거됩니다.

- vCenter 클라이언트 플러그인은 원격 플러그인으로 등록됩니다.
- 플러그인과 API에 대한 사용자 정의 권한은 vCenter Server 인스턴스에 적용됩니다.
- 사용자를 관리하기 위해 사용자 정의 역할이 생성됩니다.
- 플러그인은 vSphere 사용자 인터페이스에 바로가기로 나타납니다.

vCenter Server 인스턴스에 VASA 공급자 등록

ONTAP tools for VMware vSphere 사용하여 vCenter Server 인스턴스에 VASA 공급자를 등록할 수 있습니다. VASA 공급자 설정 섹션에는 선택한 vCenter Server에 대한 VASA 공급자 등록 상태가 표시됩니다. 다중 vCenter 배포에서는 각 vCenter Server 인스턴스에 사용자 지정 CA 인증서가 있는지 확인하세요.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 플러그인 섹션에서 바로가기 > * NetApp ONTAP 도구*를 선택합니다.
3. 설정 > *VASA 공급자 설정*을 선택하세요. VASA 공급자 등록 상태가 등록되지 않음으로 표시됩니다.

4. VASA 공급자를 등록하려면 등록 버튼을 선택하세요.
5. VASA 공급자의 이름과 자격 증명을 입력하세요. 사용자 이름에는 문자, 숫자, 밑줄만 사용할 수 있습니다. 비밀번호 길이는 8자에서 256자 사이여야 합니다.
6. *등록*을 선택하세요.
7. 등록이 성공적으로 완료되고 페이지가 새로 고쳐지면 등록된 VASA 공급자의 상태, 이름, 버전이 표시됩니다. 등록 후 등록 취소 작업이 활성화됩니다.

다음은 무엇입니까**?**

vCenter 클라이언트에서 온보딩된 VASA 공급자가 VASA 공급자 아래에 나열되어 있는지 확인하세요.

단계

1. vCenter Server 인스턴스로 이동합니다.
2. 관리자 자격 증명으로 로그인하세요.
3. 저장소 공급자 > *구성*을 선택합니다. 등록된 VASA 공급자가 올바르게 나열되어 있는지 확인하세요.

NFS VAAI 플러그인을 설치하세요

NFS vStorage API for Array Integration(NFS VAAI) 플러그인은 VMware vSphere와 NFS 스토리지 어레이를 통합하는 소프트웨어 구성 요소입니다. ONTAP tools for VMware vSphere 사용하여 NFS VAAI 플러그인을 설치하면 NFS 스토리지 어레이의 고급 기능을 활용하여 ESXi 호스트에서 스토리지 어레이 자체로 특정 스토리지 관련 작업을 오프로드할 수 있습니다.

시작하기 전에

- 다운로드 "VMware VAAI용 NetApp NFS 플러그인" 설치 패키지.
- ESXi 호스트와 vSphere 7.0U3 최신 패치 이상 버전, ONTAP 9.14.1 이상 버전이 있는지 확인하세요.
- NFS 데이터 저장소를 마운트합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 플러그인 섹션에서 바로가기 > * NetApp ONTAP 도구*를 선택합니다.
3. 설정 > *NFS VAAI 도구*를 선택합니다.
4. VAAI 플러그인이 vCenter Server에 업로드되면 기존 버전 섹션에서 변경*을 선택합니다**. VAAI** 플러그인이 **vCenter Server**에 업로드되지 않은 경우 *업로드 버튼을 선택합니다.
5. 탐색하고 선택하세요 `.vib` 파일을 선택하고 *업로드*를 선택하여 ONTAP 도구에 파일을 업로드합니다.
6. *ESXI 호스트에 설치*를 선택하고, NFS VAAI 플러그인을 설치할 ESXi 호스트를 선택한 다음, *설치*를 선택합니다.

   플러그인 설치에 적합한 ESXi 호스트만 표시됩니다. vSphere Web Client의 최근 작업 섹션에서 설치 진행 상황을 모니터링할 수 있습니다.

7. 설치 후 ESXi 호스트를 수동으로 다시 시작합니다.

   VMware 관리자가 ESXi 호스트를 다시 시작하면 ONTAP tools for VMware vSphere NFS VAAI 플러그인을

자동으로 감지하고 활성화합니다.

다음은 무엇인가요?

NFS VAAI 플러그인을 설치하고 ESXi 호스트를 재부팅한 후 VAAI 복사 오프로드에 대한 올바른 NFS 내보내기 정책을 구성해야 합니다. NFS 환경에서 VAAI를 구성할 때 다음 요구 사항을 염두에 두고 내보내기 정책 규칙을 구성하세요.

- 해당 ONTAP 볼륨은 NFSv4 호출을 허용해야 합니다.
- 루트 사용자는 루트로 유지되어야 하며 모든 접합 부모 볼륨에서 NFSv4가 허용되어야 합니다.
- VAAI 지원 옵션은 해당 NFS 서버에서 설정해야 합니다.

절차에 대한 자세한 내용은 다음을 참조하세요. "VAAI 복사 오프로드를 위한 올바른 NFS 내보내기 정책 구성" KB 문서.

관련 정보

"NFS를 통한 VMware vStorage 지원"

"NFSv4.0 활성화 또는 비활성화"

"NFSv4.2에 대한 ONTAP 지원"

ESXi 호스트 설정 구성

ESXi 서버의 다중 경로 및 시간 초과 설정을 구성하면 기본 경로에 장애가 발생할 경우 백업 스토리지 경로로 원활하게 전환할 수 있어 높은 가용성과 데이터 무결성이 보장됩니다.

ESXi 서버 다중 경로 및 시간 초과 설정 구성

ONTAP tools for VMware vSphere NetApp 스토리지 시스템에서 가장 잘 작동하는 ESXi 호스트 다중 경로 설정과 HBA 시간 초과 설정을 확인하고 설정합니다.

이 작업에 관하여

구성 및 시스템 부하에 따라 이 프로세스는 오랜 시간이 걸릴 수 있습니다. 작업 진행 상황은 최근 작업 패널에 표시됩니다.

단계

1. VMware vSphere Web 클라이언트 홈페이지에서 *호스트 및 클러스터*를 선택합니다.
2. 호스트를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *호스트 데이터 업데이트*를 선택합니다.
3. VMware vSphere Web 클라이언트의 바로가기 페이지에서 플러그인 섹션 아래에 있는 * NetApp ONTAP 도구*를 선택합니다.
4. ONTAP tools for VMware vSphere 의 개요(대시보드)에서 **ESXi** 호스트 규정 준수 카드로 이동합니다.
5. 권장 설정 적용 링크를 선택합니다.
6. 권장 호스트 설정 적용 창에서 NetApp 권장 설정을 준수하도록 업데이트할 호스트를 선택하고 *다음*을 선택합니다.

ESXi 호스트를 확장하여 현재 값을 확인할 수 있습니다.

7. 설정 페이지에서 필요에 따라 권장되는 값을 선택하세요.
8. 요약 창에서 값을 확인하고 *마침*을 선택합니다. 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

ESXi 호스트 값 설정

ONTAP tools for VMware vSphere 사용하면 ESXi 호스트에서 시간 초과 및 기타 값을 설정하여 최상의 성능과 성공적인 장애 조치를 보장할 수 있습니다. ONTAP tools for VMware vSphere 설정하는 값은 NetApp 내부 테스트를 기반으로 합니다.

ESXi 호스트에서 다음 값을 설정할 수 있습니다.

HBA/CNA 어댑터 설정

다음 매개변수를 기본값으로 설정합니다.

- 디스크.QFullSampleSize
- 디스크.QFullThreshold
- Emulex FC HBA 타임아웃
- QLogic FC HBA 시간 초과

MPIO 설정

MPIO 설정은 NetApp 스토리지 시스템의 기본 경로를 정의합니다. 이들은 사용 가능한 경로 중 어떤 것이 최적화된지(인터커넥트 케이블을 통과하는 최적화되지 않은 경로와 대조적으로)를 결정하고 해당 경로 중 하나를 기본 경로로 설정합니다.

고성능 환경이나 단일 LUN 데이터 저장소로 성능을 테스트하는 경우 라운드 로빈(VMW_PSP_RR) 경로 선택 정책(PSP)의 부하 분산 설정을 기본 IOPS 설정인 1000에서 값 1로 변경하는 것을 고려하세요.

> MPIO 설정은 NVMe, NVMe/FC 및 NVMe/TCP 프로토콜에는 적용되지 않습니다.

NFS 설정

매개변수	이 값을 다음과 같이 설정합니다…
Net.TcpipHeapSize	32
Net.TcpipHeapMax	1024MB
NFS.최대 볼륨	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128 이상
NFS.HeartbeatMaxFailures	10
NFS.하트비트 빈도	12
NFS.하트비트타임아웃	5

ONTAP 사용자 역할 및 권한 구성

ONTAP tools for VMware vSphere 및 ONTAP System Manager용 ONTAP 도구와 함께 제공되는 JSON 파일을 사용하여 스토리지 백엔드를 관리하기 위한 새로운 사용자 역할과 권한을 구성할 수 있습니다.

시작하기 전에

- _\https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip_을 사용하여 ONTAP tools for VMware vSphere 에서 ONTAP 권한 파일을 다운로드했어야 합니다.
- ONTAP 도구에서 ONTAP Privileges 파일을 다운로드했어야 합니다. `https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip`.

> 클러스터 또는 스토리지 가상 머신(SVM) 수준에서 직접 사용자를 생성할 수 있습니다. user_roles.json 파일을 사용하지 않고도 사용자를 생성할 수 있으며, 그렇게 하려면 SVM 수준에서 최소한의 권한이 필요합니다.

- 저장소 백엔드에 관리자 권한으로 로그인했어야 합니다.

단계

1. 다운로드한 *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* 파일을 추출합니다.
2. 클러스터의 클러스터 관리 IP 주소를 사용하여 ONTAP System Manager에 액세스합니다.
3. 관리자 권한으로 클러스터에 로그인합니다. 사용자를 구성하려면 다음 단계를 수행하세요.
   a. 클러스터 ONTAP 도구 사용자를 구성하려면 클러스터 > 설정 > 사용자 및 역할 창을 선택합니다.
   b. SVM ONTAP 도구 사용자를 구성하려면 저장소 **SVM** > 설정 > 사용자 및 역할 창을 선택합니다.
   c. 사용자에서 *추가*를 선택합니다.
   d. 사용자 추가 대화 상자에서 *가상화 제품*을 선택합니다.
   e. *찾아보기*하여 ONTAP Privileges JSON 파일을 선택하고 업로드합니다.

      제품 필드는 자동으로 채워집니다.

   f. 드롭다운에서 제품 기능을 *VSC, VASA 공급자 및 SRA*로 선택합니다.

      역할 필드는 선택한 제품 기능에 따라 자동으로 채워집니다.

   g. 필요한 사용자 이름과 비밀번호를 입력하세요.
   h. 사용자에게 필요한 권한(검색, 저장소 생성, 저장소 수정, 저장소 삭제, NAS/SAN 역할)을 선택한 다음 *추가*를 선택합니다.

새로운 역할과 사용자가 추가되고, 구성한 역할에 따라 자세한 권한을 볼 수 있습니다.

SVM 집계 매핑 요구 사항

데이터 저장소 프로비저닝에 SVM 사용자 자격 증명을 사용하기 위해 ONTAP tools for VMware vSphere 데이터 저장소 POST API에 지정된 집계에 볼륨을 내부적으로 생성합니다. ONTAP SVM 사용자 자격 증명을 사용하여 SVM의 매핑되지 않은 집계에 볼륨을 생성하는 것을 허용하지 않습니다. 이 문제를 해결하려면 여기에 설명된 대로

ONTAP REST API 또는 CLI를 사용하여 SVM을 집계와 매핑해야 합니다.

REST API:

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

ONTAP CLI:

```
sti115_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver        Aggregate      State         Size Type    SnapLock
Type-------------- -------------- ------- ---------- -------
--------------svm_test       sti115_vsim_ucs630f_aggr1
online     10.11GB vmdisk  non-snaplock
```

ONTAP 사용자 및 역할을 수동으로 생성

JSON 파일을 사용하지 않고 수동으로 사용자와 역할을 생성하려면 이 섹션의 지침을 따르세요.

1. 클러스터의 클러스터 관리 IP 주소를 사용하여 ONTAP System Manager에 액세스합니다.
2. 관리자 권한으로 클러스터에 로그인합니다.
   a. 클러스터 ONTAP 도구 역할을 구성하려면 클러스터 > 설정 > 사용자 및 역할 창을 선택합니다.
   b. 클러스터 SVM ONTAP 도구 역할을 구성하려면 저장소 **SVM** > 설정 > 사용자 및 역할 창을 선택하세요.
3. 역할 생성:
   a. 역할 표에서 *추가*를 선택합니다.
   b. 역할 이름*과 *역할 속성 세부 정보를 입력하세요.

      드롭다운에서 *REST API 경로*와 해당 액세스를 추가합니다.

   c. 필요한 API를 모두 추가하고 변경 사항을 저장합니다.
4. 사용자 생성:
   a. 사용자 테이블에서 *추가*를 선택합니다.
   b. 사용자 추가 대화 상자에서 *시스템 관리자*를 선택합니다.
   c. *사용자 이름*을 입력하세요.
   d. 위의 역할 만들기 단계에서 만든 옵션 중에서 *역할*을 선택합니다.
   e. 접근 권한을 부여할 응용프로그램과 인증 방법을 입력하세요. 필수 애플리케이션은 ONTAPI와 HTTP이고, 인증 유형은 *비밀번호*입니다.
   f. *사용자 비밀번호*를 설정하고 사용자를 *저장*합니다.

관리자가 아닌 글로벌 범위 클러스터 사용자에게 필요한 최소 권한 목록

이 섹션에는 users JSON 파일을 사용하지 않고 생성된 비관리자 글로벌 범위 클러스터 사용자에 필요한 최소 권한이 나와 있습니다. 로컬 범위에서 클러스터를 추가하는 경우, ONTAP tools for VMware vSphere ONTAP 프로비저닝에 읽기 권한 이상의 권한을 요구하므로 JSON 파일을 사용하여 사용자를 생성하는 것이 좋습니다.

API 사용:

API	접근 수준	에 사용됨
/api/클러스터	읽기 전용	클러스터 구성 검색
/api/cluster/licensing/licenses	읽기 전용	프로토콜별 라이센스에 대한 라이센스 확인
/api/클러스터/노드	읽기 전용	플랫폼 유형 검색
/api/보안/계정	읽기 전용	권한 검색
/api/보안/역할	읽기 전용	권한 검색
/api/storage/aggregates	읽기 전용	데이터 저장소/볼륨 프로비저닝 중 집계 공간 확인
/api/storage/cluster	읽기 전용	클러스터 수준 공간 및 효율성 데이터를 얻으려면
/api/storage/disks	읽기 전용	집계에 연결된 디스크를 가져오려면
/api/storage/qos/정책	읽기/생성/수정	QoS 및 VM 정책 관리
/api/svm/svms	읽기 전용	클러스터가 로컬로 추가된 경우 SVM 구성을 가져옵니다.
/api/네트워크/ip/인터페이스	읽기 전용	스토리지 백엔드 추가 - 관리 LIF 범위가 클러스터/SVM인지 식별합니다.
/api/storage/availability-zones	읽기 전용	SAZ 디스커버리. ONTAP 9.16.1 릴리스 이상 및 ASA r2 시스템에 적용됩니다.

VMware vSphere ONTAP API 기반 클러스터 범위 사용자를 **ONTAP tools for VMware vSphere** 생성

> 데이터 저장소에 오류가 발생한 경우 PATCH 작업과 자동 롤백을 수행하려면 검색, 생성, 수정 및 삭제 Privileges 필요합니다. 이러한 모든 권한이 부족하면 작업 흐름이 중단되고 정리에 문제가 발생합니다.

검색, 스토리지 생성, 스토리지 수정, 스토리지 삭제 권한이 있는 ONTAP tools for VMware vSphere ONTAP API 기반 사용자를 위한 ONTAP 도구를 생성하면 검색을 시작하고 ONTAP 도구 워크플로를 관리할 수 있습니다.

위에 언급된 모든 권한을 가진 클러스터 범위 사용자를 생성하려면 다음 명령을 실행하세요.

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all

security login rest-role create -role <role-name> -api
```

```
/api/private/cli/snapmirror -access all

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
-access all

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create
```

```
security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/licensing/licenses -access readonly

security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly
```

```
security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly
```

또한 ONTAP 버전 9.16.0 이상의 경우 다음 명령을 실행합니다.

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all
```

ONTAP 버전 9.16.1 이상의 ASA r2 시스템의 경우 다음 명령을 실행합니다.

```
security login rest-role create -role <role-name> -api
/api/storage/availability-zones -access readonly
```

VMware vSphere ONTAP API 기반 SVM 범위 사용자를 ONTAP tools for VMware vSphere 생성

모든 권한을 가진 SVM 범위 사용자를 생성하려면 다음 명령을 실행하세요.

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/luns
-access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
name>
```

```
security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>
```

또한 ONTAP 버전 9.16.0 이상의 경우 다음 명령을 실행합니다.

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>
```

위에서 생성한 API 기반 역할을 사용하여 새로운 API 기반 사용자를 생성하려면 다음 명령을 실행하세요.

```
security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>
```

예:

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_sti160-cluster_
```

계정 잠금을 해제하고 관리 인터페이스에 대한 액세스를 활성화하려면 다음 명령을 실행하세요.

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

예:

```
security login unlock -username testvpsraall -vserver C1_sti160-cluster
```

ONTAP tools for VMware vSphere 업그레이드

JSON 파일을 사용하여 클러스터 범위 사용자를 생성한 ONTAP tools for VMware vSphere 의 경우, 사용자 관리자 권한으로 다음 ONTAP CLI 명령을 사용하여 10.3 릴리스로 업그레이드합니다.

제품 기능에 대해서는 다음을 참조하세요.

- VSC
- VSC 및 VASA 공급자
- VSC와 SRA
- VSC, VASA 공급자 및 SRA.

클러스터 권한:

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 네임스페이스 표시*" -access all*

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 표시*" -access all*

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 호스트 표시*" -access all*

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 맵 표시*" -access all*

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme show-interface" -access read*

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 호스트 추가*" -access all*

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 맵 추가*" -access all*

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 네임스페이스 삭제*" -access all*

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 삭제*" -access all*

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 호스트 제거*" -access all*

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 맵 제거*" -access all*

json 파일을 사용하여 생성된 SVM 범위 사용자가 있는 ONTAP tools for VMware vSphere 의 경우, 관리자 권한으로 ONTAP CLI 명령을 사용하여 10.3 릴리스로 업그레이드합니다.

SVM 권한:

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 네임스페이스 표시*" -access all -vserver* <*vserver* 이름>

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 표시*" -access all -vserver* <*vserver* 이름>

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 호스트 표시*" -access all -vserver* <*vserver* 이름>

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 맵 표시*" -access all -vserver* <*vserver* 이름>

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme show-interface" -access read -vserver* <*vserver* 이름>

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 호스트 추가*" -access all -vserver* <*vserver* 이름>

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 맵 추가*" -access all -vserver* <*vserver* 이름>

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 네임스페이스 삭제*" -access all -vserver* <*vserver* 이름>

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 삭제*" -access all -vserver* <*vserver* 이름>

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 호스트 제거*" -access all -vserver* <*vserver* 이름>

보안 로그인 역할 생성 *-role* <기존 역할 이름> *-cmddirname "vserver nvme* 하위 시스템 맵 제거*" -access all -vserver* <*vserver* 이름>

기존 역할에 *vserver nvme namespace show* 및 *vserver nvme subsystem show* 명령을 추가하면 다음 명령이 추가됩니다.

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

ONTAP tools for VMware vSphere 업그레이드

ONTAP 9.16.1부터 ONTAP tools for VMware vSphere 10.4 사용자용으로 업그레이드하세요.

JSON 파일과 ONTAP 버전 9.16.1 이상을 사용하여 생성된 클러스터 범위 사용자를 가진 ONTAP tools for VMware vSphere 의 경우, 관리자 권한으로 ONTAP CLI 명령을 사용하여 10.4 릴리스로 업그레이드합니다.

제품 기능에 대해서는 다음을 참조하세요.

- VSC
- VSC 및 VASA 공급자
- VSC와 SRA
- VSC, VASA 공급자 및 SRA.

클러스터 권한:

