



ONTAP tools for VMware vSphere 설명서

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

목차

ONTAP tools for VMware vSphere 설명서	1
릴리스 노트	2
ONTAP tools 릴리스 노트	2
ONTAP tools for VMware vSphere 10.5의 새로운 기능	2
지원되는 ONTAP 플랫폼 및 vCenter Server 버전	3
ONTAP tools for VMware vSphere 9 및 10 기능 비교	3
개념	5
ONTAP 도구에 대해 알아보세요	5
ONTAP 도구의 주요 개념 및 용어	5
역할 기반 액세스 제어(RBAC)	8
ONTAP 도구 RBAC에 대해 알아보십시오	8
VMware vSphere를 사용한 RBAC	10
ONTAP를 사용한 RBAC	16
ONTAP tools for VMware vSphere 배포	20
ONTAP tools for VMware vSphere 빠른 시작	20
ONTAP 도구의 고가용성 배포 워크플로	22
ONTAP tools for VMware vSphere 요구 사항 및 구성 제한	22
시스템 요구 사항	23
최소 스토리지 및 애플리케이션 요구사항	23
포트 요구 사항	23
ONTAP tools for VMware vSphere를 vVols 데이터스토어에 배포하기 위한 구성 한계	26
VMFS 및 NFS 데이터스토어용 ONTAP tools for VMware vSphere 배포를 위한 구성 제한	26
ONTAP tools for VMware vSphere - Storage Replication Adapter (SRA)	27
ONTAP 도구 배포 전 요구 사항	27
배포 워크시트	28
네트워크 방화벽 구성	29
ONTAP 스토리지 설정	29
ONTAP tools 배포	29
ONTAP 도구 배포 오류 해결	34
로그 파일 수집	35
배포 오류 코드	35
ONTAP tools for VMware vSphere 구성	39
vCenter Server 인스턴스를 ONTAP tools에 추가합니다	39
ONTAP 도구에서 VASA Provider를 vCenter Server 인스턴스에 등록합니다	40
ONTAP tools를 사용하여 NFS VAAI 플러그인 설치	41
ONTAP tools에서 ESXi 호스트 설정을 구성합니다	42
ESXi 서버 다중 경로 및 타임아웃 설정 구성	42
ESXi 호스트 값 설정	42
ONTAP tools에 대한 ONTAP 사용자 역할 및 권한을 구성합니다	43

SVM 애그리게이트 매핑 요구 사항	44
ONTAP 사용자 및 역할을 수동으로 생성	44
ONTAP tools for VMware vSphere 10.1 사용자를 10.3 사용자로 업그레이드	52
ONTAP tools for VMware vSphere 10.3 사용자를 10.4 사용자로 업그레이드	54
ONTAP tools에 스토리지 백엔드 추가	55
ONTAP 도구에서 스토리지 백엔드를 vCenter Server 인스턴스에 연결합니다	57
ONTAP 도구에서 네트워크 액세스 구성	57
ONTAP tools에서 데이터 저장소를 생성합니다	58
데이터 저장소 및 가상 머신 보호	63
ONTAP tools에서 호스트 클러스터 보호	63
SRA 보호를 사용하여 보호	64
데이터 저장소를 보호하려면 ONTAP tools에서 SRA를 구성하십시오	64
SAN 및 NAS 환경용 ONTAP tools에서 SRA 구성	65
확장성이 높은 환경을 위해 ONTAP tools에서 SRA를 구성합니다	66
ONTAP tools를 사용하여 VMware Live Site Recovery 어플라이언스에서 SRA를 구성합니다	67
ONTAP tools에서 SRA 자격 증명 업데이트	68
ONTAP tools에서 보호 사이트 및 복구 사이트를 구성합니다	69
보호 사이트 및 복구 사이트 리소스 구성	70
ONTAP tools에서 복제된 스토리지 시스템을 검증합니다	74
ONTAP 도구의 팬아웃 보호	74
ONTAP tools for VMware vSphere 관리	78
ONTAP 도구 대시보드에 대해 알아보십시오	78
ONTAP tools가 igroup 및 익스포트 정책을 관리하는 방법	79
익스포트 정책	83
ONTAP tools에서 igroup을 관리하는 방법	84
간략한 동작 요약	84
igroup 컨텍스트	84
명명 동작	85
시나리오별 동작	85
사용자 정의 igroup 재사용 및 API 동작	86
네이티브에서 관리형으로의 전환 보기	86
발견된 네이티브 igroup의 재사용	87
ONTAP tools Manager 사용자 인터페이스에 대해 알아보십시오	88
ONTAP tools Manager 설정 관리	90
ONTAP 도구 AutoSupport 설정 편집	90
ONTAP tools에 NTP 서버 추가	91
ONTAP tools에서 VASA Provider 및 SRA 자격 증명을 재설정합니다	91
ONTAP 도구 백업 설정 편집	91
ONTAP 툴 서비스를 활성화합니다	92
ONTAP 도구 어플라이언스 설정을 변경합니다	92
ONTAP tools에 VMware vSphere 호스트 추가	93

데이터 저장소 관리	94
ONTAP 도구에서 NFS 및 VMFS 데이터 저장소를 마운트합니다	94
ONTAP 도구에서 NFS 및 VMFS 데이터 저장소 마운트 해제	94
ONTAP tools에서 vVols 데이터 저장소 마운트	95
ONTAP 도구에서 NFS 및 VMFS 데이터 저장소 크기 조정	96
ONTAP tools에서 vVols 데이터 저장소 확장	96
ONTAP tools에서 vVols 데이터스토어 축소	96
ONTAP 도구에서 데이터 저장소를 삭제합니다	97
ONTAP tools의 데이터 저장소용 ONTAP 스토리지 뷰	98
ONTAP tools의 가상 머신 스토리지 보기	98
ONTAP tools에서 스토리지 임계값 관리	99
ONTAP tools에서 스토리지 백엔드 관리	99
스토리지 검색	99
스토리지 백엔드 수정	99
스토리지 백엔드 제거	100
스토리지 백엔드에 대한 상세 보기	100
ONTAP tools에서 vCenter Server 인스턴스 관리	101
vCenter Server 인스턴스와 스토리지 백엔드 연결을 해제합니다	101
vCenter Server 인스턴스 수정	101
vCenter Server 인스턴스 제거	102
vCenter 서버 인증서 갱신	102
ONTAP 도구 인증서 관리	104
VMware vSphere 유지 관리 콘솔용 ONTAP tools에 액세스합니다	106
ONTAP 도구 유지 관리 콘솔에 대해 알아보십시오	106
ONTAP tools에 대한 원격 진단 액세스 구성	107
다른 ONTAP tools 노드에서 SSH를 시작하세요	107
ONTAP tools에서 vCenter Server 자격 증명 업데이트	108
ONTAP tools에서 인증서 유효성 검사 플래그를 변경합니다	108
ONTAP tools 보고서	110
가상 머신 관리	111
ONTAP tools를 사용한 가상 머신 마이그레이션 및 복제 시 고려 사항	111
ONTAP tools에서 가상 머신을 vVols 데이터 저장소로 마이그레이션합니다	112
ONTAP tools에서 VASA 구성을 정리합니다	112
ONTAP tools에서 VM에 데이터 디스크 연결 또는 분리	113
ONTAP tools에서 스토리지 시스템 및 호스트 검색	114
ONTAP tools를 사용하여 ESXi 호스트 설정 수정	114
비밀번호 관리	115
ONTAP tools Manager 비밀번호 변경	115
ONTAP tools Manager 비밀번호 재설정	115
ONTAP tools에서 애플리케이션 사용자 암호 재설정	116
ONTAP tools 유지 관리 콘솔 암호를 재설정합니다	116

호스트 클러스터 보호 관리	117
ONTAP tools에서 보호된 호스트 클러스터를 수정합니다.	117
ONTAP tools에서 호스트 클러스터 보호 제거	120
ONTAP tools 설정 복구	121
ONTAP 도구를 제거합니다.	122
ONTAP tools 제거 후 FlexVol 볼륨 제거	122
ONTAP tools for VMware vSphere 업그레이드	124
VMware vSphere 10.x용 ONTAP tools에서 10.5으로 업그레이드	124
ONTAP tools 업그레이드 오류 코드	126
ONTAP tools for VMware vSphere 9.xx를 10.5으로 마이그레이션	132
ONTAP tools for VMware vSphere 9.xx에서 10.5으로 마이그레이션	132
VASA Provider를 마이그레이션하고 ONTAP tools에서 SRA를 업데이트합니다.	132
VASA Provider 마이그레이션 단계	132
스토리지 복제 어댑터(SRA) 업데이트 단계	137
REST API를 사용하여 자동화	139
ONTAP 도구 REST API에 대해 알아보십시오.	139
REST 웹 서비스 기반	139
ONTAP tools Manager 환경	139
ONTAP tools REST API 구현 세부 정보	140
REST API에 액세스하는 방법	140
HTTP 세부 정보	141
인증	142
동기 및 비동기 요청	142
첫 번째 ONTAP tools REST API 호출	142
시작하기 전에	142
1단계: 액세스 토큰 획득	143
2단계: REST API 호출 실행	143
ONTAP tools REST API 참조	144
법적 고지	145
저작권	145
상표	145
특허	145
개인정보 보호정책	145
오픈 소스	145

ONTAP tools for VMware vSphere 설명서

릴리스 노트

ONTAP tools 릴리스 노트

ONTAP tools for VMware vSphere 10.5에서 사용할 수 있는 새롭고 향상된 기능에 대해 알아보십시오.

새로운 기능 및 개선 사항의 전체 목록은 [ONTAP tools for VMware vSphere 10.5의 새로운 기능](#)(를) 참조하십시오.

최신 호환성 정보는 "[NetApp 상호 운용성 매트릭스 도구](#)"를 참조하십시오.

ONTAP tools for VMware vSphere 9.12D1, 9.13D2 및 9.13P2 릴리스에서 ONTAP tools for VMware vSphere 10.5으로의 마이그레이션이 지원됩니다.

자세한 내용은 "[ONTAP tools for VMware vSphere 10.5 릴리스 노트](#)"를 참조하십시오. 릴리스 노트에 액세스하려면 NetApp 계정으로 로그인하거나 새 계정을 만들어야 합니다.

ONTAP tools for VMware vSphere 10.5의 새로운 기능

ONTAP tools for VMware vSphere 10.5에서 사용할 수 있는 새로운 기능에 대해 알아보십시오.

- 플랫폼 자격

ONTAP tools for VMware vSphere 10.5는 ASA r2 시스템에 대한 지원을 추가하여 최신 하드웨어 및 소프트웨어 구성과의 호환성을 제공합니다. 이번 릴리스에는 ONTAP 9.16.1 및 9.17.1과의 통합도 포함되어 지원되는 환경이 확장되었습니다.

- **VMware** 자격 및 인증

ONTAP tools for VMware vSphere 10.5는 최신 VMware 상호 운용성 인증 표준을 준수하여 ESXi 호스트와 vCenter Server를 모두 지원합니다.

- **MetroCluster** 지원

이번 릴리스에서는 MetroCluster 구성 지원이 도입되어 고가용성 및 재해 복구 기능이 향상되었습니다.

- 보안 및 인증서 관리

이번 릴리스에서는 자체 서명 인증서 관리 기능이 간소화되어 사용자 경험과 보안 표준 준수성이 모두 향상되었습니다. ONTAP 및 VMware vSphere 통신을 위한 ONTAP tools for VMware vSphere의 보안을 강화하기 위해 개선된 인증서 유효성 검사 워크플로를 제공합니다.

- 복제 기능 향상

이번 릴리스에서는 ASA r2 시스템에서 SRA 및 SnapMirror 활성 동기화를 포함한 계층적 일관성 그룹을 사용하는 VMFS 복제를 지원합니다. 또한 데이터 보호 및 복구를 향상시키기 위해 제로 RPO 백업을 지원합니다.

- 업그레이드 및 마이그레이션

이전 버전의 ONTAP tools for VMware vSphere에서 ONTAP tools for VMware vSphere 10.5로의 업그레이드 및 마이그레이션 프로세스는 다운타임을 최소화하고 원활한 전환을 보장하도록 원활하고 효율적으로 설계되었습니다.

지원되는 ONTAP 플랫폼 및 vCenter Server 버전

ONTAP tools for VMware vSphere 10.5 P1은 SRA 및 SnapMirror active sync 구성 요소에 대한 vCenter 고가용성(HA) 구성을 지원합니다. 이 구성에서는 vVols가 지원되지 않습니다. HA 장애 조치 중에는 vCenter가 몇 분 동안 사용할 수 없을 수 있습니다. 대규모 환경이거나 오류가 발생한 경우, 장애 조치 시간이 15분을 초과할 수 있습니다.

자세한 내용은 "[vCenter 고가용성 문서](#)"를 참조하십시오. vCenter HA에 대한 질문은 "[Broadcom 지원](#)"에 문의하십시오.

최신 버전 호환성 정보는 "[NetApp 상호 운용성 매트릭스 도구](#)"를 참조하십시오.

ONTAP tools for VMware vSphere 9 및 10 기능 비교

ONTAP tools for VMware vSphere 9에서 ONTAP tools for VMware vSphere 10.2 이상 버전으로 마이그레이션하는 것이 귀사에 적합한지 알아보십시오.



최신 호환성 정보는 "[NetApp 상호 운용성 매트릭스 도구](#)"를 참조하십시오.

기능	ONTAP tools 9.13	ONTAP tools 10.2 이상
핵심 가치 제안	향상된 보안, 규정 준수 및 자동화 기능을 통해 day-0부터 day-2 운영을 효율적으로 간소화하세요.	VMFS용 FC 및 VMFS 전용 NVMe-oF를 포함하도록 지원 범위가 확장되었습니다. NetApp SnapMirror의 사용 편의성, vSphere 메트로 스토리지 클러스터의 간편한 설정, 그리고 3개 사이트 VMware Live Site Recovery 지원
ONTAP 릴리스 자격	ONTAP 9.9.1부터 ONTAP 9.16.1까지	ONTAP tools 10.2의 경우 ONTAP 9.12.1~9.15.1. ONTAP tools 10.3의 경우 ONTAP 9.14.1, 9.15.1, 9.16.0 및 9.16.1. ONTAP tools 10.4의 경우 ONTAP 9.14.1, 9.15.1, 9.16.0 및 9.16.1. ASA r2 시스템을 사용하는 경우 ONTAP tools 10.4에는 ONTAP 9.16.1P3 이상이 필요합니다. ONTAP tools 10.5의 경우 ONTAP 9.15.1, 9.16.1 및 9.17.0
VMware 릴리스 지원	vSphere 7.x-8.x VMware Site Recovery Manager(SRM) 8.5부터 VMware Live Site Recovery 9.0까지	vSphere 7.x-8.x vSphere 9.0 ONTAP tools 10.5 이상 VMware Site Recovery Manager(SRM) 8.7부터 VMware Live Site Recovery 9.0까지 참고: ONTAP tools 10.x에서 SRM은 공유 사이트를 지원하여 확장성과 성능을 향상시킵니다.
프로토콜 지원	NFS 및 VMFS 데이터 저장소: NFS(v3 및 v4.1), VMFS(iSCSI 및 FCP)	NFS 및 VMFS 데이터 저장소: NFS(v3 및 v4.1), VMFS(iSCSI/FCP/NVMe-oF)

기능	ONTAP tools 9.13	ONTAP tools 10.2 이상
확장성	호스트 및 VM: 호스트 300개, VM 최대 1만 개 데이터 저장소: NFS 600개, VMFS 최대 50개	호스트 및 가상 머신: 호스트 600개
관측 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
데이터 보호	VMFS 및 NFS용 SRA 복제. SCV 통합 및 백업을 위한 상호 운용성.	iSCSI VMFS 및 NFS v3 데이터스토어용 SRA 복제, SMAS 및 VMware Live Site Recovery를 결합한 3개 사이트 보호. VMFS를 사용한 FCP에 대한 SRA 지원.
VASA Provider 지원	VASA 4.0	VASA 3.0

개념

ONTAP 도구에 대해 알아보세요

ONTAP tools for VMware vSphere는 가상 머신 수명 주기 관리를 위한 도구 모음입니다. VMware 에코시스템과 통합되어 데이터스토어 프로비저닝을 간소화하고 가상 머신에 대한 기본 보호 기능을 제공합니다. 이는 수평 확장이 가능하고 이벤트 기반의 마이크로서비스 모음으로, 개방형 가상 어플라이언스(OVA) 형태로 배포됩니다.

ONTAP tools for VMware vSphere은 다음을 지원합니다:

- 가상 머신(VM)의 핵심 기능(예: 보호 및 재해 복구)
- 스토리지 정책 기반 관리를 위한 VASA Provider
- 스토리지 정책 기반 관리
- 스토리지 복제 어댑터(SRA)

VMware용 ONTAP tools for VMware의 고가용성

ONTAP tools for VMware vSphere는 장애 발생 시에도 중단 없는 운영을 유지할 수 있도록 고가용성(HA) 지원을 제공합니다.

HA 솔루션은 다음과 같은 유형의 장애 발생 시 신속한 복구를 지원합니다.

- 호스트 장애 - 단일 노드 장애만 지원됩니다.
- 네트워크 오류
- 가상 머신(게스트 OS) 오류
- 애플리케이션(ONTAP tools) 오류

ONTAP tools for VMware vSphere에 대해 HA를 활성화하기 위해 추가 구성을 수행할 필요가 없습니다.



ONTAP tools for VMware vSphere는 vCenter HA를 지원하지 않습니다.

HA 기능을 사용하려면 배포 중 또는 VM 설정에서 CPU 핫 추가 및 메모리 핫 플러그가 활성화되어 있는지 확인하십시오.

ONTAP 도구의 주요 개념 및 용어

다음 절에서는 문서에서 사용된 주요 개념과 용어를 설명합니다.

인증 기관(CA)

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

일관성 그룹

일관성 그룹은 단일 단위로 관리되는 블록 모음입니다. 일관성 그룹은 스토리지 장치 및 블록 간의 데이터 일관성을 위해 동기화됩니다. ONTAP에서는 여러 블록에 걸쳐 있는 애플리케이션 워크로드에 대해 간편한 관리와 보호 기능을 제공합니다. 자세한 내용은 "[일관성 그룹](#)"을 참조하십시오.

듀얼 스택

듀얼 스택 네트워크는 IPv4 및 IPv6 주소를 동시에 사용할 수 있도록 지원하는 네트워킹 환경입니다.

고가용성(HA)

클러스터 노드는 중단 없는 운영을 위해 고가용성(HA) 쌍으로 구성됩니다.

논리 유닛 번호(LUN)

LUN(Logical Unit Number)은 SAN(Storage Area Network) 내의 논리 장치를 식별하는 데 사용되는 번호입니다. 이러한 주소 지정 가능한 장치는 일반적으로 SCSI(Small Computer System Interface) 프로토콜 또는 그 파생 프로토콜을 통해 액세스되는 논리 디스크입니다.

NVMe 네임스페이스 및 서브시스템

NVMe 네임스페이스는 논리적 블록으로 포맷할 수 있는 비휘발성 메모리 영역입니다. 네임스페이스는 FC 및 iSCSI 프로토콜의 LUN에 해당하며, NVMe 서브시스템은 igroup과 유사합니다. NVMe 서브시스템은 이니시에이터와 연결될 수 있으며, 연결된 이니시에이터는 해당 서브시스템 내의 네임스페이스에 액세스할 수 있습니다.

ONTAP tools Manager

ONTAP tools Manager는 ONTAP tools for VMware vSphere 관리자가 관리되는 vCenter Server 인스턴스와 온보딩된 스토리지 백엔드를 보다 효과적으로 제어할 수 있도록 지원합니다. 이 도구는 vCenter Server 인스턴스, 스토리지 백엔드, 인증서, 비밀번호, 로그 번들을 관리하는 데 도움이 됩니다.

Open Virtual Appliance(OVA)

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

복구 시점 목표(RPO)

RPO(복구 시점 목표)는 데이터 백업 또는 복제 빈도를 측정하는 지표입니다. 장애 발생 후 비즈니스 운영을 재개하기 위해 데이터를 복원해야 하는 정확한 시점을 지정합니다. 예를 들어, 조직의 RPO가 4시간이라면 재해 발생 시 최대 4시간 분량의 데이터 손실을 감당할 수 있다는 의미입니다.

SnapMirror 액티브 동기화

SnapMirror 액티브 싱크는 사이트 전체 장애 발생 시에도 비즈니스 서비스가 계속 운영될 수 있도록 지원하며, 보조 복사본을 사용하여 애플리케이션이 투명하게 장애 조치를 수행할 수 있도록 합니다. SnapMirror 액티브 싱크를 사용하면 수동 개입이나 사용자 지정 스크립팅 없이도 장애 조치를 실행할 수 있습니다. 자세한 내용은 "[SnapMirror 액티브 동기화](#)"을 참조하십시오.

스토리지 백엔드

스토리지 백엔드는 ESXi 호스트가 가상 머신 파일, 데이터 및 기타 리소스를 저장하는 데 사용하는 기본 스토리지 인프라입니다. 이를 통해 ESXi 호스트는 영구 데이터에 액세스하고 관리할 수 있으며, 가상화 환경에 필요한 스토리지 용량과 성능을 제공합니다.

글로벌 클러스터(스토리지 백엔드)

ONTAP 클러스터 자격 증명으로만 사용 가능한 글로벌 스토리지 백엔드는 ONTAP tools Manager 인터페이스를 통해 온보딩됩니다. 최소한의 권한으로 추가하여 vVols 관리에 필요한 필수 클러스터 리소스를 검색할 수 있습니다. 글로벌 클러스터는 SVM 사용자를 로컬에 추가하여 vVols 관리를 수행하는 멀티테넌시 시나리오에 적합합니다.

로컬 스토리지 백엔드

클러스터 또는 SVM 자격 증명을 사용하는 로컬 스토리지 백엔드는 ONTAP tools 사용자 인터페이스를 통해 추가되며 vCenter로 제한됩니다. 로컬에서 클러스터 자격 증명을 사용하는 경우 연결된 SVM은 vCenter와 자동으로 매핑되어 vVols 또는 VMFS를 관리합니다. SRA를 포함한 VMFS 관리의 경우 ONTAP tools는 글로벌 클러스터 없이도 SVM 자격 증명을 지원합니다.

스토리지 복제 어댑터(SRA)

SRA는 VMware Live Site Recovery 어플라이언스 내부에 설치되는 스토리지 공급업체별 소프트웨어입니다. 이 어댑터를 통해 Site Recovery Manager와 스토리지 컨트롤러 간의 스토리지 가상 머신(SVM) 수준 및 클러스터 수준 구성에서 통신이 가능합니다.

스토리지 가상 머신(SVM)

SVM은 ONTAP의 멀티 테넌시 단위입니다. 하이퍼바이저에서 실행되는 가상 머신과 마찬가지로 SVM은 물리적 리소스를 추상화하는 논리적 엔티티입니다. SVM은 데이터 볼륨과 하나 이상의 LIF를 포함하며, 이를 통해 클라이언트에게 데이터를 제공합니다.

균일한 구성과 불균일한 구성

- *균일한 호스트 액세스*란 두 사이트의 호스트가 양쪽 사이트의 스토리지 클러스터에 대한 모든 경로에 연결되어 있음을 의미합니다. 사이트 간 경로는 거리에 걸쳐 확장됩니다.
- *비균일 호스트 액세스*란 각 사이트의 호스트가 동일 사이트 내의 클러스터에만 연결되는 것을 의미합니다. 사이트 간 경로 및 확장된 경로는 연결되지 않습니다.



균일한 호스트 액세스는 모든 SnapMirror 활성 동기화 배포에서 지원됩니다. 비균일한 호스트 액세스는 대칭형 활성/활성 배포에서만 지원됩니다. 자세한 내용은 "[SnapMirror active sync ONTAP 개요](#)"을 참조하십시오.

가상 머신 파일 시스템(VMFS)

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

가상 볼륨(vVols)

vVols는 가상 머신에서 사용하는 스토리지에 대한 볼륨 수준의 추상화를 제공합니다. 이는 여러 가지 이점을 제공하며 기존 LUN을 사용하는 것에 대한 대안이 될 수 있습니다. vVol 데이터스토어는 일반적으로 vVols의 컨테이너 역할을 하는 단일 LUN과 연결됩니다.

VM 스토리지 정책

VM 스토리지 정책은 vCenter Server의 정책 및 프로필에서 생성합니다. vVols의 경우 NetApp vVols 스토리지 유형 공급자의 규칙을 사용하여 규칙 세트를 생성합니다.

VMware Live Site Recovery

VMware Live Site Recovery(이전 명칭: Site Recovery Manager(SRM))는 VMware 가상 환경을 위한 비즈니스 연속성, 재해 복구, 사이트 마이그레이션 및 중단 없는 테스트 기능을 제공합니다.

VMware vSphere APIs for Storage Awareness(VASA)

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

VMware vSphere Storage APIs - Array Integration(VAAI)

VAAI는 VMware vSphere ESXi 호스트와 스토리지 장치 간의 통신을 가능하게 하는 API 세트입니다. 이 API에는 호스트가 스토리지 작업을 어레이로 오프로드하는 데 사용하는 기본 작업 세트가 포함되어 있습니다. VAAI는 스토리지 집약적인 작업에서 상당한 성능 향상을 제공할 수 있습니다.

vSphere Metro 스토리지 클러스터

vSphere Metro Storage Cluster(vMSC)는 확장 클러스터 배포 환경에서 vSphere를 지원하고 활성화하는 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 사용자의 특정 구성 선택에 따라 달라집니다. 자세한 내용은 "[VMware vSphere Metro 스토리지 클러스터](#)"를 참조하십시오.

vVols 데이터스토어

vVols 데이터 저장소는 VASA Provider가 생성하고 유지 관리하는 vVols 컨테이너의 논리적 표현입니다.

제로 RPO

RPO는 복구 시점 목표(Recovery Point Objective)의 약자로, 주어진 시간 동안 허용 가능한 데이터 손실량을 나타냅니다. RPO가 0이면 데이터 손실이 전혀 허용되지 않음을 의미합니다.

역할 기반 액세스 제어(RBAC)

ONTAP 도구 RBAC에 대해 알아보십시오

역할 기반 액세스 제어(RBAC)는 조직 내 리소스에 대한 액세스를 제어하는 보안 프레임워크입니다. RBAC는 개별 사용자에게 권한을 할당하는 대신, 특정 수준의 권한을 가진 역할을 정의하여 작업을 수행하도록 함으로써 관리를 간소화합니다. 정의된 역할이 사용자에게 할당되므로 오류 발생 위험을 줄이고 조직 전체의 액세스 제어 관리를 간소화할 수 있습니다.

RBAC 표준 모델은 복잡성이 점차 증가하는 여러 구현 기술 또는 단계로 구성됩니다. 결과적으로 소프트웨어 공급업체와 고객의 요구 사항에 따라 실제 RBAC 배포는 비교적 단순한 것부터 매우 복잡한 것까지 다양할 수 있습니다.

RBAC 구성 요소

전반적으로 볼 때, 모든 RBAC 구현에는 일반적으로 몇 가지 구성 요소가 포함됩니다. 이러한 구성 요소들은 권한 부여 프로세스를 정의하는 과정에서 다양한 방식으로 서로 연결됩니다.

Privileges

`_Privilege_`는 허용하거나 거부할 수 있는 작업 또는 기능입니다. 파일 읽기와 같은 간단한 권한일 수도 있고, 특정 소프트웨어 시스템에 특화된 추상적인 작업 권한일 수도 있습니다. Privileges는 REST API 엔드포인트 및 CLI 명령에 대한 접근을 제한하도록 정의할 수도 있습니다. 모든 RBAC 구현에는 미리 정의된 Privileges가 포함되어 있으며, 관리자가 사용자 지정 Privileges를 생성할 수 있도록 허용하는 경우도 있습니다.

역할

역할(role)은 하나 이상의 권한을 포함하는 컨테이너입니다. 역할은 일반적으로 특정 작업이나 직무를 기반으로 정의됩니다. 사용자에게 역할이 할당되면 해당 역할에 포함된 모든 권한이 사용자에게 부여됩니다. 권한과 마찬가지로, 구현에는 미리 정의된 역할이 포함되며 일반적으로 사용자 지정 역할을 생성할 수 있습니다.

객체

객체는 RBAC 환경 내에서 식별되는 실제 또는 추상적인 리소스를 나타냅니다. 권한을 통해 정의된 작업은 연결된 객체에 대해 또는 연결된 객체와 함께 수행됩니다. 구현 방식에 따라 객체 유형 또는 특정 객체 인스턴스에 권한을 부여할 수 있습니다.

사용자 및 그룹

*Users*는 인증 후 적용되는 역할에 할당되거나 연결됩니다. 일부 RBAC 구현에서는 사용자에게 하나의 역할만 할당할 수 있지만, 다른 구현에서는 사용자당 여러 역할을 허용하며, 경우에 따라 한 번에 하나의 역할만 활성화할 수 있습니다. 그룹에 역할을 할당하면 보안 관리를 더욱 간소화할 수 있습니다.

권한

권한(permission)은 사용자 또는 그룹과 역할을 객체에 연결하는 정의입니다. 권한은 계층적 객체 모델에서 유용하게 사용될 수 있으며, 계층 구조 내의 하위 객체들이 선택적으로 권한을 상속받을 수 있습니다.

두 개의 RBAC 환경

ONTAP tools for VMware vSphere 10을 사용할 때 고려해야 할 두 가지 별개의 RBAC 환경이 있습니다. ONTAP tools for VMware vSphere 10은 작업을 수행하기 위해 vCenter와 ONTAP 모두에서 특정 권한이 필요합니다. ONTAP 도구는 스토리지 관리 작업을 자동화하지만 vCenter 또는 ONTAP에서 사용자 계정을 생성하지 않습니다. 서비스 계정은 필요에 따라 vSphere 관리자가 생성해야 합니다. 이 문서에서는 관리자가 ONTAP 도구를 효과적으로 관리하는 데 필요한 역할과 권한을 할당하는 방법에 대한 지침을 제공합니다.

VMware vCenter Server

VMware vCenter Server의 RBAC 구현은 vSphere Client 사용자 인터페이스를 통해 노출된 객체에 대한 액세스 제어를 제한하는 데 사용됩니다. ONTAP tools for VMware vSphere 10 설치의 일환으로, RBAC 환경이 확장되어 ONTAP tools의 기능을 나타내는 추가 객체가 포함됩니다. 이러한 객체에 대한 액세스 제어는 원격 플러그인을 통해 제공됩니다. 자세한 내용은 "[vCenter Server RBAC 환경](#)"을 참조하십시오.

ONTAP 클러스터

ONTAP tools for VMware vSphere 10은 ONTAP REST API를 통해 ONTAP 클러스터에 연결하여 스토리지 관련 작업을 수행합니다. 스토리지 리소스에 대한 액세스는 인증 시 제공된 ONTAP 사용자와 연결된 ONTAP 역할을 통해 제어됩니다. 자세한 내용은 "[ONTAP RBAC 환경](#)"을 참조하십시오.