```
security login role create -role <existing-role-name> -cmddirname "storage
availability-zone show" -access all
```

스토리지 백엔드 추가

스토리지 백엔드를 추가하면 ONTAP 클러스터를 온보딩할 수 있습니다.

이 작업에 관하여

vCenter가 연관된 SVM이 있는 테넌트 역할을 하는 다중 테넌시 설정의 경우 ONTAP 도구 관리자를 사용하여 클러스터를 추가합니다. 스토리지 백엔드를 vCenter Server와 연결하여 온보딩된 vCenter Server 인스턴스에 전역적으로 매핑합니다. vCenter 테넌트는 원하는 스토리지 가상 머신(SVM)을 온보딩해야 합니다. 이를 통해 SVM 사용자는 vVols 데이터 저장소를 프로비저닝할 수 있습니다. SVM을 사용하여 vCenter에 스토리지를 추가할 수 있습니다.

ONTAP 도구 사용자 인터페이스를 사용하여 클러스터 또는 SVM 자격 증명으로 로컬 스토리지 백엔드를 추가합니다. 이러한 스토리지 백엔드는 단일 vCenter로 제한됩니다. 로컬에서 클러스터 자격 증명을 사용하는 경우 연관된 SVM은 자동으로 vCenter에 매핑되어 vVols 또는 VMFS를 관리합니다. SRA를 포함한 VMFS 관리의 경우 ONTAP 도구는 글로벌 클러스터가 필요 없이 SVM 자격 증명을 지원합니다.

ONTAP 도구 관리자 사용

> 멀티 테넌트 설정에서는 스토리지 백엔드 클러스터를 전역적으로 추가하고 SVM을 로컬로 추가하여 SVM 사용자 자격 증명을 사용할 수 있습니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 사이드바에서 *스토리지 백엔드*를 선택합니다.
4. 스토리지 백엔드를 추가하고 서버 IP 주소 또는 FQDN, 사용자 이름 및 비밀번호 세부 정보를 제공합니다.

   > IPv4 및 IPv6 주소 관리 LIF가 지원됩니다.

vSphere 클라이언트 사용자 인터페이스 사용

> vSphere 클라이언트 사용자 인터페이스를 통해 스토리지 백엔드를 구성하는 경우 vVols 데이터스토어는 SVM 사용자를 직접 추가하는 것을 지원하지 않는다는 점에 유의하는 것이 중요합니다.

1. vSphere 클라이언트에 로그인합니다.
2. 바로가기 페이지에서 플러그인 섹션 아래에 있는 * NetApp ONTAP 도구*를 선택합니다.
3. 사이드바에서 *스토리지 백엔드*를 선택합니다.
4. 스토리지 백엔드를 추가하고 서버 IP 주소, 사용자 이름, 비밀번호, 포트 세부 정보를 제공합니다.

   > SVM 사용자를 직접 추가하려면 클러스터 기반 자격 증명과 IPv4 및 IPv6 주소 관리 LIF를 추가하거나 SVM 관리 LIF와 함께 SVM 기반 자격 증명을 제공할 수 있습니다.

다음은 무엇인가요**?**

목록이 새로 고쳐지고, 목록에서 새로 추가된 스토리지 백엔드를 볼 수 있습니다.

vCenter Server 인스턴스와 스토리지 백엔드 연결

스토리지 백엔드를 vCenter Server에 연결하여 스토리지 백엔드와 온보딩된 vCenter Server 인스턴스 간에 전역적으로 매핑을 생성합니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 사이드바에서 vCenter를 선택합니다.
4. 스토리지 백엔드와 연결할 vCenter Server 인스턴스에 대한 세로 줄임표를 선택합니다.

5. 드롭다운에서 스토리지 백엔드를 선택하여 vCenter Server 인스턴스를 필요한 스토리지 백엔드와 연결합니다.

네트워크 액세스 구성

네트워크 액세스를 구성하지 않은 경우 ESXi 호스트에서 검색된 모든 IP 주소가 기본적으로 내보내기 정책에 추가됩니다. 특정 IP 주소 몇 개만 내보내기 정책에 추가하고 나머지는 제외하도록 구성할 수 있습니다. 그러나 제외된 ESXi 호스트에서 마운트 작업을 수행하면 작업이 실패합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 플러그인 섹션 아래의 바로가기 페이지에서 * NetApp ONTAP 도구*를 선택합니다.
3. ONTAP 도구의 왼쪽 창에서 설정 > 네트워크 액세스 관리 > *편집*으로 이동합니다.

   여러 개의 IP 주소를 추가하려면 쉼표, 범위, CIDR(Classless Inter-Domain Routing) 또는 이 세 가지를 조합하여 목록을 구분하세요.

4. *저장*을 선택하세요.

데이터 저장소 만들기

호스트 클러스터 수준에서 데이터 저장소를 생성하면 대상의 모든 호스트에 데이터 저장소가 생성되어 마운트되고, 현재 사용자에게 실행 권한이 있는 경우에만 작업이 활성화됩니다.

vCenter Server 및 **ONTAP** 도구로 관리되는 데이터스토어와 기본 데이터스토어 간 상호 운용성

ONTAP tools for VMware vSphere 데이터스토어에 대한 중첩된 igroup을 생성하며, 부모 igroup은 데이터스토어에 특정하고 자식 igroup은 호스트에 매핑됩니다. ONTAP 시스템 관리자에서 플랫 igroup을 만들고 ONTAP 도구를 사용하지 않고도 이를 사용하여 VMFS 데이터 저장소를 만들 수 있습니다. 참조하다 "SAN 이니시에이터 및 igroup 관리" 자세한 내용은.

스토리지가 ONTAP 도구에 온보딩되고 데이터 저장소 검색이 실행되면 플랫 igroup과 VMFS 데이터 저장소가 ONTAP 도구에서 관리되고 중첩된 igroup으로 변환됩니다. 이전의 플랫 igroup을 사용하여 새로운 데이터 저장소를 생성할 수 없습니다. 중첩된 igroup을 재사용하려면 ONTAP 도구 사용자 인터페이스나 REST API를 사용해야 합니다.

vVols 데이터 저장소 만들기

ONTAP tools for VMware vSphere 부터 ASA r2 시스템에 thin.vVol이라는 공간 효율성을 갖춘 vVols 데이터 저장소를 생성할 수 있습니다. VASA 공급자는 vVol 데이터 저장소를 생성하는 동안 컨테이너와 원하는 프로토콜 엔드포인트를 생성합니다. 이 컨테이너에는 백업 볼륨이 없습니다.

시작하기 전에

- 루트 집계가 SVM에 매핑되지 않았는지 확인하세요.
- 선택한 vCenter에 VASA 공급자가 등록되어 있는지 확인하세요.
- ASA r2 스토리지 시스템에서는 SVM이 SVM 사용자에 대한 집계에 매핑되어야 합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *데이터 저장소 만들기*를 선택합니다.
3. vVols *데이터 저장소 유형*을 선택합니다.
4. 데이터 저장소 이름*과 *프로토콜 정보를 입력하세요.

   ASA r2 시스템은 vVols 대한 iSCSI 및 FC 프로토콜을 지원합니다.

5. 데이터스토어를 생성할 스토리지 VM을 선택하세요.
6. 고급 옵션:
   - *사용자 지정 내보내기 정책*을 선택하는 경우 모든 개체에 대해 vCenter에서 검색을 실행해야 합니다. 이 옵션은 사용하지 않는 것이 좋습니다.
   - iSCSI 및 FC 프로토콜에 대해 사용자 지정 이니시에이터 그룹 이름을 선택할 수 있습니다.

     ASA r2 스토리지 시스템 유형 SVM에서는 데이터 저장소가 논리적 컨테이너일 뿐이므로 스토리지 단위(LUN/네임스페이스)가 생성되지 않습니다.

7. 저장소 속성 창에서 새 볼륨을 만들거나 기존 볼륨을 사용할 수 있습니다. 하지만 이 두 유형의 볼륨을 결합하여 vVols 데이터 저장소를 만들 수는 없습니다.

   새 볼륨을 생성할 때 데이터 저장소에서 QoS를 활성화할 수 있습니다. 기본적으로 LUN 생성 요청마다 볼륨이 하나씩 생성됩니다. 이 단계는 ASA r2 스토리지 시스템을 사용하는 vVols 데이터 저장소에는 적용되지 않습니다.

8. 요약 창에서 선택 사항을 검토하고 *마침*을 선택하세요.

NFS 데이터 저장소 만들기

VMware 네트워크 파일 시스템(NFS) 데이터 저장소는 NFS 프로토콜을 사용하여 네트워크를 통해 ESXi 호스트를 공유 스토리지 장치에 연결합니다. NFS 데이터 저장소는 일반적으로 VMware vSphere 환경에서 사용되며 단순성, 유연성 등 여러 가지 이점을 제공합니다.

단계

1. vSphere 클라이언트에 로그인합니다.

2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *데이터 저장소 만들기*를 선택합니다.
3. 데이터 저장소 유형 필드에서 NFS를 선택합니다.
4. 이름 및 프로토콜 창에 데이터 저장소 이름, 크기 및 프로토콜 정보를 입력합니다. 고급 옵션에서 *데이터 저장소 클러스터*와 *Kerberos 인증*을 선택합니다.

   Kerberos 인증은 NFS 4.1 프로토콜을 선택한 경우에만 사용할 수 있습니다.

5. 저장소 창에서 *플랫폼*과 *저장소 VM*을 선택합니다.
6. 고급 옵션에서 *사용자 지정 내보내기 정책*을 선택하면 모든 개체에 대해 vCenter에서 검색을 실행합니다. 이 옵션은 사용하지 않는 것이 좋습니다.

   SVM의 기본/루트 볼륨 정책을 사용하여 NFS 데이터 저장소를 만들 수 없습니다.

   - 고급 옵션에서 비대칭 토글 버튼은 플랫폼 드롭다운에서 성능이나 용량이 선택된 경우에만 표시됩니다.
   - 플랫폼 드롭다운에서 모든 옵션을 선택하면 플랫폼이나 비대칭 플래그에 관계없이 vCenter에 속한 SVM을 볼 수 있습니다.
7. 저장소 속성 창에서 볼륨 생성을 위한 집계를 선택합니다. 고급 옵션에서 필요에 따라 공간 예약 및 *QoS 활성화*를 선택합니다.
8. 요약 창에서 선택 내용을 검토하고 *마침*을 선택합니다.

NFS 데이터 저장소가 생성되어 모든 호스트에 마운트됩니다.

VMFS 데이터 저장소 만들기

VMFS(가상 머신 파일 시스템)는 VMware vSphere 환경에서 가상 머신 파일을 저장하는 클러스터형 파일 시스템입니다. VMFS를 사용하면 여러 ESXi 호스트가 동일한 가상 머신 파일에 동시에 액세스할 수 있으므로 vMotion 및 고가용성과 같은 기능을 사용할 수 있습니다.

보호된 클러스터에서:

- VMFS 데이터 저장소만 생성할 수 있습니다. 보호된 클러스터에 VMFS 데이터 저장소를 추가하면 데이터 저장소가 자동으로 보호됩니다.
- 하나 이상의 보호된 호스트 클러스터가 있는 데이터 센터에는 데이터 저장소를 만들 수 없습니다.
- 부모 호스트 클러스터가 "자동화된 장애 조치 이중 정책" 유형(균일/비균일 구성) 관계로 보호되는 경우 ESXi 호스트에 데이터 저장소를 생성할 수 없습니다.
- 비동기 관계로 보호되는 ESXi 호스트에만 VMFS 데이터 저장소를 만들 수 있습니다. "자동화된 장애 조치 이중화" 정책으로 보호되는 호스트 클러스터의 일부인 ESXi 호스트에 데이터스토어를 만들고 마운트할 수 없습니다.

시작하기 전에

- ONTAP 스토리지 측에서 각 프로토콜에 대한 서비스와 LIF를 활성화합니다.
- ASA r2 스토리지 시스템의 SVM 사용자를 집계하기 위해 SVM을 매핑합니다.
- NVMe/TCP 프로토콜을 사용하는 경우 ESXi 호스트를 구성합니다.
  a. 검토하다 "VMware 호환성 가이드"

> VMware vSphere 7.0 U3 이상 버전은 NVMe/TCP 프로토콜을 지원합니다. 하지만 VMware vSphere 8.0 이상 버전을 권장합니다.

b. 네트워크 인터페이스 카드(NIC) 공급업체가 NVMe/TCP 프로토콜을 사용하는 ESXi NIC를 지원하는지 확인합니다.

c. NIC 공급업체 사양에 따라 NVMe/TCP에 대한 ESXi NIC를 구성합니다.

d. VMware vSphere 7 릴리스를 사용하는 경우 VMware 사이트의 지침을 따르세요. "NVMe over TCP 어댑터에 대한 VMkernel 바인딩 구성" NVMe/TCP 포트 바인딩을 구성합니다. VMware vSphere 8 릴리스를 사용하는 경우 다음을 따르세요. "ESXi에서 TCP를 통한 NVMe 구성" NVMe/TCP 포트 바인딩을 구성합니다.

e. VMware vSphere 7 릴리스의 경우 페이지의 지침을 따르세요. "NVMe over RDMA 또는 NVMe over TCP 소프트웨어 어댑터 활성화" NVMe/TCP 소프트웨어 어댑터를 구성합니다. VMware vSphere 8 릴리스의 경우 다음을 따르세요. "RDMA 또는 TCP 어댑터를 통한 NVMe 소프트웨어 추가" NVMe/TCP 소프트웨어 어댑터를 구성합니다.

f. 달리다"스토리지 시스템 및 호스트 검색" ESXi 호스트에 대한 작업입니다. 자세한 내용은 다음을 참조하세요. "VMFS 데이터 저장소에 대해 vSphere 8.0 업데이트 1 및 ONTAP 9.13.1을 사용하여 NVMe/TCP를 구성하는 방법" .

- NVME/FC 프로토콜을 사용하는 경우 다음 단계를 수행하여 ESXi 호스트를 구성하세요.

  a. 아직 활성화되지 않았다면 ESXi 호스트에서 NVMe over Fabrics(NVMe-oF)를 활성화하세요.

  b. SCSI 구역화를 완료합니다.

  c. ESXi 호스트와 ONTAP 시스템이 물리적 및 논리적 계층에서 연결되어 있는지 확인하세요.

FC 프로토콜에 대한 ONTAP SVM을 구성하려면 다음을 참조하세요. "FC에 대한 SVM 구성" .

VMware vSphere 8.0에서 NVMe/FC 프로토콜을 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요. "ONTAP 사용한 ESXi 8.x에 대한 NVMe-oF 호스트 구성" .

VMware vSphere 7.0에서 NVMe/FC를 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요. "ONTAP NVMe/FC 호스트 구성 가이드" 그리고 "TR-4684" .

단계

1. vSphere 클라이언트에 로그인합니다.
2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *데이터 저장소 만들기*를 선택합니다.
3. VMFS 데이터 저장소 유형을 선택하세요.
4. 이름 및 프로토콜 창에 데이터 저장소 이름, 크기 및 프로토콜 정보를 입력합니다. 기존 VMFS 데이터 저장소 클러스터에 새 데이터 저장소를 추가하려면 고급 옵션에서 데이터 저장소 클러스터 선택기를 선택합니다.
5. 저장소 창에서 저장소 VM을 선택합니다. 필요에 따라 고급 옵션 섹션에 *사용자 지정 개시자 그룹 이름*을 제공합니다. 데이터 저장소에 대해 기존 igroup을 선택하거나 사용자 정의 이름으로 새 igroup을 만들 수 있습니다.

   NVMe/FC 또는 NVMe/TCP 프로토콜을 선택하면 새로운 네임스페이스 하위 시스템이 생성되어 네임스페이스 매핑에 사용됩니다. 네임스페이스 하위 시스템은 데이터 저장소 이름을 포함하는 자동 생성된 이름을 사용하여 생성됩니다. 저장소 창의 고급 옵션에 있는 사용자 지정 네임스페이스 하위 시스템 이름 필드에서 네임스페이스 하위 시스템의 이름을 바꿀 수 있습니다.

6. 저장소 속성 창에서:

   a. 드롭다운 옵션에서 *집계*를 선택합니다.

   ASA r2 스토리지 시스템의 경우, ASA r2 스토리지가 분산 스토리지이므로 집계 옵션이 표시되지 않습니다. ASA r2 스토리지 시스템 유형으로 SVM을 선택하면 스토리지 속성 페이지에 QoS 활성화 옵션이 표시됩니다.

   b. 선택한 프로토콜에 따라 씬 유형의 공간 예비를 갖춘 저장 장치(LUN/네임스페이스)가 생성됩니다.

   ONTAP 9.16.1부터 ASA r2 스토리지 시스템은 클러스터당 최대 12개의 노드를 지원합니다.

   c. 이기종 클러스터인 12개 노드 SVM이 있는 ASA r2 스토리지 시스템에 대해 *성능 서비스 수준*을 선택합니다. 선택한 SVM이 동종 클러스터이거나 SVM 사용자를 사용하는 경우 이 옵션을 사용할 수 없습니다.

   '모든'은 기본 성능 서비스 수준(PSL) 값입니다. 이 설정은 ONTAP 균형 배치 알고리즘을 사용하여 저장 장치를 생성합니다. 하지만 필요에 따라 성능이나 익스트림 옵션을 선택할 수 있습니다.

   d. 필요에 따라 기존 볼륨 사용, **QoS** 활성화 옵션을 선택하고 세부 정보를 제공합니다.

   ASA r2 스토리지 유형에서는 볼륨 생성 또는 선택이 스토리지 유닛 생성(LUN/네임스페이스)에 적용되지 않습니다. 따라서 이러한 옵션은 표시되지 않습니다.

   기존 볼륨을 사용하여 NVMe/FC 또는 NVMe/TCP 프로토콜을 사용하는 VMFS 데이터 저장소를 만들 수 없습니다. 새 볼륨을 만들어야 합니다.

7. 요약 창에서 데이터 저장소 세부 정보를 검토하고 *마침*을 선택합니다.

   보호된 클러스터에 데이터 저장소를 생성하면 "데이터 저장소가 보호된 클러스터에 마운트되고 있습니다."라는 읽기 전용 메시지가 표시됩니다.

결과

VMFS 데이터 저장소가 생성되어 모든 호스트에 마운트됩니다.

데이터 저장소 및 가상 머신 보호

호스트 클러스터 보호를 사용하여 보호

ONTAP tools for VMware vSphere 호스트 클러스터의 보호를 관리합니다. 선택된 SVM에 속하고 클러스터의 하나 이상의 호스트에 마운트된 모든 데이터 저장소는 호스트 클러스터에서 보호됩니다.

시작하기 전에

다음 전제 조건이 충족되는지 확인하세요.

- 호스트 클러스터에는 하나의 SVM에서만 데이터 저장소가 있습니다.
- 호스트 클러스터에 마운트된 데이터스토어는 클러스터 외부의 호스트에 마운트되어서는 안 됩니다.
- 호스트 클러스터에 마운트된 모든 데이터스토어는 iSCSI/FC 프로토콜을 사용하는 VMFS 데이터스토어여야 합니다. NVMe/FC 및 NVMe/TCP 프로토콜을 사용하는 vVols, NFS 또는 VMFS 데이터스토어는 지원되지 않습니다.
- 호스트 클러스터에 마운트된 FlexVol/LUN 형성 데이터 저장소는 기존 일관성 그룹(CG)의 일부가 되어서는 안 됩니다.
- 호스트 클러스터에 마운트된 FlexVol/LUN 형성 데이터 저장소는 기존 SnapMirror 관계에 포함되어서는 안 됩니다.
- 호스트 클러스터에는 최소한 하나의 데이터 저장소가 있어야 합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *클러스터 보호*를 선택합니다.
3. 클러스터 보호 창에서 데이터 저장소 유형과 소스 저장소 가상 머신(VM) 세부 정보가 자동으로 채워집니다. 보호된 데이터 저장소를 보려면 데이터 저장소 링크를 선택하세요.
4. *일관성 그룹 이름*을 입력하세요.
5. *관계 추가*를 선택하세요.
6. * SnapMirror 관계 추가* 창에서 대상 스토리지 **VM***과 *정책 유형을 선택합니다.

   정책 유형은 비동기 또는 AutomatedFailOverDuplex가 될 수 있습니다.

   SnapMirror 관계를 AutomatedFailOverDuplex 유형 정책으로 추가하는 경우 ONTAP tools for VMware vSphere 배포된 동일한 vCenter에 대상 스토리지 VM을 스토리지 백엔드로 추가해야 합니다.

   AutomatedFailOverDuplex 정책 유형에는 균일한 호스트 구성과 비균일한 호스트 구성이 있습니다. 균일한 호스트 구성 토글 버튼을 선택하면 호스트 이니시에이터 그룹 구성이 대상 사이트에 암묵적으로 복제됩니다. 자세한 내용은 다음을 참조하세요."주요 개념 및 용어" .

7. 균일하지 않은 호스트 구성을 선택하는 경우 해당 클러스터 내의 각 호스트에 대한 호스트 액세스(소스/대상)를 선택합니다.
8. *추가*를 선택하세요.
9. 클러스터 보호 창에서 생성 작업 중에는 보호된 클러스터를 편집할 수 없습니다. 보호 기능을 삭제하고 다시 추가할

수 있습니다. 호스트 클러스터 보호 수정 작업 중에 편집 옵션을 사용할 수 있습니다. 줄임표 메뉴 옵션을 사용하여 관계를 편집하거나 삭제할 수 있습니다.

10. 보호 버튼을 선택하세요.

    vCenter 작업은 작업 ID 세부 정보와 함께 생성되고, 진행 상황은 최근 작업 패널에 표시됩니다. 이는 비동기 작업입니다. 사용자 인터페이스에는 요청 제출 상태만 표시되고 작업이 완료될 때까지 기다리지 않습니다.

11. 보호된 호스트 클러스터를 보려면 * NetApp ONTAP 도구* > 보호 > *호스트 클러스터 관계*로 이동합니다.

SRA 보호를 사용하여 보호하세요

데이터 저장소를 보호하기 위한 SRA 구성

ONTAP tools for VMware vSphere 재해 복구를 구성하기 위해 SRA 기능을 활성화하는 옵션을 제공합니다.

시작하기 전에

- vCenter Server 인스턴스를 설정하고 ESXi 호스트를 구성했어야 합니다.
- ONTAP tools for VMware vSphere 배포했어야 합니다.
- SRA 어댑터를 다운로드했어야 합니다. `.tar.gz` 파일에서 "NetApp 지원 사이트" .
- SRA 워크플로를 실행하기 전에 소스 및 대상 ONTAP 클러스터에 동일한 사용자 정의 SnapMirror 일정이 만들어져 있어야 합니다.
- "ONTAP tools for VMware vSphere 활성화" SRA 기능을 활성화합니다.

단계

1. 다음 URL을 사용하여 VMware Live Site Recovery 어플라이언스 관리 인터페이스에 로그인하세요. `https://:<srm_ip>:5480` 그런 다음 VMware VMware Live Site Recovery 어플라이언스 관리 인터페이스에서 스토리지 복제 어댑터로 이동합니다.
2. *새 어댑터*를 선택하세요.
3. SRA 플러그인용 *.tar.gz* 설치 프로그램을 VMware Live Site Recovery에 업로드합니다.
4. 어댑터를 다시 스캔하여 VMware Live Site Recovery Storage Replication 어댑터 페이지에서 세부 정보가 업데이트되었는지 확인합니다.

SAN 및 NAS 환경에 대한 SRA 구성

VMware Live Site Recovery를 위한 Storage Replication Adapter(SRA)를 실행하기 전에 스토리지 시스템을 설정해야 합니다.

SAN 환경에 대한 SRA 구성

시작하기 전에

보호 사이트와 복구 사이트에 다음 프로그램이 설치되어 있어야 합니다.

- VMware 라이브 사이트 복구

VMware Live Site Recovery 설치에 대한 설명서는 VMware 사이트에서 확인할 수 있습니다.

"VMware Live Site Recovery 정보"

- 에스에이알에이

  어댑터는 VMware Live Site Recovery에 설치됩니다.

단계

1. 보호된 사이트의 기본 스토리지 시스템에 있는 LUN에 기본 ESXi 호스트가 연결되어 있는지 확인합니다.
2. LUN이 다음이 있는 igroup에 있는지 확인하십시오. `ostype` 기본 스토리지 시스템에서 옵션이 _VMware_로 설정되었습니다.
3. 복구 사이트의 ESXi 호스트에 스토리지 가상 머신(SVM)에 대한 적절한 iSCSI 연결이 있는지 확인합니다. 보조 사이트 ESXi 호스트는 보조 사이트 스토리지에 액세스할 수 있어야 하고, 기본 사이트 ESXi 호스트는 기본 사이트 스토리지에 액세스할 수 있어야 합니다.

   ESXi 호스트에 SVM에 연결된 로컬 LUN이 있는지 확인하거나 다음을 수행하여 이 작업을 수행할 수 있습니다. `iscsi show initiators` SVM에 대한 명령. ESXi 호스트에서 매핑된 LUN에 대한 LUN 액세스를 확인하여 iSCSI 연결을 확인합니다.

NAS 환경에 대한 **SRA** 구성

시작하기 전에

보호 사이트와 복구 사이트에 다음 프로그램이 설치되어 있어야 합니다.

- VMware 라이브 사이트 복구

  VMware Live Site Recovery 설치에 대한 설명서는 VMware 사이트에서 찾을 수 있습니다.

  "VMware Live Site Recovery 정보"

- 에스에이알에이

  어댑터는 VMware Live Site Recovery와 SRA 서버에 설치됩니다.

단계

1. 보호된 사이트의 데이터스토어에 vCenter Server에 등록된 가상 머신이 포함되어 있는지 확인합니다.
2. 보호된 사이트의 ESXi 호스트가 스토리지 가상 머신(SVM)에서 NFS 내보내기 볼륨을 마운트했는지 확인합니다.
3. Array Manager 마법사를 사용하여 VMware Live Site Recovery에 어레이를 추가할 때, NFS 내보내기가 있는 IP 주소나 FQDN과 같은 유효한 주소가 **NFS** 주소 필드에 지정되어 있는지 확인하십시오. *NFS 주소 * 필드에 NFS 호스트 이름을 사용하지 마십시오.
4. 사용하다 `ping` 복구 사이트의 각 ESXi 호스트에서 명령을 실행하여 SVM에서 NFS 내보내기를 제공하는 데 사용되는 IP 주소에 액세스할 수 있는 VMkernel 포트가 호스트에 있는지 확인합니다.

확장성이 높은 환경에 맞게 **SRA** 구성

확장성이 높은 환경에서 최적의 성능을 발휘하려면 SRA(Storage Replication Adapter)에 대한

권장 설정에 따라 스토리지 시간 초과 간격을 구성해야 합니다.

저장소 공급자 설정

확장된 환경의 경우 VMware Live Site Recovery에서 다음과 같은 시간 초과 값을 설정해야 합니다.

고급 설정	시간 초과 값
`StorageProvider.resignatureTimeout`	설정 값을 900초에서 12000초로 늘립니다.
`storageProvider.hostRescanDelaySec`	60
`storageProvider.hostRescanRepeatCnt`	20
`storageProvider.hostRescanTimeoutSec`	높은 값을 설정하세요(예: 99999)

또한 다음을 활성화해야 합니다. `StorageProvider.autoResignatureMode` 옵션.

참조하다 "저장소 공급자 설정 변경" 저장소 공급자 설정을 수정하는 방법에 대한 자세한 내용은 다음을 참조하세요.

저장 설정

시간 초과가 발생하면 값을 늘리십시오. `storage.commandTimeout` 그리고 `storage.maxConcurrentCommandCnt` 더 높은 가치로.

> 지정된 시간 초과 간격은 최대값입니다. 최대 시간 초과에 도달할 때까지 기다릴 필요는 없습니다. 대부분의 명령은 설정된 최대 시간 초과 간격 내에 완료됩니다.

참조하다 "저장소 설정 변경" SAN 공급자 설정을 수정하기 위해.

VMware Live Site Recovery 어플라이언스에서 SRA 구성

VMware Live Site Recovery 어플라이언스를 배포한 후 재해 복구 관리를 활성화하기 위해 SRA(스토리지 복제 어댑터)를 구성합니다.

VMware Live Site Recovery 어플라이언스에서 SRA를 구성하면 어플라이언스 내에 ONTAP tools for VMware vSphere 저장되어 VMware Live Site Recovery와 SRA 간의 통신이 가능해집니다.

시작하기 전에

- *.tar.gz* 파일을 다운로드하세요. "NetApp 지원 사이트" .
- ONTAP 도구 관리자에서 SRA 서비스를 활성화합니다. 자세한 내용은 "서비스 활성화" 부분.
- VMware vSphere 어플라이언스용 ONTATP 도구에 vCenter Server를 추가합니다. 자세한 내용은 "vCenter 서버 추가" 부분.
- ONTAP tools for VMware vSphere 에 스토리지 백엔드를 추가합니다. 자세한 내용은 "스토리지 백엔드 추가" 부분.

단계

1. VMware Live Site Recovery 어플라이언스 화면에서 스토리지 복제 어댑터 > *새 어댑터*를 선택합니다.
2. *.tar.gz* 파일을 VMware Live Site Recovery에 업로드합니다.
3. PuTTY와 같은 SSH 클라이언트를 통해 관리자 계정으로 VMware Live Site Recovery 어플라이언스에 로그인합니다.
4. 다음 명령을 사용하여 루트 사용자로 전환합니다. `su root`
5. 명령을 실행하세요 `cd /var/log/vmware/srm` 로그 디렉토리로 이동합니다.
6. 로그 위치에서 다음 명령을 입력하여 SRA에서 사용하는 Docker ID를 가져옵니다. `docker ps -l`
7. 컨테이너 ID에 로그인하려면 다음 명령을 입력하세요. `docker exec -it -u srm <container id> sh`
8. 다음 명령을 사용하여 ONTAP tools for VMware vSphere IP 주소와 비밀번호를 사용하여 VMware Live Site Recovery를 구성합니다. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
   - 비밀번호를 작은따옴표로 묶어 제공하면 Perl 스크립트가 특수문자를 구분 기호가 아닌 비밀번호의 일부로 처리합니다.
   - ONTAP 도구 관리자에서 애플리케이션(VASA Provider/SRA) 사용자 이름과 비밀번호를 설정할 수 있습니다. 이 자격 증명을 사용하여 SRA를 VMware Live Site Recovery에 등록합니다.
   - vCenter GUID를 찾으려면 vCenter 인스턴스를 추가한 후 ONTAP 도구 관리자의 vCenter Server 페이지로 이동합니다. 참조하다"vCenter 서버 추가" 부분.
9. 어댑터를 다시 검사하여 업데이트된 세부 정보가 VMware Live Site Recovery Storage Replication 어댑터 페이지에 나타나는지 확인합니다.

결과

저장소 자격 증명이 저장되었음을 나타내는 확인 메시지가 나타납니다. 이제 SRA는 지정된 IP 주소, 포트 및 자격 증명을 사용하여 SRA 서버와 통신할 수 있습니다.

SRA 자격 증명 업데이트

VMware Live Site Recovery가 SRA와 통신하려면 자격 증명을 수정한 경우 VMware Live Site Recovery 서버에서 SRA 자격 증명을 업데이트해야 합니다.

시작하기 전에

주제에 언급된 단계를 실행했어야 합니다."VMware Live Site Recovery 어플라이언스에서 SRA 구성" .

단계

1. 다음 명령을 실행하여 VMware Live Site Recovery 머신 폴더의 캐시된 ONTAP 도구 사용자 이름 비밀번호를 삭제합니다.
   a. `sudo su <enter root password>`
   b. `docker ps`
   c. `docker exec -it <container_id> sh`
   d. `cd conf/`
   e. `rm -rf *`

2. Perl 명령을 실행하여 새 자격 증명으로 SRA를 구성합니다.
   a. `cd ..`
   b. `perl command.pl -l --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv -password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>`비밀번호 값은 작은따옴표로 묶어야 합니다.

      저장소 자격 증명이 저장되었음을 확인하는 성공 메시지가 표시됩니다. SRA는 제공된 IP 주소, 포트 및 자격 증명을 사용하여 SRA 서버와 통신할 수 있습니다.

보호 및 복구 사이트 구성

보호된 사이트의 가상 머신 그룹을 보호하려면 보호 그룹을 만들어야 합니다.

새 데이터스토어를 추가할 때 기존 데이터스토어 그룹에 포함하거나, 새 데이터스토어를 추가하고 보호를 위한 새 볼륨 또는 일관성 그룹을 생성할 수 있습니다. 보호된 일관성 그룹 또는 볼륨에 새 데이터스토어를 추가한 후에는 SnapMirror 업데이트하고 보호 사이트와 복구 사이트 모두에서 스토리지 검색을 수행합니다. 새 데이터스토어가 감지되고 보호되도록 검색을 수동으로 또는 일정에 따라 실행할 수 있습니다.

보호 사이트와 복구 사이트 쌍

vSphere Client를 사용하여 만든 보호 사이트와 복구 사이트를 페어링하여 SRA(스토리지 복제 어댑터)가 스토리지 시스템을 검색할 수 있도록 해야 합니다.

> SRA(스토리지 복제 어댑터)는 일관성 그룹의 자동 장애 조치 이중화 유형의 동기화 관계 하나와 SnapMirror 비동기 관계를 통한 팬아웃을 지원합니다. 그러나 일관성 그룹에 두 개의 비동기 SnapMirror 있는 팬아웃이나 볼륨에 있는 팬아웃 SnapMirror는 지원되지 않습니다.

시작하기 전에

- 보호된 사이트와 복구 사이트에 VMware Live Site Recovery를 설치해야 합니다.
- 보호 사이트와 복구 사이트에 SRA를 설치해야 합니다.

단계

1. vSphere Client 홈페이지에서 *사이트 복구*를 두 번 클릭하고 *사이트*를 선택합니다.
2. 개체 > 작업 > *사이트 쌍*을 선택합니다.
3. 사이트 복구 관리자 서버 페어링 대화 상자에서 보호된 사이트의 Platform Services Controller 주소를 입력한 후 *다음*을 선택합니다.
4. vCenter Server 선택 섹션에서 다음을 수행합니다.
   a. 보호된 사이트의 vCenter Server가 페어링할 수 있는 일치 후보로 나타나는지 확인합니다.
   b. SSO 관리 자격 증명을 입력한 다음 *마침*을 선택합니다.
5. 메시지가 표시되면 *예*를 선택하여 보안 인증서를 수락합니다.

결과

보호된 사이트와 복구 사이트 모두 개체 대화 상자에 나타납니다.

보호 그룹 구성

시작하기 전에

소스 사이트와 대상 사이트 모두 다음 사항에 대해 구성되어 있는지 확인해야 합니다.

- 동일한 버전의 VMware Live Site Recovery가 설치됨
- 가상 머신
- 보호 및 복구 사이트 페어링
- 소스 및 대상 데이터 저장소는 각 사이트에 마운트되어야 합니다.

단계

1. vCenter Server에 로그인하고 사이트 복구 > *보호 그룹*을 선택합니다.
2. 보호 그룹 창에서 *새로 만들기*를 선택합니다.
3. 보호 그룹에 대한 이름과 설명, 방향을 지정하고 *다음*을 선택합니다.
4. 유형 필드에서 NFS 및 VMFS 데이터 저장소에 대한 데이터 저장소 그룹(배열 기반 복제)으로 *유형 필드 옵션…*을 선택합니다. 장애 도메인은 복제가 활성화된 SVM뿐입니다. 피어링만 구현되어 있고 문제가 없는 SVM이 표시됩니다.
5. 복제 그룹 탭에서 활성화된 어레이 쌍이나 구성한 가상 머신이 있는 복제 그룹을 선택한 후 *다음*을 선택합니다.

   복제 그룹의 모든 가상 머신이 보호 그룹에 추가됩니다.

6. 기존 복구 계획을 선택하거나 *새 복구 계획에 추가*를 선택하여 새 복구 계획을 만들 수 있습니다.
7. 완료 준비 탭에서 생성한 보호 그룹의 세부 정보를 검토한 다음 *마침*을 선택합니다.

보호 및 복구 사이트 리소스 구성

네트워크 매핑 구성

보호된 사이트의 각 리소스를 복구 사이트의 적절한 리소스로 매핑할 수 있도록 두 사이트의 VM 네트워크, ESXi 호스트, 폴더와 같은 리소스 매핑을 구성해야 합니다.

다음 리소스 구성을 완료해야 합니다.

- 네트워크 매핑
- 폴더 매핑
- 리소스 매핑
- 플레이스홀더 데이터 저장소

시작하기 전에

보호 사이트와 복구 사이트를 연결했어야 합니다.

단계

1. vCenter Server에 로그인하고 사이트 복구 > *사이트*를 선택합니다.
2. 보호된 사이트를 선택하고 *관리*를 선택하세요.

3. 관리 탭에서 네트워크 매핑 > *새로 만들기*를 선택하여 새 네트워크 매핑을 만듭니다.
4. 네트워크 매핑 만들기 마법사에서 다음을 수행합니다.
    a. *이름이 일치하는 네트워크에 대한 매핑을 자동으로 준비*를 선택하고 *다음*을 선택합니다.
    b. 보호 및 복구 사이트에 필요한 데이터 센터 개체를 선택하고 *매핑 추가*를 선택합니다.
    c. 매핑이 성공적으로 생성되면 *다음*을 선택합니다.
    d. 역방향 매핑을 만드는 데 사용된 객체를 선택한 다음 *마침*을 선택합니다.

결과

네트워크 매핑 페이지에는 보호된 사이트 리소스와 복구 사이트 리소스가 표시됩니다. 사용자 환경 내의 다른 네트워크에도 동일한 단계를 따를 수 있습니다.

폴더 매핑 구성

보호된 사이트와 복구 사이트의 폴더를 매핑하여 두 사이트 간의 통신을 활성화해야 합니다.

시작하기 전에

보호 사이트와 복구 사이트를 연결했어야 합니다.

단계

1. vCenter Server에 로그인하고 사이트 복구 > *사이트*를 선택합니다.
2. 보호된 사이트를 선택하고 *관리*를 선택하세요.
3. 관리 탭에서 폴더 매핑 > 폴더 아이콘을 선택하여 새 폴더 매핑을 만듭니다.
4. 폴더 매핑 만들기 마법사에서 다음을 수행합니다.
    a. *이름이 일치하는 폴더에 대한 매핑을 자동으로 준비*를 선택하고 *다음*을 선택합니다.
    b. 보호 및 복구 사이트에 필요한 데이터 센터 개체를 선택하고 *매핑 추가*를 선택합니다.
    c. 매핑이 성공적으로 생성되면 *다음*을 선택합니다.
    d. 역방향 매핑을 만드는 데 사용된 객체를 선택한 다음 *마침*을 선택합니다.

결과

폴더 매핑 페이지에는 보호된 사이트 리소스와 복구 사이트 리소스가 표시됩니다. 사용자 환경 내의 다른 네트워크에도 동일한 단계를 따를 수 있습니다.

리소스 매핑 구성

보호 사이트와 복구 사이트에서 리소스를 매핑하여 가상 머신이 한 호스트 그룹 또는 다른 호스트 그룹으로 장애 조치되도록 구성해야 합니다.

시작하기 전에

보호 사이트와 복구 사이트를 연결했어야 합니다.

> VMware Live Site Recovery에서 리소스는 리소스 풀, ESXi 호스트 또는 vSphere 클러스터가 될 수 있습니다.

단계

1. vCenter Server에 로그인하고 사이트 복구 > *사이트*를 선택합니다.
2. 보호된 사이트를 선택하고 *관리*를 선택하세요.
3. 관리 탭에서 리소스 매핑 > *새로 만들기*를 선택하여 새 리소스 매핑을 만듭니다.
4. 리소스 매핑 만들기 마법사에서 다음을 수행합니다.
   a. *이름이 일치하는 리소스에 대한 매핑을 자동으로 준비*를 선택하고 *다음*을 선택합니다.
   b. 보호 및 복구 사이트에 필요한 데이터 센터 개체를 선택하고 *매핑 추가*를 선택합니다.
   c. 매핑이 성공적으로 생성되면 *다음*을 선택합니다.
   d. 역방향 매핑을 만드는 데 사용된 객체를 선택한 다음 *마침*을 선택합니다.

결과

리소스 매핑 페이지에는 보호된 사이트 리소스와 복구 사이트 리소스가 표시됩니다. 사용자 환경 내의 다른 네트워크에도 동일한 단계를 따를 수 있습니다.

플레이스홀더 데이터 저장소 구성

보호된 가상 머신(VM)의 복구 사이트에서 vCenter 인벤토리에 자리가 있도록 플레이스홀더 데이터스토어를 구성해야 합니다. 플레이스홀더 VM은 크기가 작고 수백 KB 이하의 용량만 사용하므로 플레이스홀더 데이터스토어는 크게 구성할 필요가 없습니다.

시작하기 전에

- 보호 사이트와 복구 사이트를 연결했어야 합니다.
- 리소스 매핑을 구성했어야 합니다.

단계

1. vCenter Server에 로그인하고 사이트 복구 > *사이트*를 선택합니다.
2. 보호된 사이트를 선택하고 *관리*를 선택하세요.
3. 관리 탭에서 플레이스홀더 데이터스토어 > *새로 만들기*를 선택하여 새로운 플레이스홀더 데이터스토어를 만듭니다.
4. 적절한 데이터 저장소를 선택하고 *확인*을 선택합니다.

   플레이스홀더 데이터 저장소는 로컬 또는 원격일 수 있으며 복제해서는 안 됩니다.

5. 복구 사이트에 대한 플레이스홀더 데이터 저장소를 구성하려면 3~5단계를 반복합니다.

어레이 관리자를 사용하여 **SRA** 구성

VMware Live Site Recovery의 Array Manager 마법사를 사용하여 SRA(스토리지 복제 어댑터)를 구성하면 VMware Live Site Recovery와 스토리지 가상 머신(SVM) 간의 상호작용을 활성화할 수 있습니다.

시작하기 전에

- VMware Live Site Recovery에서 보호 사이트와 복구 사이트를 페어링해야 합니다.

- 어레이 관리자를 구성하기 전에 온보딩된 스토리지를 구성해야 합니다.
- 보호된 사이트와 복구 사이트 간의 SnapMirror 관계를 구성하고 복제했어야 합니다.
- 다중 테넌시를 활성화하려면 SVM 관리 LIF를 활성화해야 합니다.

SRA는 클러스터 수준 관리와 SVM 수준 관리를 지원합니다. 클러스터 수준에서 스토리지를 추가하면 클러스터의 모든 SVM을 검색하고 작업을 수행할 수 있습니다. SVM 수준에서 스토리지를 추가하면 해당 SVM만 관리할 수 있습니다.

단계

1. VMware Live Site Recovery에서 어레이 관리자 > *어레이 관리자 추가*를 선택합니다.
2. VMware Live Site Recovery에서 어레이를 설명하려면 다음 정보를 입력하세요.

   a. 표시 이름 필드에 배열 관리자를 식별할 이름을 입력합니다.

   b. **SRA** 유형 필드에서 * ONTAP 용 NetApp 스토리지 복제 어댑터*를 선택합니다.

   c. 클러스터 또는 SVM에 연결하기 위한 정보를 입력하세요.

      - 클러스터에 연결하는 경우 클러스터 관리 LIF를 입력해야 합니다.
      - SVM에 직접 연결하는 경우 SVM 관리 LIF의 IP 주소를 입력해야 합니다.

      > 어레이 관리자를 구성할 때 ONTAP tools for VMware vSphere 에서 스토리지 시스템을 온보딩하는 데 사용된 것과 동일한 연결(IP 주소)을 스토리지 시스템에 사용해야 합니다. 예를 들어, 어레이 관리자 구성이 SVM 범위인 경우 ONTAP tools for VMware vSphere 의 스토리지는 SVM 수준에서 추가되어야 합니다.

   d. 클러스터에 연결하는 경우 **SVM** 이름 필드에 SVM 이름을 지정하거나 비워 두면 클러스터의 모든 SVM을 관리합니다.

   e. 볼륨 포함 목록 필드에 검색할 볼륨을 입력합니다.

      보호된 사이트에서 소스 볼륨을 입력하고 복구 사이트에서 복제된 대상 볼륨을 입력할 수 있습니다.

      예를 들어, SnapMirror 관계에 있는 볼륨 src_vol1을 볼륨 dst_vol1과 검색하려면 보호 사이트 필드에 src_vol1을 지정하고 복구 사이트 필드에 dst_vol1을 지정해야 합니다.

   f. (선택 사항) 볼륨 제외 목록 필드에 검색에서 제외할 볼륨을 입력합니다.

      보호된 사이트에서 소스 볼륨을 입력하고 복구 사이트에서 복제된 대상 볼륨을 입력할 수 있습니다.

   예를 들어 SnapMirror 관계에 있는 볼륨 _src_vol1_을 볼륨 _dst_vol1_과 제외하려면 보호 사이트 필드에 _src_vol1_을 지정하고 복구 사이트 필드에 _dst_vol1_을 지정해야 합니다.

3. *다음*을 선택하세요.
4. 배열이 검색되어 배열 관리자 추가 창 하단에 표시되는지 확인하고 *마침*을 선택합니다.

적절한 SVM 관리 IP 주소와 자격 증명을 사용하여 복구 사이트에도 동일한 단계를 따를 수 있습니다. 배열 관리자 추가 마법사의 배열 쌍 활성화 화면에서 올바른 배열 쌍이 선택되었는지, 그리고 활성화할 준비가 되었는지 확인해야 합니다.

복제된 스토리지 시스템 확인

SRA(스토리지 복제 어댑터)를 구성한 후 보호 사이트와 복구 사이트가 성공적으로 페어링되었는지 확인해야 합니다. 복제된 저장 시스템은 보호 사이트와 복구 사이트 모두에서 검색할 수 있어야 합니다.

시작하기 전에

- 저장 시스템을 구성했어야 합니다.
- VMware Live Site Recovery 어레이 관리자를 사용하여 보호 사이트와 복구 사이트를 페어링해야 합니다.
- SRA에 대한 테스트 장애 조치 작업과 장애 조치 작업을 수행하기 전에 FlexClone 라이선스와 SnapMirror 라이선스를 활성화해야 합니다.
- 소스 사이트와 대상 사이트에서 동일한 SnapMirror 정책과 일정을 적용해야 합니다.

단계

1. vCenter Server에 로그인합니다.
2. 사이트 복구 > *어레이 기반 복제*로 이동합니다.
3. 필요한 어레이 쌍을 선택하고 해당 세부 정보를 확인하세요.

   저장 시스템은 보호 사이트와 복구 사이트에서 "활성화됨" 상태로 검색되어야 합니다.