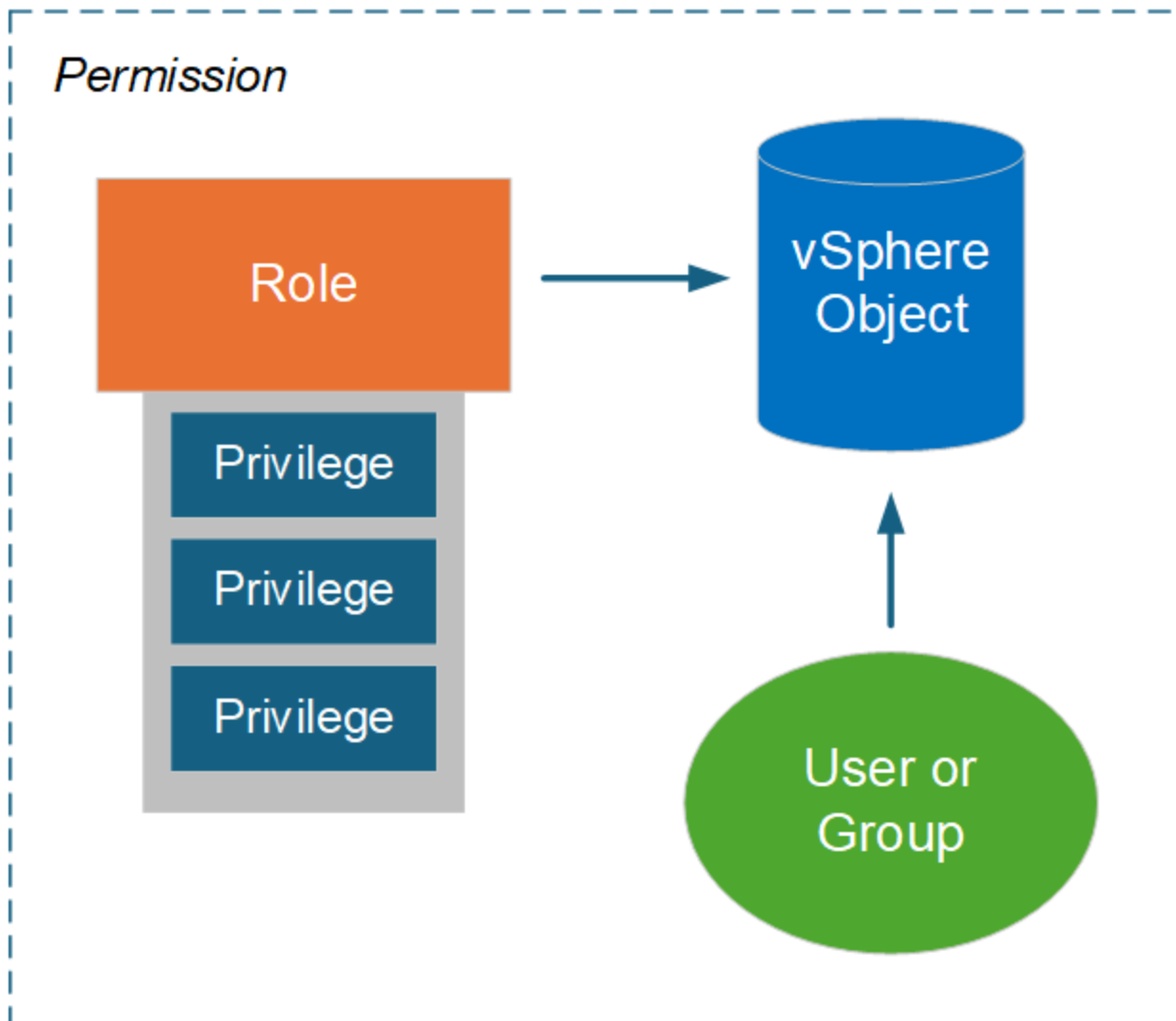
VMware vSphere를 사용한 RBAC

vCenter Server RBAC가 ONTAP 도구와 연동되는 방식

VMware vCenter Server는 vSphere 객체에 대한 액세스를 제어할 수 있는 RBAC(역할 기반 액세스 제어) 기능을 제공합니다. 이는 vCenter 중앙 집중식 인증 및 권한 부여 보안 서비스의 중요한 부분입니다.

vCenter Server 권한 그림

권한은 vCenter Server 환경에서 액세스 제어를 적용하는 기본 요소입니다. 권한은 권한 정의에 포함된 사용자 또는 그룹과 함께 vSphere 객체에 적용됩니다. vCenter 권한의 개략적인 구성은 아래 그림에서 확인할 수 있습니다.



vCenter Server 권한의 구성 요소

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

vSphere 객체

권한은 vCenter Server, ESXi 호스트, 가상 머신, 데이터스토어, 데이터 센터 및 폴더와 같은 vSphere 개체와 연결됩니다. 개체에 할당된 권한을 기반으로 vCenter Server는 각 사용자 또는 그룹이 개체에서 수행할 수 있는 작업 또는 작업을 결정합니다. ONTAP tools for VMware vSphere에 특정한 태스크의 경우, 모든 권한은 vCenter Server의 루트 또는 루트 폴더 수준에서 할당되고 검증됩니다. 자세한 내용은 ["vCenter 서버에서 RBAC 사용"](#)을(를) 참조하십시오.

Privileges 및 역할

vSphere 권한에는 ONTAP tools for VMware vSphere 10에서 사용되는 두 가지 유형이 있습니다. 이 환경에서 RBAC 작업을 간소화하기 위해 ONTAP tools는 필요한 기본 및 사용자 지정 권한이 포함된 역할을 제공합니다. 이러한 권한은 다음과 같습니다.

- 네이티브 vCenter Server Privileges

vCenter Server에서 제공하는 Privileges는 다음과 같습니다.

- ONTAP tools별 Privileges

이는 ONTAP tools for VMware vSphere에 고유한 사용자 지정 Privileges입니다.

사용자 및 그룹

Active Directory 또는 로컬 vCenter Server 인스턴스를 사용하여 사용자 및 그룹을 정의할 수 있습니다. 역할과 함께 vSphere 객체 계층 구조의 객체에 대한 권한을 생성할 수 있습니다. 이 권한은 연결된 역할의 권한에 따라 액세스 권한을 부여합니다. 역할은 사용자에게 개별적으로 직접 할당되지 않습니다. 대신 사용자 및 그룹은 더 큰 vCenter Server 권한의 일부로 역할 권한을 통해 객체에 액세스할 수 있습니다.

vCenter Server RBAC의 ONTAP tools 관련 고려 사항

운영 환경에서 사용하기 전에 고려해야 할 vCenter Server와 함께 사용하는 ONTAP tools for VMware vSphere 10 RBAC 구현의 몇 가지 측면이 있습니다.

vCenter 역할 및 관리자 계정

vCenter Server의 사용자 지정 역할을 정의하고 사용해야 하는 경우는 vSphere 객체 및 관련 관리 작업에 대한 액세스를 제한하려는 경우뿐입니다. 액세스 제한이 필요하지 않은 경우에는 관리자 계정을 대신 사용할 수 있습니다. 각 관리자 계정은 객체 계층 구조의 최상위 수준에서 관리자 역할로 정의됩니다. 이렇게 하면 ONTAP tools for VMware vSphere 10에 추가된 객체를 포함하여 vSphere 객체에 대한 전체 액세스 권한이 제공됩니다.

vSphere 객체 계층 구조

The vSphere 객체 인벤토리는 계층 구조로 구성되어 있습니다. 예를 들어 다음과 같이 계층 구조를 따라 아래로 이동할 수 있습니다.

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

모든 권한은 vSphere 객체 계층 구조에서 유효성 검사를 거치지만, VAAI 플러그인 작업은 대상 ESXi 호스트를 대상으로 유효성 검사를 거칩니다.

vCenter Server RBAC 작업을 간소화하기 위해 ONTAP tools for VMware vSphere는 다양한 관리 작업에 맞춰 사전 정의된 역할을 제공합니다.



필요한 경우 새 사용자 지정 역할을 생성할 수 있습니다. 이렇게 하려면 기존 ONTAP tools 역할 중 하나를 복제하고 필요에 따라 편집하십시오. 구성 변경 후 영향을 받는 vSphere 클라이언트 사용자는 로그아웃했다가 다시 로그인하여 변경 사항을 적용해야 합니다.

VMware vSphere용 ONTAP 도구 역할을 보려면 vSphere Client 상단의 *Menu*를 선택하고 *Administration*을 클릭한 다음 왼쪽의 *Roles*를 클릭합니다. vCenter Server 배포 또는 온보딩을 담당하는 vCenter 사용자에게 할당된 역할에는 다음 권한이 포함되어야 합니다. 배포 또는 온보딩 프로세스의 사전 요구 사항으로 이러한 권한이 구성되어 있는지 확인하십시오.

- 경보
 - 알람 확인
- 콘텐츠 라이브러리
 - 라이브러리 항목 추가
 - 템플릿 체크인
 - 템플릿 확인
 - 파일 다운로드
 - 스토리지 가져오기
 - 스토리지 읽기
 - 라이브러리 항목 동기화
 - 구독된 라이브러리 동기화
 - 구성 설정 보기
- 데이터 저장소
 - 공간 할당
 - 데이터 저장소 찾아보기
 - 저수준 파일 작업
 - 파일 제거
 - 가상 머신 파일 업데이트
 - 가상 머신 메타데이터 업데이트
- ESX Agent Manager
 - 보기
- 폴더
 - 폴더 생성
- 호스트
 - 구성

- 고급 설정
- 설정 변경
- 네트워크 구성
- 시스템 리소스
- 가상 머신 자동 시작 구성
- 로컬 작업
 - 가상 머신 생성
 - 가상 머신 삭제
 - 가상 머신 재구성
- 네트워크
 - 네트워크 할당
 - 구성
- OvfManager
 - OvfConsumer 액세스
- 호스트 프로필
 - 보기
- 리소스
 - 가상 머신을 리소스 풀에 할당
- 예약된 작업
 - 작업 생성
 - 작업 수정
 - 작업 실행
- 작업
 - 작업 생성
 - 업데이트 작업
- vApp
 - 가상 머신 추가
 - 리소스 풀 할당
 - vApp 할당
 - 생성
 - 가져오기
 - 이동
 - 전원 끄기
 - 전원 켜기

- URL에서 가져오기
- OVF 환경 보기
- 가상 머신
 - 구성 변경
 - 기존 디스크 추가
 - 새 디스크 추가
 - 기기 추가 또는 제거
 - 고급 구성
 - CPU 수 변경
 - 메모리 변경
 - 설정 변경
 - 리소스 변경
 - 가상 디스크 확장
 - 장치 설정 수정
 - 디스크 제거
 - 게스트 정보 재설정
 - 가상 머신 호환성 업그레이드
 - 재고 수정
 - 기존 항목에서 생성
 - 새로 만들기
 - 이동
 - 등록
 - 제거
 - 등록 취소
 - 상호 작용
 - 가상 머신에 대한 백업 작업
 - CD 미디어 구성
 - 플로피 미디어 구성
 - 기기 연결
 - 콘솔 상호 작용
 - VIX API를 이용한 게스트 운영 체제 관리
 - 전원 끄기
 - 전원 켜기
 - 재설정

- 일시 중단
- 프로비저닝
 - 디스크 액세스 허용
 - 클론 템플릿
 - 게스트 맞춤 설정
 - 배포 템플릿
 - 사용자 지정 사양 수정
 - 사용자 지정 사양 읽기
- 스냅샷 관리
 - 스냅샷 생성
 - 스냅샷 제거
 - 스냅샷 이름 바꾸기
 - 스냅샷으로 되돌리기

아래에 설명된 바와 같이 미리 정의된 세 가지 역할이 있습니다.

NetApp ONTAP tools for VMware vSphere 관리자

핵심 ONTAP tools for VMware vSphere 관리자 작업을 수행하는 데 필요한 모든 기본 vCenter Server 권한 및 ONTAP tools 전용 권한을 제공합니다.

NetApp ONTAP tools for VMware vSphere 읽기 전용

ONTAP 도구에 대한 읽기 전용 액세스 권한을 제공합니다. 이러한 사용자는 액세스 제어가 적용된 ONTAP tools for VMware vSphere 작업을 수행할 수 없습니다.

NetApp ONTAP tools for VMware vSphere 프로비저닝

스토리지 프로비저닝에 필요한 기본 vCenter Server 권한 및 ONTAP tools별 권한 중 일부를 제공합니다. 다음 작업을 수행할 수 있습니다.

- 새 데이터스토어 생성
- 데이터 저장소 관리

vSphere 객체 및 ONTAP 스토리지 백엔드

두 개의 RBAC 환경은 서로 연동하여 작동합니다. vSphere 클라이언트 인터페이스에서 작업을 수행할 때, vCenter Server에 정의된 ONTAP tools 역할을 먼저 확인합니다. 작업이 vSphere에서 허용되면 ONTAP 역할 권한을 검사합니다. 이 두 번째 단계는 스토리지 백엔드를 생성 및 구성할 때 사용자에게 할당된 ONTAP 역할을 기반으로 수행됩니다.

vCenter Server RBAC 작업

vCenter Server 권한 및 접근 권한을 다룰 때는 몇 가지 사항을 고려해야 합니다.

필수 권한

ONTAP tools for VMware vSphere 10 사용자 인터페이스에 액세스하려면 ONTAP tools 전용 보기 권한이 있어야 합니다. 이 권한 없이 vSphere에 로그인한 후 NetApp 아이콘을 클릭하면 ONTAP tools for VMware vSphere에서 오류 메시지가 표시되고 사용자 인터페이스에 액세스할 수 없게 됩니다.

vSphere 객체 계층 구조의 할당 수준에 따라 액세스할 수 있는 사용자 인터페이스 부분이 결정됩니다. 루트 객체에 보기 권한을 할당하면 NetApp 아이콘을 클릭하여 ONTAP tools for VMware vSphere에 액세스할 수 있습니다.

대신 보기 권한을 더 낮은 vSphere 객체 수준에 할당할 수 있습니다. 하지만 이렇게 하면 액세스하고 사용할 수 있는 ONTAP tools for VMware vSphere 메뉴가 제한됩니다.

권한 할당

vCenter Server 권한은 vSphere 객체 및 작업에 대한 액세스를 제한하려는 경우 사용해야 합니다. vSphere 객체 계층 구조에서 권한을 할당하는 위치에 따라 ONTAP tools for VMware vSphere 10 사용자가 수행할 수 있는 작업이 결정됩니다.



더욱 엄격한 접근 제어가 필요한 경우가 아니라면, 일반적으로 루트 객체 또는 루트 폴더 수준에서 권한을 할당하는 것이 좋습니다.

ONTAP tools for VMware vSphere 10에서 사용할 수 있는 권한은 스토리지 시스템과 같은 맞춤형 비 vSphere 객체에 적용됩니다. 이를 할당할 수 있는 vSphere 객체가 없으므로 가능하면 이러한 권한을 ONTAP tools for VMware vSphere 루트 객체에 할당해야 합니다. 예를 들어 ONTAP tools for VMware vSphere "스토리지 시스템 추가/수정/제거" 권한이 포함된 모든 권한은 루트 객체 수준에서 할당되어야 합니다.

객체 계층 구조에서 상위 수준에 권한을 정의할 때, 해당 권한이 하위 객체로 전달되어 상속되도록 구성할 수 있습니다. 필요한 경우, 상위 객체에서 상속된 권한을 재정의하는 추가 권한을 하위 객체에 할당할 수도 있습니다.

권한은 언제든지 수정할 수 있습니다. 권한 내의 세부 권한을 변경하는 경우, 해당 권한과 연결된 사용자는 vSphere에서 로그아웃한 후 다시 로그인해야 변경 사항이 적용됩니다.

ONTAP를 사용한 RBAC

ONTAP RBAC가 ONTAP tools와 연동되는 방식

ONTAP는 강력하고 확장 가능한 RBAC 환경을 제공합니다. RBAC 기능을 사용하여 REST API 및 CLI를 통해 노출되는 스토리지 및 시스템 작업에 대한 액세스 제어를 할 수 있습니다. ONTAP tools for VMware vSphere 10 배포와 함께 사용하기 전에 해당 환경에 대해 숙지하는 것이 좋습니다.

관리 옵션 개요

ONTAP RBAC 사용 시에는 환경 및 목표에 따라 여러 가지 옵션을 선택할 수 있습니다. 주요 관리 결정 사항에 대한 개요는 아래에 제시되어 있습니다. 자세한 내용은 ["ONTAP 자동화: RBAC 보안 개요"](#)를 참조하십시오.



ONTAP RBAC는 스토리지 환경에 맞게 조정되어 있으며 vCenter Server에서 제공하는 RBAC 구현보다 간단합니다. ONTAP에서는 사용자에게 역할을 직접 할당합니다. vCenter Server에서 사용하는 것과 같은 명시적인 권한 구성은 ONTAP RBAC에서는 필요하지 않습니다.

역할 및 권한 유형

ONTAP 사용자를 정의할 때는 ONTAP 역할이 필요합니다. ONTAP 역할에는 두 가지 유형이 있습니다.

- REST

REST 역할은 ONTAP 9.6에서 도입되었으며 일반적으로 ONTAP REST API를 통해 ONTAP에 액세스하는 사용자에게 적용됩니다. 이러한 역할에 포함된 Privileges는 ONTAP REST API 엔드포인트 및 관련 작업에 대한 액세스 제어 측면에서 정의됩니다.

- 전통적인

ONTAP 9.6 이전에 존재했던 레거시 역할입니다. RBAC의 기본 요소로 계속 사용됩니다. Privileges는 ONTAP CLI 명령에 대한 액세스 측면에서 정의됩니다.

REST 역할은 비교적 최근에 도입되었지만, 기존 역할에도 몇 가지 장점이 있습니다. 예를 들어, 추가 쿼리 매개변수를 포함하여 Privileges가 적용되는 객체를 더욱 정확하게 정의할 수 있습니다.

범위

ONTAP 역할은 두 가지 범위 중 하나로 정의할 수 있습니다. 특정 데이터 SVM(SVM 수준) 또는 전체 ONTAP 클러스터(클러스터 수준)에 적용할 수 있습니다.

역할 정의

ONTAP는 클러스터 및 SVM 수준 모두에서 미리 정의된 역할 세트를 제공합니다. 사용자 지정 역할도 정의할 수 있습니다.

ONTAP REST 역할 사용

ONTAP tools for VMware vSphere 10에 포함된 ONTAP REST 역할을 사용할 때 고려해야 할 사항이 몇 가지 있습니다.

역할 매핑

기존 역할이든 REST 역할이든, 모든 ONTAP 액세스 결정은 기본 CLI 명령어를 기반으로 이루어집니다. 하지만 REST 역할의 Privileges는 REST API 엔드포인트를 기준으로 정의되므로, ONTAP는 각 REST 역할에 대해 매핑된 기존 역할을 생성해야 합니다. 따라서 각 REST 역할은 기본 기존 역할에 매핑됩니다. 이를 통해 ONTAP는 역할 유형에 관계없이 일관된 방식으로 액세스 제어 결정을 내릴 수 있습니다. 병렬로 매핑된 역할은 수정할 수 없습니다.

CLI Privileges를 사용하여 REST 역할 정의하기

ONTAP는 항상 CLI 명령어를 사용하여 기본 수준에서 액세스 권한을 결정하기 때문에 REST 엔드포인트 대신 CLI 명령어 권한을 사용하여 REST 역할을 표현할 수 있습니다. 이러한 접근 방식의 장점 중 하나는 기존 역할에서 제공되는 더욱 세밀한 세분성을 활용할 수 있다는 것입니다.

ONTAP 역할 정의 시 관리 인터페이스

ONTAP CLI와 REST API를 사용하여 사용자와 역할을 생성할 수 있습니다. 하지만 ONTAP tools Manager를 통해 제공되는 JSON 파일과 함께 System Manager 인터페이스를 사용하는 것이 더 편리합니다. 자세한 내용은 ["ONTAP tools for VMware vSphere 10과 함께 ONTAP RBAC 사용"](#)을 참조하십시오.

ONTAP tools에 대한 ONTAP RBAC 고려 사항

운영 환경에서 사용하기 전에 고려해야 할 ONTAP tools for VMware vSphere 10 RBAC 구현과 ONTAP의 몇 가지 측면이 있습니다.

ONTAP tools for VMware vSphere는 사용자 지정 역할을 가진 ONTAP 사용자를 생성하는 기능을 지원합니다. 역할 정의는 ONTAP 클러스터에 업로드할 수 있는 JSON 파일로 제공됩니다. 사용자를 생성하고 환경 및 보안 요구 사항에 맞게 역할을 맞춤 설정할 수 있습니다.

주요 구성 단계는 아래에 간략하게 설명되어 있습니다. 자세한 내용은 ["ONTAP 사용자 역할 및 Privileges 구성"](#)을 참조하십시오.

1. 준비

ONTAP tools Manager와 ONTAP 클러스터 모두에 대한 관리자 자격 증명이 필요합니다.

2. JSON 정의 파일을 다운로드합니다.

ONTAP tools Manager 사용자 인터페이스에 로그인한 후 RBAC 정의가 포함된 JSON 파일을 다운로드할 수 있습니다.

3. 역할을 가진 ONTAP 사용자 생성

System Manager에 로그인한 후 사용자 및 역할을 생성할 수 있습니다.

1. 왼쪽에서 *클러스터*를 선택한 다음 *설정*을 선택합니다.
2. 아래로 스크롤하여 *사용자 및 역할*로 이동한 후 `→`을 클릭합니다.
3. *사용자*에서 *추가*를 선택하고 *가상화 제품*을 선택합니다.
4. 로컬 워크스테이션에서 JSON 파일을 선택하고 업로드하십시오.

4. 역할 구성

역할을 정의하는 과정에서 몇 가지 관리적 결정을 내려야 합니다. 자세한 내용은 [System Manager를 사용하여 역할 구성](#)을 참조하십시오.

System Manager를 사용하여 역할 구성

System Manager를 사용하여 새 사용자 및 역할을 생성하고 JSON 파일을 업로드한 후에는 환경 및 요구 사항에 따라 역할을 사용자 지정할 수 있습니다.

핵심 사용자 및 역할 구성

RBAC 정의는 VSC, VASA Provider 및 SRA의 조합을 포함한 여러 제품 기능으로 패키징됩니다. RBAC 지원이 필요한 환경을 선택해야 합니다. 예를 들어, 역할에 원격 플러그인 기능을 지원하도록 하려면 VSC를 선택합니다. 또한 사용자 이름과 연결된 암호를 선택해야 합니다.

Privileges

역할 권한은 ONTAP 스토리지에 필요한 액세스 수준에 따라 네 가지 세트로 구성됩니다. 역할의 기반이 되는 권한은 다음과 같습니다.

- 검색

이 역할을 통해 스토리지 시스템을 추가할 수 있습니다.

- 스토리지 생성

이 역할을 사용하면 스토리지를 생성할 수 있습니다. 또한 검색 역할과 관련된 모든 Privileges도 포함됩니다.

- 저장소 수정

이 역할을 사용하면 스토리지를 수정할 수 있습니다. 또한 스토리지 검색 및 생성 역할과 관련된 모든 Privileges도 포함됩니다.

- 스토리지 삭제

이 역할은 스토리지를 삭제할 수 있는 권한을 제공합니다. 또한 스토리지 검색, 스토리지 생성 및 스토리지 수정 역할과 관련된 모든 Privileges도 포함합니다.

역할을 부여하여 사용자를 생성합니다.

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

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

예

OTV_10_VSC_Discovery_Create

새 사용자는 '사용자 및 역할' 페이지의 목록에 추가됩니다. HTTP 및 ONTAPI 사용자 로그인 방법이 모두 지원됩니다.

ONTAP tools for VMware vSphere 배포

ONTAP tools for VMware vSphere 빠른 시작

이 빠른 시작 섹션을 통해 VMware vSphere용 ONTAP tools를 설정하십시오.

ONTAP 도구를 활용하여 초기 관리 및 프로비저닝을 수행하려면 먼저 다음 핵심 작업을 완료하십시오. 그런 다음 환경 및 보호 요구 사항에 따라 선택적 작업을 완료하십시오.

처음에는 ONTAP tools for VMware vSphere를 NFS 및 VMFS 데이터스토어를 지원하는 핵심 서비스를 제공하는 소규모 단일 노드 구성으로 배포합니다. 서비스당 추가 컨테이너, 향상된 복원력을 위해 구성을 확장하거나 vVols 데이터스토어 및 고가용성(HA)을 사용하려면 먼저 이 워크플로를 완료한 후 확장 단계를 진행하십시오. 자세한 내용은 ["HA 배포 워크플로"](#)를 참조하십시오.

1

배포 계획 수립

지원되는 배포를 위한 환경 준비가 완료되었는지 확인하십시오. vSphere, ONTAP 및 ESXi 호스트 버전이 ONTAP tools 버전과 호환되는지 확인하십시오. 충분한 CPU, 메모리 및 디스크 공간을 할당하십시오. 보안 규칙에 따라 네트워크 트래픽을 허용하도록 방화벽 또는 기타 보안 도구를 설정해야 할 수 있습니다.

vCenter 서버가 설치되어 있고 액세스 가능한지 확인하십시오.

- ["상호운용성 매트릭스 도구"](#)
- ["ONTAP tools for VMware vSphere 요구 사항 및 구성 제한"](#)
- ["시작하기 전에"](#)

2

ONTAP tools for VMware vSphere 배포

NFS 및 VMFS 데이터스토어에 대한 기본 서비스를 설정하려면 ONTAP tools 어플라이언스를 배포하십시오.

처음에는 ONTAP tools for VMware vSphere를 소규모 단일 노드 구성으로 배포합니다. vVols 데이터스토어와 고가용성(HA)을 사용하도록 구성을 확장하려면 이 워크플로를 완료한 후에 진행하면 됩니다. HA 구성으로 확장하려면 CPU 핫 추가 및 메모리 핫 플러그가 활성화되어 있는지 확인하십시오.

배포 시 템플릿 사용자 지정 필드를 주의 깊게 검토하십시오. 특히 호스트 이름, ONTAP tools IP 주소 사용 및 DNS 요구 사항을 확인하십시오.

- ["ONTAP tools for VMware vSphere 배포"](#)

3

vCenter 클라이언트 플러그인을 등록하고 설치합니다

vCenter 클라이언트 플러그인을 등록하고 필요한 권한 및 역할을 적용하려면 vCenter Server 인스턴스를 추가하십시오. vCenter Server 인스턴스를 추가하면 ONTAP tools가 원격 플러그인을 등록하고, 사용자 지정 플러그인 및 API 권한을 적용하고, 사용자 지정 역할을 생성하고, vSphere 사용자 인터페이스에 플러그인 바로 가기를 추가합니다.

- ["vCenter Server 인스턴스를 ONTAP tools에 추가합니다"](#)

4

스토리지 백엔드 구성

ONTAP 도구가 데이터스토어를 프로비저닝하고 관리할 수 있도록 ONTAP 스토리지 리소스를 연결합니다. ONTAP 클러스터에 스토리지 백엔드를 추가합니다. vCenter Server가 테넌트 SVM과 연결된 멀티테넌트 환경에서는 ONTAP 도구 관리자를 사용하여 클러스터를 추가합니다. 그런 다음 스토리지 백엔드를 vCenter Server와 연결하여 해당 vCenter 인스턴스에 대한 글로벌 매핑을 생성합니다.

ONTAP tools 사용자 인터페이스를 사용하여 클러스터 또는 SVM 자격 증명으로 로컬 스토리지 백엔드를 추가합니다. 이러한 스토리지 백엔드는 단일 vCenter로 제한됩니다. 로컬에서 클러스터 자격 증명을 사용하는 경우 연결된 SVM이 자동으로 vCenter에 매핑되어 vVols 또는 VMFS를 관리합니다. SRA를 포함한 VMFS 관리의 경우 ONTAP tools는 글로벌 클러스터 없이도 SVM 자격 증명을 지원합니다.

- ["스토리지 백엔드 추가"](#)
- ["스토리지 백엔드를 vCenter Server 인스턴스와 연결합니다."](#)

다음 작업 (선택 사항)

1

ONTAP 사용자 역할 및 권한 구성

ONTAP 기본 관리자 계정 대신 최소 권한 액세스를 위해 사용자 지정 ONTAP 역할을 구성하십시오.

- ["ONTAP 사용자 역할 및 Privileges 구성"](#)

2

여러 vCenter Server 인스턴스의 인증서 업그레이드

여러 vCenter Server 인스턴스 간에 신뢰할 수 있는 인증서 기반 통신을 사용하도록 인증서를 업그레이드하십시오.

- ["인증서 관리"](#)

3

SRA 보호 구성

NFS 및 VMFS 데이터스토어에 대한 재해 복구 보호 설정을 위해 SRA 기능을 활성화하십시오.

- ["ONTAP tools for VMware vSphere 서비스 활성화"](#)
- ["VMware Live Site Recovery 어플라이언스에서 SRA 구성"](#)

4

SnapMirror 활성 동기화 보호 활성화

SnapMirror 액티브 싱크를 사용하여 호스트 클러스터 보호를 설정하여 VMFS 데이터스토어를 보호하십시오. ONTAP 시스템에서는 필요한 클러스터와 SVM을 피어링한 다음 ONTAP tools for VMware vSphere에서 호스트 클러스터 보호를 구성하십시오. 이 옵션은 VMFS 데이터스토어에만 적용됩니다.

- ["호스트 클러스터 보호를 사용하여 보호"](#)

5

ONTAP tools 배포를 위한 백업 및 복구 설정

ONTAP tools 구성을 보호하고 장애 발생 시 신속하게 복구할 수 있도록 백업 및 복구를 설정하십시오.

ONTAP tools for VMware vSphere 10.5에서는 백업이 기본적으로 활성화되어 있으며 10분마다 실행됩니다. 장애 발생 시 설정을 복구할 수 있도록 ONTAP tools for VMware vSphere 설치 백업을 예약하십시오.

- ["백업 설정 편집"](#)
- ["ONTAP tools 설정 복구"](#)

ONTAP 도구의 고가용성 배포 워크플로

복원력을 높이고 서비스당 더 많은 컨테이너를 지원하려면 초기 ONTAP tools 배포를 고가용성(HA) 구성으로 확장하십시오. HA 설정에서 vVols 데이터스토어를 사용하려면 VASA Provider 서비스를 활성화해야 합니다.

1

배포 규모 확대

ONTAP tools for VMware vSphere 구성을 스케일 업하여 배포된 노드 수를 늘리고 구성을 HA 설정으로 변경할 수 있습니다.

- ["ONTAP tools for VMware vSphere 구성 변경"](#)

2

서비스 활성화

vVols 데이터스토어를 구성하려면 VASA Provider 서비스를 활성화해야 합니다. vCenter에 VASA 공급자를 등록하고 적절한 네트워크 및 스토리지 구성을 포함하여 스토리지 정책이 HA 요구 사항을 충족하는지 확인하십시오.

VMware Site Recovery Manager(SRM) 또는 VMware Live Site Recovery(VLSR)용 ONTAP tools 스토리지 복제 어댑터(SRA)를 사용하려면 SRA 서비스를 활성화하십시오.

- ["VASA Provider 및 SRA 서비스 활성화"](#)

3

인증서 업그레이드

vVol 데이터스토어를 여러 vCenter Server 인스턴스에서 사용하는 경우 자체 서명 인증서를 인증 기관(CA)에서 서명한 인증서로 업그레이드하십시오.

- ["인증서 관리"](#)

ONTAP tools for VMware vSphere 요구 사항 및 구성 제한

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

ONTAP tools for VMware vSphere를 VMware vCenter Server Virtual Appliance(vCSA)와 함께 사용할 수 있습니다. ESXi 호스트가 포함된 지원되는 vSphere 환경에 ONTAP tools for VMware vSphere를 배포해야 합니다.

시스템 요구 사항

- 노드별 설치 패키지 공간 요구사항
 - 씬 프로비저닝 설치의 경우 15GB
 - Thick 프로비저닝 설치의 경우 348GB
- 호스트 시스템 크기 요구 사항 아래 표는 각 배포 규모에 권장되는 메모리 용량을 보여줍니다.고가용성(HA) 배포의 경우, 표에 표시된 어플라이언스 크기의 3배가 필요합니다.

배포 유형	노드당 CPU 개수	노드당 메모리(GB)	노드당 씬 프로비저닝된 디스크 공간(GB)
소형	9	18	350
중간	13	26	350
대규모 참고: 대규모 배포는 HA 구성에만 해당됩니다.	17	34	350



백업이 활성화되면 각 ONTAP tools 클러스터는 VM이 배포된 데이터스토어에 50GB의 추가 공간이 필요합니다. 따라서 고가용성(HA)을 사용하지 않는 경우 400GB, 고가용성(HA)을 사용하는 경우 총 1100GB의 공간이 필요합니다.

최소 스토리지 및 애플리케이션 요구사항

스토리지, 호스트 및 애플리케이션	버전 요구 사항
ONTAP	9.15.1, 9.16.1 및 9.17.0
ONTAP tools 지원 ESXi 호스트	7.0.3 버전 이후
ONTAP tools 지원 vCenter Server	7.0U3 이후 버전
VASA Provider	3.0
OVA 애플리케이션	10.5
ONTAP tools 가상 머신을 배포하기 위한 ESXi 호스트	7.0U3 및 8.0U3
vCenter Server를 사용하여 ONTAP tools 가상 머신을 배포합니다	7.0 및 8.0



ONTAP tools for VMware vSphere 10.4부터 가상 머신 하드웨어 버전이 10에서 17로 변경되었습니다.

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

["상호운용성 매트릭스 도구"](#)

포트 요구 사항

다음 표는 NetApp이 사용하는 네트워크 포트와 그 용도를 설명합니다. 포트에는 세 가지 유형이 있습니다.

- 외부 포트: 이러한 포트는 Kubernetes 클러스터 또는 노드 외부에서 접근할 수 있습니다. 이를 통해 서비스는 외부 네트워크 또는 사용자와 통신할 수 있으며, 클러스터 환경 외부의 시스템과 통합할 수 있습니다.
- 노드 간 포트: 이러한 포트는 Kubernetes 클러스터 내 노드 간 통신을 가능하게 합니다. 데이터 공유 및 협업과 같은 클러스터 작업에 필요합니다. 단일 노드 배포의 경우 노드 간 포트는 해당 노드 내에서만 사용되며 외부 액세스가 필요하지 않습니다. 노드 간 포트는 클러스터 외부에서 트래픽을 허용할 수 있습니다. 방화벽 규칙을 사용하여 노드 간 포트의 인터넷 액세스를 차단하십시오.
- 내부 포트: 이러한 포트는 ClusterIP 주소를 사용하여 Kubernetes 클러스터 내부에서 통신합니다. 외부로 노출되지 않으므로 방화벽 규칙에 추가할 필요가 없습니다.



ONTAP tools 노드들이 서로 원활한 통신을 유지할 수 있도록 모든 노드가 동일한 서브넷에 있는지 확인하십시오.

포트 요구 사항 표를 펼치거나 접으려면 클릭하십시오.

서비스/구성 요소 이름	포트	프로토콜	포트 유형	설명
ntv-gateway-svc (LB)	443, 8443	TCP	외부	VASA Provider 서비스로 들어오는 통신을 위한 통과 포트입니다. VASA Provider 자체 서명 인증서와 사용자 지정 CA 인증서가 이 포트에 저장됩니다.
SSH	22	TCP	외부	원격 서버 로그인 및 명령 실행을 위한 보안 셸(Secure Shell).
rke2 서버	9345	TCP	노드 간	RKE2 슈퍼바이저 API (신뢰할 수 있는 네트워크로 제한).
kube-apiserver	6443	TCP	노드 간	Kubernetes API 서버 포트(신뢰할 수 있는 네트워크로 제한).
rpcbind/portmapper	111	TCP/UDP	노드 간	서비스 간 RPC 통신에 사용됩니다.
coredns (DNS)	53	TCP/UDP	노드 간	클러스터 내에서 이름 확인을 위한 도메인 이름 시스템(DNS) 서비스입니다.
NTP	123	UDP	노드 간	시간 동기화를 위한 네트워크 시간 프로토콜(NTP).
etcd	2379, 2380, 2381	TCP	노드 간	클러스터 데이터를 위한 키-값 저장소.
kube-vip	2112	TCP	노드 간	Kubernetes API 서버 포트.
kubelet	10248, 10250	TCP	노드 간	Kubernetes 구성 요소
kube-controller	10257	TCP	노드 간	Kubernetes 구성 요소
cloud-controller	10258	TCP	노드 간	Kubernetes 구성 요소
kube-scheduler	10259	TCP	노드 간	Kubernetes 구성 요소
kube-proxy	10249, 10256	TCP	노드 간	Kubernetes 구성 요소

서비스/구성 요소 이름	포트	프로토콜	포트 유형	설명
calico-node	9091, 9099	TCP	노드 간	Calico 네트워킹 구성 요소.
containerd	10010	TCP	노드 간	컨테이너 데몬 서비스.
VXLAN(Flannel)	8472	UDP	노드 간	포트 간 통신을 위한 오버레이 네트워크.



고가용성(HA) 배포를 위해서는 모든 노드 간에 UDP 포트 8472가 열려 있는지 확인해야 합니다. 이 포트는 노드 간 포트 통신을 가능하게 하며, 이 포트를 차단하면 노드 간 네트워킹이 중단됩니다.

ONTAP tools for VMware vSphere를 vVols 데이터스토어에 배포하기 위한 구성 한계

다음 표를 참고하여 VMware vSphere용 ONTAP tools를 구성할 수 있습니다.

배포	유형	vVols 개수	호스트 수
비-HA	작은 (S)	최대 12K	32
비-HA	중간(M)	최대 24K	64
고가용성	작은 (S)	최대 24K	64
고가용성	중간(M)	최대 50,000	128
고가용성	대형(L)	최대 10만	256



표에 표시된 호스트 수는 연결된 모든 vCenters의 총합입니다.

VMFS 및 NFS 데이터스토어용 ONTAP tools for VMware vSphere 배포를 위한 구성 제한

이 섹션에 나열된 구성 제한 사항은 NetApp에서 검증되고 지원됩니다. 실제 제한 사항은 환경 및 워크로드에 따라 다를 수 있습니다. 이러한 제한을 초과하면 성능이나 지원 가능성에 영향을 미칠 수 있으므로 권장하지 않습니다. 표를 검토할 때 다음 사항을 고려하십시오.

- 가상 머신 재해 복구(DR)는 동기식, 비동기식 또는 엄격한 동기식 정책을 사용하여 구성됩니다. NVMe 프로토콜에서는 DR이 지원되지 않습니다.
- ESXi 호스트 클러스터 보호는 SnapMirror Active Sync를 사용하는데, 이는 다중 vCenter 배포를 지원하지 않습니다.
- ONTAP tools는 배포 규모에 따라 ESXi 호스트 및 데이터 저장소의 수만 제한합니다. ONTAP tools에 연결할 수 있는 vCenter Server의 수에는 제한이 없습니다.
- ONTAP tools는 모든 스토리지 객체를 병렬로 검색합니다. ONTAP 스토리지 객체에 대한 구성 제한은 현재 사용 중인 객체 수와 관계없이 적용됩니다.
- ONTAP tools는 온보딩할 수 있는 vCenter Server의 수에 제한을 두지 않습니다. 구성 제한은 지원되는 호스트 및 데이터스토어 수에 따라 결정되며, 자세한 내용은 다음 표에 나와 있습니다.

구축	VMFS 및 NFS 데이터 저장소 수	DR이 설정된 VMFS 데이터 저장소 수	호스트 수
비HA 소형	200	80	32
비-HA 중간	250	100	32
HA Small	350	200	64
HA Medium	600	200	128
HA Large	1024	250	256

ONTAP tools for VMware vSphere - Storage Replication Adapter (SRA)

다음 표는 ONTAP tools for VMware vSphere를 사용하는 VMware Live Site Recovery 인스턴스당 지원되는 수를 보여줍니다.

vCenter 배포 크기	소형	중간
어레이 기반 복제를 사용하여 보호하도록 구성된 가상 머신의 총 개수	2000	5000
어레이 기반 복제 보호 그룹의 총 개수	250	250
복구 계획당 보호 그룹의 총 수	50	50
복제된 데이터 저장소 수	255	255
VM 개수	4000	7000

다음 표는 VMware Live Site Recovery 인스턴스 수와 해당 ONTAP tools for VMware vSphere 배포 규모를 보여줍니다.

VMware Live Site Recovery 인스턴스 수	ONTAP tools 배포 크기
최대 4개	소형
4~8	중간
8개 이상	대형

자세한 내용은 "[VMware Live Site Recovery의 운영 제한 사항](#)"을 참조하십시오.

ONTAP 도구 배포 전 요구 사항

배포를 진행하기 전에 다음 요구 사항이 충족되었는지 확인하십시오.

요구 사항	귀하의 상태
vSphere 버전, ONTAP 버전 및 ESXi 호스트 버전은 ONTAP tools 버전과 호환됩니다.	☐ 예 ☐ 아니오
vCenter Server 환경이 설정 및 구성되었습니다.	☐ 예 ☐ 아니오
브라우저 캐시가 삭제되었습니다.	☐ 예 ☐ 아니오

요구 사항	귀하의 상태
상위 vCenter Server 자격 증명을 가지고 있습니다.	☐ 예 ☐ 아니오
배포 후 등록을 위해 ONTAP tools for VMware vSphere가 연결할 vCenter Server 인스턴스의 로그인 자격 증명에 있어야 합니다.	☐ 예 ☐ 아니오
인증서가 발급된 도메인 이름은 사용자 지정 CA 인증서가 필수적인 다중 vCenter 배포 환경에서 가상 IP 주소에 매핑됩니다.	☐ 예 ☐ 아니오
도메인 이름이 의도한 IP 주소로 확인되는지 확인하기 위해 도메인 이름에 대해 nslookup 검사를 실행했습니다.	☐ 예 ☐ 아니오
인증서는 도메인 이름과 ONTAP tools의 IP 주소로 생성됩니다.	☐ 예 ☐ 아니오
ONTAP tools 애플리케이션 및 내부 서비스는 vCenter 서버에서 접근할 수 있습니다.	☐ 예 ☐ 아니오
멀티테넌트 SVM을 사용하는 경우 각 SVM에 SVM 관리 LIF가 있습니다.	☐ 예 ☐ 아니오

배포 워크시트

단일 노드 배포용

ONTAP tools for VMware vSphere 초기 배포를 위한 필수 정보를 수집하려면 다음 워크시트를 사용하십시오.

요구 사항	귀하의 값
ONTAP 툴 애플리케이션의 IP 주소입니다. ONTAP 툴 관리자 웹 인터페이스(로드 밸런서)에 액세스하기 위한 IP 주소입니다 <code>https://<ip>:8443/virtualization/ui/</code>	
내부 통신을 위한 ONTAP tools 가상 IP 주소입니다. 이 IP 주소는 여러 ONTAP tools 인스턴스가 있는 설정에서 내부 통신에 사용됩니다. 이 IP 주소는 ONTAP tools 애플리케이션의 IP 주소와 동일해서는 안 됩니다. (Kubernetes Control Plane)	
ONTAP tools 관리 노드의 DNS 호스트 이름	
기본 DNS 서버	
보조 DNS 서버	
DNS 검색 도메인	
ONTAP tools 관리 노드의 IPv4 주소입니다. 관리 네트워크에서 노드 관리 인터페이스에 사용되는 고유한 IPv4 주소입니다. SSH를 통해 ONTAP 도구 어플라이언스에 원격 진단 액세스하는 데 사용됩니다.	
IPv4 주소에 대한 서브넷 마스크	
IPv4 주소의 기본 게이트웨이	

요구 사항	귀하의 값
IPv6 주소 (선택 사항)	
IPv6 접두사 길이(선택 사항)	
IPv6 주소용 게이트웨이(선택 사항)	



위의 모든 IP 주소에 대한 DNS 레코드를 생성하십시오. 호스트 이름을 할당하기 전에 DNS에서 사용 가능한 IP 주소에 매핑해야 합니다. 모든 IP 주소는 배포를 위해 선택한 동일한 VLAN에 속해야 합니다.

고가용성(HA) 배포용

단일 노드 배포 요구 사항 외에도 고가용성(HA) 배포를 위해서는 다음 정보가 필요합니다.

요구 사항	귀하의 값
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

모든 관련 IP 주소에 대해 필요한 방화벽 포트가 열려 있는지 확인하십시오. ONTAP tools는 포트 443을 통해 LIF에 액세스해야 합니다. 필요한 포트의 전체 목록은 ["ONTAP tools for VMware vSphere 요구 사항 및 구성 제한"](#)의 포트 요구 사항 섹션을 참조하십시오.

ONTAP 스토리지 설정

ONTAP 스토리지와 ONTAP tools for VMware vSphere의 원활한 통합을 보장하려면 다음 설정을 고려하십시오.

- 스토리지 연결에 파이버 채널(FC)을 사용하는 경우, ESXi 호스트를 SVM의 FC LIF에 연결하도록 FC 스위치의 영역 설정을 구성하십시오. ["ONTAP 시스템을 사용한 FC 및 FCoE 조닝에 대해 알아보기"](#)
- ONTAP tools로 관리되는 SnapMirror 복제를 사용하려면 스토리지 관리자가 SnapMirror를 사용하기 전에 ONTAP에서 ["ONTAP 클러스터 피어 관계"](#) 및 ["ONTAP 인터클러스터 SVM 피어 관계"](#)를 생성해야 합니다.

ONTAP tools 배포

ONTAP tools for VMware vSphere 어플라이언스는 NFS 및 VMFS 데이터스토어를 지원하는 핵심 서비스를 갖춘 소형 단일 노드로 배포됩니다. ONTAP tools 배포 프로세스는 최대 45분까지 소요될 수 있습니다.

시작하기 전에

소규모 단일 노드를 배포하는 경우 콘텐츠 라이브러리는 선택 사항입니다. 다중 노드 또는 HA 배포의 경우 콘텐츠 라이브러리가 필요합니다. VMware에서 콘텐츠 라이브러리는 VM 템플릿, vApp 템플릿 및 기타 파일을 저장합니다. 콘텐츠 라이브러리를 사용하여 배포하면 네트워크 연결에 의존하지 않으므로 원활한 환경을 제공합니다.

콘텐츠 라이브러리를 생성하기 전에 다음 사항을 고려하십시오.

- 클러스터의 모든 호스트가 액세스할 수 있도록 공유 데이터 저장소에 콘텐츠 라이브러리를 생성합니다.
- ONTAP tools for VMware vSphere OVA를 배포하기 전에 콘텐츠 라이브러리를 설정하십시오.
- 어플라이언스를 HA용으로 구성하기 전에 콘텐츠 라이브러리가 생성되었는지 확인하십시오.



배포 후 콘텐츠 라이브러리에서 OVA 템플릿을 삭제하지 마십시오.



향후 HA 배포를 활성화하려면 ONTAP tools 가상 머신을 ESXi 호스트에 직접 배포하지 마십시오. 대신 ESXi 호스트 클러스터 또는 리소스 풀 내에 배포하십시오.

콘텐츠 라이브러리를 생성하려면 다음 단계를 따르십시오.

1. ONTAP tools for VMware vSphere의 바이너리(.ova) 및 서명된 인증서가 포함된 파일을 "[NetApp 지원 사이트](#)"에서 다운로드하십시오.
2. vSphere 클라이언트에 로그인합니다.
3. vSphere 클라이언트 메뉴를 선택하고 *콘텐츠 라이브러리*를 선택합니다.
4. 페이지 오른쪽에서 *만들기*를 선택합니다.
5. 라이브러리 이름을 입력하고 콘텐츠 라이브러리를 생성합니다.
6. 생성한 콘텐츠 라이브러리로 이동하세요.
7. 페이지 오른쪽에서 *Actions*를 선택하고 *Import item*을 선택한 다음 OVA 파일을 가져옵니다.



자세한 내용은 "[콘텐츠 라이브러리 생성 및 활용](#)" 블로그를 참조하십시오.



배포를 진행하기 전에 클러스터의 분산 리소스 스케줄러(DRS)를 보수적(Conservative)으로 설정하십시오. 이렇게 하면 설치 중에 가상 머신이 마이그레이션되지 않습니다.

ONTAP tools for VMware vSphere는 초기에는 고가용성(HA)을 지원하지 않는 구성으로 배포됩니다. HA 환경으로 확장하려면 CPU 핫 추가 및 메모리 핫 플러그를 활성화해야 합니다. 이 단계는 배포 과정의 일부로 수행하거나 배포 후 VM 설정을 편집하여 수행할 수 있습니다.

단계

1. ONTAP tools for VMware vSphere의 바이너리(.ova) 및 서명된 인증서가 포함된 파일을 "[NetApp 지원 사이트](#)"에서 다운로드합니다. 이미 OVA 파일을 콘텐츠 라이브러리로 가져온 경우 이 단계를 건너뛰고 다음 단계로 진행할 수 있습니다.
2. vSphere 서버에 로그인하십시오.
3. OVA를 배포할 리소스 풀, 클러스터 또는 호스트로 이동합니다.



ONTAP tools for VMware vSphere 가상 머신을 관리하는 vVols 데이터 저장소에 저장하지 마십시오.

4. 콘텐츠 라이브러리 또는 로컬 시스템에서 OVA 파일을 배포할 수 있습니다.

로컬 시스템에서	콘텐츠 라이브러리에서
a. 마우스 오른쪽 버튼을 클릭하고 *OVF 템플릿 배포... *를 선택합니다. b. URL에서 OVA 파일을 선택하거나 해당 위치로 이동한 다음 *다음*을 선택합니다.	a. 콘텐츠 라이브러리로 이동하여 배포할 라이브러리 항목을 선택합니다. b. 작업 > *이 템플릿에서 새 VM 생성*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 진행하기 전에 *하드웨어 사용자 지정*이라는 추가 단계가 활성화됩니다.
- vCenter Server 7.0.3 버전을 사용 중인 경우 배포 마지막 부분의 다음 단계는 무엇입니까? 섹션에 있는 단계를
따르십시오.

6. 컴퓨터 리소스를 선택하고 다음*을 선택합니다. 필요에 따라 *배포된 VM을 자동으로 켜기 확인란을 선택합니다.

7. 템플릿의 세부 정보를 검토하고 *다음*을 선택합니다.

8. 라이선스 계약을 읽고 동의한 후 *다음*을 선택합니다.

9. 구성의 스토리지와 디스크 형식을 선택하고 *다음*을 선택하십시오.

10. 각 소스 네트워크에 대한 대상 네트워크를 선택하고 *다음*을 선택하십시오.

11. 템플릿 사용자 지정 창에서 필수 입력란을 채우세요.

netapp-ontap-tools-for-vmware-vsphere-10.5-1773361740 - New Virtual Machine from Content Library

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

Customize template

ONTAP tools IP address

ONTAP tools virtual IP address*

vCenter Server configuration for ONTAP tools deployment

vCenter Server hostname*

vCenter Server username (user@domain.com)*

vCenter Server password*

ONTAP tools uses this IP address for internal communication

Enter the hostname of the target vCenter Server for ONTAP tools deployment.

Enter the user principal name of the vCenter Server account (for example, username@vsphere.local).
backup@vsphere.local

Enter the vCenter Server password to authenticate your login.

Password

Confirm Password

Cancel BACK NEXT

배포를 성공적으로 완료하려면 템플릿 사용자 지정 페이지의 값이 필수입니다.

다음 필드에 특히 주의하십시오:



- **호스트 이름:** ONTAP tools VM 호스트 이름을 입력합니다. 유효한 호스트 이름 형식을 사용하십시오.
- **ONTAP tools IP 주소:** ONTAP tools에 액세스하는 데 사용되는 기본 관리 인터페이스입니다.
- **IPv4 주소:** 문제 해결 및 유지 관리를 위한 진단 셸 및 SSH 액세스에 사용되는 노드 IP 주소입니다.

호스트 또는 vCenter에 DNS 이름을 사용하는 경우 해당 이름이 DNS에서 올바르게 확인되는지 확인하십시오.



vCenter 호스트 이름은 ONTAP tools 어플라이언스가 배포된 vCenter Server 인스턴스의 이름입니다.

2개의 vCenter Server 토폴로지에서 ONTAP 도구를 배포하는 경우(어플라이언스가 하나의 vCenter 인스턴스에서 호스팅되고 다른 인스턴스를 관리하는 경우) ONTAP 도구를 호스팅하는 vCenter 인스턴스에 제한된 역할을 할당할 수 있습니다. OVF 템플릿 배포에 필요한 권한만 있는 전용 vCenter 사용자 및 역할을 생성할 수 있습니다. 자세한 내용은 ["ONTAP tools for VMware vSphere 10에 포함된 역할"](#)에 나열된 역할을 참조하십시오.

ONTAP tools로 관리할 vCenter 인스턴스의 경우, vCenter 사용자 계정에 관리자 권한이 있는지 확인하십시오.

- 호스트 이름에는 문자(A-Z, a-z), 숫자(0-9) 및 하이픈(-)이 포함되어야 합니다. 듀얼 스택을 구성하려면 IPv6 주소에 매핑된 호스트 이름을 지정하십시오.



순수 IPv6는 지원되지 않습니다. IPv6 및 IPv4 주소가 모두 포함된 VLAN을 사용하는 혼합 모드가 지원됩니다.

- ONTAP tools IP 주소는 ONTAP tools와 통신하기 위한 기본 인터페이스입니다.
- IPv4는 노드 구성의 IP 주소 구성 요소로, 디버깅 및 유지 관리를 위해 노드에서 진단 셸 및 SSH 액세스를 활성화하는 데 사용할 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 사용하십시오.

The screenshot shows the 'Customize hardware' window for a new virtual machine. The left sidebar lists the configuration steps, with '8 Customize hardware' selected. The main panel shows the 'CPU' configuration. A red arrow points to the 'Enable CPU Hot Add' checkbox, which is checked. The 'Cores per Socket' is set to 1, and 'Sockets' is set to 9. Other settings include 'Reservation' at 10305 MHz, 'Limit' at Unlimited MHz, 'Shares' at Normal 1000, 'Hardware virtualization' unchecked, 'Performance Counters' unchecked, and 'Scheduling Affinity' with an information icon. At the bottom right are 'CANCEL', 'BACK', and 'NEXT' buttons.

netapp-ontap-tools-for-vmware-vsphere-10.5-1773361740 - New Virtual Machine from Content Library

- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks
- Customize template
- Customize hardware**
- Ready to complete

Customize hardware

Limit: Unlimited

Shares: Normal 1000

Hardware virtualization: ☐ Expose hardware assisted virtualization to the guest OS

Performance Counters: ☐ Enable virtualized CPU performance counters

Scheduling Affinity: [i](#)

I/O MMU: ☐ Enabled

Memory *: 18 GB

Reservation: 9 GB ☐ Reserve all guest memory (All locked)

Limit: Unlimited MB

Shares: Normal 368640

Memory Hot Plug: ☒ Enable

> Hard disks *: 5 total | 348 GB

CANCEL BACK NEXT

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

배포 작업이 생성되면 vSphere 작업 표시줄에 진행 상황이 표시됩니다.

14. 가상 머신 자동 전원 켜기 옵션을 선택하지 않은 경우, 작업 완료 후 가상 머신의 전원을 켜십시오.

VM의 웹 콘솔에서 설치 진행 상황을 추적할 수 있습니다.

OVF 형식에 오류가 있는 경우, 수정 조치를 안내하는 대화 상자가 나타납니다. 탭 버튼을 사용하여 탐색하고 필요한 변경 사항을 적용한 후 *확인*을 선택하십시오. 문제 해결을 위한 시도는 세 번까지 가능합니다. 세 번 시도 후에도 문제가 지속되면 설치 프로세스가 중단되며, 새 가상 머신에서 다시 설치를 시도하는 것이 좋습니다.

다음 단계는 무엇입니까?

ONTAP tools for VMware vSphere를 vCenter Server 7.0.3와 함께 배포한 경우, 배포 후 다음 단계를 따르십시오.

1. vCenter 클라이언트에 로그인합니다.
2. ONTAP 툴 노드의 전원을 끄십시오.
3. 인벤토리*에서 **VMware vSphere** 가상 머신용 **ONTAP tools**로 이동하여 *설정 편집 옵션을 선택하십시오.
4. **CPU** 옵션에서 **CPU** 핫 추가 활성화 확인란을 선택합니다.
5. 메모리 옵션에서 메모리 핫플러그 옆의 활성화 확인란을 선택하십시오.

ONTAP 도구 배포 오류 해결

배포 문제가 발생하는 경우 로그 및 오류 코드를 검토하여 문제를 진단하고 해결하십시오.

ONTAP tools for VMware vSphere 10.5부터 Pod에서 수집되는 로그 번들에는 MongoDB, RabbitMQ 및 Vault의 로그와 모든 Pod의 상태 및 설명이 포함됩니다. 이러한 로그는 기존 ONTAP tools 서비스 로그에 추가로 제공되어 지원 및 문제 해결 기능을 향상시킵니다.

로그 파일 수집

ONTAP tools Manager 사용자 인터페이스에서 사용 가능한 옵션을 통해 ONTAP tools for VMware vSphere의 로그 파일을 수집할 수 있습니다. 기술 지원 담당자가 문제 해결을 위해 로그 파일 수집을 요청할 수 있습니다.



ONTAP tools Manager에서 로그를 생성하면 모든 vCenter Server 인스턴스의 모든 로그가 포함됩니다. vCenter 클라이언트 사용자 인터페이스에서 로그를 생성하면 선택한 vCenter Server에 대해서만 로그가 생성됩니다.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 사이드바에서 *로그 번들*을 선택합니다.

이 작업은 몇 분 정도 소요될 수 있습니다.

4. 로그 파일을 생성하려면 *생성*을 선택하십시오.
5. 로그 번들의 레이블을 입력하고 *생성*을 선택합니다.

tar.gz 파일을 다운로드하여 기술 지원 팀에 보내십시오.

vCenter 클라이언트 사용자 인터페이스를 사용하여 로그 번들을 생성하려면 아래 단계를 따르십시오:

단계

1. vSphere 클라이언트에 로그인합니다.
2. vSphere Client 홈 페이지에서 지원 > 로그 번들 > *생성*으로 이동합니다.
3. 로그 번들 레이블을 입력하고 로그 번들을 생성합니다. 파일이 생성되면 다운로드 옵션이 표시됩니다. 다운로드에는 다소 시간이 걸릴 수 있습니다.



새로 생성된 로그 번들은 지난 3일(72시간) 이내에 생성된 로그 번들을 대체합니다.

배포 오류 코드

ONTAP tools for VMware vSphere 배포, 재부팅 및 복구 작업 중에 오류 코드가 발생할 수 있습니다. 오류 코드는 5자리 숫자로 구성되며, 앞의 두 자리는 문제가 발생한 스크립트를 나타내고, 뒤의 세 자리는 해당 스크립트 내의 특정 워크플로를 나타냅니다.

모든 오류 로그는 문제 추적 및 해결을 용이하게 하기 위해 /var/log 디렉터리의 ansible-perl-errors.log 파일에 기록됩니다. 이 로그 파일에는 오류 코드와 실패한 Ansible 작업이 포함됩니다.



이 페이지에 제공된 오류 코드는 참고용일 뿐입니다. 오류가 계속 발생하거나 해결 방법이 제시되지 않은 경우 지원팀에 문의하십시오.

다음 표에는 오류 코드와 해당 파일 이름이 나열되어 있습니다.

오류 코드	스크립트 이름
00	firstboot-network-config.pl, mode deploy
01	firstboot-network-config.pl, 업그레이드 모드
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, 비HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

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

배포 오류 코드	워크플로우	해결 방법
049	네트워크 및 유효성 검사를 위한 Perl 스크립트도 곧 할당될 예정입니다.	-
050	SSH 키 생성 실패	기본 가상 머신(VM)을 재시작합니다.
053	RKE2 설치에 실패했습니다	다음 명령을 실행하고 기본 VM을 다시 시작하거나 다시 배포하십시오. <code>sudo rke2-killall.sh</code> (모든 VM) <code>sudo rke2-uninstall.sh</code> (모든 VM).
054	kubeconfig 설정에 실패했습니다.	재배포
055	레지스트리 배포에 실패했습니다	레지스트리 Pod가 있는 경우 Pod가 준비될 때까지 기다린 후 기본 VM을 다시 시작하거나 재배포하십시오.
059	KubeVip 배포에 실패했습니다.	Kubernetes 컨트롤 플레인용 가상 IP 주소와 배포 중에 제공된 ONTAP tools IP 주소가 동일한 VLAN에 속하고 사용 가능한 IP 주소인지 확인하십시오. 이전의 모든 사항이 올바르면 재시작하십시오. 그렇지 않으면 재배포하십시오.
060	운영자 배포에 실패했습니다	재시작

061	서비스 배포에 실패했습니다	ntv-system 네임스페이스에서 get pods, get rs, get svc 등의 기본적인 Kubernetes 디버깅을 수행하여 자세한 내용과 오류 로그를 /var/log/ansible-perl-errors.log 및 /var/log/ansible-run.log에서 확인한 후 재배포하십시오.
062	ONTAP tools 서비스 배포에 실패했습니다.	자세한 내용을 확인하고 다시 배포하려면 /var/log/ansible-perl-errors.log에 있는 오류 로그를 참조하십시오.
065	Swagger 페이지 URL에 연결할 수 없습니다	재배포
066	게이트웨이 인증서 배포 후 단계에 실패했습니다.	업그레이드를 복구/완료하려면 다음을 수행하십시오. • 진단 셸을 활성화합니다. • 'sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy' 명령을 실행합니다. • /var/log/post-deploy-upgrade.log에서 로그를 확인하십시오.
088	journald에 대한 로그 로테이션 구성에 실패했습니다.	가상 머신이 호스팅되는 호스트와 호환되는 가상 머신 네트워크 설정을 확인하십시오. 다른 호스트로 마이그레이션한 후 가상 머신을 다시 시작해 볼 수 있습니다.
089	요약 로그 순환 설정 파일의 소유권 변경에 실패했습니다.	기본 VM을 재시작합니다.
096	동적 스토리지 프로비저너 설치	-
108	시딩 스크립트 실패	-

114	MongoDB 컬렉션의 내부 인증서 업데이트가 실패했습니다	배포가 오류 코드 114와 함께 실패하면 다음 단계를 완료하십시오. • 진단 셸을 활성화합니다. • 다음 명령을 실행합니다. <code>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --internal_cert_update_collection</code> • <code>`/var/log/otvng/post-deploy-upgrade.log`</code>에서 로그를 검토하십시오
-----	----------------------------------	---

재부팅 오류 코드	워크플로우	해결 방법
067	rke2-server 대기 시간이 초과되었습니다.	-
101	유지 관리/콘솔 사용자 암호를 재설정하는 데 실패했습니다.	-
102	유지 관리/콘솔 사용자 암호 재설정 중 암호 파일 삭제에 실패했습니다.	-
103	금고에서 새 유지 관리/콘솔 사용자 암호를 업데이트하는 데 실패했습니다.	-
088	journald에 대한 로그 로테이션 구성에 실패했습니다.	가상 머신이 호스팅되는 호스트와 호환되는 가상 머신 네트워크 설정을 확인하십시오. 다른 호스트로 마이그레이션한 후 가상 머신을 다시 시작해 볼 수 있습니다.
089	요약 로그 순환 설정 파일의 소유권 변경에 실패했습니다.	가상 머신을 재시작합니다.

ONTAP tools for VMware vSphere 구성

vCenter Server 인스턴스를 ONTAP tools에 추가합니다

vCenter Server 인스턴스를 ONTAP tools for VMware vSphere에 추가하여 vCenter Server 환경의 가상 데이터 저장소를 구성, 관리 및 보호할 수 있습니다. 여러 vCenter Server 인스턴스를 추가하는 경우 ONTAP tools와 각 vCenter Server 간의 안전한 통신을 위해 사용자 지정 CA 인증서가 필요합니다.

이 작업 정보

ONTAP tools는 vCenter Server와 통합되어 vSphere 클라이언트에서 직접 프로비저닝, 스냅샷 및 데이터 보호와 같은 스토리지 작업을 수행할 수 있습니다.

vCenter Server 인스턴스를 ONTAP tools에 추가하면 다음과 같은 작업이 자동으로 실행됩니다.

- ONTAP tools는 vCenter 클라이언트 플러그인을 원격 플러그인으로 등록합니다.
- 플러그인 및 API에 대한 사용자 지정 권한은 vCenter Server 인스턴스에 적용됩니다.
- 사용자 관리를 위해 사용자 지정 역할을 생성합니다.
- 해당 플러그인은 vSphere 사용자 인터페이스에 바로 가기로 표시됩니다.

시작하기 전에

- vCenter Server 인증서에 DNS 및 IP 주소 항목이 모두 포함된 유효한 SAN(Subject Alternative Name) 확장이 있는지 확인하십시오. 예를 들면 다음과 같습니다.

```
X509v3 extensions:  
    X509v3 Subject Alternative Name:  
        DNS: vcenter.example.com, DNS: vcenter, IP Address: 192.168.0.50
```

인증서에 SAN 확장이 포함되어 있지 않거나 SAN 확장에 올바른 DNS 또는 IP 주소 값이 포함되어 있지 않은 경우 인증서 유효성 검사 오류로 인해 ONTAP tools 작업이 실패할 수 있습니다.

- vCenter Server의 Primary Network Identifier(PNID)는 SAN 세부 정보에 포함되어야 합니다. PNID와 DNS 이름은 동일해야 하며 DNS에서 확인 가능해야 합니다.
- vCenter Server를 배포할 때는 정규화된 도메인 이름(FQDN)을 사용하는 것이 좋습니다. 최적의 호환성과 지원을 위해 인증서의 SAN에 DNS Name=machine_FQDN이 포함되어 있는지 확인하십시오.
- 자세한 내용은 VMware 설명서를 참조하십시오.
 - ["vSphere 다양한 솔루션 경로에 대한 인증서 요구 사항"](#)
 - ["vCenter 머신 SSL 인증서 교체 사용자 지정 인증 기관 서명 인증서"](#)
 - ["오류: Subject Alternate Name\(SAN\) 필드에 PNID가 없습니다. 유효한 인증서를 제공하십시오"](#)



FQDN을 사용할 수 없는 경우 PNID를 IP 주소로 설정하고 해당 IP 주소를 SAN에 포함할 수 있습니다. 하지만 VMware에서는 이 방법을 권장하지 않습니다.

단계

1. 웹 브라우저를 열고 다음 URL로 이동하세요: <https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. **vCenters** > *추가*를 선택하여 vCenter Server 인스턴스를 온보딩합니다. vCenter IP 주소 또는 호스트 이름, 사용자 이름, 암호 및 포트 세부 정보를 입력합니다.
4. 고급 옵션에서 vCenter Server 인증서를 자동으로 가져오거나(인증) 수동으로 업로드할 수 있습니다.



ONTAP tools에 vCenter 인스턴스를 추가하는 데 관리자 계정이 필요하지 않습니다. 관리자 계정 없이도 제한된 권한을 가진 사용자 지정 역할을 생성할 수 있습니다. 자세한 내용은 "[vCenter Server RBAC와 ONTAP tools for VMware vSphere 10 함께 사용하기](#)"를 참조하십시오.