팬아웃 보호

팬아웃 보호에서 일관성 그룹은 첫 번째 대상 ONTAP 클러스터에서는 동기 관계로, 두 번째 대상 ONTAP 클러스터에서는 비동기 관계로 이중으로 보호됩니다. SnapMirror 활성 동기화 보호 워크플로를 만들고, 편집하고, 삭제하면 동기 보호가 유지됩니다. SRM 장애 조치 및 재보호 워크플로는 비동기 보호 기능을 유지합니다.

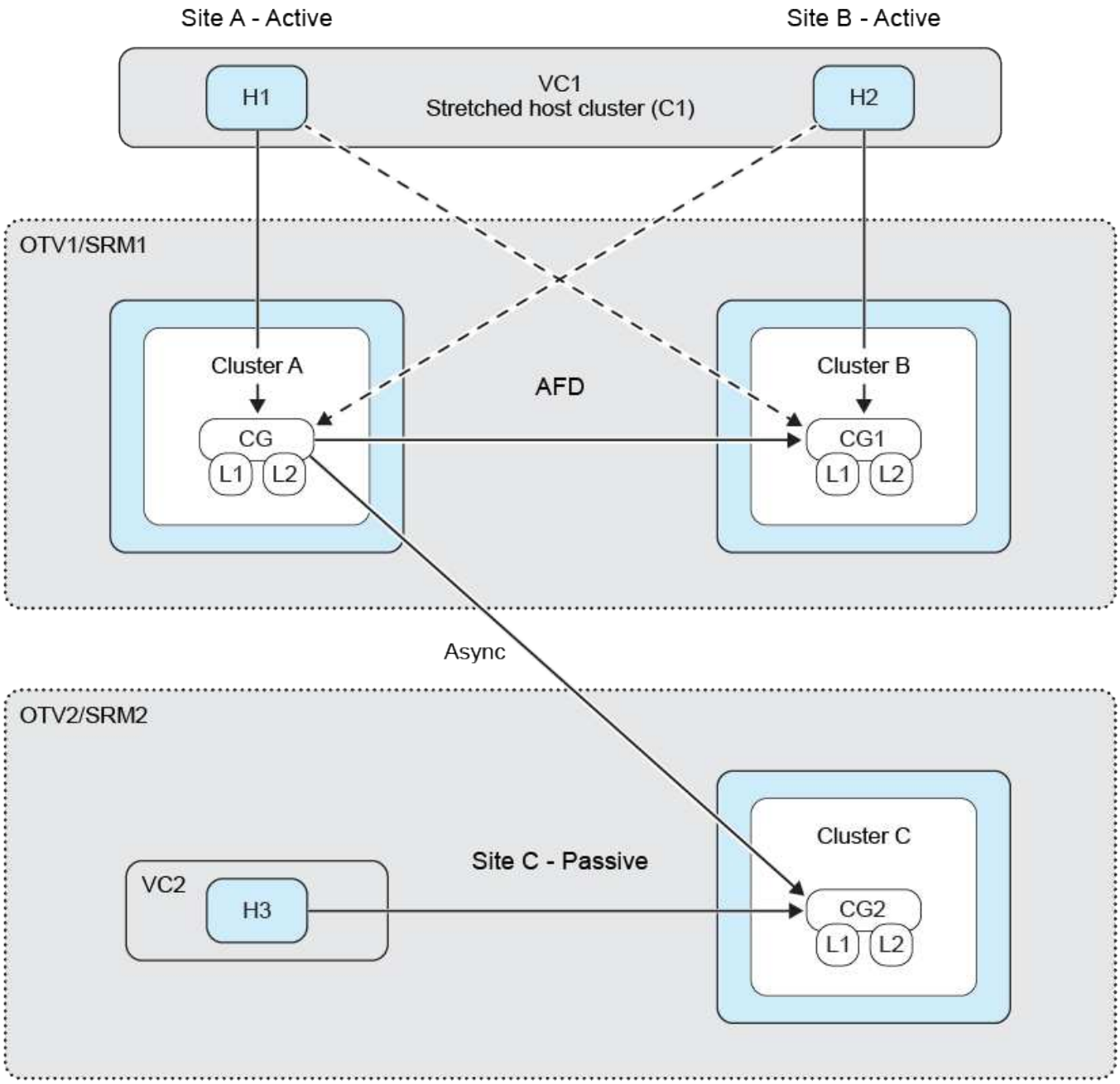
팬아웃 보호를 구축하려면 세 개의 사이트 클러스터와 SVM을 피어링해야 합니다.

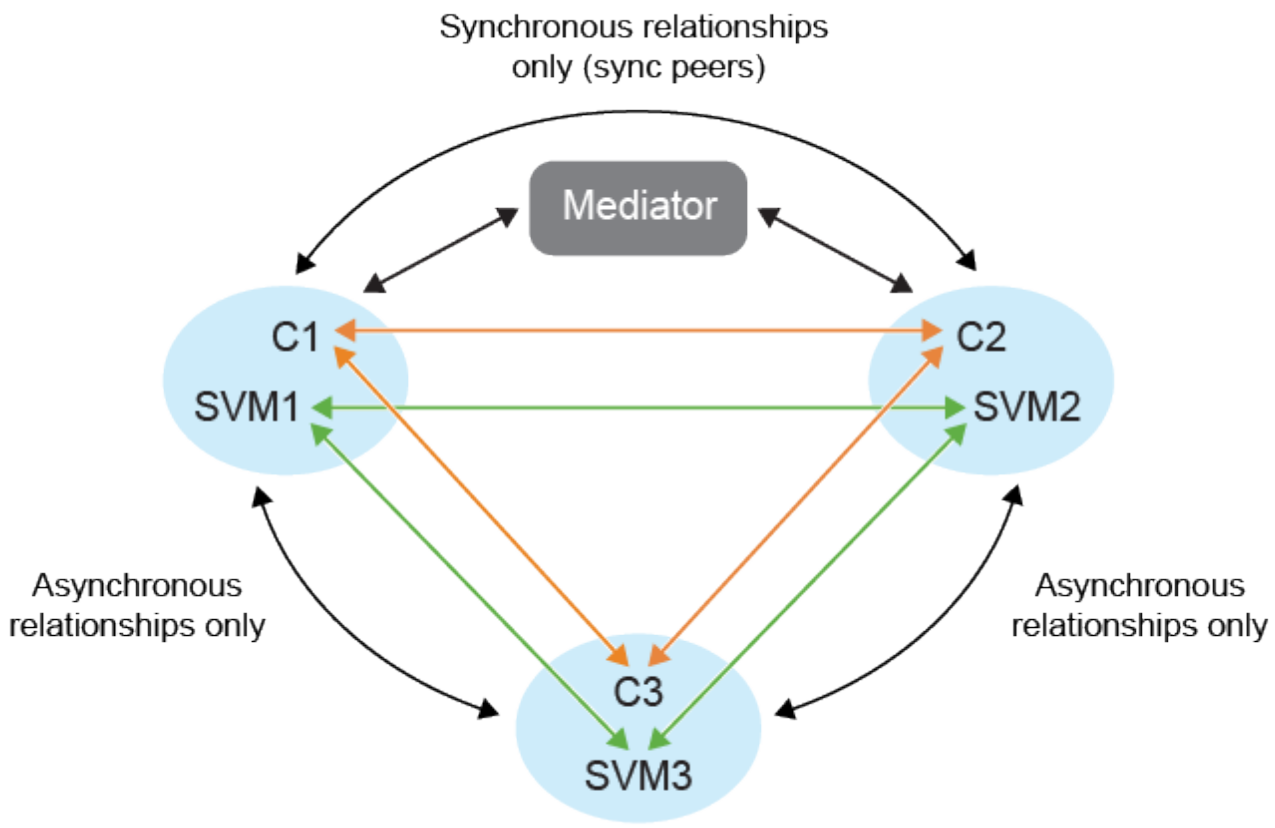
예:

만약에	그 다음에

• 소스 일관성 그룹은 클러스터 c1 및 SVM svm1에 있습니다. • 첫 번째 대상 일관성 그룹은 클러스터 c2 및 SVM svm2에 있습니다. • 두 번째 대상 일관성 그룹은 클러스터 c3 및 SVM svm3에 있습니다.	• Source ONTAP 클러스터의 클러스터 피어링은 (C1, C2)와 (C1, C3)가 됩니다. • 첫 번째 대상 ONTAP 클러스터의 클러스터 피어링은 (C2, C1) 및 (C2, C3)입니다. • 두 번째 대상 ONTAP 클러스터의 클러스터 피어링은 (C3, C1)과 (C3, C2)가 됩니다. • 소스 SVM에 대한 SVM 피어링은 (svm1, svm2)와 (svm1, svm3)이 됩니다. • 첫 번째 대상 SVM에 대한 SVM 피어링은 (svm2, svm1) 및 (svm2, svm3)이 됩니다. • 두 번째 대상 svm에 대한 SVM 피어링은 (svm3, svm1)과 (svm3, svm2)가 됩니다.

다음 다이어그램은 팬아웃 보호 구성을 보여줍니다
.


Site A - Active
Site B - Active
VC1
Stretched host cluster (C1)
H1
H2
OTV1/SRM1
Cluster A
Cluster B
AFD
CG
CG1
L1
L2
L1
L2
Async
OTV2/SRM2
Cluster C
Site C - Passive
VC2
H3
CG2
L1
L2



단계

1. 새로운 플레이스홀더 데이터 저장소를 만듭니다. 나타내다 "플레이스홀더 데이터 저장소 선택"
2. 호스트 클러스터 보호에 데이터 저장소 추가"보호된 호스트 클러스터 수정" . 비동기 및 동기 정책 유형을 모두 추가해야 합니다.

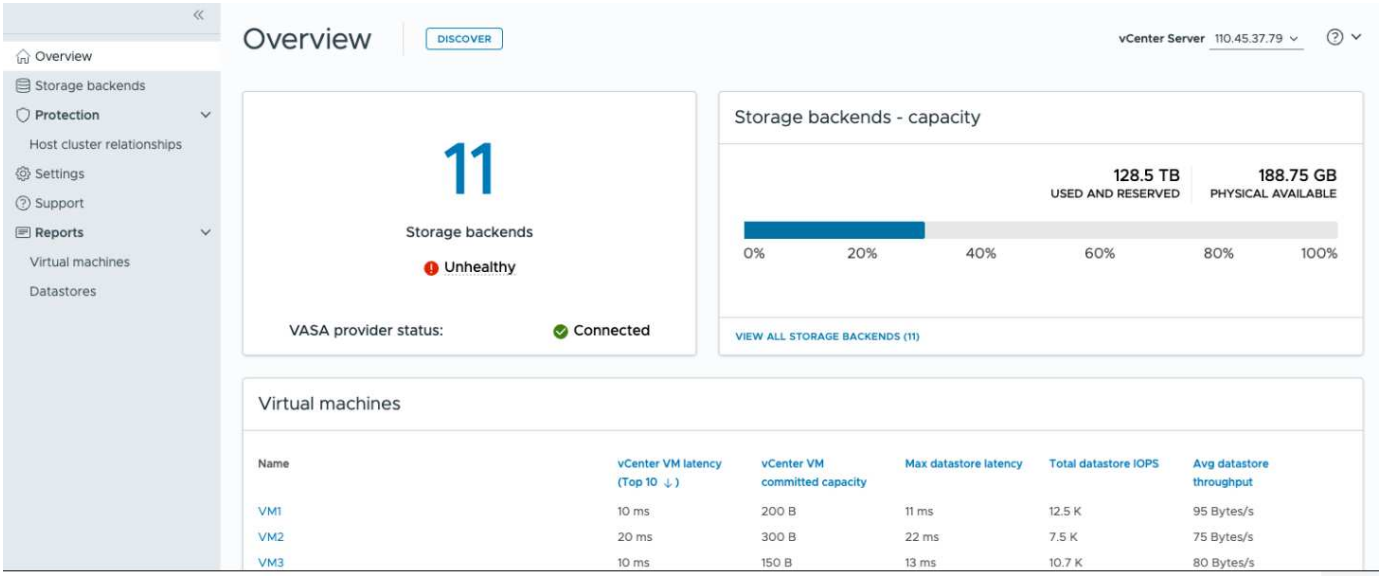
ONTAP tools for VMware vSphere 관리

ONTAP tools for VMware vSphere

vCenter 클라이언트의 바로 가기 섹션에서 ONTAP tools for VMware vSphere 선택하면 사용자 인터페이스가 개요 페이지로 이동합니다. 이 페이지는 ONTAP tools for VMware vSphere 에 대한 요약을 제공하는 대시보드 역할을 합니다.

향상된 연결 모드(ELM) 설정의 경우 vCenter Server 선택 드롭다운이 나타나고 원하는 vCenter Server를 선택하면 관련 데이터를 볼 수 있습니다. 이 드롭다운은 플러그인의 다른 모든 목록 보기에서 사용할 수 있습니다. 한 페이지에서 선택한 vCenter Server 항목은 플러그인의 모든 탭에 동일하게 적용됩니다

.



개요 페이지에서 검색 작업을 실행할 수 있습니다. 검색 작업은 vCenter 수준에서 검색을 실행하여 새로 추가되거나 업데이트된 스토리지 백엔드, 호스트, 데이터스토어 및 보호 상태/관계를 감지합니다. 예약된 검색을 기다리지 않고도 엔터티의 주문형 검색을 실행할 수 있습니다.

> 검색 작업을 수행할 권한이 있는 경우에만 작업 버튼이 활성화됩니다.

검색 요청이 제출된 후 최근 작업 패널에서 작업 진행 상황을 추적할 수 있습니다.

대시보드에는 시스템의 다양한 요소를 보여주는 여러 개의 카드가 있습니다. 다음 표는 다양한 카드와 그 의미를 보여줍니다.

카드	설명

상태	상태 카드는 스토리지 백엔드의 수와 스토리지 백엔드 및 VASA 공급자의 전반적인 상태를 보여줍니다. 모든 스토리지 백엔드 상태가 정상이면 스토리지 백엔드 상태가 정상*으로 표시되고, 스토리지 백엔드 중 하나에 문제가 있으면(알 수 없음/도달 불가/성능 저하 상태) *비정상*으로 표시됩니다. 도구 설명을 선택하여 스토리지 백엔드의 상태 세부 정보를 엽니다. 자세한 내용을 보려면 원하는 스토리지 백엔드를 선택하세요. *기타 **VASA** 공급자 상태 링크는 vCenter Server에 등록된 VASA 공급자의 현재 상태를 보여줍니다.
스토리지 백엔드 - 용량	이 카드는 선택한 vCenter Server 인스턴스의 모든 스토리지 백엔드에 대한 사용 가능한 용량과 누적된 용량을 보여줍니다. ASA r2 스토리지 시스템의 경우, 분리된 시스템이기 때문에 용량 데이터가 표시되지 않습니다.
가상 머신	이 카드는 성능 지표별로 정렬된 상위 10개 VM을 보여줍니다. 헤더를 선택하면 선택한 메트릭에 대한 상위 10개 VM이 오름차순 또는 내림차순으로 정렬됩니다. 카드에 적용된 정렬 및 필터링 변경 사항은 브라우저 캐시를 변경하거나 지울 때까지 유지됩니다.
데이터 저장소	이 카드는 성능 지표에 따라 정렬된 상위 10개 데이터 저장소를 보여줍니다. 헤더를 선택하면 선택한 지표에 대한 상위 10개 데이터 저장소가 오름차순 또는 내림차순으로 정렬됩니다. 카드에 적용된 정렬 및 필터링 변경 사항은 브라우저 캐시를 변경하거나 지울 때까지 유지됩니다. 데이터 저장소 유형 드롭다운을 통해 NFS, VMFS 또는 vVols 와 같은 데이터 저장소 유형을 선택할 수 있습니다.
ESXi 호스트 규정 준수 카드	이 카드는 설정 그룹/범주별 권장 NetApp 호스트 설정과 관련하여 선택된 vCenter에 대한 모든 ESXi 호스트 설정의 전반적인 규정 준수 상태를 보여줍니다. 권장 설정 적용 링크를 선택하면 권장 설정을 적용할 수 있습니다. 호스트의 규정 준수 상태를 선택하면 호스트 목록을 볼 수 있습니다.

ONTAP 도구 관리자 사용자 인터페이스

ONTAP tools for VMware vSphere 여러 vCenter Server 인스턴스를 관리할 수 있는 멀티 테넌트 시스템입니다. ONTAP 도구 관리자는 관리되는 vCenter Server 인스턴스와 온보딩된 스토리지 백엔드에 대한 ONTAP tools for VMware vSphere 에 대한 더 많은 제어 기능을 제공합니다.

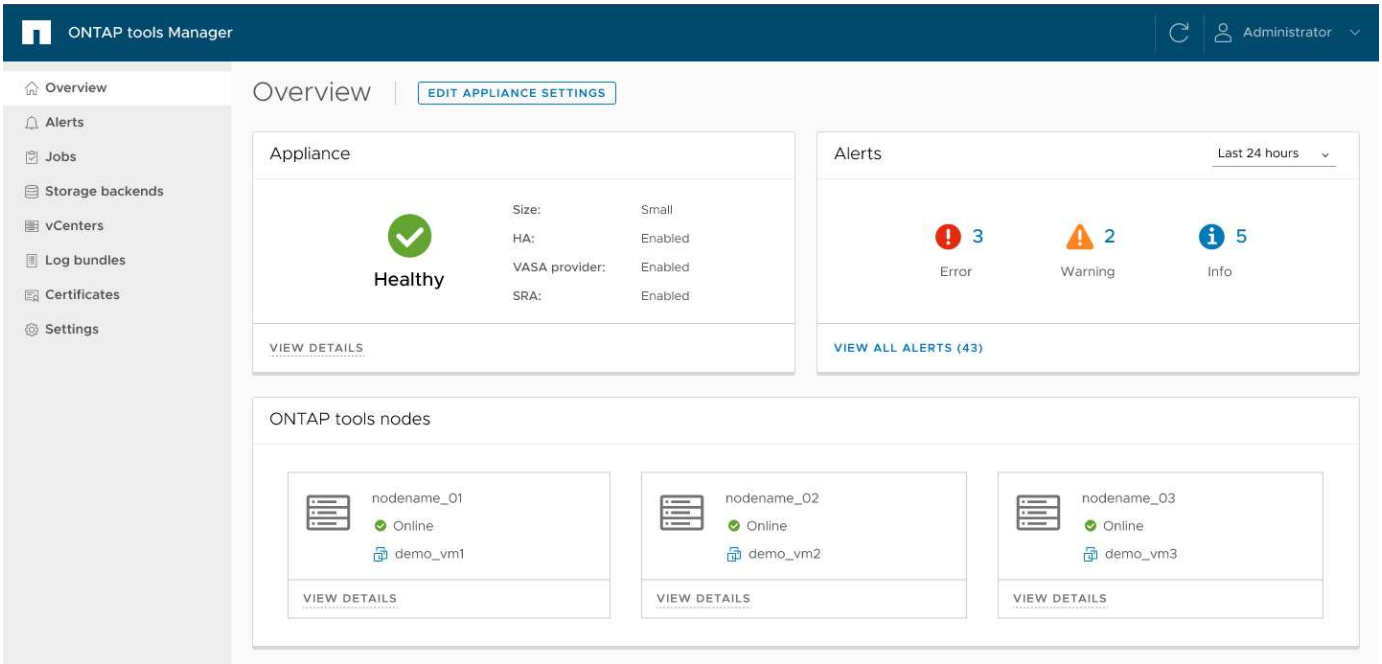
ONTAP 도구 관리자는 다음과 같은 데 도움이 됩니다.

- vCenter Server 인스턴스 관리 - ONTAP 도구에 vCenter Server 인스턴스를 추가하고 관리합니다.
- 스토리지 백엔드 관리 - ONTAP tools for VMware vSphere 에 ONTAP 스토리지 클러스터를 추가하고 관리하고 이를 전역적으로 온보딩된 vCenter Server 인스턴스에 매핑합니다.
- 로그 번들 다운로드 - ONTAP tools for VMware vSphere 에 대한 로그 파일을 수집합니다.
- 인증서 관리 - 자체 서명된 인증서를 사용자 정의 CA 인증서로 변경하고 VASA Provider 및 ONTAP 도구의 모든 인증서를 갱신하거나 새로 고칩니다.

- 비밀번호 관리 - 사용자의 OVA 애플리케이션 비밀번호를 재설정합니다.

ONTAP 도구 관리자에 액세스하려면 다음을 실행하세요.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/` 브라우저에서 ONTAP tools for VMware vSphere 로그인합니다.

ONTAP 도구 관리자 개요 섹션은 서비스 관리, 노드 크기 확장, 고가용성(HA) 활성화 등의 어플라이언스 구성을 관리하는 데 도움이 됩니다. 또한 노드와 관련된 ONTAP 도구의 전반적인 정보(상태, 네트워크 세부 정보, 알림 등)를 모니터링할 수 있습니다.



카드	설명
가전제품 카드	어플라이언스 카드는 ONTAP 도구 어플라이언스의 전반적인 상태를 제공합니다. 여기에는 기기 구성 세부 정보와 활성화된 서비스 상태가 표시됩니다. ONTAP 도구 어플라이언스에 대한 추가 정보를 보려면 세부 정보 보기 링크를 선택하세요. 편집 기기 설정 작업 작업이 진행 중일 때, 기기 포틀릿에 작업의 상태와 세부 정보가 표시됩니다.
알림 카드	알림 카드에는 HA 노드 수준 알림을 포함하여 유형별로 ONTAP 도구 알림이 나열됩니다. 알림 목록을 보려면 개수 텍스트(하이퍼링크)를 선택하세요. 링크를 클릭하면 선택한 유형으로 필터링된 알림 보기 페이지로 이동합니다.
vCenter	vCenter 카드는 시스템의 vCenter 상태를 보여줍니다.
스토리지 백엔드	스토리지 백엔드 카드는 시스템의 스토리지 백엔드 상태를 보여줍니다.
ONTAP 도구 노드 카드	ONTAP 도구 노드 카드는 노드 이름, 노드 VM 이름, 상태 및 모든 네트워크 관련 데이터가 포함된 노드 목록을 보여줍니다. *세부정보 보기*를 선택하면 선택한 노드와 관련된 추가 세부정보를 볼 수 있습니다. [참고] HA가 아닌 설정에서는 노드가 하나만 표시됩니다. HA 설정에서는 세 개의 노드가 표시됩니다.

ONTAP tools for VMware vSphere 에서 igroups 및 내보내기 정책 이해

이니시에이터 그룹(igroup)은 FC 프로토콜 호스트 WWPN(World Wide Port Name) 또는 iSCSI 호스트 정규 노드 이름의 테이블입니다. igroup을 정의하고 LUN에 매핑하여 어떤 이니시에이터가 LUN에 액세스할 수 있는지 제어할 수 있습니다.

ONTAP tools for VMware vSphere 에서 igroup은 플랫 구조로 생성 및 관리되었으며, vCenter의 각 데이터스토어는 단일 igroup과 연결되었습니다. 이 모델은 여러 데이터 저장소에서 igroup의 유연성과 재사용성을 제한했습니다. ONTAP tools for VMware vSphere 중첩된 igroup을 도입했습니다. 즉, vCenter의 각 데이터 저장소는 상위 igroup과 연결되고 각 호스트는 해당 상위 아래의 하위 igroup에 연결됩니다. 여러 데이터 저장소에서 재사용할 수 있도록 사용자 정의 이름으로 사용자 정의 상위 igroup을 정의하여 igroup을 보다 유연하고 상호 연결된 방식으로 관리할 수 있습니다. ONTAP tools for VMware vSphere 에서 LUN과 데이터 저장소를 효과적으로 관리하려면 igroup 워크플로를 이해하는 것이 필수적입니다. 다음 예에서 볼 수 있듯이 다양한 워크플로는 다양한 igroup 구성을 생성합니다.

> 언급된 이름은 단지 설명을 위한 목적으로만 사용되었으며 실제 igroup 이름을 나타내는 것이 아닙니다. ONTAP 도구에서 관리하는 igroup은 접두사 "otv_"를 사용합니다. 사용자 정의 igroup에는 원하는 이름을 지정할 수 있습니다.

용어	설명
DS<숫자>	데이터 저장소
iqn<숫자>	개시자 IQN
호스트<번호>	호스트 MoRef
lun<숫자>	LUN ID
<DSName>Igroup<번호>	기본(ONTAP 도구 관리) 상위 igroup
<호스트-모어>I그룹<번호>	어린이 i그룹
CustomIgroup<숫자>	사용자 정의 사용자 정의 부모 igroup
클래식I그룹<번호>	ONTAP 도구 9.x 버전에서 사용되는 igroup입니다.

예 **1:**

하나의 이니시에이터로 단일 호스트에 데이터 저장소를 생성합니다.

워크플로: [생성] DS1(lun1): host1(iqn1)

결과:

- DS1I그룹:
  - host1Igroup → (iqn1: lun1)

DS1에 대한 부모 igroup DS1Igroup이 ONTAP 시스템에 생성되고, lun1에 매핑된 자식 igroup host1Igroup이 생성됩니다. LUN은 항상 자식 igroup에 매핑됩니다.

예 **2:**

기존 데이터 저장소를 추가 호스트에 마운트합니다.

워크플로: [마운트] DS1(lun1): host2(iqn2)

결과:

- DS1I그룹:
  - host1Igroup → (iqn1: lun1)
  - host2Igroup → (iqn2: lun1)

자식 igroup host2Igroup이 생성되어 기존 부모 igroup DS1Igroup에 추가됩니다.

예 **3:**

호스트에서 데이터스토어 마운트 해제

워크플로: [마운트 해제] DS1(lun1): 호스트1(iqn1)

결과:

- DS1I그룹:
  - host2Igroup → (iqn2: lun1)

host1Igroup이 계층 구조에서 제거됩니다. 자식 igroup은 명시적으로 삭제되지 않습니다. 삭제는 다음 두 가지 조건에서 발생합니다.

- LUN이 매핑되지 않으면 ONTAP 시스템은 자식 igroup을 삭제합니다.
- 예약된 정리 작업은 LUN 매핑이 없는 불안정한 자식 igroup을 제거합니다. 이러한 시나리오는 ONTAP 도구로 관리되는 igroup에만 적용되며, 사용자 정의로 생성된 igroup에는 적용되지 않습니다.

예시 **4:**

데이터 저장소 삭제

워크플로: [삭제] DS1(lun1): host2(iqn2)

결과:

- DS1I그룹:
  - host2Igroup → (iqn2: lun1)

다른 데이터 저장소가 부모 igroup을 재사용하지 않으면 부모 및 자식 igroup이 제거됩니다. 자식 igroup은 명시적으로 삭제되지 않습니다.

예시 **5:**

사용자 정의 부모 igroup 아래에 여러 데이터 저장소 만들기

작업 흐름:

- [생성] DS2(lun2): host1(iqn1), host2(iqn2)
- [생성] DS3(lun3): host1(iqn1), host3(iqn3)

결과:

- 커스텀I그룹1:
  - host1Igroup → (iqn1: lun2, lun3)
  - host2Igroup → (iqn2: lun2)
  - host3Igroup → (iqn3: lun3)

CustomIgroup1은 DS2용으로 생성되어 DS3에 재사용됩니다. 자식 igroup은 공유 부모 아래에 생성되거나 업데이트되며, 각 자식 igroup은 해당 LUN에 매핑됩니다.

예시 **6:**

사용자 정의 상위 igroup 아래에 있는 하나의 데이터 저장소를 삭제합니다.

워크플로: [삭제] DS2(lun2): host1(iqn1), host2(iqn2)

결과:

- 커스텀I그룹1:
  - host1Igroup → (iqn1: lun3)
  - host3Igroup → (iqn3: lun3)
- CustomIgroup1은 재사용되지 않더라도 삭제되지 않습니다.
- LUN이 매핑되지 않으면 ONTAP 시스템은 host2Igroup을 삭제합니다.
- host1Igroup은 DS3의 lun3에 매핑되어 있으므로 삭제되지 않습니다. 사용자 지정 igroup은 재사용 상태와 관계없이 삭제되지 않습니다.

예시 **7:**

vVols 데이터 저장소 확장(볼륨 추가)

작업 흐름:

확장 전:

[확장] DS4(lun4): host4(iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

확장 후:

[확장] DS4(lun4, lun5): host4(iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

새로운 LUN이 생성되어 기존 자식 igroup host4Igroup에 매핑됩니다.

예시 **8:**

vVols 데이터 저장소 축소(볼륨 제거)

작업 흐름:

수축 전:

[축소] DS4(lun4, lun5): host4(iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

수축 후:

[축소] DS4(lun4): host4(iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

지정된 LUN(lun5)이 자식 igroup에서 매핑 해제됩니다. igroup은 최소한 하나의 매핑된 LUN이 있는 한 활성 상태를 유지합니다.

예시 **9:**

ONTAP 도구 9에서 10으로 마이그레이션(igroup 정규화)

작업 흐름

VMware vSphere 9.x 버전용 ONTAP 도구는 계층적 igroup을 지원하지 않습니다. 10.3 이상 버전으로 마이그레이션하는 동안 igroup을 계층 구조로 정규화해야 합니다.

이전 전:

[마이그레이션] DS6(lun6, lun7): host6(iqn6), host7(iqn7) → ClassicIgroup1(iqn6 & iqn7 : lun6, lun7)

ONTAP 도구 9.x 로직은 일대일 호스트 매핑을 적용하지 않고도 igroup당 여러 개의 이니시에이터를 허용합니다.

마이그레이션 후:

[마이그레이션] DS6(lun6, lun7): host6(iqn6), host7(iqn7) → ClassicIgroup1: otv_ClassicIgroup1(iqn6 & iqn7: lun6, lun7)

마이그레이션 중:

- 새로운 상위 igroup(ClassicIgroup1)이 생성됩니다.
- 원래 igroup은 otv_ 접두사로 이름이 바뀌고 자식 igroup이 됩니다.

이를 통해 계층적 모델을 준수할 수 있습니다.

관련 주제

"igroups에 대하여"

수출 정책

내보내기 정책은 ONTAP tools for VMware vSphere 에서 NFS 데이터 저장소에 대한 액세스를 제어합니다. 이들은 어떤 클라이언트가 데이터 저장소에 접근할 수 있는지, 그리고 어떤 권한을 가지고 있는지 정의합니다. 내보내기 정책은 ONTAP 시스템에서 생성 및 관리되며 NFS 데이터 저장소와 연결하여 액세스 제어를 시행할 수 있습니다. 각 내보내기 정책은 액세스가 허용되는 클라이언트(IP 주소 또는 서브넷)와 부여되는 권한(읽기 전용 또는 읽기-쓰기)을 지정하는 규칙으로 구성됩니다.

ONTAP tools for VMware vSphere 에서 NFS 데이터 저장소를 생성할 때 기존 내보내기 정책을 선택하거나 새 정책을 생성할 수 있습니다. 그런 다음 내보내기 정책이 데이터 저장소에 적용되어 권한이 있는 클라이언트만 액세스할 수

있도록 합니다.

새로운 ESXi 호스트에 NFS 데이터스토어를 마운트하면 ONTAP tools for VMware vSphere 호스트의 IP 주소를 데이터스토어와 연결된 기존 내보내기 정책에 추가합니다. 이를 통해 새로운 호스트는 새로운 내보내기 정책을 생성하지 않고도 데이터 저장소에 액세스할 수 있습니다.

ESXi 호스트에서 NFS 데이터스토어를 삭제하거나 마운트 해제하면 ONTAP tools for VMware vSphere 내보내기 정책에서 호스트의 IP 주소를 제거합니다. 다른 호스트가 해당 내보내기 정책을 사용하지 않으면 해당 정책은 삭제됩니다. NFS 데이터 저장소를 삭제하면 ONTAP tools for VMware vSphere 다른 데이터 저장소에서 재사용되지 않는 경우 해당 데이터 저장소와 연결된 내보내기 정책을 제거합니다. 내보내기 정책을 재사용하면 호스트 IP 주소가 유지되고 변경되지 않습니다. 데이터 저장소를 삭제하면 내보내기 정책은 호스트 IP 주소를 할당 해제하고 기본 내보내기 정책을 할당하여 필요한 경우 ONTAP 시스템이 해당 IP 주소에 액세스할 수 있도록 합니다.

여러 데이터스토어에서 재사용되는 내보내기 정책 할당 방식은 다릅니다. 내보내기 정책을 재사용할 경우 새 호스트 IP 주소를 정책에 추가할 수 있습니다. 공유 내보내기 정책을 사용하는 데이터스토어를 삭제하거나 마운트 해제해도 정책은 삭제되지 않습니다. 정책은 변경되지 않고 호스트 IP 주소도 제거되지 않습니다. 다른 데이터스토어와 공유되기 때문입니다. 내보내기 정책을 재사용하면 액세스 및 지연 시간 문제가 발생할 수 있으므로 권장하지 않습니다.

관련 주제

"수출 정책 만들기"

ONTAP 도구 관리 igroups 이해

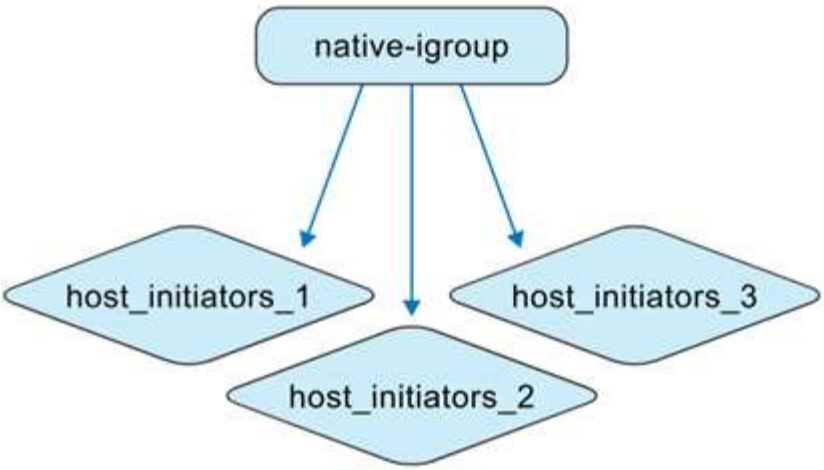
ONTAP 도구 VM과 ONTAP 스토리지 시스템을 모두 관리할 때 igroup 동작을 이해하는 것이 필수적이며, 특히 ONTAP 도구가 아닌 환경에서 ONTAP 도구 관리 환경으로 데이터 저장소를 마이그레이션할 때 더욱 그렇습니다. 이 섹션에서는 이러한 전환 중에 igroup이 어떻게 업데이트되는지 설명합니다.

ONTAP tools for VMware vSphere VMware 데이터 센터 환경 내에서 ONTAP 및 vCenter 객체의 생성과 유지 관리를 자동화하여 데이터 저장소 관리를 간소화합니다.

ONTAP tools for VMware vSphere 두 가지 다른 맥락에서 igroup을 해석합니다.

ONTAP 도구가 아닌 관리되는 igroups

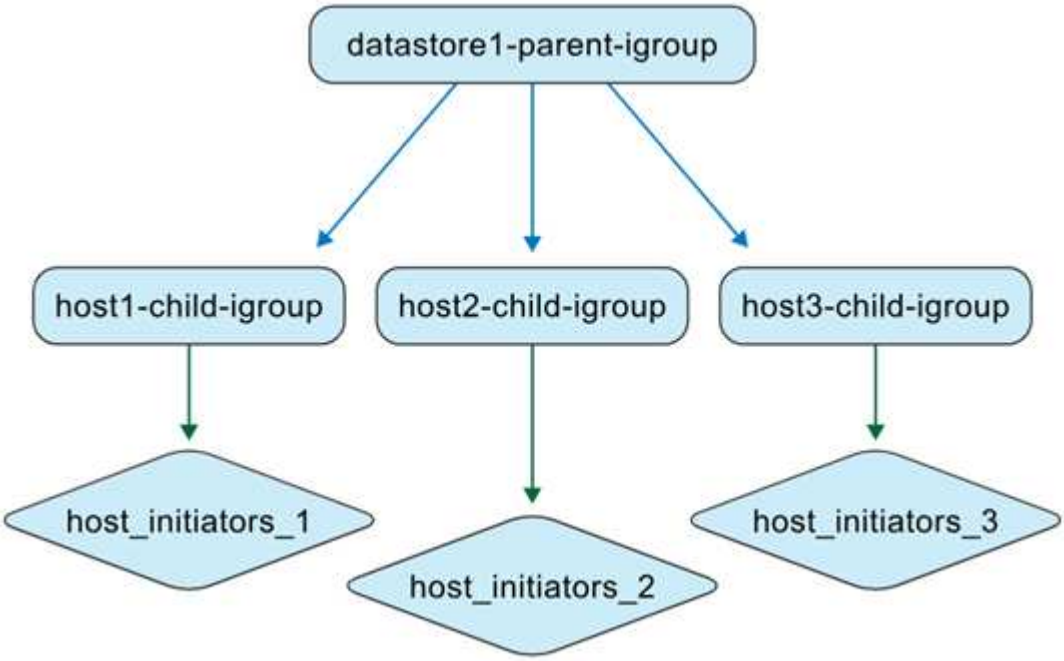
스토리지 관리자는 ONTAP 시스템에서 플랫 또는 중첩 구조로 igroup을 생성할 수 있습니다. 이 그림은 ONTAP 시스템에서 생성된 플랫 igroup을 보여줍니다.

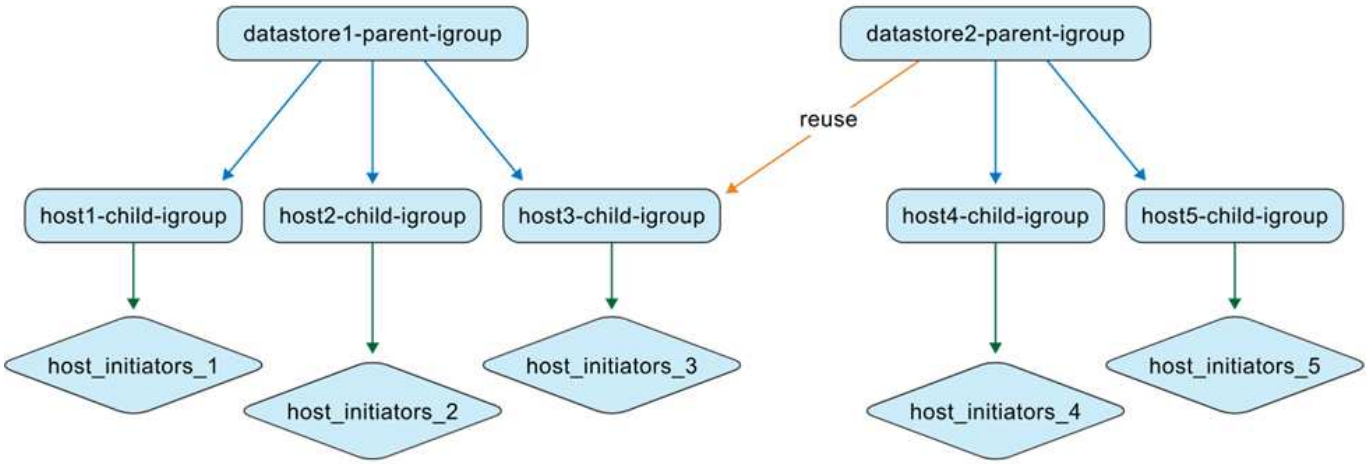


ONTAP 도구로 관리되는 **igroups**

데이터스토어를 생성할 때 ONTAP tools for VMware vSphere LUN 매핑을 더 쉽게 하기 위해 중첩 구조를 사용하여 igroup을 자동으로 생성합니다.

예를 들어, 호스트 1, 2, 3에 datastore1을 생성하여 마운트하고, 호스트 3, 4, 5에 새로운 datastore(datastore2)를 생성하여 마운트하는 경우 ONTAP 도구는 효율적인 관리를 위해 호스트 수준 igroup을 재사용합니다.





다음은 ONTAP tools for VMware vSphere 의 몇 가지 사례입니다.

기본 **igroup** 설정으로 데이터 저장소를 생성하는 경우

데이터 저장소를 생성하고 igroup 필드를 비워 두면(기본 설정), ONTAP 도구가 자동으로 해당 데이터 저장소에 대한 중첩된 igroup 구조를 생성합니다. 데이터 저장소 수준의 상위 igroup은 otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name> 패턴을 사용하여 명명됩니다. 각 호스트 수준 자식 igroup은 otv_<hostMoref>_<vcguid> 패턴을 따릅니다. ONTAP 스토리지 인터페이스의 부모 이니시에이터 그룹 섹션에서 부모(데이터 저장소 수준) igroup과 자식(호스트 수준) igroup 간의 연결을 볼 수 있습니다.

중첩된 igroup 방식을 사용하면 LUN이 자식 igroup에만 매핑됩니다. 그러면 vCenter Server 인벤토리에 새 데이터 저장소가 표시됩니다.

사용자 정의 **igroup** 이름으로 데이터 저장소를 생성하는 경우

ONTAP 도구에서 데이터 저장소를 생성하는 동안 드롭다운에서 선택하는 대신 사용자 정의 igroup 이름을 입력할 수 있습니다. 그런 다음 ONTAP 도구는 지정된 이름을 사용하여 데이터 저장소 수준에서 상위 igroup을 만듭니다. 동일한 호스트가 여러 데이터 저장소에 사용되는 경우 기존 호스트 수준(자식) igroup이 재사용됩니다. 결과적으로 새로운 데이터 저장소의 LUN은 기존 자식 igroup에 매핑되며, 이제 여러 부모 igroup(각 데이터 저장소당 하나씩)과 연결될 수 있습니다. vCenter Server 사용자 인터페이스 데이터 저장소 목록은 사용자 지정 igroup 이름으로 새 데이터 저장소가 성공적으로 생성되었음을 확인합니다.

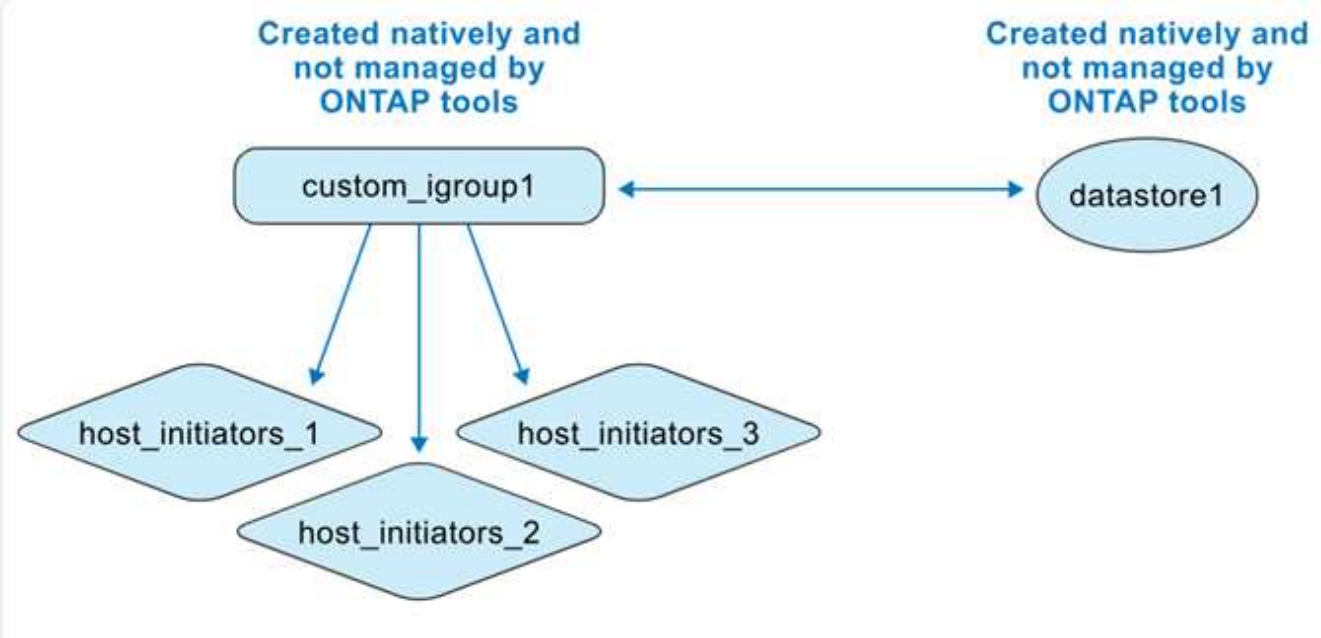
데이터 저장소 생성 중에 **igroup** 이름을 재사용하는 경우

ONTAP 도구 사용자 인터페이스를 사용하여 데이터 저장소를 만들 때 드롭다운 목록에서 기존 사용자 정의 상위 igroup을 선택할 수 있습니다. 부모 igroup을 재사용하여 다른 데이터 저장소를 만든 후 ONTAP 시스템 사용자 인터페이스에 이 연결이 표시됩니다. 새로운 데이터스토어는 vCenter Server 사용자 인터페이스에도 나타납니다.

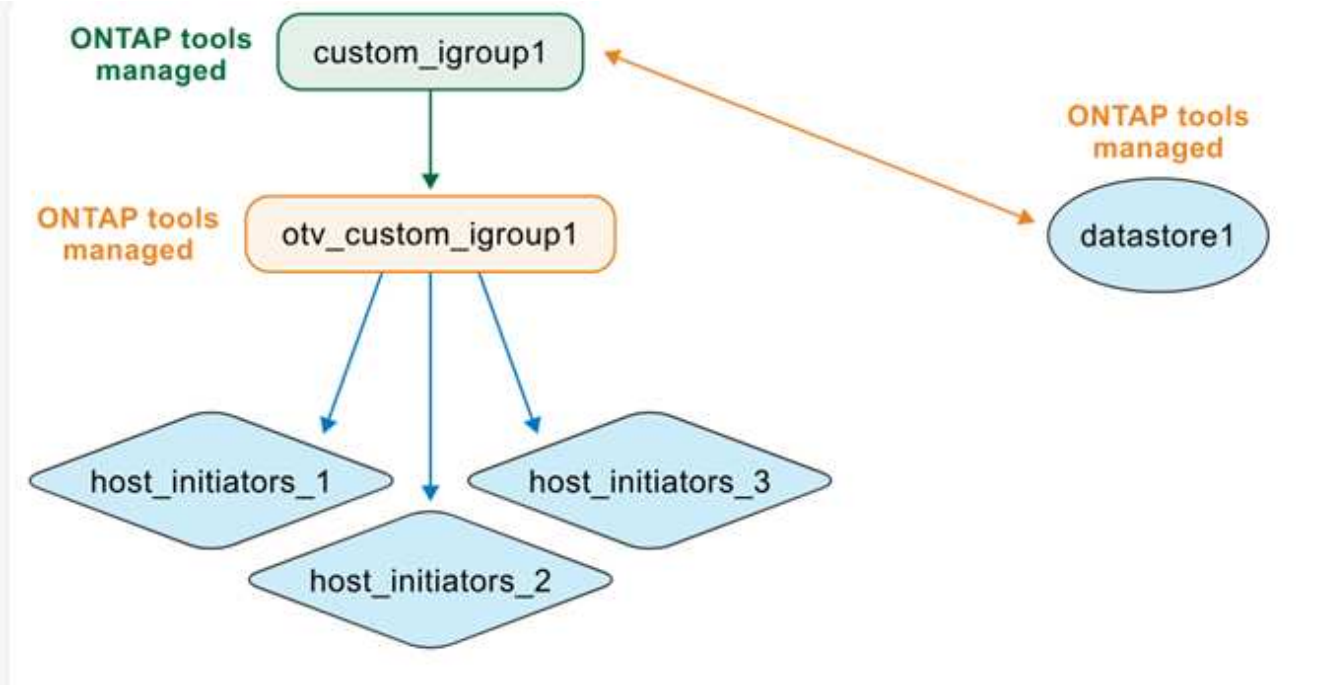
이 작업은 API를 사용하여 수행할 수도 있습니다. 데이터 저장소를 생성하는 동안 기존 igroup을 재사용하려면 API 요청 페이로드에서 igroup UUID를 지정하세요.

- ONTAP 및 vCenter에서 기본적으로 데이터스토어와 igroup을 생성하는 경우*

ONTAP 시스템과 VMware 환경에서 igroup과 데이터스토어를 직접 생성하는 경우 ONTAP 도구는 처음에는 이러한 객체를 관리하지 않습니다. 이렇게 하면 평평한 igroup 구조가 생성됩니다.



ONTAP 도구를 사용하여 기존 데이터 저장소와 igroup을 관리하려면 데이터 저장소 검색을 수행해야 합니다. ONTAP 도구는 데이터 저장소와 igroup을 식별하고 등록하며, 이를 데이터베이스의 중첩 구조로 변환합니다. 사용자 지정 이름을 사용하여 새로운 부모 igroup이 생성되고, 기존 igroup의 이름은 "otv_" 접두사로 바뀌고 자식 igroup이 됩니다. 개시자 매핑은 변경되지 않습니다. 검색 중에는 데이터 저장소에 매핑된 igroup만 변환됩니다. 이후의 igroup 구조는 아래 그림과 같습니다.



vCenter Server에서 직접 데이터스토어를 생성한 후 나중에 ONTAP 도구로 관리할 수 있습니다. 먼저 ONTAP 시스템에서 플랫 igroup을 만들고 여기에 LUN을 매핑합니다. ONTAP 도구에서 데이터 저장소 검색을 실행한 후 플랫 igroup이 중첩 구조로 변환됩니다. 그런 다음 ONTAP 도구는 igroup을 관리하고 'otv_' 접두사로 이름을 바꿉니다. LUN은 이 프로세스 내내 동일한 igroup에 매핑된 상태로 유지됩니다.

- ONTAP 도구가 기본적으로 생성된 igroup을 재사용하는 방식*

ONTAP 도구에서 데이터 저장소를 프로비저닝하려면 ONTAP 시스템에서 생성된 igroup을 사용하고 ONTAP 도구에서

관리하면 됩니다. 이러한 igroup은 사용자 정의 이니시에이터 그룹 이름 드롭다운 목록에 나타납니다. 그런 다음 데이터 저장소의 새 LUN은 "otv_NativeIgroup1"과 같은 해당 정규화된 자식 igroup에 매핑됩니다.

ONTAP tools for VMware vSphere ONTAP 도구에서 관리되지 않거나 데이터 저장소에 연결되지 않은 ONTAP 시스템에서 생성된 igroup을 감지하거나 사용하지 않습니다.

ONTAP tools for VMware vSphere 활성화

ONTAP 도구 관리자를 사용하여 관리자 비밀번호를 변경하면 ONTAP 도구 관리자를 사용하여 VASA 공급자, vVols 구성 가져오기, 재해 복구(SRA)와 같은 서비스를 활성화할 수 있습니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 개요 섹션에서 *기기 설정 편집*을 선택하세요.
4. 서비스 섹션에서는 요구 사항에 따라 VASA 공급자, vVols 구성 가져오기, 재해 복구(SRA)와 같은 선택적 서비스를 활성화할 수 있습니다.

   처음으로 서비스를 활성화할 때 VASA 공급자 및 SRA 자격 증명을 만들어야 합니다. 이는 vCenter Server에서 VASA 공급자 및 SRA 서비스를 등록하거나 활성화하는 데 사용됩니다. 사용자 이름에는 문자, 숫자, 밑줄만 사용할 수 있습니다. 비밀번호 길이는 8자에서 256자 사이여야 합니다.

   > 선택적 서비스를 비활성화하기 전에 ONTAP 도구에서 관리하는 vCenter Server가 해당 서비스를 사용하지 않는지 확인하세요.

   - vVols 구성 가져오기 허용* 옵션은 VASA 공급자 서비스가 활성화된 경우에만 표시됩니다. 이 옵션을 사용하면 ONTAP 도구 9.xx에서 ONTAP 도구 10.4로 vVols 데이터를 마이그레이션할 수 있습니다.

ONTAP tools for VMware vSphere 변경

ONTAP 도구 관리자를 사용하여 ONTAP tools for VMware vSphere 확장하여 배포에서 노드 수를 늘리거나 구성을 고가용성(HA) 설정으로 변경합니다. ONTAP tools for VMware vSphere 처음에는 단일 노드 비 HA 구성으로 배포됩니다.

> 비HA 백업이 활성화된 경우 HA로 마이그레이션하려면 먼저 백업을 비활성화한 다음 마이그레이션 후 다시 활성화하세요.

시작하기 전에

- OVA 템플릿의 OVA 버전이 노드 1과 동일한지 확인하세요. 노드 1은 ONTAP tools for VMware vSphere 처음 배포되는 기본 노드입니다.
- CPU 핫 애드와 메모리 핫 플러그가 활성화되어 있는지 확인하세요.
- vCenter Server에서 재해 복구 서비스(DRS) 자동화 수준을 부분 자동화로 설정합니다. HA를 배포한 후 완전 자동화로 되돌립니다.
- HA 설정의 노드 호스트 이름은 소문자여야 합니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 개요 섹션에서 *기기 설정 편집*을 선택하세요.
4. 구성 섹션에서는 요구 사항에 따라 노드 크기를 늘리고 HA 구성을 활성화할 수 있습니다. 변경하려면 vCenter Server 자격 증명이 필요합니다.

   ONTAP 도구가 HA 구성에 있는 경우 콘텐츠 라이브러리 세부 정보를 변경할 수 있습니다. 새로운 편집 내용을 제출할 때는 비밀번호를 다시 입력해야 합니다.

   > ONTAP tools for VMware vSphere 에서는 노드 크기를 늘릴 수만 있고, 노드 크기를 줄일 수는 없습니다. HA가 아닌 설정에서는 중간 크기 구성만 지원됩니다. HA 설정에서는 중간 및 대규모 구성이 지원됩니다.

5. HA 토글 버튼을 사용하여 HA 구성을 활성화합니다. **HA** 설정 페이지에서 다음 사항을 확인하세요.
   - 콘텐츠 라이브러리는 ONTAP 도구 노드 VM이 실행되는 동일한 vCenter Server에 속합니다. vCenter Server 자격 증명은 어플라이언스 변경 사항에 대한 OVA 템플릿의 유효성을 검사하고 다운로드하는 데 사용됩니다.
   - ONTAP 도구를 호스팅하는 가상 머신은 ESXi 호스트에 직접 배포되지 않습니다. VM은 클러스터나 리소스 풀에 배포되어야 합니다.

     > HA 구성이 활성화된 후에는 HA가 아닌 단일 노드 구성으로 되돌릴 수 없습니다.

6. 어플라이언스 설정 편집 창의 **HA** 설정 섹션에서 노드 2와 3의 세부 정보를 입력할 수 있습니다. ONTAP tools for VMware vSphere HA 설정에서 세 개의 노드를 지원합니다.

   > 대부분의 입력 옵션에는 작업 흐름을 편리하게 하기 위해 노드 1 네트워크 세부 정보가 미리 입력되어 있습니다. 하지만 마법사의 마지막 페이지로 이동하기 전에 입력 데이터를 편집할 수 있습니다. 첫 번째 노드에서 IPv6 주소가 활성화된 경우에만 다른 두 노드에 대한 IPv6 주소 세부 정보를 입력할 수 있습니다.

   ESXi 호스트에 ONTAP 도구 VM이 하나만 있는지 확인하세요. 다음 창으로 넘어갈 때마다 입력 내용이 검증됩니다.

7. 요약 섹션에서 세부 정보를 검토하고 변경 사항을 *저장*합니다.

다음은 무엇인가요**?**

개요 페이지는 배포 상태를 보여줍니다. 작업 ID를 사용하면 작업 보기에서 편집 기기 설정 작업 상태를 추적할 수도 있습니다.

HA 배포에 실패하고 새 노드의 상태가 '신규'로 표시되는 경우 HA 활성화 작업을 다시 시도하기 전에 vCenter에서 새 VM을 삭제하세요.

왼쪽 패널의 알림 탭에는 ONTAP tools for VMware vSphere 에 대한 알림이 나열됩니다.

데이터 저장소 관리

NFS 및 VMFS 데이터 저장소 마운트

데이터스토어를 마운트하면 추가 호스트에 대한 스토리지 액세스가 제공됩니다. VMware 환경에 호스트를 추가한 후 추가 호스트에 데이터스토어를 마운트할 수 있습니다.

이 작업에 관하여

- 일부 마우스 오른쪽 버튼 클릭 작업은 vSphere 클라이언트 버전과 선택한 데이터 저장소 유형에 따라 비활성화되거나 사용할 수 없습니다.
  - vSphere Client 8.0 이상 버전을 사용하는 경우 일부 마우스 오른쪽 버튼 클릭 옵션이 숨겨져 있습니다.
  - vSphere 7.0U3부터 vSphere 8.0 버전까지는 옵션이 나타나더라도 작업이 비활성화됩니다.
- 호스트 클러스터가 균일한 구성으로 보호되는 경우 마운트 데이터 저장소 옵션이 비활성화됩니다.

단계

1. vSphere Client 홈페이지에서 *호스트 및 클러스터*를 선택합니다.
2. 왼쪽 탐색 창에서 호스트가 포함된 데이터 센터를 선택합니다.
3. 호스트 또는 호스트 클러스터에 NFS/VMFS 데이터 저장소를 마운트하려면 마우스 오른쪽 버튼을 클릭하고 *NetApp ONTAP 도구* > *데이터 저장소 마운트*를 선택합니다.
4. 마운트하려는 데이터스토어를 선택하고 *마운트*를 선택합니다.

다음은 무엇인가요**?**

최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

NFS 및 VMFS 데이터 저장소 마운트 해제

데이터 저장소 마운트 해제 작업은 ESXi 호스트에서 NFS 또는 VMFS 데이터 저장소를 마운트 해제합니다. ONTAP tools for VMware vSphere 에서 검색되거나 관리되는 NFS 및 VMFS 데이터 저장소에 대해 데이터 저장소 마운트 해제 작업이 활성화됩니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. NFS 또는 VMFS 데이터 저장소 객체를 마우스 오른쪽 버튼으로 클릭하고 *데이터 저장소 마운트 해제*를 선택합니다.

   대화 상자가 열리고 데이터스토어가 마운트된 ESXi 호스트가 나열됩니다. 보호된 데이터 저장소에서 작업을 수행하면 화면에 경고 메시지가 표시됩니다.

3. 데이터스토어를 마운트 해제하려면 하나 이상의 ESXi 호스트를 선택하세요.

   모든 호스트에서 데이터스토어를 마운트 해제할 수는 없습니다. 사용자 인터페이스에서는 대신 데이터 저장소 삭제 작업을 사용할 것을 제안합니다.

4. 마운트 해제 버튼을 선택하세요.

데이터 저장소가 보호된 호스트 클러스터의 일부인 경우 경고 메시지가 표시됩니다.

> 보호된 데이터 저장소가 마운트 해제된 경우 기존 보호 설정으로 인해 부분 보호가 발생할 수 있습니다. 다음을 참조하세요. "보호된 호스트 클러스터 수정" 완벽한 보호를 가능하게 합니다.

다음은 무엇인가요?

최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

vVols 데이터 저장소 마운트

하나 이상의 추가 호스트에 VMware Virtual Volumes(vVols) 데이터 저장소를 마운트하여 추가 호스트에 대한 스토리지 액세스를 제공할 수 있습니다. API를 통해서만 vVols 데이터 저장소를 마운트 해제할 수 있습니다.

단계

1. vSphere Client 홈페이지에서 *호스트 및 클러스터*를 선택합니다.
2. 탐색 창에서 데이터 저장소가 포함된 데이터 센터를 선택합니다.
3. 데이터 저장소를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *데이터 저장소 마운트*를 선택합니다.
4. 호스트에 데이터스토어 마운트 대화 상자에서 데이터스토어를 마운트할 호스트를 선택한 다음 *마운트*를 선택합니다.

최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

NFS 및 VMFS 데이터 저장소 크기 조정

데이터스토어 크기를 조정하면 가상 머신 파일의 저장 공간을 늘릴 수 있습니다. 인프라 요구 사항이 변경되면 데이터 저장소의 크기를 변경할 수 있습니다.

이 작업에 관하여

NFS 및 VMFS 데이터 저장소의 크기만 늘릴 수 있습니다. NFS 및 VMFS 데이터 저장소의 일부인 FlexVol volume 기존 크기보다 작아질 수 없지만 최대 120%까지 커질 수 있습니다.

단계

1. vSphere Client 홈페이지에서 *호스트 및 클러스터*를 선택합니다.
2. 탐색 창에서 데이터 저장소가 포함된 데이터 센터를 선택합니다.
3. NFS 또는 VMFS 데이터 저장소를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *데이터 저장소 크기 조정*을 선택합니다.
4. 크기 조정 대화 상자에서 데이터 저장소의 새 크기를 지정하고 *확인*을 선택합니다.

vVols 데이터 저장소 확장

vCenter 개체 보기에서 데이터스토어 개체를 마우스 오른쪽 버튼으로 클릭하면 ONTAP tools for VMware vSphere 플러그인 섹션 아래에 표시됩니다. 특정 작업은 데이터 저장소 유형과

현재 사용자 권한에 따라 활성화됩니다.

> vVols 데이터 저장소 확장 작업은 ASA r2 시스템 기반 vVols 데이터 저장소에는 적용되지 않습니다.

단계

1. vSphere Client 홈페이지에서 *호스트 및 클러스터*를 선택합니다.
2. 탐색 창에서 데이터 저장소가 포함된 데이터 센터를 선택합니다.
3. 데이터 저장소를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *데이터 저장소에 스토리지 추가*를 선택합니다.
4. 볼륨 생성 또는 선택 창에서 새 볼륨을 생성하거나 기존 볼륨에서 선택할 수 있습니다. 사용자 인터페이스는 설명이 필요 없을 정도로 명확합니다. 귀하의 선택에 따라 지침을 따르세요.
5. 요약 창에서 선택 사항을 검토하고 *확장*을 선택합니다. 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

vVols 데이터 저장소 축소

데이터 저장소 삭제 작업은 선택한 데이터 저장소에 vVols 없는 경우 데이터 저장소를 삭제합니다.

> ASA r2 시스템 기반 vVols 데이터 저장소에서는 vVols 데이터 저장소 축소 작업이 지원되지 않습니다.

단계

1. vSphere Client 홈페이지에서 *호스트 및 클러스터*를 선택합니다.
2. 탐색 창에서 데이터 저장소가 포함된 데이터 센터를 선택합니다.
3. vVol 데이터 저장소를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *데이터 저장소에서 저장소 제거*를 선택합니다.
4. vVols 없는 볼륨을 선택하고 *제거*를 선택합니다.

   > vVols 가 상주하는 볼륨을 선택하는 옵션이 비활성화되었습니다.

5. 저장소 제거 팝업에서 * ONTAP 클러스터에서 볼륨 삭제* 확인란을 선택하여 데이터 저장소와 ONTAP 저장소에서 볼륨을 삭제하고 *삭제*를 선택합니다.

데이터 저장소 삭제

데이터 저장소에서 저장소 제거 작업은 vCenter Server에서 VMware vSphere가 검색하거나 관리하는 vVols 데이터 저장소에 ONTAP tools for VMware vSphere 에서 지원됩니다. 이 작업을 수행하면 vVols 데이터 저장소에서 볼륨을 제거할 수 있습니다.

특정 볼륨에 vVols 있는 경우 제거 옵션이 비활성화됩니다. 데이터 저장소에서 볼륨을 제거하는 것 외에도 ONTAP 스토리지에서 선택한 볼륨을 삭제할 수 있습니다.

vCenter Server의 ONTAP tools for VMware vSphere 에서 데이터 저장소 삭제 작업은 다음을 수행합니다.

- vVol 컨테이너를 마운트 해제합니다.

- igroup을 정리합니다. igroup을 사용하지 않으면 igroup에서 iqn을 제거합니다.
- Vvol 컨테이너를 삭제합니다.
- Flex 볼륨을 스토리지 어레이에 그대로 둡니다.

vCenter Server의 ONTAP 도구에서 NFS, VMFS 또는 vVOL 데이터스토어를 삭제하려면 아래 단계를 따르세요.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 호스트 시스템이나 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *데이터 저장소 삭제*를 선택합니다.

   해당 데이터스토어를 사용하는 가상 머신이 있는 경우 해당 데이터스토어를 삭제할 수 없습니다. 데이터 저장소를 삭제하기 전에 가상 머신을 다른 데이터 저장소로 옮겨야 합니다. 데이터 저장소가 보호된 호스트 클러스터에 속하는 경우 볼륨 삭제 확인란을 선택할 수 없습니다.

   a. NFS 또는 VMFS 데이터 저장소의 경우 데이터 저장소를 사용 중인 VM 목록이 있는 대화 상자가 나타납니다.
   b. VMFS 데이터 저장소가 ASA r2 시스템에 생성되었고 보호의 일부인 경우, 데이터 저장소를 삭제하기 전에 보호를 해제해야 합니다.
   c. vVols 데이터 저장소의 경우, 데이터 저장소 삭제 작업은 연관된 vVols 없을 때만 데이터 저장소를 삭제합니다. 데이터 저장소 삭제 대화 상자는 ONTAP 클러스터에서 볼륨을 삭제하는 옵션을 제공합니다.
   d. ASA r2 시스템 기반 vVols 데이터 저장소의 경우 백업 볼륨을 삭제하는 체크박스는 적용되지 않습니다.
3. ONTAP 스토리지의 백업 볼륨을 삭제하려면 * ONTAP 클러스터의 볼륨 삭제*를 선택합니다.

   보호된 호스트 클러스터의 일부인 VMFS 데이터 저장소에 대한 ONTAP 클러스터의 볼륨을 삭제할 수 없습니다.

데이터 저장소에 대한 **ONTAP** 스토리지 뷰

ONTAP tools for VMware vSphere 구성 탭에서 데이터스토어와 볼륨의 ONTAP 스토리지 측면 보기를 보여줍니다.

단계

1. vSphere 클라이언트에서 데이터스토어로 이동합니다.
2. 오른쪽 창에서 구성 탭을 선택합니다.
3. * NetApp ONTAP 도구* > * ONTAP 스토리지*를 선택합니다. 데이터 저장소 유형에 따라 뷰가 변경됩니다. 자세한 내용은 아래 표를 참조하세요.

데이터 저장소 유형	정보 제공
NFS 데이터 저장소	저장소 세부 정보 페이지에는 저장소 백엔드, 집계 및 볼륨 정보가 포함되어 있습니다. **NFS** 세부 정보 페이지에는 NFS 데이터 저장소와 관련된 데이터가 포함되어 있습니다.

VMFS 데이터 저장소	저장소 세부 정보 페이지에는 저장소 백엔드, 집계, 볼륨 및 저장소 가용성 영역(SAZ) 세부 정보가 포함되어 있습니다. 보관소 세부정보 페이지에는 보관소의 세부정보가 포함되어 있습니다.
vVols 데이터 저장소	모든 볼륨을 나열합니다. ONTAP 스토리지 창에서 스토리지를 확장하거나 제거할 수 있습니다. 이 보기는 ASA r2 시스템 기반 vVols 데이터 저장소에서는 지원되지 않습니다.

가상 머신 스토리지 보기

저장소 보기에는 가상 머신에서 생성된 vVols 목록이 표시됩니다.

> 이 보기는 VMware vSphere 관리 vVols 데이터 저장소 관련 디스크에 대한 ONTAP tools for VMware vSphere 하나 이상 마운트된 VM에 적용할 수 있습니다.

단계

1. vSphere Client에서 가상 머신으로 이동합니다.
2. 오른쪽 창에서 모니터 탭을 선택합니다.
3. * NetApp ONTAP 도구* > 스토리지*를 선택합니다. *저장소 세부정보가 오른쪽 창에 나타납니다. VM에 있는 vVols 목록을 볼 수 있습니다.

   '열 관리' 옵션을 사용하면 다른 열을 숨기거나 표시할 수 있습니다.

저장 임계값 관리

볼륨과 집계 용량이 특정 수준에 도달하면 vCenter Server에서 알림을 받을 임계값을 설정할 수 있습니다.

단계:

1. vSphere 클라이언트에 로그인합니다.
2. 바로가기 페이지에서 플러그인 섹션 아래에 있는 * NetApp ONTAP 도구*를 선택합니다.
3. ONTAP 도구의 왼쪽 창에서 설정 > 임계값 설정 > *편집*으로 이동합니다.
4. 임계값 편집 창에서 거의 가득 참 및 가득 참 필드에 원하는 값을 입력하고 *저장*을 선택합니다. 권장 값으로 숫자를 재설정할 수 있습니다. 권장 값은 거의 가득 찬 경우 80, 가득 찬 경우 90입니다.

스토리지 백엔드 관리

스토리지 백엔드는 ESXi 호스트가 데이터를 저장하는 데 사용하는 시스템입니다.