ONTAP 도구에서 VASA Provider를 vCenter Server 인스턴스에 등록합니다

ONTAP tools for VMware vSphere를 사용하여 VASA Provider를 vCenter Server 인스턴스에 등록하십시오. 이를 통해 스토리지 정책 기반 관리, vVols 지원 및 ONTAP 시스템에서 VMware Live Site Recovery 어플라이언스와의 통합이 가능해집니다.

VASA 공급자 설정에는 선택한 vCenter Server의 등록 상태가 표시됩니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 플러그인 섹션에서 바로가기 > *NetApp ONTAP tools*를 선택하십시오.
3. 설정 > *VASA 공급자 설정*을 선택합니다. ONTAP tools에서 VASA Provider 등록 상태가 등록되지 않음으로 표시됩니다.
4. VASA 제공업체를 등록하려면 등록 버튼을 선택하십시오.
5. VASA Provider의 이름과 자격 증명을 입력하십시오. 사용자 이름에는 문자, 숫자 및 밑줄만 사용할 수 있습니다. 비밀번호는 8자에서 256자 사이여야 합니다.
6. *등록*을 선택합니다.
7. 등록이 성공적으로 완료되고 페이지가 새로고침되면 ONTAP tools는 등록된 VASA Provider의 상태, 이름 및 버전을 표시합니다.

다음 단계

vCenter 클라이언트에서 온보딩된 VASA Provider가 VASA Provider 목록에 표시되는지 확인하십시오.

단계

1. vCenter Server 인스턴스로 이동합니다.
2. 관리자 자격 증명으로 로그인합니다.
3. **Storage Providers** > *구성*을 선택합니다. 등록된 VASA Provider가 목록에 올바르게 표시되는지 확인합니다.

ONTAP tools를 사용하여 NFS VAAI 플러그인 설치

NFS vStorage API for Array Integration(NFS VAAI) 플러그인은 VMware vSphere를 NFS 스토리지 어레이에 연결합니다. ONTAP tools for VMware vSphere를 사용하여 VAAI 플러그인을 설치하십시오. 이를 통해 ESXi 호스트 대신 NFS 스토리지 어레이에서 특정 스토리지 작업을 처리할 수 있습니다.

시작하기 전에

- ["NetApp VMware VAAI용 NFS 플러그인"](#) 설치 패키지를 다운로드하십시오.
- vSphere 7.0 U3(최신 패치 이상) 및 ONTAP 9.14.1 이상이 설치된 ESXi 호스트가 있는지 확인하십시오.
- NFS 데이터 저장소를 마운트합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 플러그인 섹션에서 바로가기 > *NetApp ONTAP tools*를 선택하십시오.
3. 설정 > *NFS VAAI 도구*를 선택합니다.
4. 이미 VAAI 플러그인을 vCenter Server에 업로드한 경우 *기존 버전*에서 *변경*을 선택하십시오. 업로드하지 않은 경우 *업로드*를 선택하십시오.
5. .vib 파일을 찾아 선택한 다음 *업로드*를 선택하여 ONTAP tools에 파일을 업로드하십시오.
6. *ESXi 호스트에 설치*를 선택하고 NFS VAAI 플러그인을 설치할 ESXi 호스트를 선택한 다음 *설치*를 선택합니다.

vSphere 웹 클라이언트에는 플러그인을 설치할 수 있는 ESXi 호스트만 표시됩니다. 최근 작업 섹션에서 설치 진행 상황을 모니터링할 수 있습니다.

7. 설치 후 ESXi 호스트를 수동으로 재시작하십시오.

ESXi 호스트를 재시작하면 ONTAP tools for VMware vSphere에서 NFS VAAI 플러그인을 자동으로 감지하고 활성화합니다.

다음 단계

NFS VAAI 플러그인을 설치하고 ESXi 호스트를 재부팅한 후 VAAI 복사 오프로드를 위한 NFS 내보내기 정책을 구성하십시오. 내보내기 정책 규칙이 다음 요구 사항을 충족하는지 확인하십시오.

- 해당 ONTAP 볼륨은 NFSv4 호출을 허용합니다.
- 루트 사용자는 루트 권한을 유지하며 모든 접합 상위 볼륨에서 NFSv4가 허용됩니다.
- VAAI 지원 옵션은 해당 NFS 서버에 설정됩니다.

자세한 내용은 ["VAAI 복사 오프로드를 위해 올바른 NFS 내보내기 정책을 구성합니다"](#) KB 문서를 참조하십시오.

관련 정보

["NFS를 통한 VMware vStorage 지원"](#)

["NFSv4.0 활성화 또는 비활성화"](#)

["ONTAP의 NFSv4.2 지원"](#)

ONTAP tools에서 ESXi 호스트 설정을 구성합니다.

ESXi 서버의 다중 경로 및 타임아웃 설정을 구성하면 데이터 가용성과 무결성을 유지하는 데 도움이 됩니다. 기본 경로를 사용할 수 없게 될 경우 백업 스토리지 경로로 자동 페일오버가 가능합니다.

ESXi 서버 다중 경로 및 타임아웃 설정 구성

ONTAP tools for VMware vSphere는 NetApp 스토리지 시스템과 가장 잘 호환되는 ESXi 호스트 다중 경로 설정 및 HBA 타임아웃 설정을 확인하고 설정합니다.

이 작업 정보

이 과정은 사용자의 설정 및 시스템 부하에 따라 시간이 걸릴 수 있습니다. 진행 상황은 최근 작업 패널에서 확인할 수 있습니다.

단계

1. VMware vSphere 웹 클라이언트 홈 페이지에서 *호스트 및 클러스터*를 선택합니다.
2. VMware vSphere 웹 클라이언트의 바로가기 페이지에서 플러그인 섹션 아래에 있는 *NetApp ONTAP tools*를 선택합니다.
3. ONTAP tools for VMware vSphere 플러그인의 개요(대시보드)에서 **ESXi** 호스트 규정 준수 카드로 이동합니다.
4. 권장 설정 적용 링크를 선택합니다.
5. 권장 호스트 설정 적용 창에서 NetApp 권장 설정을 사용하도록 업데이트할 호스트를 선택하고 *다음*을 선택합니다.



ESXi 호스트를 확장하면 현재 값을 확인할 수 있습니다.

6. 설정 페이지에서 필요에 따라 권장 값을 선택하십시오.
7. 요약 창에서 값을 확인하고 *완료*를 선택합니다. 최근 작업 패널에서 진행 상황을 확인할 수 있습니다.

ESXi 호스트 값 설정

ONTAP tools for VMware vSphere를 사용하여 ESXi 호스트의 시간 초과 및 기타 값을 설정하여 최적의 성능과 장애 조치를 구현할 수 있습니다. 이러한 값은 NetApp 테스트를 기반으로 설정됩니다.

ESXi 호스트에서 다음 값을 설정할 수 있습니다.

HBA/CNA 어댑터 설정

다음 매개변수를 기본값으로 설정합니다.

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Emulex FC HBA 타임아웃
- QLogic FC HBA 타임아웃

MPIO 설정

MPIO 설정은 NetApp 스토리지 시스템에 가장 적합한 경로를 선택합니다. MPIO 설정은 최적의 경로를 선택하고 이를 사용합니다.

고성능 환경이나 단일 LUN 데이터스토어를 사용한 테스트 시에는 라운드 로빈(VMW_PSP_RR) 경로 선택 정책(PSP)의 로드 밸런싱 설정을 조정하여 성능을 향상시킬 수 있습니다. 기본 IOPS 값을 1000에서 1로 설정하십시오.



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

NFS 설정

매개변수	이 값을 ...로 설정하십시오.
Net.TcpipHeapSize	32
Net.TcpipHeapMax	1024 MB
NFS.MaxVolumes	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128 이상
NFS.HeartbeatMaxFailures	10
NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

ONTAP tools에 대한 ONTAP 사용자 역할 및 권한을 구성합니다

이 섹션을 사용하여 ONTAP tools for VMware vSphere 및 ONTAP System Manager를 사용하는 스토리지 백엔드에 대한 ONTAP 사용자 역할 및 Privileges를 구성하십시오. 제공된 JSON 파일을 사용하여 역할을 할당하거나, 사용자 및 역할을 수동으로 생성하거나, 관리자가 아닌 계정에 필요한 최소 Privileges를 적용할 수 있습니다.

시작하기 전에

- `_https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip` 을 사용하여 ONTAP tools for VMware vSphere에서 ONTAP Privileges 파일을 다운로드하십시오. zip 파일을 다운로드하면 두 개의 JSON 파일이 있습니다. ASA r2 시스템을 구성할 때는 ASA r2 전용 JSON 파일을 사용하십시오.



클러스터 수준 또는 스토리지 가상 머신(SVM) 수준에서 직접 사용자를 생성할 수 있습니다. `user_roles.json` 파일을 사용하지 않는 경우, 사용자에게 필요한 최소 SVM 권한이 부여되었는지 확인하십시오.

- 스토리지 백엔드에 대한 관리자 권한으로 로그인하십시오.

단계

1. 다운로드한 `https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip` 파일의 압축을 푸세요.
2. 클러스터의 클러스터 관리 IP 주소를 사용하여 ONTAP System Manager에 액세스하십시오.

3. 관리자 권한으로 클러스터에 로그인합니다. 사용자를 구성하려면 다음을 수행합니다.
 - a. 클러스터 ONTAP tools 사용자를 구성하려면 클러스터 > 설정 > 사용자 및 역할 창을 선택하십시오.
 - b. SVM ONTAP tools 사용자를 구성하려면 스토리지 **SVM** > 설정 > 사용자 및 역할 창을 선택하십시오.
 - c. 사용자 아래에서 *추가*를 선택합니다.
 - d. 사용자 추가 대화 상자에서 *가상화 제품*을 선택합니다.
 - e. 찾아보기 를 사용하여 ONTAP Privileges JSON 파일을 선택하고 업로드하십시오. ASA r2 이외의 시스템에서는 users_roles.json 파일을 선택하고, ASA r2 시스템에서는 users_roles_ASAr2.json 파일을 선택하십시오.

ONTAP tools는 제품 필드를 자동으로 채웁니다.

- f. 드롭다운 메뉴에서 제품 기능을 *VSC, VASA Provider 및 SRA*로 선택하십시오.

ONTAP tools는 사용자가 선택한 제품 기능에 따라 역할 필드를 자동으로 채웁니다.

- g. 필수 사용자 이름과 비밀번호를 입력합니다.
- h. 사용자에게 필요한 Privileges(Discovery, Create Storage, Modify Storage, Destroy Storage, NAS/SAN Role)를 선택한 다음 *추가*를 선택합니다.

ONTAP tools가 새 역할과 사용자를 추가합니다. 구성한 역할에 대한 Privileges를 확인할 수 있습니다.

SVM 애그리게이트 매핑 요구 사항

SVM 사용자 자격 증명을 사용하여 데이터스토어를 프로비저닝할 때, ONTAP tools for VMware vSphere는 데이터스토어 POST API에 지정된 애그리게이트에 볼륨을 생성합니다. ONTAP는 SVM 사용자가 SVM에 매핑되지 않은 애그리게이트에 볼륨을 생성하는 것을 방지합니다. 볼륨을 생성하기 전에 ONTAP REST API 또는 CLI를 사용하여 SVM을 필요한 애그리게이트에 매핑하십시오.

REST API:

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

ONTAP CLI:

```
still15_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver      Aggregate      State      Size Type      SnapLock
Type-----
-----svm_test      still15_vsim_ucs630f_aggr1
online      10.11GB vmdisk  non-snaplock
```

ONTAP 사용자 및 역할을 수동으로 생성

JSON 파일 없이 수동으로 사용자 및 역할을 생성합니다.

1. 클러스터의 클러스터 관리 IP 주소를 사용하여 ONTAP System Manager에 액세스하십시오.
2. 관리자 권한으로 클러스터에 로그인합니다.
 - a. 클러스터 ONTAP tools 역할을 구성하려면 클러스터 > 설정 > *사용자 및 역할*을 선택하십시오.
 - b. 클러스터 SVM ONTAP tools 역할을 구성하려면 스토리지 **SVM** > 설정 > *사용자 및 역할*을 선택하십시오.
3. 역할 생성:
 - a. 역할 테이블에서 *추가*를 선택합니다.
 - b. 역할 이름 및 역할 속성 세부 정보를 입력합니다.

*REST API 경로*를 추가하고 드롭다운 목록에서 액세스 권한을 선택합니다.
 - c. 필요한 API를 모두 추가하고 변경 사항을 저장합니다.
4. 사용자 생성:
 - a. 사용자 테이블에서 *추가*를 선택합니다.
 - b. 사용자 추가 대화 상자에서 *System Manager*를 선택합니다.
 - c. *사용자 이름*을 입력하세요.
 - d. 위의 역할 생성 단계에서 생성된 옵션 중에서 *역할*을 선택합니다.
 - e. 액세스 권한을 부여할 애플리케이션과 인증 방법을 입력합니다. ONTAPI와 HTTP는 필수 애플리케이션이며, 인증 유형은 *Password*입니다.
 - f. *사용자 비밀번호*를 설정하고 사용자를 *저장*합니다.

관리자 권한이 없는 전역 범위 클러스터 사용자에게 필요한 최소 권한 목록

이 페이지는 JSON 파일 없이 관리자 권한이 없는 전역 범위 클러스터 사용자에게 필요한 최소 권한을 나열합니다. 클러스터가 로컬 범위에 있는 경우 ONTAP tools for VMware vSphere는 ONTAP에서 프로비저닝하기 위해 읽기 권한 이상이 필요하므로 JSON 파일을 사용하여 사용자를 생성하십시오.

API를 사용하여 기능에 액세스할 수 있습니다.

API	액세스 수준	사용 대상
/api/cluster	읽기 전용	클러스터 구성 검색
/api/cluster/licensing/licenses	읽기 전용	프로토콜별 라이선스 확인
/api/cluster/nodes	읽기 전용	플랫폼 유형 검색
/api/security/accounts	읽기 전용	권한 발견
/api/security/roles	읽기 전용	권한 발견
/api/storage/aggregates	읽기 전용	데이터 저장소/볼륨 프로비저닝 중 애그리게이트 공간 확인
/api/storage/cluster	읽기 전용	클러스터 수준의 공간 및 효율성 데이터를 얻으려면
/api/storage/disks	읽기 전용	집합체에 연결된 디스크를 얻으려면
/api/storage/qos/policies	읽기/생성/수정	QoS 및 VM 정책 관리

/api/svm/svms	읽기 전용	클러스터가 로컬에 추가될 때 SVM 구성을 가져오려면.
/api/network/ip/interfaces	읽기 전용	스토리지 백엔드 추가 - 관리 LIF 범위가 클러스터/SVM임을 식별합니다.
/api/storage/availability-zones	읽기 전용	SAZ 검색. ONTAP 9.16.1 릴리스 이상 및 ASA r2 시스템에 적용됩니다.
/api/cluster/metrocluster	읽기 전용	MetroCluster 상태 및 구성 세부 정보를 가져옵니다.

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



데이터 저장소에 대한 PATCH 작업 및 자동 롤백을 수행하려면 검색, 생성, 수정 및 삭제 권한이 필요합니다. 이러한 권한이 없으면 워크플로 및 정리 작업에 문제가 발생할 수 있습니다.

검색, 생성, 수정 및 삭제 권한을 가진 ONTAP API 기반 사용자는 ONTAP tools 워크플로를 관리할 수 있습니다.

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

```
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
```

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

또한 ONTAP 버전 9.16.0 이상에서는 다음 명령을 실행하십시오.

```
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 실행하십시오.

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

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

모든 Privileges를 가진 SVM 범위 사용자를 생성하려면 다음 명령을 실행하십시오.

```
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 이상에서는 다음 명령을 실행하십시오.

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

이전에 생성한 API 기반 역할을 사용하여 새 API 기반 사용자를 생성하려면 다음 명령을 실행하십시오.

```
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_stil60-cluster_
```

다음 명령을 실행하여 계정 잠금을 해제하고 관리 인터페이스 액세스를 활성화하십시오.

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

예:

```
security login unlock -username testvpsraall -vserver C1_stil60-cluster
```

ONTAP tools for VMware vSphere 10.1 사용자를 10.3 사용자로 업그레이드

JSON 파일을 사용하여 클러스터 범위 사용자를 생성한 ONTAP tools for VMware vSphere 10.1 사용자는 user admin 권한으로 다음 ONTAP CLI 명령을 사용하여 10.3 릴리스로 업그레이드하십시오.

제품 기능 관련:

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

클러스터 권한:

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show"
-access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show"
-access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access
all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access
all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access
all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove"
-access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove"
-access all
```

JSON 파일을 사용하여 SVM 범위 사용자를 생성한 ONTAP tools for VMware vSphere 10.1 사용자는 관리자 권한으로 ONTAP CLI 명령을 사용하여 10.3 릴리스로 업그레이드하십시오.

SVM 권한:

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all
-vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all
-vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show"
-access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show"
-access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read
```

`-vserver <vserver-name>`

`security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all -vserver <vserver-name>`

`security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all -vserver <vserver-name>`

`security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all -vserver <vserver-name>`

`security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all -vserver <vserver-name>`

`security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all -vserver <vserver-name>`

`security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all -vserver <vserver-name>`

다음 명령을 활성화하려면 기존 역할에 `vserver nvme namespace show` 및 `vserver nvme subsystem show` 명령을 추가하십시오.

```
vserver nvme namespace create  
  
vserver nvme namespace modify  
  
vserver nvme subsystem create  
  
vserver nvme subsystem modify
```

ONTAP tools for VMware vSphere 10.3 사용자를 10.4 사용자로 업그레이드

ONTAP 9.16.1부터 ONTAP tools for VMware vSphere 10.3 사용자를 10.4 사용자로 업그레이드하십시오.

JSON 파일을 사용하여 클러스터 범위 사용자를 생성하고 ONTAP 버전 9.16.1 이상인 ONTAP tools for VMware vSphere 10.3 사용자는 관리자 권한으로 ONTAP CLI 명령을 사용하여 10.4 릴리스로 업그레이드하십시오.

제품 기능 관련:

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

클러스터 권한:

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

ONTAP tools에 스토리지 백엔드 추가

ONTAP tools for VMware vSphere를 사용하여 ESXi 호스트의 스토리지 백엔드를 추가하고 관리할 수 있습니다. 클러스터 또는 SVM을 온보딩하고, MetroCluster 지원을 활성화하고, 안전한 연결을 위한 인증서를 검증할 수 있습니다. ONTAP tools Manager 또는 vSphere 클라이언트를 사용하여 스토리지 백엔드를 구성하고, 인증서 상태를 모니터링하고, 클러스터 변경 후 리소스를 수동으로 다시 검색할 수 있습니다.

로컬에 스토리지 백엔드를 추가하려면 ONTAP tools 인터페이스에서 클러스터 또는 SVM 자격 증명을 사용하십시오. 로컬 스토리지 백엔드는 선택한 vCenter Server에서만 사용할 수 있습니다. ONTAP tools는 vVols 또는 VMFS 데이터스토어 관리를 위해 SVM을 vCenter Server에 매핑합니다. VMFS 데이터스토어 및 SRA 워크플로우의 경우, 클러스터를 전역적으로 매핑하지 않고 SVM 자격 증명을 사용할 수 있습니다.

글로벌 스토리지 백엔드를 추가하려면 ONTAP tools Manager에서 ONTAP 클러스터 자격 증명을 사용하십시오. 글로벌 스토리지 백엔드를 사용하면 vVol 관리에 필요한 클러스터 리소스를 식별하는 검색 워크플로를 수행할 수 있습니다. 멀티테넌트 환경에서는 SVM 사용자를 로컬에 추가하여 vVols 데이터스토어를 관리할 수 있습니다.

글로벌 및 로컬 스토리지 백엔드에 대한 자세한 내용은 KB 문서 ["OTV 10: 스토리지 백엔드 글로벌 및 로컬 범위란 무엇인가"](#)를 참조하십시오.

MetroCluster 지원이 ONTAP에서 활성화된 경우 소스 및 대상 클러스터를 로컬 또는 글로벌 스토리지 백엔드로 온보딩하십시오.

시작하기 전에

인증서에 유효한 SAN(Subject Alternative Name) 필드가 포함되어 있는지 확인하십시오. ONTAP 시스템은 SAN 필드를 사용하여 클러스터 및 SVM 관리 LIF를 식별합니다.

ONTAP tools Manager 사용



멀티테넌트 환경에서는 스토리지 백엔드 클러스터를 전역적으로 추가하고 SVM을 로컬로 추가하여 SVM 사용자 자격 증명을 사용할 수 있습니다.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 사이드바에서 *스토리지 백엔드*를 선택합니다.
4. 스토리지 백엔드를 추가하고 서버 IP 주소 또는 FQDN, 사용자 이름 및 비밀번호 정보를 제공하십시오.



IPv4 및 IPv6 주소 관리 LIF가 지원됩니다.

5. ONTAP 클러스터 인증서를 자동으로 가져와서 승인하거나, 인증서 위치를 찾아 수동으로 업로드할 수 있습니다.



필요한 경우 유지 관리 콘솔에서 SAN(Subject Alternative Name) 유효성 검사를 비활성화할 수 있습니다. 자세한 내용은 "[인증서 유효성 검사 플러그인 변경](#)"을 참조하십시오.

6. 추가하는 스토리지 백엔드가 MetroCluster 구성의 일부인 경우, ONTAP Tools Manager에 피어링된 클러스터를 추가하라는 팝업 메시지가 표시됩니다. *추가*를 선택하고 MetroCluster 피어 스토리지 백엔드에 대한 세부 정보를 입력하십시오.



ONTAP 시스템이 전환 및 스위치백을 수행한 후 ONTAP tools 검색을 수동으로 실행하십시오.

vSphere 클라이언트 사용자 인터페이스 사용



vVols 데이터스토어는 vSphere 클라이언트 사용자 인터페이스를 통한 SVM 사용자의 직접 추가를 지원하지 않습니다.

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



클러스터 기반 자격 증명과 IPv4 또는 IPv6 관리 LIF를 사용하여 스토리지 백엔드를 추가할 수 있습니다. SVM 사용자를 직접 추가하려면 SVM 기반 자격 증명과 SVM 관리 LIF를 제공하십시오. 클러스터가 이미 온보딩된 경우 해당 클러스터에서 SVM 사용자를 다시 온보딩할 수 없습니다.

5. ONTAP 클러스터 인증서를 자동으로 가져와서 승인하거나, 인증서 위치를 찾아 수동으로 업로드할 수 있습니다.
6. 추가된 스토리지 백엔드가 MetroCluster 구성의 일부인 경우, ONTAP tools는 **MetroCluster** 피어 추가

화면을 표시합니다. 피어 스토리지 백엔드를 추가하려면 *피어 추가*를 선택하십시오.



ONTAP 시스템이 전환 및 스위치백을 수행한 후 ONTAP tools 검색을 수동으로 실행하십시오.

ONTAP tools는 스토리지 백엔드 페이지에 새로 추가된 스토리지 백엔드를 나열합니다. 인증서가 30일 이내에 만료되는 경우, ONTAP tools는 인증서 만료일 옆에 경고를 표시합니다. 만료 후에 ONTAP tools는 스토리지 시스템에 연결할 수 없기 때문에 스토리지 백엔드를 알 수 없음으로 표시합니다.

관련 정보

"OTV 10: 스토리지 백엔드 글로벌 및 로컬 범위란 무엇인가"

"클러스터를 MetroCluster 구성으로 설정"

ONTAP 도구에서 스토리지 백엔드를 vCenter Server 인스턴스에 연결합니다

vCenter Server 인스턴스와 스토리지 백엔드를 연결하여 모든 vCenter Server 인스턴스에서 액세스할 수 있도록 하십시오. MetroCluster 구성의 경우, 스토리지 백엔드 클러스터를 연결할 때 해당 피어 클러스터도 vCenter Server와 연결해야 합니다.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 사이드바에서 vCenter를 선택합니다.
4. 스토리지 백엔드에 연결하려는 vCenter Server 인스턴스 옆에 있는 세로 점 세 개(...)를 선택합니다.
5. 드롭다운 메뉴에서 선택한 vCenter Server 인스턴스와 연결할 스토리지 백엔드를 선택합니다.

ONTAP 도구에서 네트워크 액세스 구성

기본적으로 ESXi 호스트에서 검색된 모든 IP 주소는 네트워크 액세스를 구성하지 않는 한 내보내기 정책에 자동으로 추가됩니다. 특정 IP 주소에서만 액세스를 허용하도록 내보내기 정책을 수정할 수 있습니다. 제외된 ESXi 호스트가 마운트 작업을 시도하면 작업이 실패합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 플러그인 섹션의 바로가기 페이지에서 *NetApp ONTAP tools*를 선택하십시오.
3. ONTAP tools의 왼쪽 창에서 설정 > 네트워크 액세스 관리 > *편집*으로 이동합니다.

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

4. *저장*을 선택합니다.

ONTAP tools에서 데이터 저장소를 생성합니다

호스트 클러스터 수준에서 데이터 저장소를 생성하면 ONTAP tools는 해당 데이터 저장소를 모든 대상 호스트에 마운트하고 필요한 권한이 있는 경우에만 작업을 활성화합니다.

기본 데이터 저장소와 **vCenter Server** 및 **ONTAP tools**로 관리되는 데이터 저장소 간의 상호 운용성

ONTAP tools for VMware vSphere 10.4부터 ONTAP tools는 데이터스토어에 대한 중첩 igroup을 생성합니다. 상위 igroup은 데이터스토어에 특화되고 하위 igroup은 호스트에 매핑됩니다. ONTAP System Manager에서 플랫폼 igroup을 생성하고 이를 사용하여 ONTAP tools를 사용하지 않고도 VMFS 데이터스토어를 생성할 수 있습니다. 자세한 내용은 ["SAN 이니시에이터 및 igroup 관리"](#)을 참조하십시오.

스토리지를 온보딩하고 데이터스토어 검색을 실행하면 ONTAP tools가 VMFS 데이터스토어의 플랫폼 igroup을 중첩 igroup으로 변경합니다. 이전의 플랫폼 igroup을 사용하여 새 데이터스토어를 생성할 수 없습니다. 중첩 igroup을 재사용하려면 ONTAP tools 인터페이스 또는 REST API를 사용하십시오.

vVols 데이터스토어를 생성합니다.

ONTAP tools for VMware vSphere 10.3부터 ASA r2 시스템에서 공간 효율성을 thin으로 설정하여 vVols 데이터스토어를 생성할 수 있습니다. vVol, VASA Provider는 vVol 데이터스토어를 생성하는 동안 컨테이너와 원하는 프로토콜 엔드포인트를 생성합니다. VASA Provider는 이 컨테이너에 백업 볼륨을 할당하지 않습니다.

시작하기 전에

- 루트 애그리게이트가 SVM에 매핑되지 않도록 하십시오.
- VASA Provider가 선택한 vCenter에 등록되어 있는지 확인하십시오.
- ASA r2 스토리지 시스템에서 SVM은 SVM 사용자를 위해 애그리게이트에 매핑되어야 합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 **NetApp ONTAP tools** > *데이터 저장소 생성*을 선택합니다.
3. *데이터 저장소 유형*으로 vVols를 선택합니다.
4. 데이터 저장소 이름*과 *프로토콜 정보를 입력하십시오.



ASA r2 시스템은 vVols에 대해 iSCSI 및 FC 프로토콜을 지원합니다.

5. 데이터스토어를 생성할 스토리지 VM을 선택합니다.
6. 고급 옵션에서:
 - *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 **Custom initiator group** 이름을 선택할 수 있습니다.



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

7. 저장소 속성 창에서 새 볼륨을 생성하거나 기존 볼륨을 사용할 수 있습니다. 하지만 이 두 가지 유형의 볼륨을 결합하여 vVols 데이터스토어를 생성할 수는 없습니다.

새 볼륨을 생성할 때 데이터스토어에서 QoS를 활성화할 수 있습니다. 기본적으로 LUN 생성 요청마다 하나의 볼륨이 생성됩니다. ASA r2 스토리지 시스템의 vVols 데이터스토어의 경우 이 단계를 건너뛸 수 있습니다.

8. 요약 창에서 선택 내용을 검토하고 *완료*를 선택하십시오.

NFS 데이터스토어 생성

NFS 데이터스토어는 NFS 프로토콜을 사용하여 ESXi 호스트를 공유 스토리지에 연결합니다. 간단하고 유연하며 VMware vSphere 환경에서 사용됩니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 **NetApp ONTAP tools** > *데이터 저장소 생성*을 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 프로토콜이 선택된 경우에만 사용할 수 있습니다.

5. 스토리지 창에서 플랫폼 및 스토리지 **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 볼륨 정책 또는 루트 볼륨 정책을 사용하여 NFS 데이터스토어를 생성할 수 없습니다.

- 고급 옵션에서 비대칭 토글 버튼은 플랫폼 드롭다운 메뉴에서 성능 또는 용량이 선택된 경우에만 표시됩니다.
 - 플랫폼 드롭다운 메뉴에서 모두 옵션을 선택하면 vCenter의 모든 SVM을 볼 수 있습니다. 플랫폼 및 비대칭 플래그는 가시성에 영향을 미치지 않습니다.
7. 저장소 속성 창에서 볼륨 생성을 위한 애그리게이트를 선택합니다. 고급 옵션에서 필요에 따라 공간 예약 및 *QoS 활성화*를 선택합니다.
 8. 요약 창에서 선택 사항을 검토하고 완료를 선택하십시오.

ONTAP tools는 NFS 데이터스토어를 생성하고 모든 호스트에 마운트합니다.

VMFS 데이터스토어 생성

VMFS는 가상 머신 파일을 저장하는 클러스터형 파일 시스템입니다. 여러 ESXi 호스트가 vMotion 및 고가용성 기능을 위해 동일한 VM 파일에 동시에 액세스할 수 있습니다.

보호된 클러스터에서:

- VMFS 데이터스토어만 생성할 수 있습니다. 보호된 클러스터에 VMFS 데이터스토어를 추가하면 자동으로 보호됩니다.
- 보호된 호스트 클러스터가 하나 이상 있는 데이터 센터에는 데이터 저장소를 생성할 수 없습니다.
- 상위 호스트 클러스터가 "자동 장애 조치 이중화 정책"(균일 또는 비균일 구성)으로 보호되는 경우 ESXi 호스트에 데이터 저장소를 생성할 수 없습니다.
- VMFS 데이터스토어는 비동기 관계로 보호되는 ESXi 호스트에만 생성할 수 있습니다. "자동 장애 조치 이중화" 정책으로 보호되는 호스트 클러스터의 일부인 ESXi 호스트에는 데이터스토어를 생성하고 마운트할 수 없습니다.

시작하기 전에

- ONTAP 스토리지 측에서 각 프로토콜에 대한 서비스 및 LIF를 활성화하십시오.
- ASA r2 스토리지 시스템의 SVM 사용자를 위해 SVM을 애그리게이트에 매핑합니다.
- NVMe/TCP 프로토콜을 사용하는 경우 ESXi 호스트를 구성하십시오.

- a. 검토 "[VMware 호환성 가이드](#)"



VMware vSphere 7.0 U3 이상 버전은 NVMe/TCP 프로토콜을 지원합니다. 하지만 VMware vSphere 8.0 이상 버전을 사용하는 것이 좋습니다.

- b. 네트워크 인터페이스 카드(NIC) 공급업체가 NVMe/TCP 프로토콜을 사용하는 ESXi NIC를 지원하는지 확인하십시오.
- c. NIC 공급업체 사양에 따라 ESXi NIC를 NVMe/TCP용으로 설정하십시오.
- d. VMware vSphere 7 릴리스를 사용하는 경우 VMware 사이트 "[NVMe over TCP 어댑터에 대한 VMkernel 바인딩 구성](#)"의 지침에 따라 NVMe/TCP 포트 바인딩을 구성하십시오. VMware vSphere 8 릴리스를 사용하는 경우 "[ESXi에서 TCP를 통한 NVMe 구성](#)"에 따라 NVMe/TCP 포트 바인딩을 구성하십시오.
- e. VMware vSphere 7 릴리스의 경우, NVMe/TCP 소프트웨어 어댑터를 구성하려면 페이지 "[NVMe over RDMA 또는 NVMe over TCP 소프트웨어 어댑터 활성화](#)"의 지침을 따르십시오. VMware vSphere 8 릴리스의 경우, NVMe/TCP 소프트웨어 어댑터를 구성하려면 "[RDMA를 통한 소프트웨어 NVMe 또는 TCP를 통한 NVMe 어댑터 추가](#)"를 따르십시오.
- f. ESXi 호스트에서 "[스토리지 시스템 및 호스트 검색](#)" 작업을 실행하십시오. 자세한 내용은 "[vSphere 8.0 업데이트 1 및 ONTAP 9.13.1을 사용하여 VMFS 데이터스토어에 NVMe/TCP를 구성하는 방법](#)"을 참조하십시오.