스토리지를 발견하세요

예약된 검색으로 스토리지 세부 정보가 업데이트될 때까지 기다리지 않고도 필요에 따라 스토리지 백엔드 검색을 실행할 수 있습니다.

아래 단계에 따라 스토리지 백엔드를 찾아보세요.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 바로가기 페이지에서 플러그인 섹션 아래에 있는 * NetApp ONTAP 도구*를 선택합니다.
3. ONTAP 도구의 왼쪽 창에서 *스토리지 백엔드*로 이동하여 스토리지 백엔드를 선택합니다.
4. 세로 줄임표 메뉴를 선택하고 *저장소 검색*을 선택하세요.

최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

스토리지 백엔드 수정

이 섹션의 단계에 따라 스토리지 백엔드를 수정하세요.

1. vSphere 클라이언트에 로그인합니다.
2. 바로가기 페이지에서 플러그인 섹션 아래에 있는 * NetApp ONTAP 도구*를 선택합니다.
3. ONTAP 도구의 왼쪽 창에서 *스토리지 백엔드*로 이동하여 스토리지 백엔드를 선택합니다.
4. 수직 타원 메뉴를 선택하고 *수정*을 선택하여 자격 증명이나 포트 이름을 수정합니다. 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

다음 단계에 따라 ONTAP 도구 관리자를 사용하여 글로벌 ONTAP 클러스터에 대한 수정 작업을 수행할 수 있습니다.

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다. `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 사이드바에서 스토리지 백엔드를 선택하세요.
4. 수정하려는 스토리지 백엔드를 선택하세요.
5. 세로 줄임표 메뉴를 선택하고 *수정*을 선택합니다.
6. 자격 증명이나 포트를 수정할 수 있습니다. 스토리지 백엔드를 수정하려면 *사용자 이름*과 *비밀번호*를 입력하세요.

스토리지 백엔드 제거

스토리지 백엔드를 제거하기 전에 스토리지 백엔드에 연결된 모든 데이터스토어를 삭제해야 합니다. 스토리지 백엔드를 제거하려면 아래 단계를 따르세요.

1. vSphere 클라이언트에 로그인합니다.
2. 바로가기 페이지에서 플러그인 섹션 아래에 있는 * NetApp ONTAP 도구*를 선택합니다.
3. ONTAP 도구의 왼쪽 창에서 *스토리지 백엔드*로 이동하여 스토리지 백엔드를 선택합니다.
4. 세로 줄임표 메뉴를 선택하고 *제거*를 선택합니다. 스토리지 백엔드에 데이터스토어가 포함되어 있지 않은지 확인하세요. 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

ONTAP 도구 관리자를 사용하여 글로벌 ONTAP 클러스터에 대한 제거 작업을 수행할 수 있습니다.

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 사이드바에서 *스토리지 백엔드*를 선택합니다.
4. 제거할 스토리지 백엔드를 선택하세요
5. 세로 줄임표 메뉴를 선택하고 *제거*를 선택합니다.

스토리지 백엔드의 드릴다운 보기

스토리지 백엔드 페이지에는 모든 스토리지 백엔드가 나열되어 있습니다. 클러스터 아래의 개별 자식 SVM이 아닌, 추가한 스토리지 백엔드에서 스토리지 검색, 수정 및 제거 작업을 수행할 수 있습니다.

스토리지 백엔드에서 부모 클러스터나 자식 클러스터를 선택하면 해당 구성 요소의 전반적인 요약을 볼 수 있습니다. 부모 클러스터를 선택하면 저장소 검색, 수정, 제거 작업을 수행할 수 있는 작업 드롭다운이 표시됩니다.

요약 페이지에는 다음과 같은 세부 정보가 제공됩니다.

- 스토리지 백엔드의 상태
- 용량 정보
- VM에 대한 기본 정보
- IP 주소, 네트워크 포트와 같은 네트워크 정보입니다. 자식 SVM의 경우 정보는 부모 스토리지 백엔드와 동일합니다.
- 저장소 백엔드에 허용되고 제한되는 Privileges . 자식 SVM의 경우 정보는 부모 스토리지 백엔드와 동일합니다. Privileges 클러스터 기반 스토리지 백엔드에만 표시됩니다. SVM을 스토리지 백엔드로 추가하면 권한 정보가 표시되지 않습니다.
- SVM 또는 클러스터에 대해 분리 속성이 "true"로 설정된 경우 ASA r2 시스템 클러스터 드릴다운 보기에는 로컬 계층 탭이 포함되지 않습니다.
- ASA r2 SVM 시스템의 경우 용량 포틀릿이 표시되지 않습니다. 용량 포털은 SVM 또는 클러스터에 대해 분리 속성이 "true"로 설정된 경우에만 필요합니다.
- ASA r2 SVM 시스템의 경우 기본 정보 섹션에 플랫폼 유형이 표시됩니다.

인터페이스 탭은 인터페이스에 대한 자세한 정보를 제공합니다.

로컬 티어 탭은 집계 목록에 대한 자세한 정보를 제공합니다.

vCenter Server 인스턴스 관리

vCenter Server 인스턴스는 호스트, 가상 머신, 스토리지 백엔드를 제어할 수 있는 중앙 관리 플랫폼입니다.

vCenter Server 인스턴스와 스토리지 백엔드 연결 해제

vCenter Server 목록 페이지에는 연관된 스토리지 백엔드 수가 표시됩니다. 각 vCenter Server 인스턴스에는 스토리지 백엔드와 연결하거나 연결 해제하는 옵션이 있습니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 사이드바에서 필요한 vCenter Server 인스턴스를 선택합니다.
4. 스토리지 백엔드와 연결하거나 연결 해제하려는 vCenter Server에 대한 세로 줄임표를 선택합니다.
5. *저장소 백엔드 분리*를 선택합니다.

vCenter Server 인스턴스 수정

vCenter Server 인스턴스를 수정하려면 아래 단계를 따르세요.

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 사이드바에서 해당 vCenter Server 인스턴스를 선택하세요.
4. 수정하려는 vCenter Server에 대한 세로 줄임표를 선택하고 *수정*을 선택합니다.
5. vCenter Server 인스턴스 세부 정보를 수정하고 *수정*을 선택합니다.

vCenter Server 인스턴스 제거

vCenter Server를 제거하기 전에 해당 서버에 연결된 모든 스토리지 백엔드를 제거해야 합니다.

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 사이드바에서 해당 vCenter Server 인스턴스를 선택하세요.
4. 제거하려는 vCenter Server에 대한 세로 줄임표를 선택하고 *제거*를 선택합니다.

> vCenter Server 인스턴스를 제거하면 애플리케이션에서 더 이상 유지 관리되지 않습니다.

ONTAP 도구에서 vCenter Server 인스턴스를 제거하면 다음 작업이 자동으로 수행됩니다.

- 플러그인이 등록되지 않았습니다.
- 플러그인 권한과 플러그인 역할이 제거됩니다.

인증서 관리

배포 중에 ONTAP 도구와 VASA 공급자에 대한 자체 서명 인증서가 기본적으로 생성됩니다. ONTAP 도구 관리자 인터페이스를 사용하면 인증서를 갱신하거나 사용자 정의 CA로 업그레이드할 수 있습니다. 다중 vCenter 배포에서는 사용자 지정 CA 인증서가 필수입니다.

시작하기 전에

- 인증서가 발급된 도메인 이름은 가상 IP 주소에 매핑되어야 합니다.
- 도메인 이름에 대해 nslookup 검사를 실행하여 도메인이 의도한 IP 주소로 확인되는지 확인합니다.
- 인증서는 도메인 이름과 ONTAP 도구 IP 주소로 생성해야 합니다.

ONTAP 도구 IP 주소는 정규화된 도메인 이름(FQDN)에 매핑되어야 합니다. 인증서에는 주체 또는 주체 대체 이름에 ONTAP 도구 IP 주소에 매핑된 동일한 FQDN이 포함되어야 합니다.

CA 서명 인증서에서 자체 서명 인증서로 전환할 수 없습니다.

ONTAP 도구 인증서 업그레이드

ONTAP 도구 탭에는 인증서 유형(자체 서명/CA 서명) 및 도메인 이름과 같은 세부 정보가 표시됩니다. 배포하는 동안 기본적으로 자체 서명된 인증서가 생성됩니다. 인증서를 갱신하거나 CA로 업그레이드할 수 있습니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 인증서 > * ONTAP 도구* > *갱신*을 선택하여 인증서를 갱신합니다.

   인증서가 만료되었거나 만료일이 다가오는 경우 인증서를 갱신할 수 있습니다. 인증서 유형이 CA 서명인 경우 갱신 옵션을 사용할 수 있습니다. 팝업 창에서 서버 인증서, 개인 키, 루트 CA 및 중간 인증서 세부 정보를 제공합니다.

   > 인증서가 갱신될 때까지 시스템은 오프라인 상태가 되며, ONTAP 도구 관리자 인터페이스에서 로그아웃됩니다.

4. 자체 서명된 인증서를 사용자 지정 CA 인증서로 업그레이드하려면 인증서 > * ONTAP 도구* > **CA**로 업그레이드 옵션을 선택합니다.
   a. 팝업 창에서 서버 인증서, 서버 인증서 개인 키, 루트 CA 인증서, 중간 인증서 파일을 업로드합니다.
   b. 이 인증서를 생성한 도메인 이름을 입력하고 인증서를 업그레이드하세요.

   > 업그레이드가 완료될 때까지 시스템은 오프라인 상태가 되며, ONTAP 도구 관리자 인터페이스에서 로그아웃됩니다.

VASA 공급자 인증서 업그레이드

ONTAP tools for VMware vSphere VASA Provider에 대한 자체 서명 인증서와 함께 배포됩니다. 이를 통해 vVols 데이터스토어에 대해 단 하나의 vCenter Server 인스턴스만 관리할 수 있습니다. 여러 vCenter Server 인스턴스를 관리하고 해당 인스턴스에서 vVols 기능을 활성화하려면 자체 서명된 인증서를 사용자 지정 CA 인증서로 변경해야 합니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 인증서 > **VASA** 공급자 또는 * ONTAP 도구* > *갱신*을 선택하여 인증서를 갱신합니다.
4. 인증서 > **VASA** 공급자 또는 * ONTAP 도구* > *CA로 업그레이드*를 선택하여 자체 서명 인증서를 사용자 지정 CA 인증서로 업그레이드합니다.
   a. 팝업 창에서 서버 인증서, 서버 인증서 개인 키, 루트 CA 인증서, 중간 인증서 파일을 업로드합니다.
   b. 이 인증서를 생성한 도메인 이름을 입력하고 인증서를 업그레이드하세요.

   > 업그레이드가 완료될 때까지 시스템은 오프라인 상태가 되며, ONTAP 도구 관리자 인터페이스에서 로그아웃됩니다.

ONTAP tools for VMware vSphere 에 액세스하세요

ONTAP tools for VMware vSphere 개요

ONTAP 도구의 유지 관리 콘솔을 사용하여 애플리케이션, 시스템 및 네트워크 구성을 관리할 수 있습니다. 관리자 비밀번호와 유지 관리 비밀번호를 변경할 수 있습니다. 지원 번들을 생성하고, 다양한 로그 수준을 설정하고, TLS 구성을 보고 관리하고, 원격 진단을 시작할 수도 있습니다.

ONTAP tools for VMware vSphere 배포한 후 유지 관리 콘솔에 액세스하려면 VMware 도구가 설치되어 있어야 합니다. 당신은 사용해야 합니다 `maint` ONTAP 도구의 유지 관리 콘솔에 로그인하기 위해 배포 중에 구성한 사용자 이름과 비밀번호입니다. 유지 관리 또는 루트 로그인 콘솔에서 파일을 편집하려면 *nano*를 사용해야 합니다.

> 비밀번호를 설정해야 합니다. `diag` 원격 진단을 활성화하는 동안 사용자입니다.

ONTAP tools for VMware vSphere 의 요약 탭을 사용하여 유지 관리 콘솔에 액세스해야 합니다. 선택할 때 , 유지관리 콘솔이 시작됩니다.

콘솔 메뉴	옵션
애플리케이션 구성	1. 서버 상태 요약 표시 2. VASA Provider Services 및 SRA Services에 대한 LOG 수준 변경
시스템 구성	1. 가상 머신 재부팅 2. 가상 머신 종료 3. 'maint' 사용자 비밀번호 변경 4. 시간대 변경 5. 감옥 디스크 크기 늘리기(/jail) 6. 치받이 7. VMware 도구 설치
네트워크 구성	1. IP 주소 설정 표시 2. 도메인 이름 검색 설정 표시 3. 도메인 이름 검색 설정 변경 4. 정적 경로 표시 5. 정적 경로 변경 6. 변경 사항 커밋 7. 호스트에 ping 보내기 8. 기본 설정 복원

지원 및 진단	1. 진단 셸에 액세스 2. 원격 진단 액세스 활성화 3. 백업을 위한 vCenter 자격 증명 제공 4. 백업을 하세요

원격 진단 액세스 구성

ONTAP tools for VMware vSphere 구성하여 diag 사용자의 SSH 액세스를 활성화할 수 있습니다.

시작하기 전에

vCenter Server 인스턴스에 대해 VASA 공급자 확장 기능을 활성화해야 합니다.

이 작업에 관하여

SSH를 사용하여 diag 사용자 계정에 액세스하는 데는 다음과 같은 제한이 있습니다.

- SSH를 활성화할 때마다 로그인 계정은 하나만 허용됩니다.
- 다음 중 하나가 발생하면 diag 사용자 계정에 대한 SSH 액세스가 비활성화됩니다.
  - 시간이 만료되었습니다.

    로그인 세션은 다음 날 자정까지만 유효합니다.

  - SSH를 사용하여 다시 diag 사용자로 로그인합니다.

단계

1. vCenter Server에서 VASA Provider에 대한 콘솔을 엽니다.
2. 유지 관리 사용자로 로그인합니다.
3. 입력하다 `4` 지원 및 진단을 선택하세요.
4. 입력하다 `2` 원격 진단 액세스 사용을 선택합니다.
5. 입력하다 `y` 원격 진단 액세스를 활성화하려면 확인 대화 상자를 사용하세요.
6. 원격 진단 액세스를 위한 비밀번호를 입력하세요.

다른 노드에서 **SSH** 시작

업그레이드하기 전에 다른 노드에서 SSH를 시작해야 합니다.

시작하기 전에

vCenter Server 인스턴스에 대해 VASA 공급자 확장 기능을 활성화해야 합니다.

이 작업에 관하여

업그레이드하기 전에 각 노드에서 이 절차를 수행하세요.

단계

1. vCenter Server에서 VASA Provider에 대한 콘솔을 엽니다.
2. 유지 관리 사용자로 로그인합니다.
3. 입력하다 `4` 지원 및 진단을 선택하세요.
4. 입력하다 `1` 진단 셸 액세스를 선택합니다.
5. 입력하다 `y` 계속하려면.
6. *sudo systemctl restart ssh* 명령을 실행합니다.

vCenter Server 및 ONTAP 자격 증명 업데이트

유지 관리 콘솔을 사용하여 vCenter Server 인스턴스와 ONTAP 자격 증명을 업데이트할 수 있습니다.

시작하기 전에

유지 관리 사용자 로그인 자격 증명이 필요합니다.

이 작업에 관하여

배포 후 vCenter Server, ONTAP 또는 Data LIF에 대한 자격 증명을 변경한 경우 이 절차를 사용하여 자격 증명을 업데이트해야 합니다.

단계

1. vCenter Server에서 VASA Provider에 대한 콘솔을 엽니다.
2. 유지 관리 사용자로 로그인합니다.
3. 입력하다 `2` 시스템 구성 메뉴를 선택하세요.
4. 입력하다 `9` ONTAP 자격 증명을 변경하려면.
5. 입력하다 `10` vCenter 자격 증명을 변경하려면.

ONTAP 도구 보고서

ONTAP tools for VMware vSphere 가상 머신과 데이터 저장소에 대한 보고서를 제공합니다. vCenter 클라이언트의 바로 가기 섹션에서 ONTAP tools for VMware vSphere NetApp ONTAP 도구를 선택하면 사용자 인터페이스가 개요 페이지로 이동합니다. 가상 머신과 데이터 저장소 보고서를 보려면 보고서 탭을 선택하세요.

가상 머신 보고서는 검색된 가상 머신(ONTAP 스토리지 기반 데이터 저장소에서 최소 1개의 디스크가 있어야 함) 목록과 성능 지표를 보여줍니다. VM 레코드를 확장하면 모든 디스크 관련 데이터 저장소 정보가 표시됩니다.

데이터스토어 보고서는 모든 유형의 ONTAP 스토리지 백엔드에서 프로비저닝된 ONTAP tools for VMware vSphere 목록을 성능 측정항목과 함께 보여줍니다.

열 관리 옵션을 사용하면 다양한 열을 숨기거나 표시할 수 있습니다.

로그 파일을 수집합니다

ONTAP 도구 관리자 사용자 인터페이스에서 제공되는 옵션을 통해 ONTAP tools for VMware vSphere 의 로그 파일을 수집할 수 있습니다. 기술 지원팀은 문제 해결을 위해 로그 파일을 수집해 달라고 요청할 수 있습니다.

> ONTAP 도구 관리자에서 로그를 생성하면 모든 vCenter Server 인스턴스에 대한 모든 로그가 포함됩니다. vCenter 클라이언트 사용자 인터페이스에서 로그를 생성하는 범위는 선택한 vCenter Server에 국한됩니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 사이드바에서 *로그 번들*을 선택합니다.

   이 작업에는 몇 분이 걸릴 수 있습니다.
4. *생성*을 선택하여 로그 파일을 생성합니다.
5. 로그 번들에 대한 라벨을 입력하고 *생성*을 선택합니다.

   tar.gz 파일을 다운로드하여 기술 지원팀으로 보내세요.

vCenter 클라이언트 사용자 인터페이스를 사용하여 로그 번들을 생성하려면 아래 단계를 따르세요.

단계

1. vSphere 클라이언트에 로그인합니다.
2. vSphere Client 홈페이지에서 지원 > 로그 번들 > *생성*으로 이동합니다.
3. 로그 번들 레이블을 입력하고 로그 번들을 생성하세요. 파일이 생성되면 다운로드 옵션이 표시됩니다. 다운로드하는 데 시간이 다소 걸릴 수 있습니다.

> 생성된 로그 번들은 지난 3일 또는 72시간 내에 생성된 로그 번들을 대체합니다.

가상 머신 관리

가상 머신을 마이그레이션하거나 복제할 때의 고려 사항

데이터 센터에서 기존 가상 머신을 마이그레이션할 때는 몇 가지 고려 사항을 알아야 합니다.

보호된 가상 머신 마이그레이션

보호된 가상 머신을 다음으로 마이그레이션할 수 있습니다.

- 다른 ESXi 호스트의 동일한 vVols 데이터 저장소

- 동일한 ESXi 호스트에 서로 다른 호환 vVols 데이터 저장소가 있음
- 다른 ESXi 호스트의 서로 다른 호환 vVols 데이터 저장소

가상 머신이 다른 FlexVol volume 으로 마이그레이션되면 해당 메타데이터 파일도 가상 머신 정보로 업데이트됩니다. 가상 머신이 동일한 스토리지를 사용하지만 다른 ESXi 호스트로 마이그레이션되는 경우 기본 FlexVol volume 메타데이터 파일은 수정되지 않습니다.

보호된 가상 머신 복제

보호된 가상 머신을 다음으로 복제할 수 있습니다.

- 복제 그룹을 사용하는 동일한 FlexVol volume 의 동일한 컨테이너

  동일한 FlexVol 볼륨의 메타데이터 파일이 복제된 가상 머신 세부 정보로 업데이트됩니다.

- 복제 그룹을 사용하는 다른 FlexVol volume 의 동일한 컨테이너

  복제된 가상 머신이 배치된 FlexVol volume 메타데이터 파일은 복제된 가상 머신 세부 정보로 업데이트됩니다.

- 다른 컨테이너 또는 vVols 데이터 저장소

  복제된 가상 머신이 배치된 FlexVol volume 메타데이터 파일은 가상 머신 세부 정보를 업데이트합니다.

VMware는 현재 VM 템플릿에 복제된 가상 머신을 지원하지 않습니다.

보호된 가상 머신의 복제본이 지원됩니다.

참조하다 "복제를 위한 가상 머신 생성" 자세한 내용은.

가상 머신 스냅샷

현재는 메모리가 없는 가상 머신 스냅샷만 지원됩니다. 가상 머신에 메모리가 포함된 스냅샷이 있는 경우 해당 가상 머신은 보호 대상으로 간주되지 않습니다.

메모리 스냅샷이 있는 보호되지 않은 가상 머신도 보호할 수 없습니다. 이 릴리스에서는 가상 머신에 대한 보호를 활성화하기 전에 메모리 스냅샷을 삭제해야 합니다.

ASA r2 스토리지 유형을 사용하는 Windows VM의 경우 가상 머신의 스냅샷을 찍으면 읽기 전용 스냅샷이 됩니다. VM에 대한 전원 공급 요청이 있을 때 VASA 공급자는 읽기 전용 스냅샷을 사용하여 LUN을 생성한 다음 IOPS를 활성화합니다. 전원 끄기 요청 중에 VASA 공급자는 생성된 LUN을 삭제한 다음 IOPS를 비활성화합니다.

NFS 및 **VMFS** 데이터 저장소가 있는 가상 머신을 **vVols** 데이터 저장소로 마이그레이션

NFS 및 VMFS 데이터 저장소에서 가상 머신을 가상 볼륨(vVols) 데이터 저장소로 마이그레이션하여 정책 기반 VM 관리 및 기타 vVols 기능을 활용할 수 있습니다. vVols 데이터 저장소를 사용하면 증가된 워크로드 요구 사항을 충족할 수 있습니다.

시작하기 전에

마이그레이션하려는 가상 머신에서 VASA Provider가 실행되고 있지 않은지 확인하세요. VASA Provider를 실행하는 가상 머신을 vVols 데이터 저장소로 마이그레이션하는 경우 vVols 데이터 저장소에 있는 가상 머신의 전원을 켜는 것을

포함하여 모든 관리 작업을 수행할 수 없습니다.

이 작업에 관하여

NFS 및 VMFS 데이터스토어에서 vVols 데이터스토어로 마이그레이션하는 경우 vCenter Server는 VMFS 데이터스토어에서 데이터를 이동할 때 VAAI(vStorage APIs for Array Integration) 오프로드를 사용하지만 NFS VMDK 파일에서는 사용하지 않습니다. VAAI 오프로드는 일반적으로 호스트의 부하를 줄입니다.

단계

1. 마이그레이션하려는 가상 머신을 마우스 오른쪽 버튼으로 클릭하고 *마이그레이션*을 선택합니다.
2. *저장 공간만 변경*을 선택한 후 *다음*을 선택합니다.
3. 마이그레이션하는 데이터스토어의 기능과 일치하는 가상 디스크 형식, VM 스토리지 정책 및 vVol 데이터스토어를 선택합니다.
4. 설정을 검토하고 *마침*을 선택합니다.

VASA 정리

이 섹션의 단계에 따라 VASA 정리를 수행하세요.

VASA 정리를 수행하기 전에 모든 vVols 데이터 저장소를 제거하는 것이 좋습니다.

단계

1. \ https://OTV_IP:8143/Register.html 로 이동하여 플러그인 등록을 취소하세요.
2. vCenter Server에서 해당 플러그인을 더 이상 사용할 수 없는지 확인하세요.
3. ONTAP tools for VMware vSphere 종료합니다.
4. ONTAP tools for VMware vSphere 삭제합니다.

가상 머신에서 데이터 디스크를 연결하거나 분리합니다.

가상 머신에 데이터 디스크 연결

가상 머신에 데이터 디스크를 연결하여 저장 용량을 확장합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 인벤토리에서 가상 머신을 마우스 오른쪽 버튼으로 클릭하고 *설정 편집*을 선택합니다.
3. 가상 하드웨어 탭에서 *기존 하드 디스크*를 선택합니다.
4. 디스크가 있는 가상 머신을 선택하세요.
5. 연결할 디스크를 선택하고 *확인*을 선택하세요

결과

하드 디스크가 가상 하드웨어 장치 목록에 나타납니다.

가상 머신에서 데이터 디스크 분리

더 이상 필요하지 않으면 가상 머신에 연결된 데이터 디스크를 분리할 수 있습니다. 가상 머신에서 디스크를 분리해도 디스크는 자동으로 삭제되지 않고 ONTAP 스토리지 시스템에 그대로 남아 있습니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 인벤토리에서 가상 머신을 마우스 오른쪽 버튼으로 클릭하고 *설정 편집*을 선택합니다.
3. 디스크 위로 포인터를 가져가서 *제거*를 선택하세요.

> 디스크가 가상 머신에서 제거됩니다. 다른 가상 머신이 디스크를 공유하는 경우 디스크 파일은 삭제되지 않습니다.

관련 정보

"가상 머신에 새 하드 디스크 추가"

"가상 머신에 기존 하드 디스크 추가"

스토리지 시스템 및 호스트 검색

vSphere Client에서 ONTAP tools for VMware vSphere 처음 실행하면 ONTAP 도구는 ESXi 호스트, 해당 LUN 및 NFS 내보내기, 그리고 해당 LUN 및 내보내기를 소유한 NetApp 스토리지 시스템을 검색합니다.

시작하기 전에

- 모든 ESXi 호스트는 전원이 켜져 있고 연결되어 있어야 합니다.
- 검색할 모든 스토리지 가상 머신(SVM)이 실행 중이어야 하며, 각 클러스터 노드에는 사용 중인 스토리지 프로토콜(NFS 또는 iSCSI)에 대해 최소한 하나의 데이터 LIF가 구성되어 있어야 합니다.

이 작업에 관하여

언제든지 새로운 스토리지 시스템을 발견하거나 기존 스토리지 시스템에 대한 정보를 업데이트하여 최신 용량 및 구성 정보를 얻을 수 있습니다. ONTAP tools for VMware vSphere 스토리지 시스템에 로그인하는 데 사용하는 자격 증명을 수정할 수도 있습니다.

ONTAP tools for VMware vSphere 스토리지 시스템을 검색하는 동안 vCenter Server 인스턴스에서 관리하는 ESXi 호스트로부터 정보를 수집합니다.

단계

1. vSphere Client 홈페이지에서 *호스트 및 클러스터*를 선택합니다.
2. 필요한 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *호스트 데이터 업데이트*를 선택합니다.

   확인 대화 상자에서 선택 사항을 확인하세요.

3. 상태가 있는 검색된 스토리지 컨트롤러를 선택하세요. `Authentication Failure` 작업 > *수정*을 선택하세요.

4. 저장 시스템 수정 대화 상자에 필요한 정보를 입력합니다.
5. 모든 스토리지 컨트롤러에 대해 4단계와 5단계를 반복합니다. `Authentication Failure` 상태.

검색 프로세스가 완료되면 다음 작업을 수행하세요.

- ONTAP tools for VMware vSphere 사용하여 어댑터 설정 열, MPIO 설정 열 또는 NFS 설정 열에 알림 아이콘이 표시되는 호스트에 대한 ESXi 호스트 설정을 구성합니다.
- 저장 시스템 자격 증명을 제공하세요.

ONTAP 도구를 사용하여 ESXi 호스트 설정 수정

ONTAP tools for VMware vSphere 대시보드를 사용하여 ESXi 호스트 설정을 편집할 수 있습니다.

시작하기 전에

ESXi 호스트 설정에 문제가 있는 경우 대시보드의 ESXi 호스트 시스템 포틀릿에 문제가 표시됩니다. 문제를 선택하면 문제가 있는 ESXi 호스트의 호스트 이름이나 IP 주소를 볼 수 있습니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 바로가기 페이지에서 플러그인 섹션 아래에 있는 * NetApp ONTAP 도구*를 선택합니다.
3. ONTAP tools for VMware vSphere 의 개요(대시보드)에서 **ESXi** 호스트 규정 준수 포틀릿으로 이동합니다.
4. 권장 설정 적용 링크를 선택합니다.
5. 권장 호스트 설정 적용 창에서 NetApp 권장 호스트 설정을 준수하려는 호스트를 선택하고 *다음*을 선택합니다.

   ESXi 호스트를 확장하여 현재 값을 확인할 수 있습니다.

6. 설정 페이지에서 필요에 따라 권장되는 값을 선택하세요.
7. 요약 창에서 값을 확인하고 *마침*을 선택합니다. 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

관련 정보

"ESXi 호스트 설정 구성"

비밀번호 관리

ONTAP 도구 관리자 비밀번호 변경

ONTAP 도구 관리자를 사용하여 관리자 비밀번호를 변경할 수 있습니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.

3. 화면 오른쪽 상단에 있는 관리자 아이콘을 선택하고 *비밀번호 변경*을 선택하세요.
4. 비밀번호 변경 팝업창에 이전 비밀번호와 새 비밀번호 세부 정보를 입력합니다. 비밀번호 변경에 대한 제약 조건은 사용자 인터페이스 화면에 표시됩니다.
5. 변경 사항을 적용하려면 *변경*을 선택하세요.

ONTAP 도구 관리자 비밀번호 재설정

ONTAP 도구 관리자 비밀번호를 잊어버린 경우 ONTAP tools for VMware vSphere 에서 생성한 토큰을 사용하여 관리자 자격 증명을 재설정할 수 있습니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 로그인 화면에서 비밀번호 재설정 옵션을 선택하세요.

   관리자 비밀번호를 재설정하려면 ONTAP tools for VMware vSphere 사용하여 재설정 토큰을 생성해야 합니다.

   a. vCenter Server에서 유지 관리 콘솔을 엽니다.
   b. 시스템 구성 옵션을 선택하려면 '2'를 입력하세요.
   c. 'maint' 사용자 비밀번호를 변경하려면 '3'을 입력하세요.
3. 비밀번호 변경 팝업 창에서 비밀번호 재설정 토큰, 사용자 이름 및 새 비밀번호 세부 정보를 입력합니다.
4. 변경 사항을 적용하려면 *재설정*을 선택하세요. 비밀번호 재설정이 성공하면 새로운 비밀번호로 로그인할 수 있습니다.

애플리케이션 사용자 비밀번호 재설정

애플리케이션 사용자 비밀번호는 vCenter Server에 SRA 및 VASA 공급자를 등록하는 데 사용됩니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 사이드바에서 *설정*을 선택하세요.
4. **VASA/SRA** 자격 증명 화면에서 *비밀번호 재설정*을 선택합니다.
5. 새로운 비밀번호를 입력하고 새 비밀번호 입력을 확인하세요.
6. 변경 사항을 적용하려면 *재설정*을 선택하세요.

유지 관리 콘솔 사용자 비밀번호 재설정

게스트 OS 재시작 작업 중 grub 메뉴에 유지 관리 콘솔 사용자 비밀번호 재설정 옵션이 표시됩니다. 이 옵션은 해당 VM에 있는 유지 관리 콘솔 사용자 비밀번호를 업데이트하는 데 사용됩니다. 비밀번호 재설정이 완료되면 VM이 재시작되어 새 비밀번호를 설정합니다. HA 배포

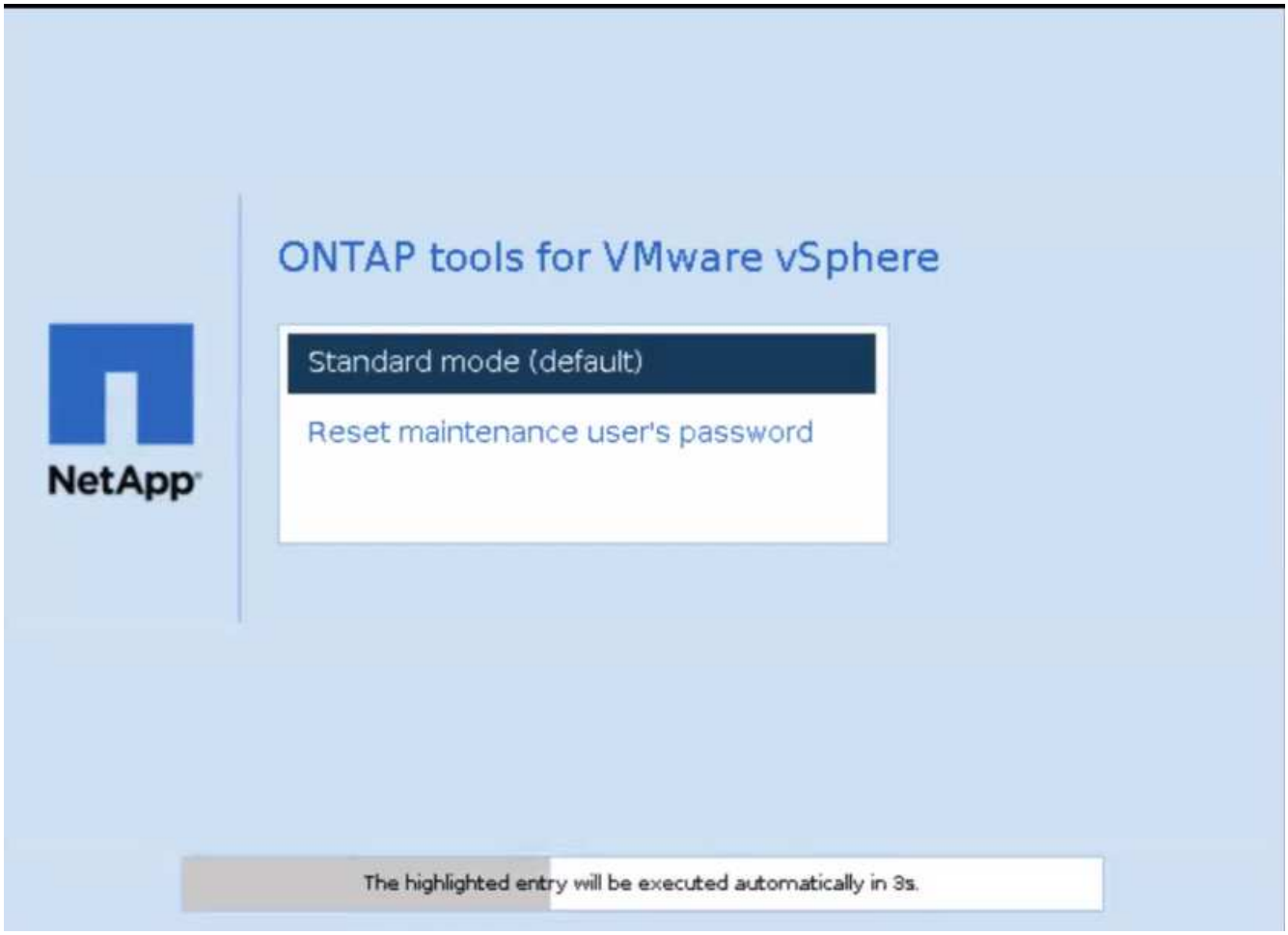
시나리오에서는 VM 재시작 후 다른 두 VM의 비밀번호가 자동으로 업데이트됩니다.

> ONTAP tools for VMware vSphere 의 경우 첫 번째 노드(node1)에서 유지 관리 콘솔 사용자 비밀번호를 변경해야 합니다.

단계

1. vCenter Server에 로그인하세요
2. VM을 마우스 오른쪽 버튼으로 클릭하고 전원 > *게스트 OS 다시 시작*을 선택합니다. 시스템을 다시 시작하면 다음 화면이 나타납니다

.



옵션을 선택하는 데 5초가 주어집니다. 아무 키나 누르면 진행이 멈추고 GRUB 메뉴가 정지됩니다.

3. 유지관리 사용자 비밀번호 재설정 옵션을 선택하세요. 유지 관리 콘솔이 열립니다.
4. 콘솔에 새 비밀번호 세부 정보를 입력하세요. 비밀번호를 성공적으로 재설정하려면 새 비밀번호와 새 비밀번호 세부 정보를 다시 입력해야 합니다. 올바른 비밀번호를 입력할 수 있는 기회는 세 번입니다. 새로운 비밀번호를 성공적으로 입력하면 시스템이 다시 시작됩니다.
5. 계속하려면 Enter를 누르세요. VM에서 비밀번호가 업데이트됩니다.

> VM의 전원을 켜는 동안에도 동일한 GRUB 메뉴가 나타납니다. 하지만 비밀번호 재설정 옵션은 게스트 **OS** 재시작 옵션과 함께만 사용해야 합니다.

호스트 클러스터 보호 관리

보호된 호스트 클러스터 수정

수정 보호의 일부로 다음 작업을 수행할 수 있습니다. 동일한 워크플로에서 모든 변경 작업을 수행할 수 있습니다.

- 보호된 클러스터에 새로운 데이터 저장소나 호스트를 추가합니다.
- 보호 설정에 새로운 SnapMirror 관계를 추가합니다.
- 보호 설정에서 기존 SnapMirror 관계를 삭제합니다.
- 기존 SnapMirror 관계를 수정합니다.

호스트 클러스터 보호 모니터링

이 절차를 사용하여 호스트 클러스터 보호 상태를 모니터링합니다. 모든 보호된 호스트 클러스터와 해당 보호 상태, SnapMirror 관계, 데이터 저장소 및 해당 SnapMirror 상태를 모니터링할 수 있습니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. * NetApp ONTAP 도구* > 보호 > *호스트 클러스터 관계*로 이동합니다.

   보호 열 아래의 아이콘은 보호 상태를 보여줍니다.

3. 자세한 내용을 보려면 아이콘 위에 마우스를 올려 놓으세요.

새로운 데이터 저장소 또는 호스트 추가

이 절차를 사용하여 새로 추가된 데이터 저장소나 호스트를 보호하세요. vCenter 기본 사용자 인터페이스를 사용하여 보호된 클러스터에 새 호스트를 추가하거나 호스트 클러스터에 새 데이터 저장소를 만들 수 있습니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 보호된 클러스터의 속성을 편집하려면 다음 중 하나를 수행할 수 있습니다.
   a. * NetApp ONTAP 도구* > 보호 > *호스트 클러스터 관계*로 이동하여 클러스터에 대한 줄임표 메뉴를 선택하고 *편집*을 선택합니다.
   b. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *클러스터 보호*를 선택합니다.
3. vCenter 네이티브 사용자 인터페이스에서 데이터 저장소를 생성한 경우 해당 데이터 저장소는 보호되지 않은 것으로 표시됩니다. 사용자 인터페이스는 클러스터의 모든 데이터 저장소와 해당 보호 상태를 대화 상자에 표시합니다. 완벽한 보호를 위해 보호 버튼을 선택하세요.
4. 새로운 ESXi 호스트를 추가한 경우 보호 상태가 부분적으로 보호됨으로 표시됩니다. SnapMirror 설정에서 줄임표 메뉴를 선택하고 *편집*을 선택하여 새로 추가된 ESXi 호스트의 근접성을 설정합니다.

> 비동기 유형 관계의 경우, 3차 사이트의 대상 SVM을 동일한 ONTAP 도구 인스턴스에 추가할 수 없으므로 편집 작업이 지원되지 않습니다. 하지만 대상 SVM의 시스템 관리자 또는 CLI를 사용하여 관계 구성을 변경할 수 있습니다.

5. 필요한 변경 사항을 적용한 후 *저장*을 선택하세요.
6. 클러스터 보호 창에서 변경 사항을 확인할 수 있습니다.

vCenter 작업이 생성되고 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

새로운 **SnapMirror** 관계 추가

단계

1. vSphere 클라이언트에 로그인합니다.
2. 보호된 클러스터의 속성을 편집하려면 다음 중 하나를 수행할 수 있습니다.
   a. * NetApp ONTAP 도구* > 보호 > *호스트 클러스터 관계*로 이동하여 클러스터에 대한 줄임표 메뉴를 선택하고 *편집*을 선택합니다.
   b. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *클러스터 보호*를 선택합니다.
3. *관계 추가*를 선택합니다.
4. 비동기 또는 **AutomatedFailOverDuplex** 정책 유형으로 새 관계를 추가합니다.
5. *보호*를 선택하세요.

   클러스터 보호 창에서 변경 사항을 확인할 수 있습니다.

vCenter 작업이 생성되고 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

기존 **SnapMirror** 관계 삭제

비동기 SnapMirror 관계를 삭제하려면 보조 사이트 SVM 또는 클러스터를 ONTAP tools for VMware vSphere 의 스토리지 백엔드로 추가해야 합니다. 모든 SnapMirror 관계를 삭제할 수는 없습니다. 관계를 삭제하면 ONTAP 클러스터의 해당 관계도 제거됩니다. AutomatedFailOverDuplex SnapMirror 관계를 삭제하면 대상의 데이터 저장소가 매핑 해제되고 일관성 그룹, LUN, 볼륨 및 igroup이 대상 ONTAP 클러스터에서 제거됩니다.

관계를 삭제하면 보조 사이트에서 재검색이 트리거되어 호스트에서 활성 경로로 매핑되지 않은 LUN을 제거합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 보호된 클러스터의 속성을 편집하려면 다음 중 하나를 수행할 수 있습니다.
   a. * NetApp ONTAP 도구* > 보호 > *호스트 클러스터 관계*로 이동하여 클러스터에 대한 줄임표 메뉴를 선택하고 *편집*을 선택합니다.
   b. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *클러스터 보호*를 선택합니다.
3. SnapMirror 설정에서 줄임표 메뉴를 선택하고 *삭제*를 선택합니다.

vCenter 작업이 생성되고 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

기존 **SnapMirror** 관계 수정

비동기 SnapMirror 관계를 수정하려면 보조 사이트 SVM 또는 클러스터를 ONTAP tools for VMware vSphere 의 스토리지 백엔드로 추가해야 합니다. AutomatedFailOverDuplex SnapMirror 관계인 경우 균일한 구성의 경우 호스트 근접성을 수정하고, 균일하지 않은 구성의 경우 호스트 액세스를 수정할 수 있습니다. 비동기 및 AutomatedFailOverDuplex 정책 유형을 서로 바꿔 사용할 수 없습니다. 클러스터에서 새로 검색된 호스트에 대한 근접성이나 액세스를 설정할 수 있습니다.

> 기존 비동기 SnapMirror 관계를 편집할 수 없습니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 보호된 클러스터의 속성을 편집하려면 다음 중 하나를 수행할 수 있습니다.
   a. * NetApp ONTAP 도구* > 보호 > *호스트 클러스터 관계*로 이동하여 클러스터에 대한 줄임표 메뉴를 선택하고 *편집*을 선택합니다.
   b. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP 도구* > *클러스터 보호*를 선택합니다.
3. AutomatedFailOverDuplex 정책 유형을 선택한 경우 호스트 근접성 또는 호스트 액세스 세부 정보를 추가합니다.
4. 보호 버튼을 선택하세요.

vCenter 작업이 생성되고 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

호스트 클러스터 보호 제거

호스트 클러스터 보호를 제거하면 데이터 저장소가 보호되지 않습니다.

단계

1. 보호된 호스트 클러스터를 보려면 * NetApp ONTAP 도구* > 보호 > *호스트 클러스터 관계*로 이동합니다.

   이 페이지에서는 보호된 호스트 클러스터와 해당 보호 상태, SnapMirror 관계 및 해당 SnapMirror 상태를 모니터링할 수 있습니다.

2. 호스트 클러스터 보호 창에서 클러스터에 대한 줄임표 메뉴를 선택한 다음 *보호 제거*를 선택합니다.

AutoSupport 비활성화

처음으로 스토리지 시스템을 구성하는 경우 AutoSupport 기본적으로 활성화됩니다. 이 기능이 활성화된 후 24시간 이내에 기술 지원팀에 메시지가 전송됩니다. AutoSupport 비활성화하면 더 이상 사전 지원 및 모니터링을 받을 수 없습니다.

> AutoSupport 활성화해 두는 것이 좋습니다. 이는 문제 탐지 및 해결 속도를 높이는 데 도움이 됩니다. 이 시스템은 AutoSupport 정보를 수집하여 비활성화된 경우에도 로컬에 저장합니다. 하지만 어떤 네트워크에도 보고서를 전송하지는 않습니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.

https://<ONTAPtoolsIP>:8443/virtualization/ui/

2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 설정 > 원격측정 > 편집 옵션을 선택하세요.
4. * AutoSupport* 옵션의 선택을 해제하고 변경 사항을 저장합니다.

AutoSupport 프록시 URL 업데이트

네트워크 액세스 제어나 보안 조치에 프록시 서버가 사용되는 시나리오에서 AutoSupport 기능이 제대로 작동하도록 하려면 AutoSupport 프록시 URL을 업데이트하세요. 이를 통해 AutoSupport 데이터를 적절한 프록시를 통해 라우팅하여 안전한 전송과 규정 준수가 가능해집니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   https://<ONTAPtoolsIP>:8443/virtualization/ui/
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 사이드바에서 *설정*을 선택하세요.
4. 설정 > 원격측정 > 편집 옵션을 선택하세요.
5. 유효한 *프록시 URL*을 입력하고 변경 사항을 저장합니다.

   AutoSupport 비활성화하면 프록시 URL도 비활성화됩니다.

NTP 서버 추가

ONTAP 도구 어플라이언스의 타임 클록을 동기화하려면 NTP 서버 세부 정보를 입력하세요.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   https://<ONTAPtoolsIP>:8443/virtualization/ui/
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 설정 > **NTP** 서버 > 편집 옵션을 선택하세요.
4. 쉼표로 구분된 정규화된 도메인 이름(FQDN), IPv4 또는 IPv6 주소를 입력하세요.

   업데이트된 값을 보려면 화면을 새로 고치세요.

백업을 생성하고 ONTAP 도구 설정을 복구합니다.

ONTAP tools for VMware vSphere 부터 어플라이언스는 동적 스토리지 프로비저너를 사용하므로 제로 RPO를 달성할 수 없습니다. 하지만 RPO를 거의 0에 가깝게 달성할 수도 있습니다. 거의 0에 가까운 RPO를 달성하려면 설정 백업을 만들고 새 가상 머신에 복원해야 합니다.

> 비HA 백업이 활성화된 경우 HA로 마이그레이션하려면 먼저 백업을 비활성화한 다음 마이그레이션 후 다시 활성화하세요.

백업을 생성하고 백업 파일을 다운로드합니다.

단계

1. vCenter Server에서 유지 관리 콘솔을 엽니다.
2. 유지 관리 사용자로 로그인합니다.
3. 입력하다 4 *지원 및 진단*을 선택하세요.
4. 입력하다 3 시스템 백업 활성화 옵션을 선택하세요.
5. HA가 아닌 경우 ONTAP 도구 가상 머신이 배포된 vCenter 자격 증명을 입력합니다.
6. 백업 빈도 값을 5분에서 60분 사이로 입력하세요.
7. *Enter*를 누르세요

   이렇게 하면 백업이 생성되고 정기적으로 가상 머신의 데이터 저장소에 백업이 푸시됩니다.

8. 백업에 액세스하려면 저장소 섹션으로 이동하여 가상 머신의 데이터 저장소를 선택하세요.
9. 파일 섹션을 선택하세요.

   파일 섹션에서 디렉토리를 볼 수 있습니다. 디렉토리 이름은 ONTAP 도구 IP 주소가 되며, 여기서 점(.)은 밑줄로 바뀌고 _backup_이 접미사로 붙습니다.

10. 백업에 대한 자세한 내용을 보려면 파일 > *다운로드*에서 backup_info.txt 파일을 다운로드하세요.

다시 덮다

설정을 복구하려면 기존 가상 머신의 전원을 끄고 초기 배포에 사용된 OVA를 사용하여 새 가상 머신을 배포합니다.

새 가상 머신에 동일한 ONTAP 도구 IP 주소를 사용해야 하며, 서비스 활성화, 노드 크기, HA 모드 등의 시스템 구성은 초기 배포와 동일해야 합니다.

백업 파일에서 설치 프로그램을 복구하려면 다음 단계를 수행하세요.

1. vCenter Server에서 유지 관리 콘솔을 엽니다.
2. 유지 관리 사용자로 로그인합니다.
3. 입력하다 4 *지원 및 진단*을 선택하세요.
4. 입력하다 2 원격 진단 액세스 활성화 옵션을 선택하고 진단 액세스에 대한 새 비밀번호를 만듭니다.
5. 다운로드한 디렉토리에서 백업 하나를 선택하세요. 최신 백업 파일 이름은 *backup_info.txt* 파일에 기록됩니다.
6. 아래 명령을 실행하여 백업을 새 가상 머신에 복사하고 메시지가 표시되면 진단 암호를 입력합니다.

```
scp <Backup_X.tar.enc> diag@<node_ip>:/home/diag/system_recovery.tar.enc
```

명령에 언급된 대상 경로와 파일 이름(/home/diag/system_recovery.tar.enc)을 변경하지 마세요.

7. 백업 파일을 복사한 후 진단 셸에 로그인하여 다음 명령을 실행합니다.

```
sudo perl /home/maint/scripts/post-deploy-upgrade.pl -recovery
```

로그는 */var/log/post-deploy-upgrade.log* 파일에 기록됩니다.

8. 성공적으로 복구되면 서비스와 vCenter 개체가 복원됩니다.

ONTAP tools for VMware vSphere 제거

ONTAP tools for VMware vSphere 제거하면 도구의 모든 데이터가 삭제됩니다.

단계

1. ONTAP tools for VMware vSphere 에서 모든 가상 머신을 제거하거나 이동합니다.
   - 가상 머신을 제거하려면 다음을 참조하세요. "VM 및 VM 템플릿 제거 및 재등록"
   - 관리되지 않는 데이터 저장소로 이동하려면 다음을 참조하세요. "Storage vMotion을 사용하여 가상 머신을 마이그레이션하는 방법"
2. "데이터 저장소 삭제"ONTAP tools for VMware vSphere 에서 생성되었습니다.
3. VASA 공급자를 활성화한 경우 ONTAP 도구에서 설정 > **VASA** 공급자 설정 > *등록 취소*를 선택하여 모든 vCenter 서버에서 VASA 공급자를 등록 취소합니다.
4. vCenter Server 인스턴스에서 모든 스토리지 백엔드를 연결 해제합니다. "vCenter Server 인스턴스와 스토리지 백엔드 연결 해제" .
5. 모든 스토리지 백엔드를 삭제합니다. "스토리지 백엔드 관리" .
6. VMware Live Site Recovery에서 SRA 어댑터를 제거합니다.
   a. 포트 5480을 사용하여 VMware Live Site Recovery 어플라이언스 관리 인터페이스에 관리자로 로그인합니다.
   b. *저장소 복제 어댑터*를 선택합니다.
   c. 적절한 SRA 카드를 선택하고 드롭다운 메뉴에서 *삭제*를 선택합니다.
   d. 어댑터 삭제 결과를 확인하고 *삭제*를 선택하세요.
7. ONTAP tools for VMware vSphere 에 온보딩된 vCenter 서버 인스턴스를 삭제합니다. "vCenter Server 인스턴스 관리" .
8. vCenter Server에서 ONTAP tools for VMware vSphere 전원을 끄고 VM을 삭제합니다.

다음은 무엇인가요**?**

"FlexVol 볼륨 제거"

FlexVol 볼륨 제거

VMware 배포를 위해 ONTAP 도구에 전용 ONTAP 클러스터를 사용하면 사용되지 않는

FlexVol 볼륨이 많이 생성됩니다. ONTAP tools for VMware vSphere 제거한 후에는 성능에 미치는 영향을 방지하기 위해 FlexVol 볼륨을 제거해야 합니다.

단계

1. 첫 번째 노드 VM에서 ONTAP tools for VMware vSphere 확인합니다.

   cat /opt/netapp/meta/ansible_vars.yaml | *grep -i* 프로토콜

   iSCSI 배포인 경우 igroup도 삭제해야 합니다.

2. FlexVol 볼륨 목록을 가져옵니다.

   kubectl 지속적 볼륨 설명 | *grep internalName* | *awk -F'=' '{print $2}'*

3. vCenter Server에서 VM을 제거합니다. 참조하다 "VM 및 VM 템플릿 제거 및 재등록" .
4. FlexVol 볼륨을 삭제합니다. 참조하다 "FlexVol volume 삭제" . 볼륨을 삭제하는 CLI 명령에서 FlexVol 볼륨의 정확한 이름을 지정합니다.
5. iSCSI 배포의 경우 ONTAP 스토리지 시스템에서 SAN igroup을 삭제합니다. 참조하다 "SAN 이니시에이터 및 igroup 보기 및 관리" .

ONTAP tools for VMware vSphere 업그레이드

ONTAP tools for VMware vSphere 에서 10.4로 업그레이드

ONTAP tools for VMware vSphere 에서 10.4로 업그레이드할 수 있습니다. 하지만 ONTAP 도구 10.0 또는 10.1에서 10.4로 직접 업그레이드하는 것은 지원되지 않습니다.

메모:

- ASA r2 시스템에서는 더 많은 스토리지 가용성 영역(SAZ)을 추가하기 전에 ONTAP 9.16.1을 사용하여 ONTAP tools for VMware vSphere 로 업그레이드해야 합니다.
- ONTAP tools for VMware vSphere 에서 10.4 릴리스로의 업그레이드가 실패하면 롤백이 지원되지 않습니다. 설정을 복구하려면 ONTAP tools for VMware vSphere 에 RPO를 사용하고 ONTAP tools for VMware vSphere 에 거의 0에 가까운 RPO 또는 스냅샷 복구를 사용합니다.

시작하기 전에

HA가 아닌 업그레이드의 경우 ONTAP 도구 VM의 전원을 끄고, HA 업그레이드의 경우 가상 머신(VM) 설정에 다음 변경 사항을 적용하기 전에 첫 번째 노드의 전원을 끕니다.

ONTAP tools for VMware vSphere 에서 업그레이드하는 경우, 업그레이드 작업을 진행하기 전에 다음 단계를 완료해야 합니다. * 서비스 데이터는 VM에 로컬로 저장되므로 각 노드에 100GB 하드 디스크를 추가합니다. * 배포 버전에 따라 전원이 꺼진 VM의 CPU와 메모리를 변경합니다. CPU 및 RAM 핫 플러그인을 활성화합니다.

+

배포 유형	노드당 **CPU**(코어)	노드당 메모리(**GB**)	노드당 디스크 공간(**GB**)	총 **CPU**(코어)	메모리(**GB**)	총 디스크 공간(**GB**)
비HA 소형	9	18	350	9	18	350
비HA 매체	13	26	350	13	26	350
HA 스몰	9	18	350	27	54	1050
HA 중간	13	26	350	39	78	1050
HA 대형	17	34	350	51	102	1050

- 변경이 완료되면 VM의 전원을 켜고 서비스가 실행 상태가 될 때까지 기다립니다.
- HA 배포의 경우 리소스를 변경하고 CPU와 RAM에 대한 핫 플러그인을 활성화하고 두 번째와 세 번째 노드에도 100GB 하드 디스크를 추가합니다. 이 노드를 재부팅할 필요는 없습니다.
- ONTAP 도구 10.2를 사용하여 어플라이언스를 로컬 경로(간편 배포)로 배포한 경우 업그레이드하기 전에 정지 스냅샷을 찍어야 합니다.

ONTAP tools for VMware vSphere 에서 10.1로 업그레이드하는 경우 업그레이드 작업을 진행하기 전에 다음 단계를 완료해야 합니다. 진단 활성화

1. vCenter Server에서 ONTAP 도구로 콘솔을 엽니다.
2. 유지 관리 사용자로 로그인합니다.
3. *지원 및 진단*을 선택하려면 *4*를 입력하세요.

4. *원격 진단 액세스 활성화*를 선택하려면 *2*를 입력하세요.
5. 원하는 비밀번호를 설정하려면 *y*를 입력하세요.
6. 터미널/퍼티에서 사용자 이름을 'diag'로 하고 이전 단계에서 설정한 비밀번호를 사용하여 VM IP 주소에 로그인합니다.

MongoDB 백업하기

다음 명령을 실행하여 MongoDB 백업을 수행합니다.

- kn exec -it ntv-mongodb-0 sh - kn은 kubectl -n ntv-system의 별칭입니다.
- Pod 내부에서 *env | grep MONGODB_ROOT_PASSWORD* 명령을 실행합니다.
- 포드에서 나오려면 *exit* 명령을 실행하세요.
- 위 명령에서 설정한 MONGO_ROOT_PASSWORD를 바꾸려면 *kn exec ntv-mongodb-0 --mongodump -u root -p MONGODB_ROOT_PASSWORD --archive=/tmp/mongodb-backup.gz --gzip* 명령을 실행합니다.
- 위 명령을 사용하여 생성된 mongodb 백업을 포드에서 호스트로 복사하려면 *kn cp ntv-mongodb-0:/tmp/mongodb-backup.gz ./mongodb-backup.gz* 명령을 실행합니다.

모든 볼륨의 퀘이즈 스냅샷을 찍으세요

- 'kn get pvc' 명령을 실행하고 명령 출력을 저장합니다.
- 다음 방법 중 하나를 사용하여 모든 볼륨의 스냅샷을 하나씩 찍습니다.
  - CLI에서 *volume snapshot create -vserver <vserver_name> -volume <volume_name> -snapshot <snapshot_name>* 명령을 실행합니다.
  - ONTAP 시스템 관리자 사용자 인터페이스에서 검색 창에 볼륨 이름을 입력하여 검색한 다음, 이름을 선택하여 해당 볼륨을 엽니다. 스냅샷으로 가서 해당 볼륨의 스냅샷을 추가합니다.

vCenter에서 **ONTAP tools for VMware vSphere** 의 스냅샷을 만듭니다**(HA** 배포의 경우 **3**개 **VM,** 비 **HA** 배포의 경우 **1**개 **VM)**

- vSphere 클라이언트 사용자 인터페이스에서 VM을 선택합니다.
- 스냅샷 탭으로 가서 스냅샷 찍기 버튼을 선택하세요. VM의 정지된 스냅샷을 찍습니다. 참조하다 "가상 머신의 스냅샷을 찍습니다" 자세한 내용은.

업그레이드를 수행하기 전에 "generate-support-bundle-job" 접두사가 붙은 로그 번들에서 완료된 포드를 삭제합니다. 지원 번들 생성이 진행 중이면 완료될 때까지 기다린 후 Pod를 삭제하세요.

모든 유형의 업그레이드에는 100GB 하드 디스크 드라이브(HDD)를 추가해야 합니다. HDD를 추가하려면 다음 작업을 수행하세요.

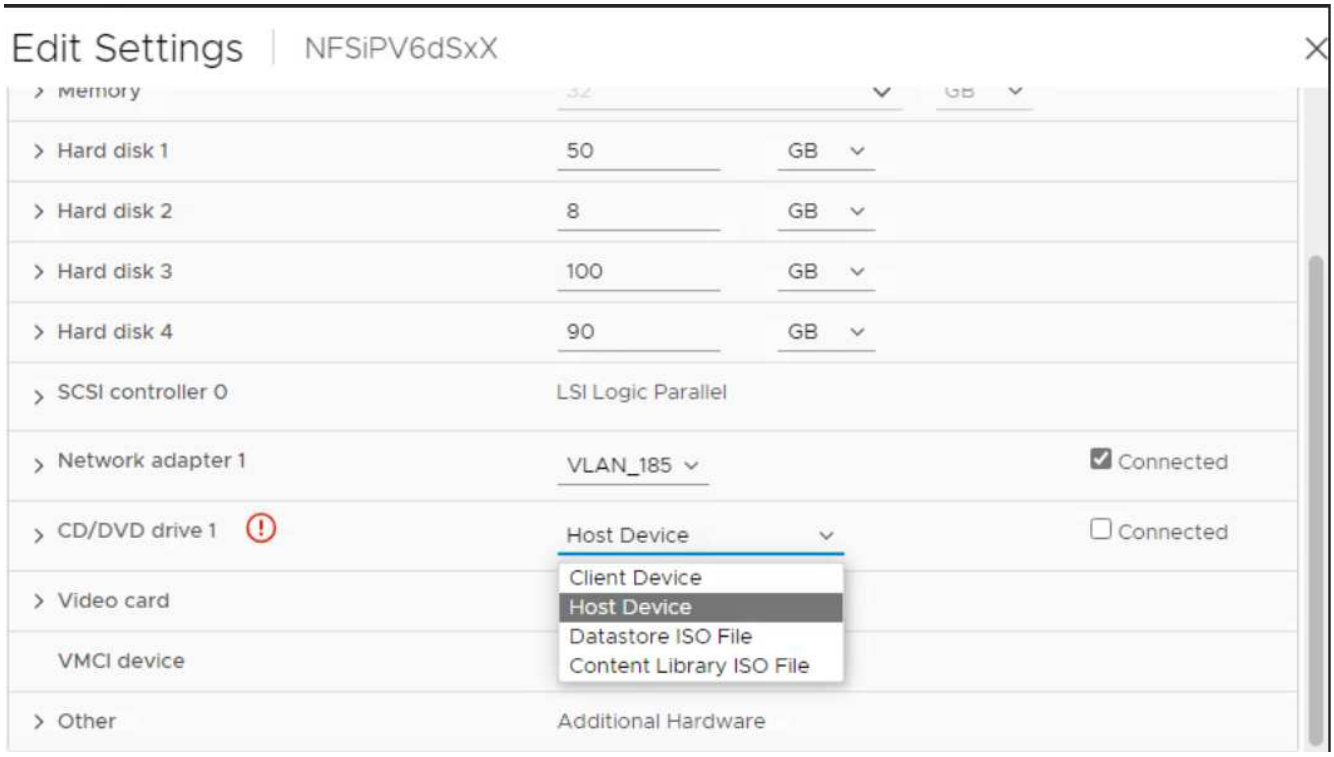
1. 단일 노드 구성에서 VM을 선택하거나 HA 구성에서 세 개의 VM을 모두 선택합니다.
2. VM을 마우스 오른쪽 버튼으로 클릭하고 새 장치 추가 > *하드 디스크*를 선택합니다.
3. 새 하드 디스크 필드에 100GB HDD를 추가합니다.
4. *적용*을 선택하세요

하드 디스크를 추가한 후 해당 구성에 맞게 VM 리소스를 업데이트하고 기본 VM을 다시 시작합니다.

새로운 HDD가 생성됩니다. 동적 스토리지 프로비저너는 이 HDD를 사용하여 볼륨을 생성하거나 복제합니다.

단계

1. ONTAP tools for VMware vSphere 콘텐츠 라이브러리에 업로드합니다.
2. 기본 VM 페이지에서 작업 > *설정 편집*을 선택합니다.
3. **CD/DVD** 드라이브 필드 아래의 편집 설정 창에서 콘텐츠 라이브러리 ISO 파일을 선택합니다.
4. ISO 파일을 선택하고 확인*을 선택합니다. ***CD/DVD** 드라이브 필드에서 연결됨 확인란을 선택합니다
.



5. vCenter Server에서 ONTAP 도구로 콘솔을 엽니다.
6. 유지 관리 사용자로 로그인합니다.
7. *3*을 입력하여 시스템 구성 메뉴를 선택합니다.
8. 업그레이드 옵션을 선택하려면 *7*을 입력하세요.
9. 업그레이드하면 다음 작업이 자동으로 수행됩니다.
   a. 인증서 업그레이드
   b. 원격 플러그인 업그레이드

ONTAP tools for VMware vSphere 로 업그레이드한 후 다음을 수행할 수 있습니다.

- 관리자 사용자 인터페이스에서 서비스 비활성화
- 비 HA 설정에서 HA 설정으로 이동
- HA가 아닌 소규모 구성을 HA가 아닌 중규모 구성으로 확장하거나 HA 중규모 또는 대규모 구성으로 확장합니다.
- HA가 아닌 업그레이드의 경우 ONTAP 도구 VM을 재부팅하여 변경 사항을 반영합니다. HA 업그레이드의 경우 첫 번째 노드를 재부팅하여 노드의 변경 사항을 반영합니다.

다음은 무엇입니까?

ONTAP tools for VMware vSphere 의 이전 릴리스에서 10.4로 업그레이드한 후 SRA 어댑터를 다시 검사하여 VMware Live Site Recovery Storage Replication 어댑터 페이지에서 세부 정보가 업데이트되었는지 확인하세요.

업그레이드가 성공적으로 완료되면 다음 절차에 따라 ONTAP 에서 Trident 볼륨을 수동으로 삭제합니다.

> ONTAP tools for VMware vSphere HA가 아닌 소규모 또는 중규모(로컬 경로) 구성인 경우 이러한 단계는 필요하지 않습니다.

1. vCenter Server에서 ONTAP 도구로 콘솔을 엽니다.
2. 유지 관리 사용자로 로그인합니다.
3. 지원 및 진단 메뉴를 선택하려면 *4*를 입력하세요.
4. 진단 셸 액세스 옵션을 선택하려면 *1*을 입력합니다.
5. 다음 명령을 실행하세요