• NVMe/FC 프로토콜을 사용하는 경우 다음 단계를 수행하여 ESXi 호스트를 구성하십시오.

- a. 아직 활성화하지 않았다면 ESXi 호스트에서 NVMe over Fabrics(NVMe-oF)를 활성화하십시오.
- b. SCSI 조닝을 완료합니다.
- c. ESXi 호스트와 ONTAP 시스템이 물리적 및 논리적 계층에서 연결되어 있는지 확인하십시오.

FC 프로토콜용 ONTAP SVM을 구성하려면 다음을 참조하십시오. "[FC용 SVM 구성](#)"

VMware vSphere 8.0에서 NVMe/FC 프로토콜을 사용하는 방법에 대한 자세한 내용은 "[ESXi 8.x with ONTAP에 대한 NVMe-oF 호스트 구성](#)"를 참조하십시오.

VMware vSphere 7.0에서 NVMe/FC를 사용하는 방법에 대한 자세한 내용은 "[ONTAP NVMe/FC 호스트 구성 가이드](#)" 및 "[TR-4684](#)"을 참조하십시오.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 **NetApp ONTAP tools** > *데이터 저장소 생성*을 선택합니다.
3. VMFS 데이터 저장소 유형을 선택합니다.
4. 이름 및 프로토콜 창에 데이터스토어 이름, 크기 및 프로토콜 정보를 입력합니다. 기존 VMFS 클러스터에 새 데이터스토어를 추가하려면 고급 옵션에서 데이터스토어 클러스터를 선택합니다.
5. **Storage** 창에서 스토리지 VM을 선택합니다. 필요에 따라 고급 옵션 섹션에서 *사용자 지정 이니시에이터 그룹 이름*을 입력합니다. 데이터스토어에 대해 기존 igroup을 선택하거나 사용자 지정 이름으로 새 igroup을 생성할 수 있습니다.

NVMe/FC 또는 NVMe/TCP 프로토콜을 선택하면 새 네임스페이스 서브시스템이 생성되어 네임스페이스 매핑에 사용됩니다. ONTAP tools는 데이터스토어 이름을 포함하는 자동 생성된 이름을 사용하여 네임스페이스 서브시스템을 생성합니다. **Storage** 창의 고급 옵션에 있는 **custom namespace subsystem name** 필드에서 네임스페이스 서브시스템의 이름을 변경할 수 있습니다.

6. 스토리지 속성 창에서:

- a. 드롭다운 옵션에서 *Aggregate*를 선택합니다.



ASA r2 스토리지 시스템의 경우 스토리지가 분산되어 있으므로 집계(**Aggregate**) 옵션이 표시되지 않습니다. ASA r2 스토리지 시스템 유형으로 SVM을 선택하면 스토리지 속성 페이지에 QoS 활성화 옵션이 표시됩니다.

- b. ONTAP tools는 선택한 프로토콜을 기반으로 씬 스페이스 예약이 있는 스토리지 단위 (LUN/Namespace)를 생성합니다.



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

- c. 이기종 클러스터인 12노드 SVM을 사용하는 ASA r2 스토리지 시스템에 대해 *성능 서비스 수준*을 선택하십시오. 선택한 SVM이 동종 클러스터이거나 SVM 사용자를 사용하는 경우에는 이 옵션을 사용할 수 없습니다.

'Any'는 기본 성능 서비스 수준(PSL) 값입니다. 이 설정은 ONTAP 균형 배치 알고리즘을 사용하여 스토리지 유닛을 생성합니다. 하지만 필요에 따라 성능 또는 익스트림 옵션을 선택할 수 있습니다.

- d. 필요에 따라 기존 볼륨 사용 및 **QoS** 활성화 옵션을 선택하고 세부 정보를 입력하십시오.



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 데이터스토어를 생성할 수 없습니다. VMFS 데이터스토어를 위한 새 볼륨을 생성하십시오.

7. 요약 창에서 데이터 저장소 세부 정보를 검토하고 *완료*를 선택합니다.



보호된 클러스터에 데이터 저장소를 생성하면 "The datastore is being mounted on a protected Cluster."라는 읽기 전용 메시지가 표시될 수 있습니다.

결과

ONTAP tools는 VMFS 데이터스토어를 생성하고 모든 호스트에 마운트합니다.

데이터 저장소 및 가상 머신 보호

ONTAP tools에서 호스트 클러스터 보호

ONTAP tools for VMware vSphere는 호스트 클러스터 보호를 관리합니다. 선택한 SVM에 속하고 클러스터의 하나 이상의 호스트에 마운트된 모든 데이터 저장소는 호스트 클러스터로 보호됩니다.

시작하기 전에

호스트 클러스터를 보호하기 전에 다음 요구 사항을 충족하는지 확인하십시오.

- 호스트 클러스터에는 단일 SVM의 데이터 저장소만 포함되어 있습니다.
- 호스트 클러스터의 데이터 저장소는 클러스터 외부의 호스트에 마운트되지 않습니다.
- 호스트 클러스터에 마운트된 데이터 저장소는 iSCSI 또는 FC 프로토콜을 사용하는 VMFS 데이터 저장소입니다. vVols, NFS 또는 NVMe/FC 및 NVMe/TCP 프로토콜을 사용하는 VMFS 데이터 저장소는 사용할 수 없습니다.
- 호스트에 마운트된 FlexVol/LUN 볼륨 기반 데이터 저장소는 어떤 일관성 그룹에도 속하지 않습니다.
- 호스트에 마운트된 FlexVol/LUN 볼륨 기반 데이터 저장소는 어떠한 SnapMirror 관계에도 포함되지 않습니다.
- 호스트 클러스터에는 하나 이상의 데이터 저장소가 포함되어 있습니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools* > *클러스터 보호*를 선택합니다.
3. 클러스터 보호 창에서 시스템은 데이터 저장소 유형과 소스 스토리지 가상 머신(VM) 세부 정보를 자동으로 채웁니다. 보호된 데이터 저장소를 보려면 데이터 저장소 링크를 선택하십시오.
4. *관계 추가*를 선택합니다.
5. **SnapMirror** 관계 추가 창에서 대상 스토리지 **VM***과 *정책 유형을 선택합니다.

정책 유형은 비동기 또는 AutomatedFailOverDuplex일 수 있습니다.

SnapMirror 관계를 AutomatedFailOverDuplex 유형 정책으로 추가할 때, ONTAP tools for VMware vSphere가 배포된 동일한 vCenter에 대상 스토리지 VM을 스토리지 백엔드로 추가해야 합니다.

AutomatedFailOverDuplex 정책 유형에는 균일 호스트 구성과 비균일 호스트 구성이 있습니다. 균일 호스트 구성 토글 버튼을 선택하면 호스트 이니시에이터 그룹 구성이 대상 사이트에 암묵적으로 복제됩니다. 자세한 내용은 ["핵심 개념 및 용어"](#)를 참조하십시오.

6. 비균일 호스트 구성을 선택하는 경우, 해당 클러스터 내의 각 호스트에 대한 호스트 액세스(소스/대상)를 선택합니다.
7. *추가*를 선택합니다.
8. 호스트 클러스터 보호는 호스트 클러스터 보호 수정 작업을 사용하여 편집할 수 있습니다. 관계는 줄임표 메뉴 옵션을 사용하여 편집하거나 삭제할 수 있습니다.
9. 보호 버튼을 선택합니다.

시스템은 vCenter 작업 ID 세부 정보가 포함된 vCenter 작업을 생성하고 최근 작업 패널에 진행 상황을 표시합니다. 이 작업은 비동기 작업이므로 사용자 인터페이스에는 요청 제출 상태만 표시되고 작업 완료를 기다리지 않습니다.

10. 보호된 호스트 클러스터를 보려면 * NetApp ONTAP tools* > 보호 > *호스트 클러스터 관계*로 이동하십시오. 일관성 그룹을 선택하여 용량, 연결된 데이터 저장소 및 하위 일관성 그룹을 확인합니다.



생성 후 1시간 이내에 보호 기능을 해제해야 하는 경우 먼저 스토리지 검색을 실행하십시오.

관련 정보

["VMware vSphere Metro Storage Cluster\(vMSC\)"](#)

SRA 보호를 사용하여 보호

데이터 저장소를 보호하려면 **ONTAP tools**에서 **SRA**를 구성하십시오

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

시작하기 전에

- vCenter Server 인스턴스를 설정하고 ESXi 호스트를 구성해야 합니다.
- ONTAP tools for VMware vSphere를 배포해야 합니다.
- SRA 어댑터 .tar.gz 파일을 ["NetApp 지원 사이트"](#)에서 다운로드해야 합니다.
- SRA 워크플로우를 실행하기 전에 소스 및 대상 ONTAP 클러스터 모두에 동일한 사용자 지정 SnapMirror 일정이 있어야 합니다.
- ["ONTAP tools for VMware vSphere 서비스 활성화"](#) SRA 기능을 활성화합니다.

단계

1. URL `https://<srn\_ip>:5480`을 사용하여 VMware Live Site Recovery 어플라이언스 관리 인터페이스에 로그인한 다음 VMware Live Site Recovery 어플라이언스 관리 인터페이스에서 Storage Replication Adapters로 이동합니다.
2. *새 어댑터*를 선택합니다.
3. SRA 플러그인용 .tar.gz 설치 프로그램을 VMware Live Site Recovery에 업로드하십시오.
4. VMware Live Site Recovery 스토리지 복제 어댑터 페이지에서 세부 정보가 업데이트되었는지 확인하려면 어댑터를 다시 스캔하십시오.



장애 조치 후에는 데이터 저장소에 대해 확장, 마운트 및 삭제와 같은 작업이 사용 불가능할 수 있습니다. 데이터 저장소 검색을 수행하여 컨텍스트 메뉴의 적절한 작업을 새로 고치고 표시하십시오.



재보호 작업을 수행할 때마다 양쪽 사이트 모두에서 스토리지 검색을 수행해야 합니다.

SRA 보호 기능을 사용하는 새로운 설정에서는 항상 테스트 페일오버를 실행해야 합니다. 테스트 페일오버를 건너뛰면 재보호 작업이 실패할 수 있습니다.

팬아웃 구성에서 자동 페일오버 듀플렉스 및 비동기 SnapMirror에 대해 SnapMirror 소스가 사이트 B로 변경되는

SnapMirror Active Sync 페일오버 후, 사이트 B와 C 간에 테스트 페일오버를 실행하십시오. 이 단계를 건너뛰면 재보호 작업이 실패할 수 있습니다.

관련 정보

["VMware Site Recovery Manager를 사용하여 NFS 데이터스토어에 대한 재해 복구 구성"](#)

SAN 및 NAS 환경용 ONTAP tools에서 SRA 구성

VMware Live Site Recovery용 스토리지 복제 어댑터(SRA)를 실행하기 전에 스토리지 시스템을 설정해야 합니다.

SAN 환경에 맞게 SRA 구성



SRA 워크플로의 일관성 그룹은 Unified 및 ASA r2 스토리지 시스템 모두에서 SAN 프로토콜(iSCSI 및 Fibre Channel)을 통해서만 지원됩니다.

시작하기 전에

보호 사이트와 복구 사이트에 다음 프로그램이 설치되어 있어야 합니다.

- VMware Live Site Recovery: VMware 웹사이트에서는 VMware Live Site Recovery 설치 관련 문서를 제공합니다.

["VMware Live Site Recovery 정보"](#)

- SRA: VMware Live Site Recovery에 어댑터를 설치합니다.

iSCSI 프로토콜 구성의 경우 SRA 워크플로우를 실행하기 전에 다음 사항에 유의하십시오.

- 보호된 사이트: iSCSI 스토리지 어댑터 및 데이터 LIF 세부 정보는 데이터 저장소를 프로비저닝할 때 자동으로 구성됩니다. 수동 구성은 필요하지 않습니다.
- 복구 사이트: 재해 복구를 위한 리소스 매핑에 포함된 각 ESXi 호스트에서 iSCSI 스토리지 어댑터를 수동으로 구성해야 합니다. 각 호스트에서 어댑터를 개별적으로 구성하는 번거로움을 피하려면 SRA 워크플로가 구성된 SVM을 사용하여 복구 사이트에 iSCSI 유형의 자리 표시자 데이터 저장소를 생성하십시오. 이렇게 하면 iSCSI 어댑터와 필요한 데이터 LIF IP 주소가 매핑된 모든 ESXi 호스트에 자동으로 추가됩니다. 자세한 내용은 ["ONTAP tools에서 플레이스홀더 데이터 저장소를 구성합니다"](#)을(를) 참조하십시오.

단계

1. 보호 대상 사이트의 운영 스토리지 시스템에 있는 LUN에 운영 ESXi 호스트가 연결되어 있는지 확인하십시오.
2. 운영 스토리지 시스템에서 LUN이 `ostype` 옵션이 `_VMware_`로 설정된 `igroup`에 있는지 확인합니다.
3. 복구 사이트의 ESXi 호스트가 스토리지 가상 머신(SVM)에 대해 적절한 iSCSI 및 Fibre Channel 연결을 갖추고 있는지 확인하십시오. 보조 사이트의 ESXi 호스트는 보조 사이트 스토리지에 액세스할 수 있어야 하고, 기본 사이트의 ESXi 호스트는 기본 사이트 스토리지에 액세스할 수 있어야 합니다.

이 작업은 ESXi 호스트의 SVM에 로컬 LUN이 연결되어 있는지 확인하거나 `iscsi show initiators` SVM에서 명령을 실행하여 수행할 수 있습니다. iSCSI 연결을 확인하려면 ESXi 호스트에서 매핑된 LUN에 대한 LUN 액세스 권한을 확인하십시오.



SRA 워크플로에서 NFS에 대한 일관성 그룹은 지원되지 않습니다. NFS 데이터 저장소 볼륨이 일관성 그룹에 배치되고 보호되는 경우 장치 검색 작업이 실패합니다. SRA를 사용하여 NFS 데이터 저장소를 보호할 때는 일관성 그룹을 사용하지 마십시오.

시작하기 전에

보호 사이트와 복구 사이트에 다음 프로그램이 설치되어 있어야 합니다.

- VMware Live Site Recovery: VMware Live Site Recovery 설치 관련 문서는 VMware 웹사이트에서 확인하실 수 있습니다 - "[VMware Live Site Recovery 정보](#)"
- SRA: VMware Live Site Recovery 및 SRA 서버에 어댑터를 설치합니다.

단계

1. 보호 대상 사이트의 데이터 저장소에 vCenter Server에 등록된 가상 머신이 있는지 확인하십시오.
2. 보호 대상 사이트의 ESXi 호스트가 스토리지 가상 머신(SVM)에서 NFS 익스포트 볼륨을 마운트했는지 확인하십시오.
3. Array Manager 마법사를 사용하여 VMware Live Site Recovery에 어레이를 추가할 때 **NFS Addresses** 필드에 NFS 익스포트가 있는 유효한 IP 주소가 지정되어 있는지 확인하십시오. **NFS Addresses** 필드에 NFS 호스트 이름 또는 FQDN을 사용하지 마십시오.
4. 복구 사이트의 각 ESXi 호스트에서 ping 명령을 사용하여 호스트에 SVM에서 NFS 내보내기를 제공하는 데 사용되는 IP 주소에 액세스할 수 있는 VMkernel 포트가 있는지 확인하십시오.

확장성이 높은 환경을 위해 **ONTAP tools**에서 **SRA**를 구성합니다

대규모 환경에서 최적의 성능을 발휘하려면 스토리지 복제 어댑터(SRA)에 권장되는 설정에 따라 스토리지 시간 초과 간격을 구성해야 합니다.

스토리지 공급자 설정

확장된 환경을 위한 VMware Live Site Recovery의 시간 초과 값은 다음과 같이 설정해야 합니다.

고급 설정	타임아웃 값
<code>StorageProvider.resignatureTimeout</code>	설정값을 900초에서 12000초로 늘립니다.
<code>storageProvider.hostRescanDelaySec</code>	60
<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	높은 값을 설정합니다(예: 99999).

해당 `StorageProvider.autoResignatureMode` 옵션도 활성화해야 합니다.

스토리지 공급자 설정 수정에 대한 자세한 내용은 "[스토리지 공급자 설정 변경](#)"를 참조하십시오.

스토리지 설정

타임아웃이 발생하면 `storage.commandTimeout` 및 `storage.maxConcurrentCommandCnt`의 값을 더 높은 값으로 늘리십시오.



지정된 타임아웃 간격은 최대값입니다. 최대 타임아웃 시간이 될 때까지 기다릴 필요는 없습니다. 대부분의 명령은 설정된 최대 타임아웃 간격 내에 완료됩니다.

SAN Provider 설정 수정에 대한 자세한 내용은 "[스토리지 설정 변경](#)"를 참조하십시오.

ONTAP tools를 사용하여 VMware Live Site Recovery 어플라이언스에서 SRA를 구성합니다

VMware Live Site Recovery 어플라이언스를 배포한 후 재해 복구 관리를 활성화하도록 스토리지 복제 어댑터(SRA)를 구성하십시오.

VMware Live Site Recovery 어플라이언스에서 SRA를 구성하면 VMware vSphere용 ONTAP tools 자격 증명이 어플라이언스 내에 저장되어 VMware Live Site Recovery와 SRA 간의 통신이 가능해집니다.

시작하기 전에

- `.tar.gz` 파일을 "[NetApp 지원 사이트](#)"에서 다운로드합니다.
- ONTAP tools Manager에서 SRA 서비스를 활성화하십시오. 자세한 내용은 "[서비스 활성화](#)" 섹션을 참조하십시오.
- vCenter 서버를 ONTAP tools for VMware vSphere 어플라이언스에 추가합니다. 자세한 내용은 "[vCenter 서버 추가](#)" 섹션을 참조하십시오.
- ONTAP tools for VMware vSphere에 스토리지 백엔드를 추가합니다. 자세한 내용은 "[스토리지 백엔드 추가](#)" 섹션을 참조하십시오.



ONTAP tools에서 vCenter 인증서 패치를 적용한 경우, (:5480) 포트를 사용하여 VMware Live Site Recovery 어플라이언스에서 vCenter 구성을 업데이트하십시오. 자세한 내용은 "[Site Recovery Manager 어플라이언스 재구성](#)"을 참조하십시오.

단계

1. VMware Live Site Recovery 어플라이언스 화면에서 스토리지 복제 어댑터 > *새 어댑터*를 선택합니다.
2. `.tar.gz` 파일을 VMware Live Site Recovery에 업로드하십시오.
3. PuTTY와 같은 SSH 클라이언트를 사용하여 관리자 계정으로 VMware Live Site Recovery 어플라이언스에 로그인합니다.
4. 다음 명령을 사용하여 루트 사용자로 전환합니다: `su root`
5. 명령을 실행하여 `cd /var/log/vmware/srm` 로그 디렉토리로 이동합니다.
6. 로그 위치에서 SRA에서 사용하는 Docker ID를 얻으려면 다음 명령을 입력하십시오. `docker ps -l`
7. 컨테이너 ID에 로그인하려면 다음 명령을 입력합니다. `docker exec -it -u srm <container id> sh`
8. 다음 명령을 사용하여 VMware Live Site Recovery를 ONTAP tools for VMware vSphere IP 주소 및 암호로 구성하십시오: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`

- 암호를 입력할 때 작은따옴표로 묶어야 Perl 스크립트가 특수 문자를 구분 기호가 아닌 암호의 일부로 처리합니다.
- 처음 서비스를 활성화할 때 ONTAP tools Manager에서 애플리케이션(VASA Provider/SRA) 사용자 이름과 암호를 설정할 수 있습니다. 이 자격 증명을 사용하여 SRA를 VMware Live Site Recovery에 등록하십시오.
- vCenter GUID를 찾으려면 vCenter 인스턴스를 추가한 후 ONTAP tools Manager의 vCenter 서버 페이지로 이동하십시오. "[vCenter 서버 추가](#)" 섹션을 참조하십시오.

9. 업데이트된 세부 정보가 VMware Live Site Recovery 스토리지 복제 어댑터 페이지에 표시되는지 확인하려면 어댑터를 다시 스캔하십시오.

결과 스토리지 자격 증명에 저장되었음을 나타내는 확인 메시지가 나타납니다. 이제 지정된 IP 주소, 포트 및 자격 증명을 사용하여 SRA로 SRA 서버와 통신할 수 있습니다.

ONTAP tools에서 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

해당 항목에 언급된 단계를 실행했어야 합니다 "[VMware Live Site Recovery 어플라이언스에서 SRA 구성](#)".

단계

1. VMware Live Site Recovery 시스템에서 캐시된 ONTAP tools 자격 증명을 삭제하려면 다음 명령을 실행하십시오.
 - a. `sudo su <enter root password>`
 - b. `docker ps`
 - c. `docker exec -it <container_id> sh`
 - d. `cd conf/`
 - e. `rm -rf *`
2. 새 자격 증명으로 SRA를 구성하려면 Perl 명령을 실행하십시오.
 - a. `cd ..`
 - b. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>` 비밀번호 값 주위에 작은따옴표(')를 붙여야 합니다.

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

인증서 변경 후 VMware Live Site Recovery 어플라이언스에서 vCenter 재구성

vCenter 인증서가 변경되는 경우(예: vCenter 업그레이드 후) Site Recovery 확장 프로그램에서 지문 불일치 오류가 발생할 수 있습니다. 다음 단계를 수행하여 이 문제를 해결하십시오.

단계

1. VMware Live Site Recovery 어플라이언스에서 vCenter 재구성

- a. 브라우저에서 VMware Live Site Recovery 어플라이언스 관리 인터페이스를 엽니다.
https://<SRM_IP>:5480
- b. * 요약 * 탭을 선택합니다.
- c. vCenter Server 연결에 대해 *재구성*을 선택하십시오.

이 작업은 vCenter에서 최신 인증서 지문을 가져와 수락합니다.

2. 사이트 페어링 재연결(오류가 지속되는 경우)

재구성 후에도 지문 불일치 오류가 계속 발생하는 경우:

- a. vCenter 사용자 인터페이스에 로그인합니다.
- b. **Site Recovery** 확장 프로그램으로 이동합니다.
- c. **Site Pairing** 섹션을 찾으십시오.
- d. 업데이트된 인증서를 사용하여 사이트 페어링을 다시 설정하려면 *다시 연결*을 선택하십시오.

ONTAP tools에서 보호 사이트 및 복구 사이트를 구성합니다

보호 대상 사이트에서 가상 머신 그룹을 보호하려면 보호 그룹을 생성해야 합니다.

새 데이터스토어를 추가할 때 기존 데이터스토어 그룹에 포함시키거나, 새 데이터스토어를 추가하고 보호를 위해 새 볼륨 또는 일관성 그룹을 생성할 수 있습니다. 보호된 일관성 그룹 또는 볼륨에 새 데이터스토어를 추가한 후에 SnapMirror를 업데이트하고 보호 사이트와 복구 사이트 모두에서 스토리지 검색을 수행해야 합니다. 새 데이터스토어가 감지되고 보호되도록 검색을 수동으로 또는 예약된 시간에 실행할 수 있습니다.

보호된 사이트와 복구 사이트 페어링

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



스토리지 복제 어댑터(SRA)는 일관성 그룹에서 Automated Failover Duplex 유형의 동기 관계 하나와 비동기 SnapMirror 관계를 사용하여 팬아웃을 지원합니다. 그러나 일관성 그룹에서 두 개의 비동기 SnapMirror 관계를 사용하거나 볼륨에서 SnapMirror 관계를 사용하여 팬아웃하는 것은 지원되지 않습니다. Vault 유형의 SnapMirror 관계는 이러한 팬아웃 제한에 포함되지 않습니다. SRA의 일관성 그룹 지원은 Unified 및 ASA r2 스토리지 시스템의 SAN 프로토콜(iSCSI 및 파이버 채널)로 제한됩니다. NFS의 경우 일관성 그룹이 지원되지 않습니다. NFS 데이터스토어 볼륨이 일관성 그룹에 속한 경우 장치 검색 작업이 실패합니다.

시작하기 전에

- 보호 대상 사이트와 복구 사이트 모두에 VMware Live Site Recovery가 설치되어 있어야 합니다.
- 보호 사이트와 복구 사이트 모두에 SRA가 설치되어 있어야 합니다.

단계

1. vSphere Client 홈 페이지에서 사이트 복구 아이콘을 두 번 클릭한 다음 *사이트*를 선택합니다.
2. 개체 > 작업 > *사이트 페어링*을 선택합니다.
3. **Pair Site Recovery Manager Servers** 대화 상자에서 보호 대상 사이트의 Platform Services Controller 주소를 입력한 다음 *다음*을 선택합니다.

4. Select vCenter Server 섹션에서 다음 작업을 수행합니다.
 - a. 보호 대상 사이트의 vCenter Server가 페어링 대상 후보로 표시되는지 확인하십시오.
 - b. SSO 관리자 자격 증명을 입력한 다음 *완료*를 선택하십시오.
5. 보안 인증서를 수락하라는 메시지가 표시되면 *예*를 선택하십시오.

결과

개체 대화 상자에는 보호된 사이트와 복구 사이트가 모두 표시됩니다.

보호 그룹 구성

시작하기 전에

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

- 동일한 버전의 VMware Live Site Recovery가 설치되어 있습니다.
- 가상 머신
- 쌍을 이루는 보호 사이트 및 복구 사이트
- 원본 및 대상 데이터 저장소는 각각의 사이트에 마운트되어야 합니다.

단계

1. vCenter Server에 로그인하고 사이트 복구 > *보호 그룹*을 선택합니다.
2. 보호 그룹 창에서 *새로 만들기*를 선택합니다.
3. 보호 그룹의 이름과 설명을 지정하고 방향을 선택한 다음 *다음*을 선택하십시오.
4. **Type** 필드에서 NFS 및 VMFS 데이터 저장소에 대해 *Type field option...*을 데이터 저장소 그룹(어레이 기반 복제)으로 선택합니다. 장애 도메인은 복제가 활성화된 SVM으로 구성됩니다. 피어링만 구현되어 있고 문제가 없는 SVM이 표시됩니다.
5. 복제 그룹 탭에서 활성화된 어레이 쌍 또는 구성한 가상 머신이 포함된 복제 그룹을 선택한 다음 *다음*을 선택합니다.

복제 그룹에 있는 모든 가상 머신이 보호 그룹에 추가됩니다.

6. 기존 복구 계획을 선택하거나 *새 복구 계획에 추가*를 선택하여 새 복구 계획을 생성할 수 있습니다.
7. Ready to complete 탭에서 생성한 보호 그룹의 세부 정보를 검토한 다음 *Finish*를 선택합니다.

보호 사이트 및 복구 사이트 리소스 구성

ONTAP tools에서 네트워크 매핑을 구성합니다

보호 사이트의 각 리소스를 복구 사이트의 적절한 리소스에 매핑할 수 있도록 양쪽 사이트에서 VM 네트워크, ESXi 호스트 및 폴더와 같은 리소스 매핑을 구성해야 합니다.

다음 리소스 구성을 완료해야 합니다.

- 네트워크 매핑
- 폴더 매핑

- 리소스 매핑
- 자리 표시자 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 선택합니다.
3. 관리 탭에서 네트워크 매핑 > *새로 만들기*를 선택하여 새 네트워크 매핑을 생성합니다.
4. 네트워크 매핑 생성 마법사에서 다음을 수행하십시오.
 - a. *일치하는 이름을 가진 네트워크에 대한 매핑을 자동으로 준비*를 선택하고 *다음*을 선택합니다.
 - b. 보호 사이트와 복구 사이트에 필요한 데이터 센터 개체를 선택하고 *매핑 추가*를 선택합니다.
 - c. 매핑이 성공적으로 생성되면 *다음*을 선택합니다.
 - d. 이전에 역매핑을 생성하는 데 사용했던 개체를 선택한 다음 *완료*를 선택합니다.

결과

네트워크 매핑 페이지에는 보호된 사이트 리소스와 복구 사이트 리소스가 표시됩니다. 환경 내 다른 네트워크에 대해서도 동일한 단계를 따르면 됩니다.

ONTAP tools에서 폴더 매핑을 구성합니다

보호 사이트와 복구 사이트 간의 통신을 가능하게 하려면 두 사이트의 폴더를 매핑해야 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 선택합니다.
3. 새 폴더 매핑을 만들려면 관리 탭에서 폴더 매핑 > 폴더 아이콘을 선택합니다.
4. 폴더 매핑 생성 마법사에서 다음 단계를 수행하십시오.
 - a. *이름이 일치하는 폴더에 대한 매핑을 자동으로 준비*를 선택하고 *다음*을 선택합니다.
 - b. 보호 사이트와 복구 사이트에 필요한 데이터 센터 개체를 선택하고 *매핑 추가*를 선택합니다.
 - c. 매핑이 성공적으로 생성되면 *다음*을 선택합니다.
 - d. 이전에 역매핑을 생성하는 데 사용했던 개체를 선택한 다음 *완료*를 선택합니다.

결과

폴더 매핑 페이지에는 보호된 사이트 리소스와 복구 사이트 리소스가 표시됩니다. 환경 내 다른 폴더에 대해서도 동일한 단계를 따르면 됩니다.

ONTAP tools에서 리소스 매핑을 구성합니다

보호 사이트와 복구 사이트의 리소스를 매핑하여 가상 머신이 두 호스트 그룹 중 하나로 장애 조치되도록 구성해야 합니다.

시작하기 전에

보호 사이트와 복구 사이트를 연결했어야 합니다.



VMware Live Site Recovery에서 리소스는 리소스 풀, ESXi 호스트 또는 vSphere 클러스터일 수 있습니다.

단계

1. vCenter Server에 로그인하고 사이트 복구 > *사이트*를 선택합니다.
2. 보호된 사이트를 선택하고 *관리*를 선택합니다.
3. 관리 탭에서 리소스 매핑 > *새로 만들기*를 선택하여 새 리소스 매핑을 생성합니다.
4. 리소스 매핑 생성 마법사에서 다음 단계를 수행하십시오.
 - a. *일치하는 이름을 가진 리소스에 대한 매핑을 자동으로 준비*를 선택하고 *다음*을 선택합니다.
 - b. 보호 사이트와 복구 사이트에 필요한 데이터 센터 개체를 선택하고 *매핑 추가*를 선택합니다.
 - c. 매핑이 성공적으로 생성되면 *다음*을 선택합니다.
 - d. 이전에 역매핑을 생성하는 데 사용했던 개체를 선택한 다음 *완료*를 선택합니다.

결과

리소스 매핑 페이지에는 보호된 사이트 리소스와 복구 사이트 리소스가 표시됩니다. 환경 내 다른 리소스에 대해서도 동일한 단계를 따르면 됩니다.

ONTAP tools에서 플레이스홀더 데이터 저장소를 구성합니다

보호 대상 가상 머신(VM)을 위해 복구 사이트의 vCenter 인벤토리에 공간을 예약하려면 자리 표시자 데이터 저장소를 구성하십시오. 자리 표시자 VM은 크기가 작고 일반적으로 수백 킬로바이트만 사용하므로 자리 표시자 데이터 저장소에는 최소한의 용량만 필요합니다.

시작하기 전에

- 보호 사이트와 복구 사이트가 연결되어 있는지 확인하십시오.
- 리소스 매핑이 구성되었는지 확인하십시오.

단계

1. vCenter Server에 로그인하고 사이트 복구 > *사이트*를 선택합니다.
2. 보호된 사이트를 선택하고 *관리*를 선택합니다.
3. 관리 탭에서 **Placeholder Datastores** > *New*를 선택하여 새 플레이스홀더 데이터 저장소를 생성합니다.
4. 적절한 데이터 저장소를 선택하고 *확인*을 선택하십시오.



플레이스홀더 데이터스토어는 로컬 또는 원격 스토리지에 있을 수 있지만 복제는 필요하지 않습니다.

5. 3단계부터 5단계까지를 반복하여 복구 사이트에 대한 자리 표시자 데이터 저장소를 구성합니다.

ONTAP 도구의 어레이 관리자를 사용하여 **SRA**를 구성합니다

VMware Live Site Recovery와 스토리지 가상 머신(SVM) 간의 상호 작용을 활성화하려면 VMware Live Site Recovery의 어레이 관리자 마법사를 사용하여 SRA(Storage Replication Adapter)를 구성할 수 있습니다.

시작하기 전에

- VMware Live Site Recovery에서 보호 사이트와 복구 사이트를 페어링했어야 합니다.
- 어레이 관리자를 구성하기 전에 온보딩된 스토리지를 먼저 구성해야 합니다.
- 보호 대상 사이트와 복구 사이트 간의 SnapMirror 관계를 구성하고 복제했어야 합니다.
- 멀티테넌시를 활성화하려면 SVM 관리 LIF를 활성화해야 합니다.