```
sudo python3 /home/maint/scripts/ontap_cleanup.py
```

6. ONTAP 사용자 이름과 비밀번호를 입력하세요

이렇게 하면 ONTAP tools for VMware vSphere 에서 사용되는 ONTAP 의 모든 Trident 볼륨이 삭제됩니다.

관련 정보

"ONTAP tools for VMware vSphere 에서 10.4로 마이그레이션"

업그레이드 오류 코드

ONTAP tools for VMware vSphere 중 오류 코드가 발생할 수 있습니다. 오류 코드는 5자리 숫자로, 처음 두 자리는 문제가 발생한 스크립트를 나타내고, 마지막 세 자리는 해당 스크립트 내의 특정 워크플로를 나타냅니다.

모든 오류 로그는 ansible-perl-errors.log 파일에 기록되어 문제를 쉽게 추적하고 해결할 수 있습니다. 이 로그 파일에는 오류 코드와 실패한 Ansible 작업이 포함되어 있습니다.

> 이 페이지에 제공된 오류 코드는 참조용일 뿐입니다. 오류가 지속되거나 해결 방법이 언급되지 않으면 지원팀에 문의하세요.

다음 표에는 오류 코드와 해당 파일 이름이 나열되어 있습니다.

오류 코드	스크립트 이름
00	firstboot-network-config.pl, 배포 모드
01	firstboot-network-config.pl, 모드 업그레이드
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, 배포, HA

04	firstboot-deploy-otv-ng.pl, 배포, 비HA
05	firstboot-deploy-otv-ng.pl, 재부팅
06	firstboot-deploy-otv-ng.pl, 업그레이드, HA
07	firstboot-deploy-otv-ng.pl, 업그레이드, 비 HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

오류 코드의 마지막 세 자리는 스크립트 내의 특정 워크플로 오류를 나타냅니다.

업그레이드 오류 코드	작업 흐름	해결
052	ISO는 현재 버전과 동일할 수도 있고, 현재 버전보다 두 개 상위 버전일 수도 있습니다.	현재 버전과 호환되는 ISO 버전을 사용하여 업그레이드하세요.
068	데비안 패키지 롤백이 실패했습니다.	0 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하세요.
069	파일 복원에 실패했습니다	0 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하세요.
070	백업 삭제에 실패했습니다	-
071	Kubernetes 클러스터가 정상적이지 않았습니다.	-
074	ISO 마운트에 실패했습니다	/var/log/upgrade-run.log를 확인하고 업그레이드를 다시 시도하세요.
075	업그레이드 사전 검사에 실패했습니다.	업그레이드를 다시 시도하세요.
076	레지스트리 업그레이드에 실패했습니다	0 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하세요.
077	레지스트리 롤백이 실패했습니다	0 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하세요.
078	운영자 업그레이드에 실패했습니다	0 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하세요.
079	운영자 롤백이 실패했습니다	0 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하세요.
080	서비스 업그레이드에 실패했습니다	0 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하세요.
081	서비스 롤백이 실패했습니다	0 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하세요.

업그레이드 오류 코드	작업 흐름	해결
082	컨테이너에서 이전 이미지를 삭제하는 데 실패했습니다.	0 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하세요.
083	백업 삭제에 실패했습니다	0 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하세요.
084	JobManager를 Production으로 다시 변경하는 데 실패했습니다.	업그레이드를 복구/완료하려면 아래 단계를 따르세요. 1. 진단 셸 2를 활성화합니다. 다음 명령을 실행합니다: *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 3. /var/log/post-deploy-upgrade.log에서 로그를 확인하세요.
087	업그레이드 후 단계가 실패했습니다.	업그레이드를 복구/완료하려면 다음 단계를 수행하세요. 1. 진단 셸 2를 활성화합니다. *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 명령 3을 실행합니다. /var/log/post-deploy-upgrade.log에서 로그를 확인하세요.
088	journald에 대한 로그 회전 구성에 실패했습니다.	VM이 호스팅되는 호스트와 호환되는 VM 네트워크 설정을 확인하세요. VM을 다른 호스트로 마이그레이션하고 다시 시작해 보세요.
089	요약 로그 회전 구성 파일의 소유권을 변경하는 데 실패했습니다.	업그레이드를 다시 시도하세요.
095	OS 업그레이드에 실패했습니다	OS 업그레이드에 대한 복구가 없습니다. ONTAP 도구 서비스가 업그레이드되고 새로운 포드가 실행됩니다.
096	동적 스토리지 프로비저너 설치	업그레이드 로그를 확인하고 업그레이드를 다시 시도하세요.
097	업그레이드를 위한 서비스 제거에 실패했습니다.	0 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도합니다.
098	ntv-system에서 동적 스토리지 프로비저너 네임스페이스로 dockercred 비밀을 복사하는 데 실패했습니다.	업그레이드 로그를 확인하고 업그레이드를 다시 시도하세요.
099	새로운 HDD 추가를 검증하지 못했습니다.	HA의 경우 모든 노드에 새 HDD를 추가하고, HA가 아닌 경우 하나의 노드에 새 HDD를 추가합니다.
108	시드 스크립트가 실패했습니다	-

업그레이드 오류 코드	작업 흐름	해결
109	영구 볼륨 데이터 백업에 실패했습니다.	업그레이드 로그를 확인하고 업그레이드를 다시 시도하세요.
110	영구 볼륨 데이터 복원에 실패했습니다.	0 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하세요.
111	RKE2에 대한 etcd 시간 초과 매개변수 업데이트가 실패했습니다.	업그레이드 로그를 확인하고 업그레이드를 다시 시도하세요.
112	동적 스토리지 프로비저너 제거에 실패했습니다.	-
113	보조 노드의 리소스 새로 고침이 실패했습니다.	업그레이드 로그를 확인하고 업그레이드를 다시 시도하세요.
104	보조 노드 재시작이 실패했습니다.	노드를 하나씩 수동으로 다시 시작합니다.
100	커널 롤백이 실패했습니다	-
051	동적 스토리지 프로비저너 업그레이드가 실패했습니다.	업그레이드 로그를 확인하고 업그레이드를 다시 시도하세요.
056	마이그레이션 백업 삭제에 실패했습니다.	해당 없음

ONTAP tools for VMware vSphere 부터는 Zero RPO가 지원되지 않습니다.

자세히 알아보세요 "버전 10.0에서 10.1로 업그레이드가 실패한 경우 ONTAP tools for VMware vSphere 복원하는 방법"

ONTAP tools for VMware vSphere 10.4로 마이그레이션

ONTAP tools for VMware vSphere 에서 10.4로 마이그레이션

ONTAP tools for VMware vSphere NetApp ONTAP 도구를 버전 9.xx에서 10.x로 옮기려면 버전 전반에 걸쳐 중요한 제품 업데이트와 개선 사항이 적용되므로 마이그레이션 프로세스가 필요합니다.

ONTAP tools for VMware vSphere 에서 ONTAP tools for VMware vSphere 로 마이그레이션할 수 있습니다.

설정에 NFS 및 VMFS 데이터 저장소가 있고 vVols 데이터 저장소가 없는 경우 ONTAP 도구 9.xx를 제거하고 ONTAP 도구 10.x를 배포하기만 하면 됩니다. 하지만 설정에 vVols 데이터 저장소가 포함된 경우 VASA 공급자와 SRA를 마이그레이션하는 프로세스를 거쳐야 합니다.

다음 표에서는 두 가지 시나리오에서의 마이그레이션 프로세스를 간략하게 설명합니다.

설정에 **vVols** 데이터 저장소가 있는 경우	설정에 **NFS** 및 **VMFS** 데이터 저장소만 포함된 경우
단계: 1. "VASA 공급자 마이그레이션" 2. "VM 스토리지 정책 생성"	단계: 1. 환경에서 ONTAP 도구 9.xx를 제거합니다. 참조하다 "환경에서 OTV 9.xx를 제거하는 방법" NetApp 기술 자료 문서. 2. "ONTAP tools for VMware vSphere 배포 및 구성" 3. "SRA 업데이트" 4. "VM 스토리지 정책 생성"

ONTAP tools for VMware vSphere 에서 10.4로 마이그레이션한 후, NVMe/FC 프로토콜을 사용하는 vVols 데이터 저장소는 작동하지 않습니다. ONTAP 도구 10.4는 VMFS 데이터 저장소에서만 NVMe-oF 프로토콜을 지원하기 때문입니다.

VASA 공급자를 마이그레이션하고 SRA를 업데이트합니다.

VASA 공급자를 마이그레이션하는 단계

1. ONTAP tools for VMware vSphere 에서 Derby PORT 1527을 활성화하려면 루트 사용자를 활성화하고 SSH를 통해 CLI에 로그인합니다. 그런 다음 다음 명령을 실행합니다.

   ```
   iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
   ```

2. ONTAP tools for VMware vSphere 배포합니다.
3. ONTAP tools for VMware vSphere 로 마이그레이션하려는 vCenter Server 인스턴스를 추가합니다. . "vCenter Server 인스턴스 추가" 자세한 내용은.
4. ONTAP 도구 플러그인을 위한 vCenter 서버 API에서 로컬로 스토리지 백엔드를 온보딩합니다.
5. Swagger 또는 Postman에서 다음 API를 실행하여 마이그레이션합니다.

   curl -X POST

`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migration-jobs`

다음 URL을 통해 Swagger에 액세스할 수 있습니다. `https://$FQDN_IP_PORT/', for example: `\https://10.67.25.33:8443 .`

HTTP 메서드 및 엔드포인트

이 REST API 호출은 다음 메서드와 엔드포인트를 사용합니다.

HTTP 방식	길
우편	/api/v1

처리 유형

비동기

컬 예시

curl -X POST'https://<OTV-NG-IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs' \ --header 'x-auth: <인증 토큰>' \ --header '콘텐츠 유형: application/json' \ --data '{ "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "username": "xxxxx", "password": "" }, "database_password": "" }'

다른 릴리스 마이그레이션에 대한 요청 본문:

{ "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "사용자 이름": "xxxxx", "비밀번호": "*" } }

JSON 출력 예시

작업 객체가 반환됩니다. 다음 단계에서 사용하려면 작업 식별자를 저장해야 합니다.

{ "id": 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "실행 중" }

6. Swagger에서 다음 URI를 사용하여 상태를 확인하세요.