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

단계

1. VMware Live Site Recovery에서 **Array Managers** > *Add Array Manager*를 선택합니다.
2. VMware Live Site Recovery에서 어레이를 설명하려면 다음 정보를 입력하십시오.

- a. 표시 이름 필드에 어레이 관리자를 식별할 이름을 입력하십시오.
- b. **SRA** 유형 필드에서 *NetApp Storage Replication Adapter for ONTAP*를 선택합니다.
- c. 클러스터 또는 SVM에 연결하기 위한 정보를 입력하십시오.
 - 클러스터에 연결하는 경우 클러스터 관리 LIF를 입력해야 합니다.
 - SVM에 직접 연결하는 경우 SVM 관리 LIF의 IP 주소를 입력해야 합니다.



어레이 관리자를 구성할 때는 ONTAP tools for VMware vSphere에서 스토리지 시스템을 온보딩하는 데 사용된 것과 동일한 연결(IP 주소)을 스토리지 시스템에 사용해야 합니다. 예를 들어, 어레이 관리자 구성이 SVM 범위로 설정된 경우 ONTAP tools for VMware vSphere의 스토리지는 SVM 레벨에서 추가해야 합니다.

- d. 클러스터에 연결하는 경우 **SVM** 이름 필드에 SVM 이름을 지정하거나, 클러스터의 모든 SVM을 관리하려면 비워 두십시오.
- e. 검색할 볼륨을 포함할 볼륨 목록 필드에 입력하십시오.

보호 사이트에 소스 볼륨을 입력하고 복구 사이트에 복제 대상 볼륨을 입력할 수 있습니다.

예를 들어 볼륨 dst_vol1과 SnapMirror 관계로 연결된 볼륨 src_vol1을 검색하려면 보호 사이트 필드에 src_vol1을, 복구 사이트 필드에 dst_vol1을 지정해야 합니다.

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

보호 사이트에 소스 볼륨을 입력하고 복구 사이트에 복제 대상 볼륨을 입력할 수 있습니다.

예를 들어, 볼륨 `_dst_vol1_`과 SnapMirror 관계로 연결된 볼륨 `_src_vol1_`을 제외하려면 보호 사이트 필드에 `_src_vol1_`을, 복구 사이트 필드에 `_dst_vol1_`을 지정해야 합니다.

3. *다음*을 선택하십시오.
4. 어레이가 검색되어 어레이 관리자 추가 창 하단에 표시되는지 확인하고 *마침*을 선택합니다.

적절한 SVM 관리 IP 주소와 자격 증명을 사용하여 복구 사이트에 대해서도 동일한 단계를 수행할 수 있습니다. 어레이 관리자 추가 마법사의 어레이 쌍 활성화 화면에서 올바른 어레이 쌍이 선택되었는지, 그리고 활성화 준비가 완료되었는지 확인해야 합니다.

ONTAP tools에서 복제된 스토리지 시스템을 검증합니다

스토리지 복제 어댑터(SRA)를 구성한 후 보호 사이트와 복구 사이트가 성공적으로 페어링되었는지 확인해야 합니다. 복제된 스토리지 시스템은 보호 사이트와 복구 사이트 모두에서 검색 가능해야 합니다.

시작하기 전에

- 스토리지 시스템을 구성해야 합니다.
- VMware Live Site Recovery 어레이 관리자를 사용하여 보호 사이트와 복구 사이트를 페어링했어야 합니다.
- FlexClone 라이선스와 SnapMirror 라이선스는 SRA에 대한 테스트 페일오버 작업 및 페일오버 작업을 수행하기 전에 활성화해야 합니다.
- 원본 사이트와 대상 사이트에 동일한 SnapMirror 정책 및 일정이 설정되어 있어야 합니다.
- 사용자 지정 일정을 사용하는 사용자 지정 SnapMirror 정책을 사용하는 경우 보호 사이트와 복구 사이트 모두에 동일한 일정과 정책을 구성해야 합니다.
- 사용자 지정 SnapMirror 정책(기본 일정 또는 사용자 지정 일정)을 사용하는 경우 새 정책이 인식되도록 ONTAP tools에서 스토리지 검색을 수행해야 합니다. 그렇지 않으면 테스트 페일오버 및 페일오버를 포함한 SRA 워크플로가 실패합니다. 다음 시점에서 스토리지 검색을 수행하십시오.
 - 복구 사이트에서 사용자 지정 정책을 생성한 후
 - 재보호 작업 후에는 보호 대상 사이트에 정책이 다시 생성됩니다.

단계

1. vCenter 서버에 로그인하십시오.
2. **Site Recovery > Array Based Replication** 으로 이동합니다.
3. 필요한 어레이 쌍을 선택하고 해당 세부 정보를 확인하십시오.

스토리지 시스템은 보호 사이트와 복구 사이트에서 **Enabled** 상태로 검색되어야 합니다.

ONTAP 도구의 팬아웃 보호

팬아웃 보호 시나리오에서 일관성 그룹은 첫 번째 대상 ONTAP 클러스터에서는 동기 관계를, 두 번째 대상 ONTAP 클러스터에서는 비동기 관계를 통해 이중으로 보호됩니다. SnapMirror 활성화 동기화 보호 워크플로(생성, 편집, 삭제)는 동기 보호를 유지합니다. VMware Live Site Recovery 어플라이언스 장애 조치 및 재보호 워크플로는 비동기 보호를 유지합니다.



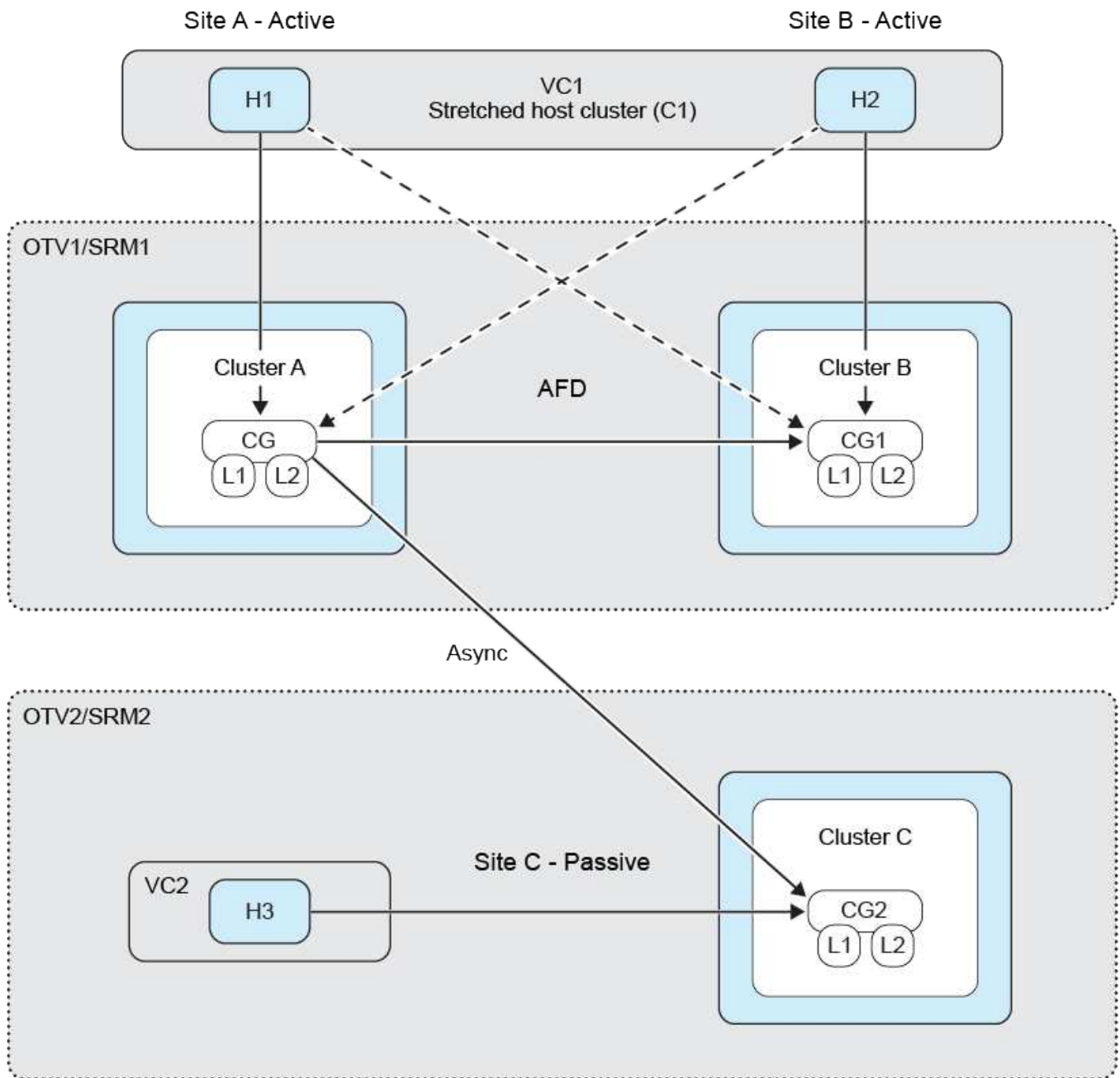
SVM 사용자에게 대해서는 팬아웃이 지원되지 않습니다.

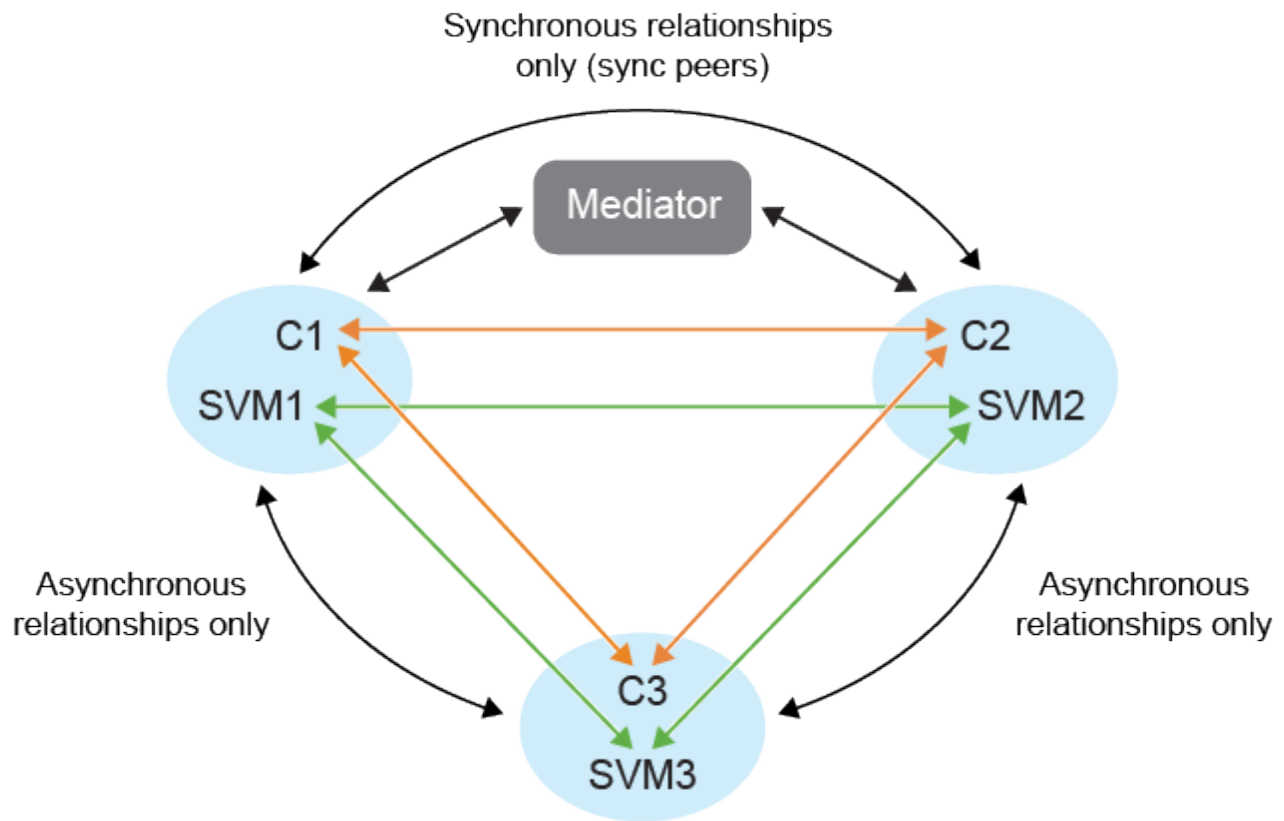
팬아웃 보호를 설정하려면 세 사이트 클러스터와 SVM을 피어링해야 합니다.

예:

만약에	그 다음에
- 소스 일관성 그룹은 클러스터 c1 및 SVM svm1에 있습니다. - 첫 번째 대상 일관성 그룹은 클러스터 c2와 SVM svm2에 있습니다. - 두 번째 대상 일관성 그룹은 클러스터 c3 및 SVM svm3에 있습니다.	- 소스 ONTAP 클러스터의 클러스터 피어링은 (C1, C2) 및 (C1, C3)이 됩니다. - 첫 번째 대상 ONTAP 클러스터에서의 클러스터 피어링은 (C2, C1) 및 (C2, C3)이 될 것이며 - 두 번째 대상 ONTAP 클러스터의 클러스터 피어링은 (C3, C1) 및 (C3, C2)가 됩니다. - 소스 SVM에 대한 SVM 피어링은 (svm1, svm2) 및 (svm1, svm3)이 됩니다. - 첫 번째 목적지 SVM에 대한 SVM 피어링은 (svm2, svm1) 및 (svm2, svm3)이 되고 - 두 번째 대상 SVM에 대한 SVM 피어링은 (svm3, svm1) 및 (svm3, svm2)가 됩니다.

다음 다이어그램은 팬아웃 보호 구성을 보여 줍니다.





단계

1. 새로운 임시 데이터 저장소를 선택하십시오. 단계별 보호를 위한 임시 데이터 저장소 선택 기준은 다음과 같습니다.
 - 보호 대상 호스트 클러스터에 자리 표시자 데이터 저장소를 배치하지 마십시오.
 - 호스트 클러스터에 자리 표시자 데이터 저장소를 포함해야 하는 경우 SnapMirror 활성 동기화 보호를 설정하기 전에 VMware Live Site Recovery 어플라이언스에 추가하십시오. 이렇게 설정하면 자리 표시자 데이터 저장소를 보호 대상에서 제외할 수 있습니다.

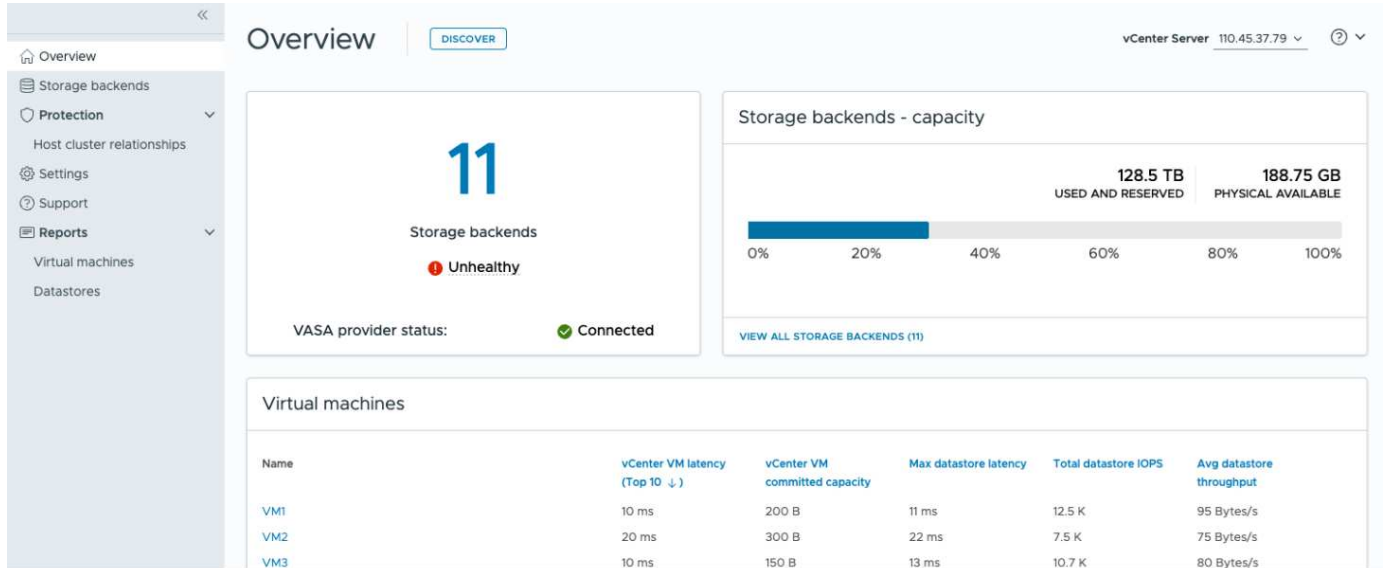
자세한 내용은 "[자리 표시자 데이터 저장소 선택](#)"을(를) 참조하십시오.
2. "[보호된 호스트 클러스터 수정](#)"에 따라 호스트 클러스터 보호에 데이터 저장소를 추가하십시오. 비동기 및 동기 정책 유형을 모두 추가하십시오.

ONTAP tools for VMware vSphere 관리

ONTAP 도구 대시보드에 대해 알아보십시오

vCenter 클라이언트의 바로 가기 섹션에서 ONTAP tools for VMware vSphere 플러그인 아이콘을 선택하면 개요 페이지가 열립니다. 이 대시보드는 ONTAP tools for VMware vSphere 플러그인의 요약 정보를 제공합니다.

향상된 링크 모드(ELM)에서는 vCenter Server 드롭다운 메뉴가 나타납니다. vCenter Server를 선택하여 해당 데이터를 볼 수 있습니다. 이 드롭다운 메뉴는 플러그인의 모든 목록 보기에서 사용할 수 있습니다. 한 페이지에서 vCenter Server를 선택하면 플러그인의 다른 탭으로 이동해도 선택한 vCenter Server가 유지됩니다.



개요 페이지에서 검색 작업을 실행할 수 있습니다. 검색 작업은 vCenter 수준에서 새로 추가되거나 업데이트된 스토리지 백엔드, 호스트, 데이터스토어 및 보호 상태 또는 관계를 감지합니다. 예약된 검색을 기다리지 않고 필요에 따라 검색을 실행할 수 있습니다.



검색 버튼은 검색을 수행하는 데 필요한 Privileges가 있는 경우에만 활성화됩니다.

검색 요청이 제출되면 최근 작업 패널에서 작업 진행 상황을 확인할 수 있습니다.

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

카드	설명
상태	상태 카드에는 스토리지 백엔드 수와 스토리지 백엔드 및 VASA Provider의 전반적인 상태가 표시됩니다. 스토리지 백엔드 상태는 모든 스토리지 백엔드 상태가 정상일 경우 정상*으로 표시되고, 스토리지 백엔드 중 하나라도 문제가 발생하면(알 수 없음/접근 불가/성능 저하 상태) *비정상*으로 표시됩니다. 툴팁을 선택하면 스토리지 백엔드의 상태 세부 정보가 열립니다. 자세한 내용을 보려면 스토리지 백엔드를 선택하십시오. *기타 VASA Provider 상태 링크는 vCenter Server에 등록된 VASA Provider의 현재 상태를 표시합니다.

스토리지 백엔드 - 용량	이 카드는 선택한 vCenter Server 인스턴스의 모든 스토리지 백엔드에 대한 총 사용량 및 가용 용량을 보여줍니다. ASA r2 스토리지 시스템의 경우 스토리지가 분산되어 있으므로 용량 데이터가 표시되지 않습니다.
가상 머신	이 카드에는 성능 지표별로 정렬된 상위 10개 VM이 표시됩니다. 헤더를 선택하면 선택한 지표에 대해 오름차순 또는 내림차순으로 정렬된 상위 10개 VM을 볼 수 있습니다. 카드에서 변경한 정렬 및 필터링 내용은 브라우저 캐시를 삭제하거나 설정을 변경할 때까지 유지됩니다.
데이터 저장소	이 카드에는 성능 지표별로 정렬된 상위 10개 데이터 저장소가 표시됩니다. 헤더를 선택하면 선택한 지표에 대해 오름차순 또는 내림차순으로 정렬된 상위 10개 데이터 저장소를 볼 수 있습니다. 카드에서 변경한 정렬 및 필터링 내용은 브라우저 캐시를 삭제하거나 변경할 때까지 유지됩니다. 데이터 저장소 유형 드롭다운 메뉴에서 NFS, VMFS 또는 vVols 등 데이터 저장소 유형을 선택할 수 있습니다.
ESXi 호스트 규정 준수 카드	이 카드는 모든 ESXi 호스트(선택한 vCenter의 경우)가 그룹 또는 범주별로 권장되는 NetApp 호스트 설정을 따르는지 여부를 보여줍니다. 권장 설정 적용 링크를 선택하여 권장 설정을 적용할 수 있습니다. 호스트의 준수 상태를 선택하면 호스트 목록을 볼 수 있습니다.

ONTAP tools가 igroup 및 익스포트 정책을 관리하는 방법

이니시에이터 그룹(igroups)은 FC 프로토콜 호스트의 WWPN(World Wide Port Name) 또는 iSCSI 호스트의 정규화된 노드 이름으로 구성된 테이블입니다. igroups를 정의하고 LUN에 매핑하여 어떤 이니시에이터가 LUN에 액세스할 수 있는지 제어할 수 있습니다.

ONTAP tools for VMware vSphere 9.x에서는 iGroup이 평면 구조로 생성 및 관리되었으며, vCenter의 각 데이터스토어는 단일 iGroup과 연결되었습니다. 이 모델은 유연성을 제한하고 여러 데이터스토어에서 iGroup을 재사용하는 데 제약을 주었습니다. ONTAP tools for VMware vSphere는 중첩 iGroup을 도입하여 vCenter의 각 데이터스토어가 상위 iGroup과 연결되고, 각 호스트는 해당 상위 iGroup 아래의 하위 iGroup에 연결됩니다. 사용자 정의 이름을 사용하여 사용자 지정 상위 iGroup을 정의하고 여러 데이터스토어에서 재사용하여 iGroup 관리를 간소화할 수 있습니다. ONTAP tools for VMware vSphere에서 LUN 및 데이터스토어를 관리하려면 iGroup 워크플로를 이해하십시오. 다음 예와 같이 다양한 워크플로는 서로 다른 iGroup 구성을 생성합니다.



언급된 이름은 예시를 위한 것이며 실제 igroup 이름은 아닙니다. ONTAP tools로 관리되는 igroup은 "otv_" 접두사를 사용합니다. 사용자 지정 igroup에는 원하는 이름을 지정할 수 있습니다.

용어	설명
DS<number>	데이터 저장소
iqn<number>	개시자 IQN
호스트<number>	호스트 MoRef
lun<number>	LUN ID

<DSName>igroup<number>	기본(ONTAP tools 관리) 상위 igroup
<Host-Moref>igroup<number>	차일드 igroup
Customigroup<number>	사용자 정의 사용자 지정 상위 igroup
Classicigroup<number>	ONTAP tools 9.x 버전에서 사용되는 igroup입니다.

예시 1:

단일 호스트에 하나의 이니시에이터를 사용하여 데이터 저장소 생성

워크플로우: [생성] DS1(lun1): host1(iqn1)

결과:

- DS1igroup:
 - host1igroup → (iqn1: lun1)

ONTAP DS1에 대한 상위 igroup DS1igroup을 생성하고 하위 igroup host1igroup을 lun1에 매핑합니다. 시스템은 항상 LUN을 하위 igroup에 매핑합니다.

예시 2:

기존 데이터 저장소를 추가 호스트에 마운트

워크플로우: [마운트] DS1 (lun1): host2 (iqn2)

결과:

- DS1igroup:
 - host1igroup → (iqn1: lun1)
 - host2igroup → (iqn2: lun1)

ONTAP tools for VMware vSphere는 하위 igroup인 host2igroup을 생성하고 이를 기존 상위 igroup인 DS1igroup에 추가합니다.

예시 3:

호스트에서 데이터 저장소 마운트 해제

워크플로: [마운트 해제] DS1 (lun1): host1 (iqn1)

결과:

- DS1igroup:
 - host2igroup → (iqn2: lun1)

ONTAP tools for VMware vSphere는 계층 구조에서 host1igroup을 제거합니다. 시스템은 하위 igroup을 명시적으로 삭제하지 않습니다. 다음 두 가지 조건에서 삭제합니다.

- 매핑된 LUN이 없으면 ONTAP 시스템은 하위 igroup을 삭제합니다.
- 예약된 정리 작업은 LUN 매핑이 없는 사용되지 않는 하위 igroup을 제거합니다. 이러한 시나리오는 ONTAP 도구로 관리되는 igroup에만 적용되며, 사용자 지정으로 생성된 igroup에는 적용되지 않습니다.

예시 4:

데이터 저장소 삭제

워크플로우: [삭제] DS1 (lun1): host2 (iqn2)

결과:

- DS1lgroup:
 - host2lgroup → (iqn2: lun1)

다른 데이터 저장소에서 부모 iGroup을 재사용하지 않는 한 부모 및 자식 iGroup은 삭제됩니다. 자식 iGroup은 명시적으로 삭제되지 않습니다.

예시 5:

사용자 정의 상위 igroup 아래에 여러 데이터 저장소 생성

워크플로우:

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

결과:

- Customlgroup1:
 - host1lgroup → (iqn1: lun2, lun3)
 - host2lgroup → (iqn2: lun2)
 - host3lgroup → (iqn3: lun3)

Customlgroup1은 DS2용으로 생성되고 DS3에서 재사용됩니다. 하위 igroup은 공유 상위 igroup 아래에서 생성되거나 업데이트되며, 각 하위 igroup은 관련 LUN에 매핑됩니다.

예시 6:

사용자 지정 상위 igroup 아래에 있는 데이터 저장소 하나를 삭제합니다.

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

결과:

- Customlgroup1:
 - host1lgroup → (iqn1: lun3)
 - host3lgroup → (iqn3: lun3)
- Customlgroup1은 재사용되지 않더라도 삭제되지 않습니다.
- 매핑된 LUN이 없으면 ONTAP 시스템은 host2lgroup을 삭제합니다.
- host1lgroup은 DS3의 lun3에 매핑되어 있으므로 삭제되지 않습니다. 사용자 지정 igroup은 재사용 여부와 관계없이 절대 삭제되지 않습니다.

예시 7:

vVols 데이터스토어 확장(볼륨 추가)

워크플로우:

확장 전:

[확장] DS4(lun4): host4(iqn4)

- DS4lgroup: host4lgroup → (iqn4: lun4)

확장 후:

[확장] DS4(lun4, lun5): 호스트4(iqn4)

- DS4lgroup: host4lgroup → (iqn4: lun4, lun5)

새로운 LUN이 생성되어 기존 하위 igroup인 host4lgroup에 매핑됩니다.

예시 8:

vVols 데이터스토어 축소(볼륨 제거)

워크플로우:

수축 전:

[Shrink] DS4(lun4, lun5): host4(iqn4)

- DS4lgroup: host4lgroup → (iqn4: lun4, lun5)

축소 후:

[Shrink] DS4(lun4): host4(iqn4)

- DS4lgroup: host4lgroup → (iqn4: lun4)

지정된 LUN(lun5)이 하위 igroup에서 매핑 해제되었습니다. igroup은 하나 이상의 매핑된 LUN이 있는 한 활성 상태를 유지합니다.

예시 9:

ONTAP tools 9에서 10으로의 마이그레이션(igroup 정규화)

워크플로우

ONTAP tools for VMware vSphere 9.x 버전은 계층적 igroup을 지원하지 않습니다. 10.3 이상 버전으로 마이그레이션하는 동안 igroup을 계층적 구조로 정규화해야 합니다.

마이그레이션 전:

[마이그레이션] DS6(lun6, lun7): 호스트6(iqn6), 호스트7(iqn7) → Classiclgroup1(iqn6 및 iqn7 : lun6, lun7)

ONTAP tools 9.x의 로직은 일대일 호스트 매핑을 강제하지 않고도 igroup당 여러 이니시에이터를 허용합니다.

마이그레이션 후:

[마이그레이션] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → Classiclgroup1: otv_Classiclgroup1 (iqn6 & iqn7 : lun6, lun7)

마이그레이션 중:

- 새로운 상위 igroup(Classiclgroup1)이 생성됩니다.
- 원래 igroup은 otv_ 접두사가 붙어 이름이 변경되고 하위 igroup이 됩니다.

이는 계층적 모델의 준수를 보장합니다.

ONTAP tools 10.5P2부터 마이그레이션된 igroup은 더 이상 사용되지 않으면 삭제됩니다. 이전 버전에서는 마이그레이션된 igroup이 제거되지 않았습니다. 다음 사항에 유의하십시오.

- 마이그레이션된 igroup은 데이터 저장소 간에 재사용할 수 없습니다.
- 사용자 정의 igroup은 삭제되지 않으며 계속 재사용할 수 있습니다.

관련 주제

["igroups 소개"](#)

엑스포트 정책

내보내기 정책은 ONTAP tools for VMware vSphere에서 NFS 데이터 저장소 액세스 및 클라이언트 권한을 제어합니다. 내보내기 정책은 ONTAP 시스템에서 생성 및 관리되며 NFS 데이터 저장소와 함께 사용하여 액세스 제어를 적용할 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 vSphere에서 NFS 데이터스토어를 생성할 때 기존 내보내기 정책을 선택하거나 새 정책을 생성할 수 있습니다. 그러면 내보내기 정책이 데이터스토어에 적용되어 권한이 있는 클라이언트만 액세스할 수 있게 됩니다.

새로운 ESXi 호스트에 NFS 데이터스토어를 마운트하면 ONTAP tools for VMware vSphere는 해당 데이터스토어와 연결된 기존 내보내기 정책에 호스트의 IP 주소를 추가합니다. 이렇게 하면 새 호스트에서 새 내보내기 정책을 생성하지 않고도 데이터스토어에 액세스할 수 있습니다.

ESXi 호스트에서 NFS 데이터스토어를 삭제하거나 마운트 해제하면 ONTAP tools for VMware vSphere는 내보내기 정책에서 해당 호스트의 IP 주소를 제거합니다. 다른 호스트에서 해당 내보내기 정책을 사용하지 않는 경우 정책이 삭제됩니다. NFS 데이터스토어를 삭제하면 ONTAP tools for VMware vSphere는 해당 데이터스토어와 연결된 내보내기 정책을 다른 데이터스토어에서 재사용하지 않는 경우 제거합니다. 내보내기 정책이 재사용되는 경우 호스트 IP 주소를 유지하며 변경되지 않습니다. 데이터스토어를 삭제하면 내보내기 정책에서 호스트 IP 주소 할당이 해제되고 기본 내보내기 정책이 할당되어 ONTAP 시스템에서 필요한 경우 해당 데이터스토어에 액세스할 수 있습니다.

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

관련 주제

["엑스포트 정책을 생성합니다"](#)

ONTAP tools에서 igroup을 관리하는 방법

ONTAP 도구 VM과 ONTAP 스토리지 시스템을 모두 관리하는 경우, 특히 ONTAP 도구로 관리되지 않는 환경에서 관리되는 환경으로 데이터스토어를 이동할 때 igroup의 동작 방식을 이해하는 것이 중요합니다. 이 페이지에서는 ONTAP tools for VMware vSphere가 igroup을 표현하고 관리하는 방식을 설명합니다. 이는 이전 릴리스와 현재의 중첩 igroup 모델 간의 동작 차이를 이해하기 위한 개념적인 정보입니다.

ONTAP tools for VMware vSphere 10.4부터 ONTAP tools는 ONTAP 및 vCenter 객체를 자동으로 생성하고 유지 관리하여 VMware 데이터 센터 환경에서 데이터 저장소 관리를 간소화합니다. ONTAP tools for VMware vSphere 10.5 P2부터는 마이그레이션된 igroup이 더 이상 사용되지 않을 경우 자동으로 삭제됩니다.

간략한 동작 요약

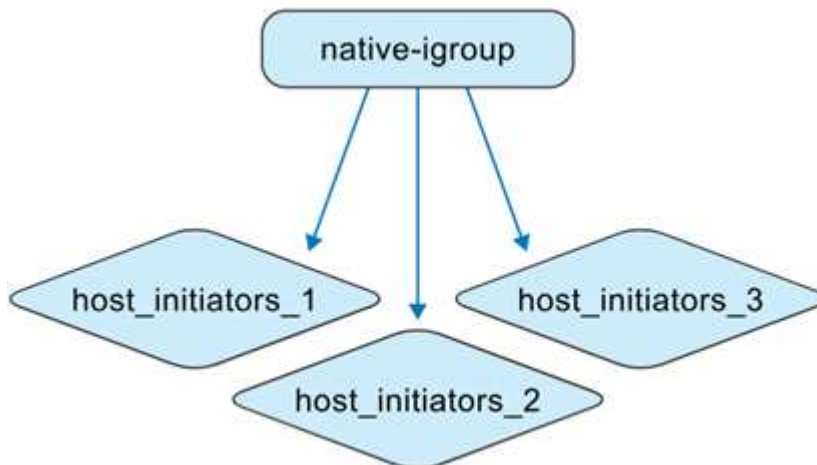
- ONTAP tools for VMware vSphere로 관리되는 VMFS 데이터 저장소는 중첩된 igroup을 사용합니다. 데이터 저장소 컨텍스트당 하나의 상위 igroup과 호스트당 하나의 하위 igroup이 있습니다.
- LUN 매핑은 하위 igroup에 적용됩니다.
- 사용자 지정 상위 igroup은 데이터 저장소 간에 재사용할 수 있습니다.
- ONTAP tools for VMware vSphere 9.x에서 마이그레이션된 igroup은 재사용할 수 없습니다.

igroup 컨텍스트

ONTAP tools for VMware vSphere는 두 가지 컨텍스트에서 igroup을 처리합니다.

ONTAP 외 도구로 관리되는 igroups

스토리지 관리자는 ONTAP 시스템에서 평면 또는 중첩 구조로 igroup을 생성할 수 있습니다. 다음 그림은 ONTAP에서 직접 생성된 평면 igroup을 보여줍니다.

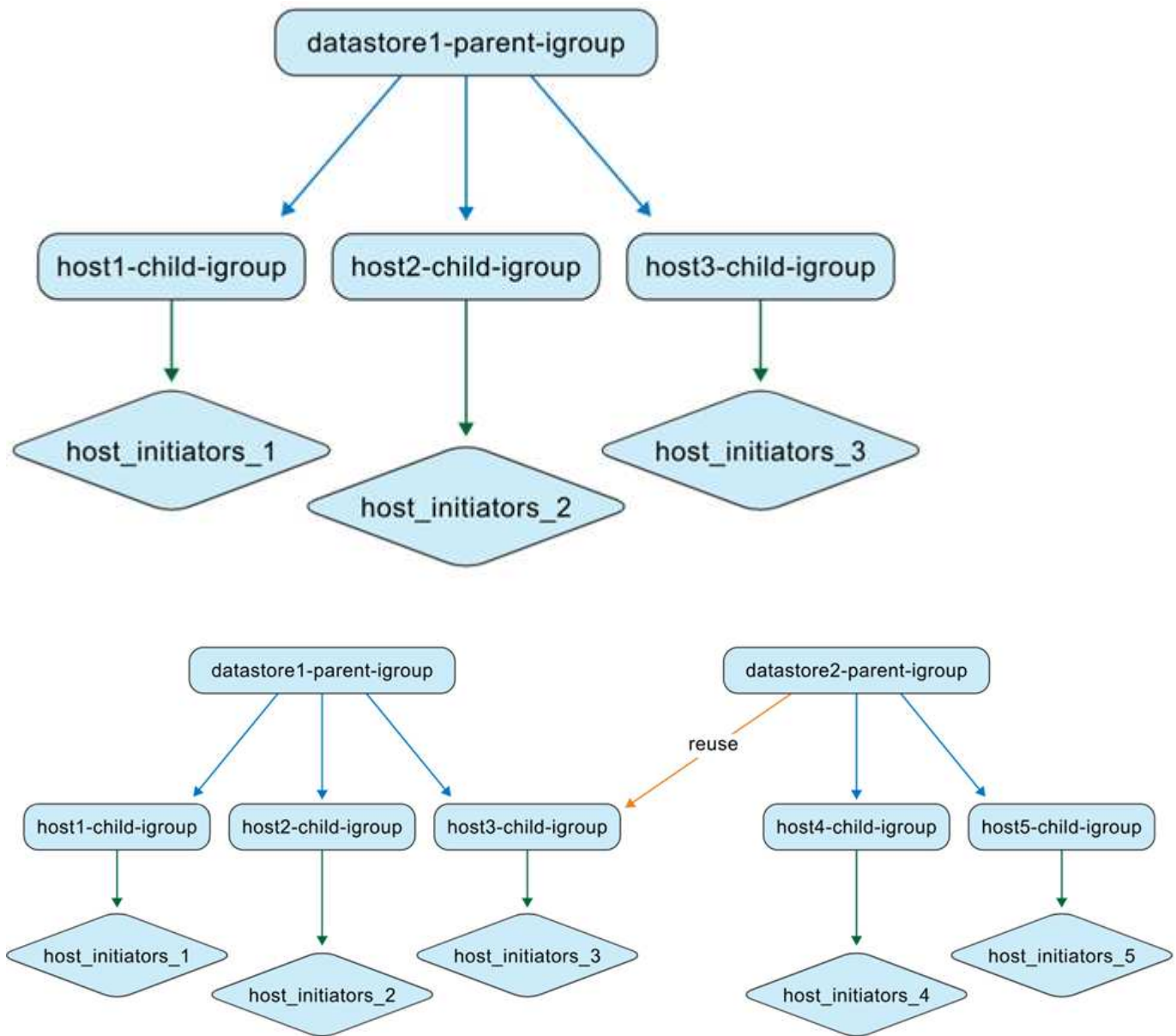


ONTAP tools 관리 igroup

데이터스토어를 생성할 때 ONTAP tools for VMware vSphere는 중첩 구조로 igroup을 생성합니다.

예를 들어, datastore1이 생성되어 호스트 1, 2, 3에 마운트되고, 새로운 데이터스토어(datastore2)가 생성되어 호스트

3, 4, 5에 마운트되면 ONTAP tools는 효율적인 관리를 위해 호스트 수준의 igroup을 재사용합니다.



명명 동작

데이터 저장소를 생성할 때 igroup 필드를 비워두면 ONTAP tools는 기본적으로 중첩된 igroup 구조를 생성합니다.

- 상위 igroup 명명 패턴: `otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>`
- 하위 igroup 명명 패턴: `otv_<hostMoref>_<vcguid>`

ONTAP 시스템 인터페이스는 상위 이니시에이터 그룹 필드에서 상위 및 하위 igroup 간의 관계를 보여줍니다.

시나리오별 동작

시나리오	상위 igroup 동작	하위 igroup 동작	LUN 매핑 및 가시성
기본 igroup 설정으로 생성된 데이터 저장소	기본 ONTAP tools 관리 상위 igroup 이 생성됩니다.	호스트 수준의 하위 igroup 은 필요에 따라 생성됩니다.	LUN은 하위 igroup 에 매핑됩니다. 데이터 저장소가 vCenter Server 인벤토리에 나타납니다.
사용자 지정 igroup 이름으로 생성된 데이터 저장소	지정된 이름으로 사용자 지정 상위 igroup 이 생성됩니다.	호스트가 중복될 경우 기존 호스트 수준 하위 igroup 이 재사용됩니다.	새 데이터스토어 LUN이 재사용되거나 새로 생성된 하위 igroup 에 매핑됩니다. 데이터스토어가 vCenter Server에 나타납니다.
데이터 저장소 생성 중에 기존 사용자 지정 igroup 이 재사용됩니다	기존의 사용자 지정 상위 igroup 이 선택되어 재사용됩니다.	하위 igroup 은 호스트 멤버십에 따라 재사용되거나 확장됩니다.	새 데이터스토어 LUN은 연결된 하위 igroup 을 통해 매핑됩니다. 데이터스토어가 vCenter Server에 나타납니다.
데이터스토어와 igroup 은 ONTAP 및 vCenter에서 기본적으로 생성된 후 ONTAP tools에서 검색됩니다	ONTAP tools는 관리 컨텍스트에 상위 igroup 을 생성하고 원래 igroup 이름을 유지합니다.	ONTAP tools는 원래 igroup 의 이름을 <code>otv_</code> 접두사로 변경하고 계층 구조에서 하위 igroup 으로 나타냅니다.	이니시에이터 매핑은 변경되지 않습니다. 검색 중에 데이터 저장소에 매핑된 igroup 만 변환됩니다.

사용자 정의 **igroup** 재사용 및 API 동작

ONTAP tools for VMware vSphere 사용자 인터페이스에서 데이터 저장소를 생성하는 동안 드롭다운 목록에서 기존 사용자 지정 상위 **igroup**을 재사용할 수 있습니다.

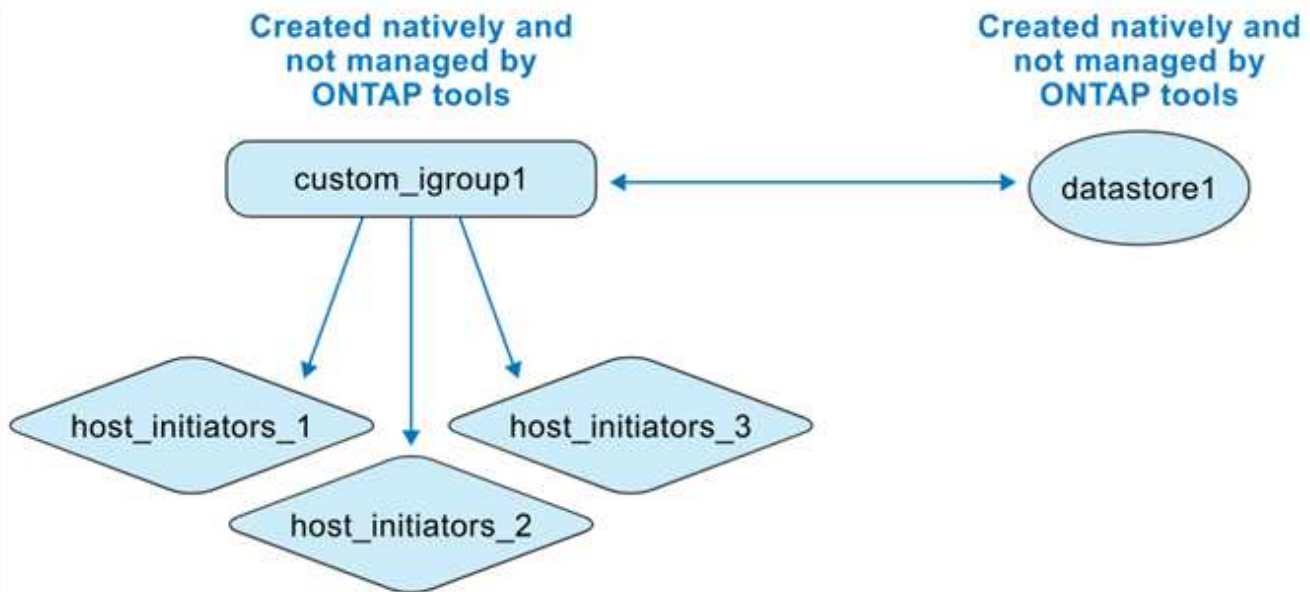
API를 통해서도 동일한 동작이 지원됩니다. 데이터 저장소 생성 중에 기존 **igroup**을 재사용하려면 API 요청 페이로드에 **igroup UUID**를 제공하십시오.



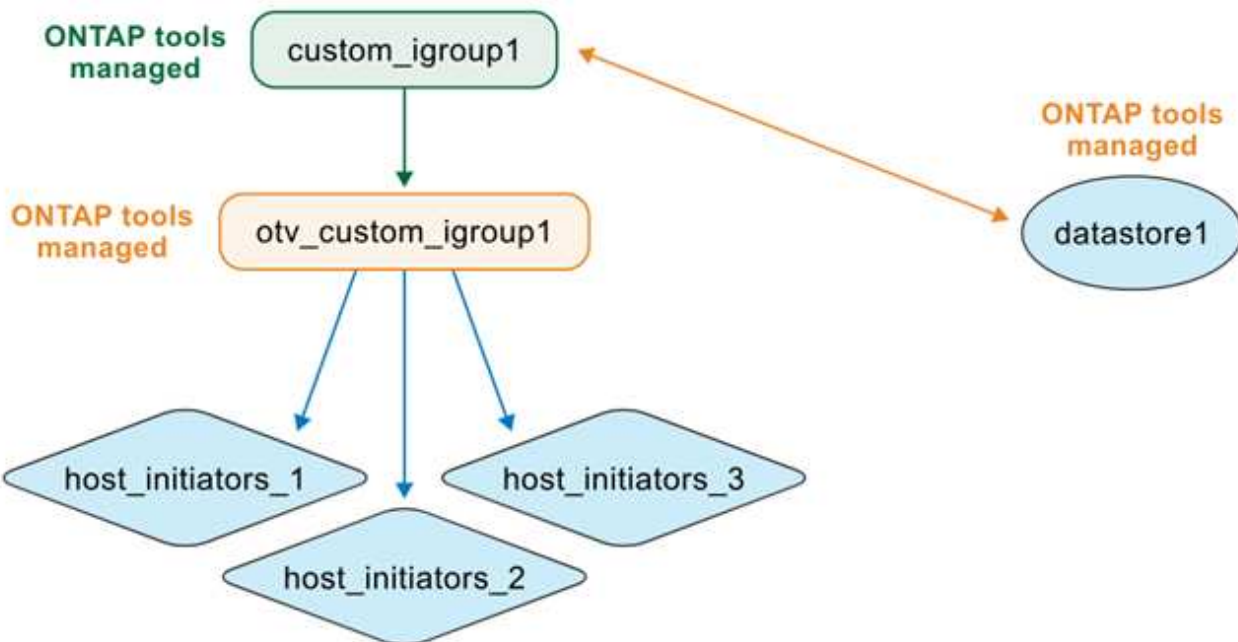
사용자 정의 **igroup**만 재사용할 수 있습니다. ONTAP tools 9.x에서 마이그레이션된 **igroup**은 재사용할 수 없으며, ONTAP tools 10.5 P2부터는 더 이상 사용하지 않을 경우 자동으로 삭제됩니다.

네이티브에서 관리형으로의 전환 보기

ONTAP 시스템 및 VMware 환경에서 **igroup**과 데이터스토어를 직접 생성하는 경우, ONTAP tools는 초기에는 이러한 객체를 관리하지 않습니다. 따라서 **igroup** 구조가 평면적으로 생성됩니다.



데이터 저장소 검색 후 ONTAP tools는 데이터 저장소에 매핑된 igroup을 식별하고 등록한 다음 중첩 모델로 표현합니다. 상위 igroup은 데이터 저장소 수준에서 표현되고, 기존 igroup은 `otv_` 접두사가 붙은 하위 igroup으로 이름이 변경되며, 이니시에이터 매핑은 변경되지 않습니다.



ONTAP tools for VMware vSphere는 ONTAP 시스템에서 생성되었지만 데이터 저장소에 매핑되지 않았거나 ONTAP tools에 연결되지 않은 igroup을 감지하거나 관리하지 않습니다. 검색 중에 ONTAP tools는 검색된 데이터 저장소에 매핑된 igroup만 변환하며, 다른 igroup은 관리되지 않은 상태로 유지됩니다.

발견된 네이티브 igroup의 재사용

ONTAP tools for VMware vSphere가 검색된 네이티브 igroup을 관리한 후에는 해당 igroup이 데이터 저장소 생성을 위한 사용자 지정 이니시에이터 그룹 이름 드롭다운 목록에서 사용 가능해집니다.

새 데이터 저장소 LUN은 정규화된 하위 igroup에 매핑됩니다(예: otv_NativeIgroup1).

ONTAP tools for VMware vSphere는 ONTAP tools로 관리되지 않거나 데이터스토어에 연결되지 않은 ONTAP 시스템에서 생성된 igroup을 감지하거나 사용하지 않습니다.

ONTAP tools Manager 사용자 인터페이스에 대해 알아보십시오

ONTAP tools for VMware vSphere는 멀티 테넌시(multi-tenancy)를 지원하여 여러 vCenter Server 인스턴스를 관리할 수 있습니다.

ONTAP Tools Manager는 ONTAP tools for VMware vSphere, vCenter Server 인스턴스, 스토리지 백엔드 및 고가용성(HA) 및 노드 확장과 같은 어플라이언스 구성을 관리하는 웹 기반 콘솔입니다.

ONTAP tools Manager는 다음과 같은 기능을 제공합니다.

- 경고 관리 - ONTAP tools for VMware vSphere에서 생성된 경고를 보고 필터링합니다.
- 스토리지 백엔드 관리 - ONTAP 스토리지 클러스터를 추가 및 관리하고, 이를 vCenter Server 인스턴스에 전역으로 매핑할 수 있습니다.
- vCenter Server 인스턴스 관리 - ONTAP tools 내에서 vCenter Server 인스턴스를 추가하고 관리합니다.
- 작업 모니터링 - ONTAP tools 플러그인 인터페이스와 ONTAP tools Manager 인터페이스에서 시작된 비동기 작업을 모니터링하고 디버깅할 수 있습니다. 기간별로 작업을 필터링하고, 페이지 크기를 조정하고, 오류 및 하위 작업을 포함한 작업 세부 정보를 볼 수 있습니다. 실패 상태를 클릭하면 오류 세부 정보를 볼 수 있습니다. 하위 작업이 있는 작업의 경우 행을 확장하여 설명과 상태를 볼 수 있습니다. 하위 작업의 경우 작업의 드릴다운 기능을 사용하여 세부 정보를 볼 수 있습니다.
- 로그 번들 다운로드 - ONTAP tools for VMware vSphere 문제 해결을 위한 로그 파일을 수집합니다.
- 인증서 관리 - 자체 서명 인증서를 사용자 지정 CA 인증서로 교체하고 VASA Provider 및 ONTAP tools에 대한 인증서를 갱신하거나 새로 고칠 수 있습니다.
- 비밀번호 재설정 - VASA Provider 및 SRA의 비밀번호를 변경합니다.
- 어플라이언스 설정 관리 - HA 활성화 및 노드 크기 확장 등 ONTAP tools 어플라이언스를 구성합니다.

ONTAP tools Manager에 액세스하려면 브라우저에서 ``https://<ONTAPtoolsIP>:8443/virtualization/ui/``을 실행하고 배포 중에 제공한 VMware vSphere용 ONTAP tools 관리자 자격 증명으로 로그인하십시오.

ONTAP tools Manager

?
refresh
admin

Overview
Alerts
Storage backends
vCenters
Jobs
Log bundles
Certificates
Settings

Overview

EDIT APPLIANCE SETTINGS

Appliance

Healthy

Size
HA ①
VASA Provider ①
SRA ①

Small
Enabled
Enabled
Enabled

VIEW DETAILS

Alerts

Last 24 hours

No alerts

VIEW ALL ALERTS (0)

vCenters

1
Healthy

VIEW ALL VCENTERS (1)

Storage backends

No storage backends added

VIEW ALL STORAGE BACKENDS (0)

ONTAP tools nodes

vee-lab3-vm41

Healthy

Deploy_OVA_b29c029_998

VIEW DETAILS

vee-lab3-vm184

Healthy

Deploy_OVA_b29c029_9982

VIEW DETAILS

vee-lab3-vm187

Healthy

Deploy_OVA_b29c029_9983

VIEW DETAILS

카드	설명
어플라이언스 카드	어플라이언스 카드에는 ONTAP 툴 어플라이언스의 전체 상태, 구성 세부 정보 및 활성화된 서비스 상태가 표시됩니다. 자세한 내용을 보려면 세부 정보 보기 링크를 선택하십시오. 어플라이언스 설정을 변경하면 변경이 완료될 때까지 카드에 작업 상태와 세부 정보가 표시됩니다.
알림 카드	알림 카드에는 HA 노드 수준 알림을 포함하여 유형별로 분류된 ONTAP tools 알림이 표시됩니다. 개수 하이퍼링크를 클릭하면 선택한 알림 유형으로 필터링된 알림 페이지로 이동하여 자세한 알림을 볼 수 있습니다.
vCenters 카드	vCenters 카드에는 ONTAP tools로 관리되는 모든 vCenter Server 인스턴스의 상태가 표시됩니다. 해당 링크를 선택하여 각 vCenter의 세부 정보를 볼 수 있으며, 선택한 인스턴스에 대한 자세한 정보가 있는 페이지로 이동합니다.
스토리지 백엔드 카드	스토리지 백엔드 카드에는 ONTAP tools에 구성된 모든 ONTAP 스토리지 클러스터의 상태 및 연결 상태가 표시됩니다. 각 스토리지 백엔드에 대한 자세한 내용은 해당 링크를 선택하여 확인할 수 있으며, 링크를 선택하면 선택한 클러스터에 대한 자세한 정보가 있는 페이지로 이동합니다.

89

카드	설명
ONTAP tools 노드 카드	ONTAP tools 노드 카드에는 노드 이름, VM 이름, 상태 및 네트워크 정보를 포함하여 어플라이언스의 모든 노드가 표시됩니다. 특정 노드에 대한 자세한 내용을 보려면 *세부 정보 보기*를 선택하십시오. [참고] 비 HA 구성의 경우 단일 노드만 표시됩니다. HA 구성에서는 세 개의 노드가 표시됩니다.

ONTAP tools Manager 설정 관리

ONTAP 도구 AutoSupport 설정 편집

ONTAP tools for VMware vSphere를 처음 구성할 때 AutoSupport는 기본적으로 활성화됩니다. 활성화 후 24시간 후에 기술 지원팀에 메시지를 보냅니다.

AutoSupport 비활성화

AutoSupport를 비활성화하면 사전 예방적 지원 및 모니터링을 더 이상 받지 못하게 됩니다.



AutoSupport 기능은 문제 감지 및 해결 속도를 높여주므로 활성화 상태로 유지하는 것이 좋습니다. AutoSupport이 비활성화된 경우에도 시스템은 정보를 계속 수집하여 로컬에 저장하지만, 네트워크를 통해 보고서를 전송하지는 않습니다.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 설정 > 원격 측정 > 편집 옵션을 선택합니다.
4. **AutoSupport** 옵션의 선택을 해제하고 변경 사항을 저장합니다.

AutoSupport 프록시 URL 업데이트

AutoSupport 프록시 URL을 업데이트하여 AutoSupport 기능이 안전한 데이터 전송을 위해 프록시 서버를 통해 데이터를 라우팅하도록 하십시오.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 사이드바에서 *설정*을 선택합니다.
4. 설정 > 원격 측정 > 편집 옵션을 선택합니다.
5. 유효한 *프록시 URL*을 입력하고 변경 사항을 저장하세요.

AutoSupport를 비활성화하면 프록시 URL도 비활성화됩니다.

ONTAP tools에 NTP 서버 추가

ONTAP tools 어플라이언스의 시간 클록을 동기화하려면 NTP 서버 정보를 입력하십시오.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 설정 > **NTP** 서버 > 편집 옵션을 선택합니다.
4. 심표로 구분된 정규화된 도메인 이름(FQDN), IPv4 또는 IPv6 주소를 입력하십시오.

화면을 새로 고쳐 업데이트된 값을 확인하십시오.

ONTAP tools에서 VASA Provider 및 SRA 자격 증명을 재설정합니다

VASA Provider 또는 SRA 자격 증명을 잊어버린 경우 ONTAP tools Manager 인터페이스를 사용하여 새 비밀번호로 재설정할 수 있습니다. 새 비밀번호는 8자에서 256자 사이여야 합니다.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 설정 > **VASA Provider / SRA** 자격 증명 > 비밀번호 재설정 옵션을 선택하십시오.
4. 새 비밀번호를 입력하고 확인하십시오.
5. 변경 사항을 적용하려면 *저장*을 선택합니다.

ONTAP 도구 백업 설정 편집

ONTAP tools for VMware vSphere 10.5부터 백업 기능이 기본적으로 활성화되어 있으며 10분마다 백업이 생성됩니다. 백업 기능을 비활성화하거나 백업 빈도를 편집할 수 있습니다.

백업을 비활성화하지 마십시오. 백업을 비활성화하면 ONTAP 도구가 낮은 RPO를 유지하는 데 지장을 초래합니다. 백업을 비활성화해도 기존 백업 파일은 삭제되지 않습니다. 백업 빈도는 10분에서 60분 사이로 변경할 수 있습니다.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 설정 > 백업 > 편집 옵션을 선택합니다.
4. 편집 창에서 백업을 비활성화하거나 백업 빈도를 편집할 수 있습니다.

ONTAP 툴 서비스를 활성화합니다

ONTAP Tools Manager를 사용하여 관리자 암호를 변경하면 VASA Provider, vVols 구성 가져오기 및 ONTAP Tools Manager를 사용한 재해 복구(SRA)와 같은 서비스를 활성화할 수 있습니다.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 개요 섹션에서 *기기 설정 편집*을 선택하십시오.
4. 서비스 섹션에서는 필요에 따라 VASA 공급자, vVols 구성 가져오기 및 재해 복구(SRA)와 같은 선택적 서비스를 활성화할 수 있습니다.

서비스를 처음 활성화할 때는 VASA Provider 및 SRA 자격 증명을 생성해야 합니다. 이러한 자격 증명은 vCenter Server에서 VASA Provider 및 SRA 서비스를 등록하거나 활성화하는 데 사용됩니다. 사용자 이름에는 문자, 숫자 및 밑줄만 사용할 수 있습니다. 암호 길이는 8자에서 256자 사이여야 합니다.



선택적 서비스를 비활성화하기 전에 ONTAP tools에서 관리하는 vCenter 서버에서 해당 서비스를 사용하지 않는지 확인하십시오.

- vVols 구성 가져오기 허용* 옵션은 VASA Provider 서비스가 활성화된 경우에만 표시됩니다. 이 옵션을 사용하면 ONTAP tools 9.xx에서 ONTAP tools 10.5로 vVols 데이터를 마이그레이션할 수 있습니다.

ONTAP 도구 어플라이언스 설정을 변경합니다

ONTAP tools Manager를 사용하여 노드 수를 늘리거나 고가용성(HA)을 활성화하여 ONTAP tools for VMware vSphere 구성을 확장할 수 있습니다. 기본적으로 ONTAP tools for VMware vSphere 어플라이언스는 단일 노드, 비HA 구성으로 배포됩니다.

시작하기 전에

- OVA 템플릿의 OVA 버전이 노드 1과 동일한지 확인하십시오. 노드 1은 ONTAP tools for VMware vSphere OVA가 처음 배포되는 기본 노드입니다.
- CPU 핫 추가 및 메모리 핫 플러그가 활성화되어 있는지 확인하십시오.
- vCenter Server에서 재해 복구 서비스(DRS) 자동화 수준을 부분 자동화로 설정합니다. 고가용성(HA)을 배포한 후에는 자동화 수준을 완전 자동화로 되돌립니다.
- 고가용성(HA) 설정에서 노드 호스트 이름은 소문자여야 합니다.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 개요 섹션에서 *기기 설정 편집*을 선택하십시오.

4. 구성 섹션에서 노드 크기를 확장하고 HA 구성을 활성화합니다. vCenter Server 자격 증명을 사용하여 변경하십시오.

HA 구성에서 콘텐츠 라이브러리 세부 정보를 변경할 수 있습니다. 각 편집마다 암호를 입력해야 합니다.



ONTAP tools for VMware vSphere에서는 노드 크기를 늘릴 수는 있지만 줄일 수는 없습니다. 비 HA 설정에서는 중간 크기 구성만 지원됩니다. HA 설정에서는 중간 및 대형 구성이 지원됩니다.

5. HA 토글 버튼을 사용하여 HA 구성을 활성화합니다. **HA** 설정 페이지에서 다음 사항을 확인하십시오.

- 콘텐츠 라이브러리는 ONTAP 도구 노드 VM이 실행되는 vCenter Server에 속합니다. vCenter Server 자격 증명은 어플라이언스 변경을 위한 OVA 템플릿을 검증하고 다운로드하는 데 사용됩니다.
- ONTAP 도구를 호스팅하는 가상 머신은 ESXi 호스트에 직접 배포되지 않습니다. 해당 VM은 클러스터 또는 리소스 풀에 배포해야 합니다.



HA 구성이 활성화된 후에는 HA를 지원하지 않는 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 vSphere는 HA 설정에서 세 개의 노드를 지원합니다.



ONTAP tools는 워크플로를 간소화하기 위해 대부분의 입력 옵션을 노드 1의 네트워크 정보로 미리 채웁니다. 마법사의 마지막 페이지로 이동하기 전에 입력 데이터를 편집할 수 있습니다. 나머지 두 노드의 IPv6 주소 정보는 ONTAP tools 관리 노드에서 IPv6 주소가 활성화된 경우에만 입력할 수 있습니다.

각 ESXi 호스트에는 ONTAP tools VM이 하나만 있어야 합니다. 입력값은 다음 창으로 이동할 때마다 유효성 검사를 거칩니다.

7. 요약 섹션의 세부 정보를 검토하고 변경 사항을 *저장*합니다.

다음 단계

개요 페이지에서는 배포 상태를 확인할 수 있습니다. 또한 작업 보기에서 작업 ID를 사용하여 어플라이언스 설정 편집 작업 상태를 추적할 수 있습니다.

HA 배포가 실패하고 새 노드 상태가 '새로 생성됨'인 경우, HA를 다시 활성화하기 전에 vCenter에서 새 VM을 삭제하십시오.

왼쪽 패널의 알림 탭에는 VMware vSphere용 ONTAP tools에 대한 알림이 나열됩니다.

ONTAP tools에 VMware vSphere 호스트 추가

새 VMware vSphere 호스트를 ONTAP tools for VMware vSphere에 추가하여 호스트의 데이터스토어를 관리하고 보호할 수 있습니다.

단계

1. 다음 페이지의 워크플로에 따라 VMware vSphere 클러스터에 호스트를 추가하십시오: "[빠른 시작 워크플로를 사용하여 ESX 호스트를 vSphere 클러스터에 추가하는 방법](#)"
2. 호스트를 추가한 후 ONTAP tools 메인 메뉴로 이동하여 개요 패널에서 *검색*을 선택합니다. 검색 프로세스가 완료될 때까지 기다립니다. 또는 예약된 호스트 검색이 완료될 때까지 기다릴 수도 있습니다.

결과

이제 새 호스트가 ONTAP tools for VMware vSphere에 의해 검색되고 관리됩니다. 새 호스트에서 데이터스토어를 관리할 수 있습니다.

관련 주제

- ["vVols 데이터스토어 마운트"](#) 새로운 호스트에서.
- ["NFS 및 VMFS 데이터스토어 마운트"](#) 새로운 호스트에서.

데이터 저장소 관리

ONTAP 도구에서 NFS 및 VMFS 데이터 저장소를 마운트합니다

데이터스토어를 마운트하면 추가 호스트에서 스토리지에 액세스할 수 있습니다. VMware 환경에 호스트를 추가한 후 해당 호스트에 데이터스토어를 마운트할 수 있습니다.



"vSphere 클러스터에 ESX 호스트 추가 워크플로"를 사용하여 새 ESXi 호스트를 추가할 때 예약된 호스트 검색이 완료될 때까지 기다린 후 ONTAP tools에 표시되도록 하십시오. 또는 NetApp ONTAP tools 개요 화면에서 수동으로 검색을 실행할 수 있습니다.

이 작업 정보

- vSphere 클라이언트 버전 및 선택한 데이터스토어 유형에 따라 일부 마우스 오른쪽 클릭 작업이 비활성화되거나 사용할 수 없을 수 있습니다.
 - vSphere 클라이언트 8.0 이상 버전을 사용하는 경우 마우스 오른쪽 버튼 클릭 옵션 중 일부가 숨겨져 있습니다.
 - vSphere 7.0U3부터 vSphere 8.0 버전까지는 옵션이 표시되더라도 해당 작업은 비활성화됩니다.
- vSphere는 호스트 클러스터가 균일한 구성으로 보호되는 경우 데이터스토어 마운트 옵션을 비활성화합니다.

단계

1. vSphere Client 홈 페이지에서 *호스트 및 클러스터*를 선택합니다.
2. 왼쪽 탐색 창에서 호스트가 포함된 데이터 센터를 선택합니다.
3. 호스트 또는 호스트 클러스터에 NFS/VMFS 데이터스토어를 마운트하려면 마우스 오른쪽 버튼을 클릭하고 *NetApp ONTAP tools* > *데이터스토어 마운트*를 선택하십시오.
4. 마운트할 데이터 저장소를 선택하고 *마운트*를 선택합니다.

다음 단계

최근 작업 패널에서 진행 상황을 확인할 수 있습니다.

관련 주제

["새로운 VMware vSphere 호스트 추가"](#)

ONTAP 도구에서 NFS 및 VMFS 데이터 저장소 마운트 해제

데이터스토어 마운트 해제 작업은 ESXi 호스트에서 NFS 또는 VMFS 데이터스토어를 제거합니다. 이 작업은 ONTAP tools for VMware vSphere에서 검색되거나 관리되는 데이터스토어에 사용할 수 있습니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. NFS 또는 VMFS 데이터스토어 개체를 마우스 오른쪽 버튼으로 클릭하고 *데이터스토어 마운트 해제*를 선택합니다.

vSphere 클라이언트는 데이터스토어를 마운트하는 ESXi 호스트 목록을 표시하는 대화 상자를 엽니다. 보호된 데이터스토어에서 작업을 수행할 경우 화면에 경고 메시지가 표시됩니다.