```
curl
`\https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID
>?includeSubJobsAndTasks=true`
```

작업을 완료한 후 마이그레이션 보고서를 검토하세요. 이 보고서는 작업 데이터에 포함되어 있으며 작업 응답에서 접근할 수 있습니다.

7. vCenter Server에 ONTAP tools for VMware vSphere 추가"VASA 공급자 등록" ONTAP tools for VMware vSphere 사용.
8. "VASA 공급자 활성화"ONTAP tools for VMware vSphere 서비스.
9. 유지 관리 콘솔에서 ONTAP tools for VMware vSphere 중지합니다.

VASA 공급자를 삭제하지 마세요.

이전 VASA Provider가 중지되면 vCenter Server는 ONTAP tools for VMware vSphere 로 장애 조치됩니다. 모든 데이터스토어와 VM에 액세스할 수 있게 되고 ONTAP tools for VMware vSphere 에서 서비스를 제공합니다.

10. ONTAP tools for VMware vSphere 에서 마이그레이션된 NFS 및 VMFS 데이터 저장소는 데이터 저장소 검색 작업이 트리거된 후에만 ONTAP tools for VMware vSphere 에 표시되며, 완료하는 데 최대 30분이 걸릴 수 있습니다. VMware vSphere 플러그인 사용자 인터페이스 페이지의 ONTAP 도구 개요 페이지에 데이터 저장소가 표시되는지 확인하세요.
11. Swagger 또는 Postman에서 다음 API를 사용하여 패치 마이그레이션을 수행합니다.

HTTP 메서드 및 엔드포인트

이 REST API 호출은 다음 메서드와 엔드포인트를 사용합니다.

HTTP 방식	길
반점	/api/v1

처리 유형

비동기

컬 예시

curl -X 패치 `https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/84dr73bd-9173-65r7-w345-8ufdbb887d43`

JSON 출력 예시

작업 객체가 반환됩니다. 다음 단계에서 사용하려면 작업 식별자를 저장해야 합니다.

{ "id": 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "실행 중" }

패치 작업을 위한 요청 본문이 비어 있습니다.

UUID는 마이그레이션 후 API에 대한 응답으로 반환된 마이그레이션 UUID입니다.

패치 마이그레이션 API를 실행한 후 모든 VM이 스토리지 정책을 준수합니다.

다음은 무엇입니까**?**

마이그레이션을 완료하고 ONTAP 도구 10.4를 vCenter Server에 등록한 후 다음 단계를 따르세요.

- *검색*이 완료될 때까지 기다리면 모든 호스트에서 인증서가 자동으로 새로 고쳐집니다.
- 데이터스토어 및 가상 머신 작업을 시작하기 전에 충분한 시간을 두십시오. 필요한 대기 시간은 구성 내 호스트, 데이터스토어 및 가상 머신 수에 따라 다릅니다. 대기하지 않으면 간헐적인 운영 장애가 발생할 수 있습니다.

업그레이드 후 가상 머신의 규정 준수 상태가 오래된 경우 다음 단계에 따라 스토리지 정책을 다시 적용하세요.

1. 데이터 저장소로 이동하여 요약 > *VM 스토리지 정책*을 선택합니다.

   VM 스토리지 정책 준수 아래의 준수 상태가 *오래됨*으로 표시됩니다.

2. 저장소 VM 정책과 해당 VM을 선택하세요.
3. *적용*을 선택하세요

   *VM 스토리지 정책 준수*의 준수 상태가 이제 준수로 표시됩니다.

관련 정보

- "ONTAP tools for VMware vSphere 에 대해 알아보세요"
- "ONTAP tools for VMware vSphere 에서 10.4로 업그레이드"

스토리지 복제 어댑터(**SRA**)를 업데이트하는 단계

시작하기 전에

복구 계획에서 보호 사이트는 현재 VM이 실행 중인 위치를 나타내고, 복구 사이트는 VM이 복구될 위치를 나타냅니다. SRM 인터페이스는 보호 사이트와 복구 사이트에 대한 세부 정보와 함께 복구 계획의 상태를 표시합니다. 복구 계획에서 **CleanupP** 및 **Reprotect** 버튼은 비활성화되어 있지만, TEST 및 RUN 버튼은 활성화되어 있습니다. 이는 사이트가 데이터 복구를 위해 준비되었음을 나타냅니다. SRA를 마이그레이션하기 전에 한 사이트는 보호 상태이고 다른 사이트는 복구 상태인지 확인하십시오.

> 장애 조치가 완료되었지만 재보호가 보류 중인 경우 마이그레이션을 시작하지 마세요. 마이그레이션을 진행하기 전에 재보호 프로세스가 완료되었는지 확인하세요. 테스트 장애 조치가 진행 중인 경우 테스트 장애 조치를 정리하고 마이그레이션을 시작합니다.

1. VMware Site Recovery에서 VMware vSphere 9.xx용 ONTAP 도구 SRA 어댑터를 삭제하려면 다음 단계를 따르세요.
   a. VMware Live Site Recovery 구성 관리 페이지로 이동
   b. 저장소 복제 어댑터 섹션으로 이동합니다.
   c. 줄임표 메뉴에서 *구성 재설정*을 선택합니다.
   d. 줄임표 메뉴에서 *삭제*를 선택합니다.
2. 보호 사이트와 복구 사이트 모두에서 이 단계를 수행합니다.
   a. "ONTAP tools for VMware vSphere 활성화"
   b. 다음 단계를 사용하여 ONTAP tools for VMware vSphere 설치합니다."VMware Live Site Recovery 어플라이언스에서 SRA 구성" .
   c. VMware Live Site Recovery 사용자 인터페이스 페이지에서 어레이 검색 및 장치 검색 작업을 수행하고 마이그레이션 전과 같이 장치가 표시되는지 확인합니다.

REST API를 사용하여 자동화

ONTAP tools for VMware vSphere 에 대해 알아보세요.

ONTAP tools for VMware vSphere 가상 머신 수명 주기 관리를 위한 도구 세트입니다. 여기에는 자동화 프로세스의 일부로 사용할 수 있는 강력한 REST API가 포함되어 있습니다.

REST 웹 서비스 기반

REST(Representational State Transfer)는 웹 서비스 API 설계를 포함하여 분산 웹 애플리케이션을 만드는 데 사용되는 스타일입니다. 이는 서버 기반 리소스를 노출하고 해당 상태를 관리하기 위한 기술 세트를 확립합니다.

자원과 국가 대표

리소스는 REST 웹 서비스 애플리케이션의 기본 구성 요소입니다. REST API를 설계할 때 두 가지 중요한 초기 작업이 있습니다.

- 시스템 또는 서버 기반 리소스 식별
- 리소스 상태 및 연관된 상태 전환 작업을 정의합니다.

클라이언트 애플리케이션은 명확하게 정의된 메시지 흐름을 통해 리소스 상태를 표시하고 변경할 수 있습니다.

HTTP 메시지

하이퍼텍스트 전송 프로토콜(HTTP)은 웹 서비스 클라이언트와 서버가 리소스에 대한 메시지를 교환하는 데 사용되는 프로토콜입니다. 이는 생성, 읽기, 업데이트, 삭제와 같은 일반적인 작업을 기반으로 하는 CRUD 모델을 따릅니다. HTTP 프로토콜에는 요청 및 응답 헤더와 응답 상태 코드가 포함됩니다.

JSON 데이터 포맷

사용 가능한 메시지 형식은 여러 가지가 있지만 가장 인기 있는 옵션은 JSON(JavaScript Object Notation)입니다. JSON은 일반 텍스트로 간단한 데이터 구조를 표현하기 위한 산업 표준이며, 리소스와 원하는 작업을 설명하는 상태 정보를 전송하는 데 사용됩니다.

보안

보안은 REST API의 중요한 측면입니다. ONTAP tools for VMware vSphere 네트워크 상의 HTTP 트래픽을 보호하는 데 사용되는 TLS(전송 계층 보안) 프로토콜 외에도 인증을 위해 액세스 토큰을 사용합니다. 액세스 토큰을 획득하여 후속 API 호출에 사용해야 합니다.

비동기 요청 지원

ONTAP tools for VMware vSphere 대부분의 요청을 동기적으로 수행하며 작업이 완료되면 상태 코드를 반환합니다. 또한 완료하는 데 오랜 시간이 걸리는 작업에 대해 비동기 처리를 지원합니다.

ONTAP 도구 관리자 환경

ONTAP 도구 관리자 환경에는 고려해야 할 여러 가지 측면이 있습니다.

가상 머신

ONTAP tools for VMware vSphere vSphere 원격 플러그인 아키텍처를 사용하여 배포됩니다. REST API 지원을 포함한 소프트웨어는 별도의 가상 머신에서 실행됩니다.

ONTAP 도구 IP 주소

ONTAP tools for VMware vSphere 가상 머신 기능에 대한 게이트웨이를 제공하는 단일 IP 주소를 제공합니다. 초기 구성 중에 주소를 제공해야 하며 해당 주소는 내부 로드 밸런서 구성 요소에 할당됩니다. 이 주소는 ONTAP 도구 관리자 사용자 인터페이스에서 사용되며 Swagger 문서 페이지와 REST API에 직접 액세스하는 데에도 사용됩니다.

두 개의 REST API

ONTAP tools for VMware vSphere 외에도 ONTAP 클러스터에는 자체 REST API가 있습니다. ONTAP 도구 관리자는 ONTAP REST API를 클라이언트로 사용하여 스토리지 관련 작업을 수행합니다. 이 두 API는 별개이고 구별된다는 점을 명심하는 것이 중요합니다. 자세한 내용은 다음을 참조하세요. "ONTAP 자동화" .

ONTAP tools for VMware vSphere 에 대한 구현 세부 정보

REST는 공통적인 기술과 모범 사례를 확립하지만, 각 API의 정확한 구현은 설계 선택에 따라 달라질 수 있습니다. ONTAP tools for VMware vSphere 사용하기 전에 해당 도구가 어떻게 설계되었는지 숙지해야 합니다.

REST API에는 vCenter 및 집계와 같은 여러 리소스 범주가 포함됩니다. 검토하다"API 참조" 자세한 내용은.

REST API에 접근하는 방법

포트와 함께 ONTAP 도구 IP 주소를 통해 ONTAP tools for VMware vSphere 액세스할 수 있습니다. 전체 URL에는 다음을 포함한 여러 부분이 있습니다.

- ONTAP 도구 IP 주소 및 포트
- API 버전
- 리소스 카테고리
- 특정 리소스

초기 설정 과정에서 IP 주소를 구성해야 하며, 포트는 8443으로 고정되어 있습니다. URL의 첫 번째 부분은 ONTAP tools for VMware vSphere 에서 일관되며, 엔드포인트 간에 리소스 범주와 특정 리소스만 변경됩니다.

> 아래 예시의 IP 주소와 포트 값은 단지 설명 목적으로만 사용됩니다. 사용자 환경에 맞게 이 값을 변경해야 합니다.

인증 서비스에 액세스하는 예

```
https://10.61.25.34:8443/virtualization/api/v1/auth/login
```

이 URL은 POST 메서드를 사용하여 액세스 토큰을 요청하는 데 사용할 수 있습니다.

vCenter 서버를 나열하는 예

```
https://10.61.25.34:8443/virtualization/api/v1/vcenters
```

이 URL은 GET 메서드를 사용하여 정의된 vCenter 서버 인스턴스 목록을 요청하는 데 사용할 수 있습니다.

HTTP 세부 정보

ONTAP tools for VMware vSphere HTTP 및 관련 매개변수를 사용하여 리소스 인스턴스와 컬렉션에 대해 작업을

수행합니다. HTTP 구현에 대한 세부 사항은 아래와 같습니다.

HTTP 메서드

REST API가 지원하는 HTTP 메서드 또는 동사는 아래 표에 나와 있습니다.

방법	크러드	설명
얻다	읽다	리소스 인스턴스 또는 컬렉션에 대한 개체 속성을 검색합니다. 이것은 컬렉션과 함께 사용될 경우 목록 작업으로 간주됩니다.
우편	만들다	입력 매개변수를 기반으로 새로운 리소스 인스턴스를 생성합니다.
놓다	업데이트	제공된 JSON 요청 본문으로 전체 리소스 인스턴스를 업데이트합니다. 사용자가 수정할 수 없는 키 값은 그대로 유지됩니다.
반점	업데이트	요청에서 선택한 변경 사항 집합을 리소스 인스턴스에 적용하도록 요청합니다.
삭제	삭제	기존 리소스 인스턴스를 삭제합니다.

요청 및 응답 헤더

다음 표는 REST API와 함께 사용되는 가장 중요한 HTTP 헤더를 요약한 것입니다.

헤더	유형	사용 참고 사항
수용하다	요구	이는 클라이언트 애플리케이션이 수용할 수 있는 콘텐츠 유형입니다. 유효한 값에는 '*/*` 또는 `application/json` .
x-인증	요구	클라이언트 애플리케이션을 통해 요청을 발행하는 사용자를 식별하는 액세스 토큰이 포함되어 있습니다.
콘텐츠 유형	응답	서버에서 반환됨 `Accept` 요청 헤더.

HTTP 상태 코드

REST API에서 사용하는 HTTP 상태 코드는 아래와 같습니다.

암호	의미	설명
200	OK	새로운 리소스 인스턴스를 생성하지 않는 호출의 경우 성공을 나타냅니다.
201	생성됨	리소스 인스턴스에 대한 고유 식별자가 있는 개체가 성공적으로 생성되었습니다.
202	수락됨	요청이 수락되었고 요청을 수행하기 위한 백그라운드 작업이 생성되었습니다.
204	내용이 없습니다	요청은 성공했지만 콘텐츠가 반환되지 않았습니다.
400	잘못된 요청	요청 입력이 인식되지 않거나 부적절합니다.
401	허가받지 않음	사용자에게 권한이 없으므로 인증이 필요합니다.
403	금지됨	인증 오류로 인해 접근이 거부되었습니다.
404	찾을 수 없음	요청에 언급된 리소스가 존재하지 않습니다.
409	갈등	개체가 이미 존재하기 때문에 개체를 생성하려는 시도가 실패했습니다.

암호	의미	설명
500	내부 오류	서버에서 일반적인 내부 오류가 발생했습니다.

입증

REST API에 대한 클라이언트 인증은 액세스 토큰을 사용하여 수행됩니다. 토큰 및 인증 프로세스의 관련 특징은 다음과 같습니다.

- 클라이언트는 ONTAP 도구 관리자 자격 증명(사용자 이름 및 비밀번호)을 사용하여 토큰을 요청해야 합니다.
- 토큰은 JSON 웹 토큰(JWT) 형식으로 지정됩니다.
- 각 토큰은 60분 후에 만료됩니다.
- 클라이언트의 API 요청에는 토큰이 포함되어야 합니다. `x-auth` 요청 헤더.

참조하다"첫 번째 REST API 호출" 액세스 토큰을 요청하고 사용하는 예를 들어 보겠습니다.

동기 및 비동기 요청

대부분의 REST API 호출은 빠르게 완료되므로 동기적으로 실행됩니다. 즉, 요청이 완료된 후 상태 코드(예: 200)를 반환합니다. 완료하는 데 시간이 오래 걸리는 요청은 백그라운드 작업을 사용하여 비동기적으로 실행됩니다.

비동기적으로 실행되는 API 호출을 실행한 후 서버는 202 HTTP 상태 코드를 반환합니다. 이는 요청이 수락되었지만 아직 완료되지 않았음을 나타냅니다. 백그라운드 작업을 쿼리하여 성공 또는 실패 등의 상태를 확인할 수 있습니다.

비동기 처리는 데이터 저장소 및 vVol 작업을 포함한 여러 유형의 장기 실행 작업에 사용됩니다. 자세한 내용은 Swagger 페이지에서 REST API의 작업 관리자 범주를 참조하세요.

ONTAP tools for VMware vSphere

curl을 사용하여 API 호출을 실행하면 ONTAP tools for VMware vSphere 를 시작할 수 있습니다.

시작하기 전에

curl 예제에 필요한 정보와 매개변수를 검토해야 합니다.

필수 정보

다음이 필요합니다.

- ONTAP tools for VMware vSphere
- ONTAP 도구 관리자 관리자(사용자 이름 및 비밀번호)에 대한 자격 증명

매개변수와 변수

아래에 제시된 curl 예제에는 Bash 스타일 변수가 포함되어 있습니다. Bash 환경에서 이러한 변수를 설정하거나 명령을 실행하기 전에 수동으로 업데이트할 수 있습니다. 변수를 설정하면 셸은 실행하기 전에 각 명령에 값을 대입합니다. 변수는 아래 표에 설명되어 있습니다.

변하기 쉬운	설명
$FQDN_IP_포트	ONTAP 도구 관리자의 정규화된 도메인 이름 또는 IP 주소와 포트 번호입니다.
$MYUSER	ONTAP 도구 관리자 계정의 사용자 이름입니다.
$MYPASSWORD	ONTAP 도구 관리자 사용자 이름과 연결된 비밀번호입니다.
$액세스_토큰	ONTAP 도구 관리자가 발급한 액세스 토큰입니다.

다음 Linux CLI 명령과 출력은 변수를 설정하고 표시하는 방법을 보여줍니다.

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

1단계: 액세스 토큰 획득

REST API를 사용하려면 액세스 토큰을 얻어야 합니다. 액세스 토큰을 요청하는 방법의 예는 아래와 같습니다. 귀하의 환경에 적합한 값으로 대체해야 합니다.

```
curl --request POST \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/login” \
--header "Content-Type: application/json" \
--header "Accept: */*" \
-d "{"username": "$MYUSER", "password": "$MYPASSWORD"}"
```

응답에서 제공된 액세스 토큰을 복사하여 저장합니다.

2단계: REST API 호출 실행

액세스 토큰을 받으면 curl을 사용하여 REST API 호출을 실행할 수 있습니다. 첫 번째 단계에서 획득한 액세스 토큰을 포함하세요.

컬 예시

```
curl --request GET \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/vcenters" \
--header "Accept: */*" \
--header "x-auth: $ACCESS_TOKEN"
```

JSON 응답에는 ONTAP 도구 관리자에 구성된 VMware vCenter 인스턴스 목록이 포함됩니다.

ONTAP tools for VMware vSphere 에 대한 API 참조

ONTAP tools for VMware vSphere 모든 API 호출에 대한 세부 정보가 포함되어 있습니다. 이

참고 자료는 자동화 애플리케이션을 개발할 때 유용합니다.

Swagger 사용자 인터페이스를 통해 ONTAP tools for VMware vSphere 온라인으로 액세스할 수 있습니다. ONTAP tools for VMware vSphere 의 IP 주소 또는 FQDN과 포트가 필요합니다.

단계

1. 브라우저에 다음 URL을 입력하고 변수에 적절한 IP 주소와 포트 조합을 입력한 다음 **Enter** 키를 누릅니다.

   ```
   https://$FQDN_IP_PORT/
   ```

   예

   ```
   https://10.61.25.33:8443/
   ```

2. 개별 API 호출의 예로, **vCenters** 범주로 스크롤하여 엔드포인트 옆에 있는 *GET*을 선택합니다. `/virtualization/api/v1/vcenters`

법적 고지 사항

법적 고지사항은 저작권 표시, 상표, 특허 등에 대한 정보를 제공합니다.

저작권

"https://www.netapp.com/company/legal/copyright/"

상표

NETAPP, NETAPP 로고 및 NetApp 상표 페이지에 나열된 마크는 NetApp, Inc.의 상표입니다. 다른 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

"https://www.netapp.com/company/legal/trademarks/"

특허

NetApp 이 소유한 현재 특허 목록은 다음에서 확인할 수 있습니다.

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

개인정보 보호정책

"https://www.netapp.com/company/legal/privacy-policy/"

오픈소스

공지 파일은 NetApp 소프트웨어에서 사용되는 타사 저작권 및 라이선스에 대한 정보를 제공합니다.

"ONTAP tools for VMware vSphere 에 대한 알림"

저작권 정보

Copyright © 2025 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 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.