3. 데이터스토어를 마운트 해제할 ESXi 호스트를 하나 이상 선택하십시오.

모든 호스트에서 데이터 저장소를 마운트 해제할 수는 없습니다. 사용자 인터페이스에서는 대신 데이터 저장소 삭제 작업을 사용하도록 안내합니다.

4. 마운트 해제 버튼을 선택합니다.

데이터 저장소가 보호된 호스트 클러스터의 일부인 경우 경고 메시지가 표시됩니다.



보호된 데이터 저장소가 마운트 해제되면 기존 보호 설정으로 인해 부분적인 보호만 적용될 수 있습니다. 완전한 보호를 활성화하려면 "[보호된 호스트 클러스터 수정](#)"을 참조하십시오.

다음 단계

최근 작업 패널에서 진행 상황을 확인할 수 있습니다.

ONTAP tools에서 vVols 데이터 저장소 마운트

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



"[vSphere 클러스터에 ESX 호스트 추가 워크플로](#)"를 사용하여 새 ESXi 호스트를 추가할 때 예약된 호스트 검색이 완료될 때까지 기다린 후 ONTAP tools에 표시되도록 하십시오. 또는 NetApp ONTAP tools 개요 화면에서 수동으로 검색을 실행할 수 있습니다.

단계

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

최근 작업 패널에는 진행 상황이 표시됩니다.

관련 주제

["새로운 VMware vSphere 호스트 추가"](#)

ONTAP 도구에서 NFS 및 VMFS 데이터 저장소 크기 조정

데이터스토어 크기 조정은 가상 머신 파일의 저장 공간을 늘릴 수 있는 기능입니다. 인프라 요구 사항이 변경됨에 따라 데이터스토어 크기를 변경할 수 있습니다.

이 작업 정보

NFS 및 VMFS 데이터스토어의 크기를 늘릴 수 있습니다. 이러한 데이터스토어의 FlexVol 볼륨은 현재 크기보다 작아질 수는 없지만 최대 120%까지 커질 수 있습니다.

단계

1. vSphere Client 홈 페이지에서 *호스트 및 클러스터*를 선택합니다.
2. 탐색 창에서 데이터 저장소가 포함된 데이터 센터를 선택합니다.
3. NFS 또는 VMFS 데이터스토어를 마우스 오른쪽 버튼으로 클릭하고 **NetApp ONTAP tools** > *데이터스토어 크기 조정*을 선택합니다.
4. 크기 조정 대화 상자에서 데이터 저장소의 새 크기를 입력하고 *확인*을 선택합니다.

ONTAP tools에서 vVols 데이터 저장소 확장

vCenter 객체 보기에서 데이터스토어 객체를 마우스 오른쪽 버튼으로 클릭하면 플러그인 섹션에 ONTAP tools for VMware vSphere에 대해 지원되는 작업이 표시됩니다. 특정 작업은 데이터스토어 유형과 현재 사용자 권한에 따라 활성화됩니다.



vVols 데이터스토어 확장 작업은 ASA r2 시스템 기반 vVols 데이터스토어에 적용되지 않습니다.

단계

1. vSphere Client 홈 페이지에서 *호스트 및 클러스터*를 선택합니다.
2. 탐색 창에서 데이터 저장소가 포함된 데이터 센터를 선택합니다.
3. 데이터스토어를 마우스 오른쪽 버튼으로 클릭하고 *NetApp ONTAP tools* > *데이터스토어에 스토리지 추가*를 선택합니다.
4. 볼륨 생성 또는 선택 창에서 새 볼륨을 생성하거나 기존 볼륨 중에서 선택할 수 있습니다. 화면의 지시에 따라 선택하십시오.
5. 요약 창에서 선택 사항을 검토하고 *확장*을 선택합니다. 최근 작업 패널에서 진행 상황을 확인할 수 있습니다.

ONTAP tools에서 vVols 데이터스토어 축소

이 페이지에서는 vVols 데이터스토어에서 볼륨을 제거하는 방법을 설명합니다.

vCenter Server의 ONTAP tools에서 관리하는 모든 vVols 데이터 저장소에서 '데이터 저장소에서 스토리지 제거' 작업을 사용하십시오.

vVols이 포함된 볼륨에서는 스토리지를 제거할 수 없습니다. 이러한 볼륨에 대해서는 제거 옵션이 비활성화됩니다. 데이터스토어에서 볼륨을 제거할 때 ONTAP 스토리지에서 선택한 볼륨을 삭제하는 옵션도 사용할 수 있습니다.



vVols 데이터스토어 축소 작업은 ASA r2 시스템 기반 vVols 데이터스토어에서 지원되지 않습니다.

단계

1. vSphere Client 홈 페이지에서 *호스트 및 클러스터*를 선택합니다.
2. 탐색 창에서 데이터 저장소가 포함된 데이터 센터를 선택합니다.
3. vVol 데이터스토어를 마우스 오른쪽 버튼으로 클릭하고 **NetApp ONTAP tools** > *데이터스토어에서 스토리지 제거*를 선택합니다.
4. vVols이 없는 볼륨을 선택하고 *제거*를 선택합니다.



vVols가 위치한 볼륨을 선택하는 옵션이 비활성화되었습니다.

5. 저장소 제거 팝업 창에서 **ONTAP** 클러스터에서 볼륨 삭제 확인란을 선택하여 데이터 저장소와 ONTAP 저장소에서 볼륨을 삭제한 다음 *삭제*를 선택합니다.

ONTAP 도구에서 데이터 저장소를 삭제합니다

이 페이지에서는 vCenter Server에서 ONTAP tools를 사용하여 NFS, VMFS 또는 vVols 데이터스토어를 삭제하는 방법을 설명합니다.

데이터 저장소를 삭제하면 데이터 저장소 유형에 따라 다음과 같은 작업이 수행됩니다.

- vVol 컨테이너가 마운트 해제되었습니다.
- igroup이 사용되지 않으면 해당 이니시에이터가 igroup에서 제거됩니다.
- vVol 컨테이너가 삭제되었습니다.
- Flex 볼륨은 스토리지 어레이에 남아 있습니다.

선택한 데이터스토어에 vVols이 없는 경우에만 데이터스토어를 삭제할 수 있습니다.

단계

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



가상 머신에서 사용하는 데이터 저장소는 삭제할 수 없습니다. 삭제하기 전에 가상 머신을 다른 데이터 저장소로 이동하십시오. 보호된 호스트 클러스터의 일부인 볼륨은 삭제할 수 없습니다.

- a. NFS 또는 VMFS 데이터스토어의 경우, 해당 데이터스토어를 사용하는 가상 머신 목록이 포함된 대화 상자가 나타납니다.
- b. VMFS 데이터스토어에 연결된 가상 머신이 없는 경우 확인 대화 상자가 표시됩니다. 호스트 클러스터 보호가 활성화되어 있고 AFD 관계가 있는 경우 2차 스토리지 요소를 정리할 수 있습니다.
- c. ASA r2 시스템에서 보호된 VMFS 데이터스토어의 경우 삭제하기 전에 보호를 해제해야 합니다. ONTAP 9.17.1 및 ONTAP tools for VMware vSphere 10.5부터는 보호된 데이터스토어를 삭제할 수 있습니다. 보호 그룹에 해당 데이터스토어가 하나뿐인 경우 호스트 클러스터 보호가 자동으로 제거됩니다.
- d. vVols 데이터스토어의 경우, vVols가 하나도 없는 경우에만 데이터스토어를 삭제할 수 있습니다. 데이터스토어 삭제 대화 상자에는 ONTAP 클러스터에서 볼륨을 제거하는 옵션이 포함되어 있습니다.
- e. ASA r2 시스템의 vVols 데이터스토어의 경우, 데이터스토어 삭제 옵션을 사용하여 ONTAP에서 백업 볼륨을 삭제할 수 없습니다.

3. ONTAP 스토리지의 백업 볼륨을 삭제하려면 *ONTAP 클러스터의 볼륨 삭제*를 선택하십시오.



보호된 호스트 클러스터의 일부인 통합 ONTAP 스토리지의 VMFS 데이터스토어의 경우 ONTAP 클러스터에서 볼륨을 삭제할 수 없습니다.

NFS, VMFS 또는 vVols 데이터스토어를 삭제하면 상위 igroup은 ONTAP 시스템에 남아 있습니다. LUN에 매핑되지 않은 하위 igroup은 자동으로 삭제됩니다. ONTAP tools는 매핑되지 않은 기본 상위 igroup을 제거하기 위해 매일 정리 작업을 수행합니다. 사용자 지정 상위 igroup은 ONTAP에서 수동으로 삭제하십시오. ONTAP tools는 오래된 상위 igroup을 재사용할 수 없습니다.

ONTAP tools의 데이터 저장소용 ONTAP 스토리지 뷰

ONTAP tools for VMware vSphere는 구성 탭에서 데이터스토어와 해당 볼륨의 ONTAP 스토리지 측면 보기를 표시합니다.

단계

1. vSphere 클라이언트에서 데이터스토어로 이동합니다.
2. 오른쪽 창에서 구성 탭을 선택합니다.
3. **NetApp ONTAP tools** > *ONTAP Storage*를 선택하십시오. 데이터스토어 유형에 따라 보기가 변경됩니다. 아래 표를 참조하십시오.

데이터 저장소 유형	정보 제공 가능
NFS 데이터 저장소	Storage details 페이지에는 스토리지 백엔드, 애그리게이트 및 볼륨 정보가 포함됩니다. NFS details 페이지에는 NFS 데이터스토어와 관련된 데이터가 포함됩니다.
VMFS 데이터 저장소	스토리지 세부 정보 페이지에는 스토리지 백엔드, 애그리게이트, 볼륨 및 스토리지 가용성 영역(SAZ) 세부 정보가 표시됩니다. 스토리지 유닛 세부 정보 페이지에는 스토리지 유닛에 대한 세부 정보가 표시됩니다.
vVols 데이터스토어	모든 볼륨 목록을 표시합니다. ONTAP 스토리지 창에서 스토리지를 확장하거나 제거할 수 있습니다. ONTAP tools는 ASA r2 시스템 기반 vVols 데이터스토어에 대해 이 보기를 지원하지 않습니다.

ONTAP tools의 가상 머신 스토리지 보기

스토리지 보기에는 가상 머신이 생성하는 vVols 목록이 표시됩니다.



이 보기는 ONTAP tools for VMware vSphere 관리형 vVols 데이터스토어의 디스크가 하나 이상 있는 VM에 적용됩니다.

단계

1. vSphere Client에서 가상 머신으로 이동합니다.
2. 오른쪽 창에서 모니터 탭을 선택합니다.

3. **NetApp ONTAP tools** > 스토리지*를 선택합니다. 오른쪽 창에 *스토리지 세부 정보가 나타납니다. VM에 있는 vVols 목록을 볼 수 있습니다.

'열 관리' 옵션을 사용하여 다양한 열을 숨기거나 표시할 수 있습니다.

ONTAP tools에서 스토리지 임계값 관리

볼륨 및 총 용량이 특정 수준에 도달했을 때 vCenter Server에서 알림을 받도록 임계값을 설정할 수 있습니다.

단계:

1. vSphere 클라이언트에 로그인합니다.
2. 바로가기 페이지에서 플러그인 섹션 아래에 있는 *NetApp ONTAP tools*를 선택합니다.
3. ONTAP tools의 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. 임계값을 권장 기본값인 *거의 가득 참 80, 가득 참 90으로 복원할 수 있습니다.

ONTAP tools에서 스토리지 백엔드 관리

스토리지 백엔드는 ESXi 호스트가 데이터 저장을 위해 사용하는 시스템입니다.

스토리지 검색

예약된 검색을 기다리지 않고 필요에 따라 스토리지 백엔드 검색을 실행하여 스토리지 세부 정보를 즉시 업데이트할 수 있습니다. MetroCluster 구성의 경우, 스위치오버 후 ONTAP tools 검색을 수동으로 실행하십시오.

스토리지 백엔드를 검색하려면 아래 단계를 따르십시오.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 바로가기 페이지에서 플러그인 섹션 아래에 있는 *NetApp ONTAP tools*를 선택합니다.
3. ONTAP tools의 왼쪽 창에서 *스토리지 백엔드*로 이동하여 스토리지 백엔드를 선택합니다.
4. 세로 점 세 개 메뉴를 선택하고 *저장소 검색*을 선택합니다.

최근 작업 패널에서 진행 상황을 확인할 수 있습니다.

스토리지 백엔드 수정

스토리지 백엔드 자격 증명 또는 포트 이름을 수정할 수 있습니다. ONTAP tools Manager를 사용하여 글로벌 ONTAP 클러스터의 스토리지 백엔드를 수정할 수도 있습니다. 인증서 만료일이 30일 이내인 경우 ONTAP tools에서 경고 메시지가 표시됩니다. 스토리지 백엔드를 수정하고 ONTAP 관리자로부터 새 인증서를 업로드합니다.

스토리지 백엔드를 수정하면 ONTAP tools for VMware vSphere가 스토리지 백엔드를 검색하여 스토리지 세부 정보를 업데이트합니다.

스토리지 백엔드를 수정하려면 이 섹션의 단계를 따르십시오.

1. vSphere 클라이언트에 로그인합니다.
2. 바로가기 페이지에서 플러그인 섹션 아래에 있는 *NetApp ONTAP tools*를 선택합니다.
3. ONTAP tools의 왼쪽 창에서 *스토리지 백엔드*로 이동하여 스토리지 백엔드를 선택합니다.
4. 세로 점 세 개로 된 메뉴를 선택하고 *수정*을 선택하여 자격 증명 또는 포트 이름을 수정합니다. 최근 작업 패널에서 진행 상황을 확인할 수 있습니다.

ONTAP tools Manager를 사용하여 다음과 같이 글로벌 ONTAP 클러스터를 수정하십시오.

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 사이드바에서 스토리지 백엔드를 선택합니다.
4. 수정할 스토리지 백엔드를 선택합니다.
5. 세로 점 세 개 메뉴를 선택하고 *수정*을 선택합니다.
6. 자격 증명 또는 포트를 수정할 수 있습니다. 저장소 백엔드를 수정하려면 *사용자 이름*과 *암호*를 입력하십시오.

스토리지 백엔드 제거

스토리지 백엔드를 제거하기 전에 해당 백엔드에 연결된 모든 데이터 저장소를 제거해야 합니다. 스토리지 백엔드를 제거하려면 아래 단계를 따르십시오.

1. vSphere 클라이언트에 로그인합니다.
2. 바로가기 페이지에서 플러그인 섹션 아래에 있는 *NetApp ONTAP tools*를 선택합니다.
3. ONTAP tools의 왼쪽 창에서 *스토리지 백엔드*로 이동하여 스토리지 백엔드를 선택합니다.
4. 세로 점 세 개 메뉴를 선택하고 *제거*를 선택하세요. 스토리지 백엔드에 데이터 저장소가 없는지 확인하십시오. 최근 작업 패널에서 진행 상황을 확인할 수 있습니다.

ONTAP tools Manager를 사용하여 글로벌 ONTAP 클러스터를 제거할 수 있습니다.

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 사이드바에서 *스토리지 백엔드*를 선택합니다.
4. 제거할 스토리지 백엔드를 선택합니다
5. 세로 점 세 개 메뉴를 선택하고 *제거*를 선택합니다.

스토리지 백엔드에 대한 상세 보기

스토리지 백엔드 페이지에는 모든 스토리지 백엔드가 나열됩니다. 추가한 스토리지 백엔드에 대해서는 스토리지 검색, 수정 및 제거 작업을 수행할 수 있지만, 클러스터 아래의 개별 하위 SVM에 대해서는 이러한 작업을 수행할 수 없습니다.

상위 클러스터 또는 하위 클러스터를 선택하여 구성 요소 요약 확인하십시오. 상위 클러스터의 경우, 작업 드롭다운

메뉴를 사용하여 스토리지를 검색하거나, 스토리지 백엔드를 수정 또는 제거할 수 있습니다.

요약 페이지에는 다음과 같은 세부 정보가 제공됩니다.

- 스토리지 백엔드 상태
- 용량 정보
- VM에 대한 기본 정보
- 인증서 상태 및 만료일과 같은 인증서 세부 정보입니다.
- 네트워크의 IP 주소 및 포트와 같은 네트워크 정보입니다. 자식 SVM의 경우, 정보는 부모 스토리지 백엔드와 동일합니다.
- 스토리지 백엔드에 허용 및 제한된 Privileges입니다. 하위 SVM의 경우 상위 스토리지 백엔드와 동일한 정보가 표시됩니다. ONTAP tools는 클러스터 기반 스토리지 백엔드에 대해서만 Privileges를 표시합니다. 스토리지 백엔드로 SVM을 추가하면 Privileges 정보가 표시되지 않습니다.
- ASA r2 시스템 클러스터 드릴다운 보기에서 SVM 또는 클러스터에 대해 분산 속성이 "true"로 설정된 경우 로컬 계층 탭이 포함되지 않습니다.
- ASA r2 SVM 시스템의 경우 용량 포털이 표시되지 않습니다. 용량 포털은 SVM 또는 클러스터에 대해 분산 속성이 "true"로 설정된 경우에만 필요합니다.
- ASA r2 SVM 시스템의 경우 기본 정보 섹션에 플랫폼 유형이 표시됩니다.

인터페이스 탭에서는 인터페이스에 대한 자세한 정보를 제공합니다.

로컬 티어 탭에서는 애그리게이트 목록에 대한 자세한 정보를 제공합니다.

ONTAP tools에서 vCenter Server 인스턴스 관리

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

vCenter Server 인스턴스와 스토리지 백엔드 연결을 해제합니다.

vCenter Server 목록 페이지에는 연결된 스토리지 백엔드 수가 표시됩니다. 각 vCenter Server 인스턴스는 스토리지 백엔드를 연결하거나 연결 해제할 수 있는 옵션을 가지고 있습니다.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 사이드바에서 필요한 vCenter Server 인스턴스를 선택하십시오.
4. 스토리지 백엔드와 연결 또는 연결 해제하려는 vCenter Server 옆에 있는 세로 점 세 개(...)를 선택하십시오.
5. *스토리지 백엔드 연결 해제*를 선택합니다.

vCenter Server 인스턴스 수정

vCenter Server 인스턴스를 수정하려면 아래 단계를 따르십시오.

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 사이드바에서 해당 vCenter Server 인스턴스를 선택하십시오.
4. 수정하려는 vCenter Server 옆의 세로 점 세 개(...)를 선택한 다음 *수정*을 선택합니다.
5. **vCenter** 수정 창에서 사용자 이름, 암호 및 포트 정보를 입력합니다.
6. 인증서를 업로드하고 *수정*을 선택합니다.

vCenter Server 인스턴스 제거

vCenter 서버를 제거하기 전에 모든 스토리지 백엔드를 제거하십시오.

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 사이드바에서 해당 vCenter Server 인스턴스를 선택하십시오.
4. 제거하려는 vCenter 서버 옆의 세로 점 세 개(...)를 선택한 다음 *제거*를 선택합니다.



vCenter Server 인스턴스를 제거하면 애플리케이션에서 더 이상 해당 인스턴스를 관리하지 않습니다.

ONTAP tools에서 vCenter Server 인스턴스를 제거하면 다음 작업이 자동으로 수행됩니다.

- 플러그인이 등록되지 않았습니다.
- 플러그인 권한 및 플러그인 역할이 제거됩니다.

vCenter 서버 인증서 갱신

ONTAP tools는 vCenter 인증서 만료일이 임박했거나 만료되었을 때 알림을 표시합니다. vCenter 인증서를 갱신한 후 다음 단계에 따라 새 인증서를 ONTAP tools에 업로드하십시오.

1. ONTAP 도구 원격 진단 셀에 로그인합니다.
2. 진단 셀에서 갱신된 vCenter 인증서를 가져옵니다.

```
echo | openssl s_client connect <vcenter>:443 2>&1 | sed -n '/-BEGIN
CERTIFICATE/,/END CERTIFICATE/p'
```

3. 인증서가 Base 64 ASCII 형식이고 시작 및 끝 줄이 포함되어 있는지 확인하십시오. 예를 들면 다음과 같습니다.

```

---{}BEGIN CERTIFICATE{}---
MIIFUzCCA7ugAwIBAgIJANogLapcl5oSMA0GCSqGSIb3DQEBCwUAMIGJMqwwCgYD
VQQDDAN2YzExFDASBgoJkiaJk/IsZAEZFgRkZW1vMRUwEwYKczImiZPyLQBGRIYF
bG9jYWwxZzAjbGVBAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRwwGgYDVQQK
DBN2YzEuZGVtby5uZXRhcHAuY29tMQwwCgYDVQQLDANMT0QwHhcNMjQwNDA1MTgw
NTE4WhcNMjYwNDA1MTgwNTE4WjBzMRwwGgYDVQQDDBN2YzEuZGVtby5uZXRhcHAu
Y29tMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcn5pYTESMBAGA1UEBwwJ
UGFsbyBBbHRvMQ8wDQYDVQQKDAZOZXRhYXN0ZXRhYXN0ZXRhYXN0ZXRhYXN0ZXRh
KoZiHvcNAQEBBQADgGAPADCCAYoCggGBALU8OCWMtA2gvIC/OTw/7xucvPVuM+b8
DhzvNpQ2phjfr6ctEhbntPpqPdu+t2CKK7l0mzg3D9cJ/rvMvdDDXr0tgaDloi2u
ZDW0CaF0QhLopNfRXMoogBZ66csEhViAy3CHTcOse770mA/PyoHgrCPZngVLZiiQ
TIWpdQMbEEzFIkrLfc70UW2MzfublrsH7Dn/kOu/iCSlVJWixKf7SmZtVQ5ZxBTD
UlJSiqoXleRXGyunArEvrIpOY9kkKXUElm3hGnk/ZmiuBJ+HqUYqYW+H+7vE3lKa
6NEqDX+tZotxTx2bXMjeiIWU30ZbshgeXlIG9qc49clBoC9iGjavhctOcaXg/W3h
dLKK5ds3rpRERgMg6VMkrfiqAJuiq+b3sTvXMAul/3hL7hz5QABAE/hP4ZvIHV02
WWDQRLiuVFAcDAyvCrO9Irx0Gk1RyRShKYakdWxZ3hhMdLuGq0yvRXqolIb94zwO
JfBJHjFTOA/GqwromZgiTzJkKq5xbN8MFwIDAQABo4HSMIHPMAsGA1UdDwQEAwIF
4DA7BgNVHREENDAYgRVlbWFpbEBkZW1vLm5ldGFwcC5jb22HBMCoAB+CE3ZjMS5k
ZW1vLm5ldGFwcC5jb20wHQYDVRO0BBYEFJ0V0zY+JRpFrEt3lovAY4BLFXmAMB8G
A1UdIwQYMBAAAFENf6fRWF3OJQNTPIduPk6kjA78MEMGCCsGAQUFBwEBBDcwNTAz
BggrBgEFBQcwAoYnaHR0cHM6Ly92YzEuZGVtby5uZXRhcHAuY29tL2FmZC92ZWZl
L2NhMA0GCSqGSIb3DQEBCwUAA4IBgQBaDfK7GBM4vmhzYCqGrr6KB+h3qeTJ+Y0Y
5nIPRP1HucawDQ8QTay605ddJ8gFGoxkOQDn9tdXWXGjnTRFOT8R+Hw/nUfVSiDP
sYienbl6copzUNwtqh+m9Ifow74Gf+ulRzEC0EAV01X/nTEYH6NKM6Wy7y7F8g5J
lrpM3JY90ZChMqHO3Av/88rbErfQ/gU1brJ3u9Gks4e20Z7Ff312ZKhWRuJDln2Z
0tc/gp90N9GxaVvELovq/pdjaZ8xiXCxa6piicrJd9WnqMHlgmXP2PIBDxMDBWBG
gwsfs5H7VG9MJYks6lViNsGclo0EwEdF0MfoB3JtsWpPWq6+jBua0Jm7/aFCU+Ht
mykr0gaV7muegoiBQuDma4EkAI3lD7ZlUgJQaw157NTk4RW3TFcbtViBHJkM54Hr
iVm0cl+2BZni/QTMh/MkVW2dYXJ3NuNlqqfzFY+bUfkzkR4SneMk0HX3joNNYDJv
siO7bL+k/Pxql27NVIhuCoVJAAlCI7ak=
---{}END CERTIFICATE{}---

```

- 출력 결과를 복사하여 바탕화면에 .pem 확장자를 가진 텍스트 파일로 저장하세요.
- 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
- 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
- 사이드바에서 해당 vCenter Server 인스턴스를 선택하십시오.
- 수정하려는 vCenter Server 옆의 세로 점 세 개(...)를 선택한 다음 *수정*을 선택합니다.
- vCenter** 수정 창에서 사용자 이름, 암호 및 포트 정보를 입력합니다.
- 인증서를 업로드하고 *수정*을 선택합니다.

관련 정보

"원격 진단 액세스 구성"

ONTAP 도구 인증서 관리

ONTAP 도구 및 VASA Provider 배포 시 기본적으로 자체 서명 인증서가 생성됩니다. ONTAP 도구 관리자 인터페이스를 사용하여 이 인증서를 갱신하거나 사용자 지정 CA 인증서로 교체할 수 있습니다. 여러 vCenter 배포 환경에서는 사용자 지정 CA 인증서를 사용해야 합니다.

시작하기 전에

시작하기 전에 다음 사항을 준비해야 합니다.

- 가상 IP 주소에 매핑된 도메인 이름입니다.
- 도메인 이름에 대한 nslookup이 성공적으로 완료되어 올바른 IP 주소로 확인됩니다.
- 도메인 이름과 ONTAP tools IP 주소로 생성된 인증서.



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



CA 서명 인증서에서 자체 서명 인증서로 전환할 수는 없습니다.

ONTAP tools 인증서 업그레이드

ONTAP tools 탭에는 인증서 유형(자체 서명/CA 서명) 및 도메인 이름과 같은 세부 정보가 표시됩니다. 배포 시 기본적으로 자체 서명 인증서가 생성됩니다. 인증서를 갱신하거나 CA 인증서로 업그레이드할 수 있습니다.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 인증서를 갱신하려면 인증서 > **ONTAP tools** > *갱신*을 선택하십시오.

인증서가 만료되었거나 만료일이 임박한 경우 갱신할 수 있습니다. 갱신 옵션은 CA 서명 인증서 유형에만 사용 가능합니다. 팝업 창에서 서버 인증서, 개인 키, 루트 CA 및 중간 인증서 정보를 입력하십시오.



인증서가 갱신될 때까지 시스템은 오프라인 상태가 되며, ONTAP tools Manager 인터페이스에서 로그아웃됩니다.

4. 자체 서명 인증서를 사용자 지정 CA 인증서로 업그레이드하려면 인증서 > **ONTAP tools** > **CA**로 업그레이드 옵션을 선택하십시오.
 - a. 팝업 창에서 서버 인증서, 서버 인증서 개인 키, 루트 CA 인증서 및 중간 인증서 파일을 업로드하십시오.
 - b. 이 인증서를 생성한 로드 밸런서 IP의 FQDN을 입력하고 인증서를 업그레이드하십시오.



업그레이드가 완료될 때까지 시스템은 오프라인 상태가 되며, ONTAP tools Manager 인터페이스에서 로그아웃됩니다.

VASA Provider 인증서 업그레이드

ONTAP tools for VMware vSphere는 VASA Provider용 자가 서명 인증서와 함께 배포됩니다. 이 경우 vVols 데이터스토어에 대해 하나의 vCenter Server 인스턴스만 관리할 수 있습니다. 여러 vCenter Server 인스턴스를 관리하고 해당 인스턴스에서 vVols 기능을 활성화하려면 자가 서명 인증서를 사용자 정의 CA 인증서로 변경해야 합니다.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 인증서를 갱신하려면 인증서 > **VASA Provider** 또는 **ONTAP tools** > *갱신*을 선택하십시오.
4. 자체 서명 인증서를 사용자 지정 CA 인증서로 업그레이드하려면 인증서 > **VASA Provider** 또는 **ONTAP tools** > *CA로 업그레이드*를 선택하십시오.
 - a. 팝업 창에서 서버 인증서, 서버 인증서 개인 키, 루트 CA 인증서 및 중간 인증서 파일을 업로드하십시오.
 - b. 이 인증서를 생성한 로드 밸런서 IP의 FQDN을 입력하고 인증서를 업그레이드하십시오.



업그레이드가 완료될 때까지 시스템은 오프라인 상태가 되며, ONTAP tools Manager 인터페이스에서 로그아웃됩니다.

VMware vSphere 유지 관리 콘솔용 ONTAP tools에 액세스합니다

ONTAP 도구 유지 관리 콘솔에 대해 알아보십시오

ONTAP tools for VMware vSphere의 유지 관리 콘솔을 사용하면 애플리케이션, 시스템 및 네트워크 설정을 관리할 수 있습니다. 관리자 및 유지 관리 암호를 업데이트하고, 지원 번들을 생성하고, 로그 수준을 구성하고, TLS 설정을 관리하고, 원격 진단을 활성화할 수 있습니다.

ONTAP tools for VMware vSphere를 배포한 후 유지 관리 콘솔에 액세스할 수 없는 경우 vCenter Server에서 VMware 도구를 설치하십시오. 배포 시 설정한 maint 사용자 이름과 암호를 사용하여 로그인합니다. 유지 관리 또는 루트 로그인 콘솔에서 *nano*를 사용하여 파일을 편집하십시오.



원격 진단을 활성화하는 동안 diag 사용자의 암호를 설정해야 합니다.

배포된 ONTAP tools for VMware vSphere의 요약 탭을 사용하여 유지 관리 콘솔에 액세스해야 합니다.  을 선택하면 유지 관리 콘솔이 시작됩니다.

콘솔 메뉴	옵션
애플리케이션 구성	1. 서버 상태 요약 표시 2. ONTAP tools 서비스의 로그 레벨 변경 3. 인증서 유효성 검사 플래그 변경
시스템 구성	1. 가상 머신 재부팅 2. 가상 머신 종료 3. 'maint' 사용자 암호 변경 4. 시간대 변경 5. jail 디스크 크기 늘리기(/jail) 6. 업그레이드 7. VMware Tools 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 셸 액세스 2. 원격 진단 액세스 활성화 3. 백업을 위해 vCenter 자격 증명을 제공하십시오. 4. 백업 수행
---------	---

ONTAP tools에 대한 원격 진단 액세스 구성

ONTAP tools for VMware vSphere를 구성하여 diag 사용자에게 대한 SSH 액세스를 활성화할 수 있습니다.

시작하기 전에

vCenter Server 인스턴스에 VASA 공급자 확장 기능을 활성화하십시오.

이 작업 정보

SSH를 사용하여 diag 사용자 계정에 액세스하는 데에는 다음과 같은 제한 사항이 있습니다.

- SSH 활성화 시 로그인 계정은 하나만 허용됩니다.
- 다음 중 하나가 발생하면 diag 사용자 계정에 대한 SSH 액세스가 비활성화됩니다.
 - 시간이 만료되었습니다.

로그인 세션은 다음 날 자정(밤 12시)에 만료됩니다.

- SSH를 사용하여 diag 사용자로 다시 로그인합니다.

단계

1. vCenter 서버에서 VASA Provider 콘솔을 엽니다.
2. 유지보수 사용자로 로그인합니다.
3. Enter `4`를 입력하여 *지원 및 진단*을 선택합니다.
4. `2`를 입력하여 *원격 진단 액세스 활성화*를 선택합니다.
5. 확인 대화 상자에 `y`을 입력하여 원격 진단 액세스를 활성화합니다.
6. 원격 진단 액세스를 위한 비밀번호를 입력하십시오.

다른 ONTAP tools 노드에서 SSH를 시작하세요

업그레이드하기 전에 다른 노드에서 SSH를 시작해야 합니다.

시작하기 전에

vCenter Server 인스턴스에 VASA 공급자 확장 기능을 활성화하십시오.

이 작업 정보

업그레이드하기 전에 각 노드에서 이 절차를 반복하십시오.

단계

1. vCenter 서버에서 VASA Provider 콘솔을 엽니다.
2. 유지보수 사용자로 로그인합니다.
3. Enter `4`를 눌러 지원 및 진단을 선택합니다.
4. Enter `1`를 눌러 Access diagnostic shell을 선택합니다.
5. 진행하려면 `y`을(를) 입력하세요.
6. `sudo systemctl restart ssh` 명령을 실행합니다.

ONTAP tools에서 vCenter Server 자격 증명 업데이트

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

시작하기 전에

유지보수 사용자 로그인 자격 증명이 필요합니다.

이 작업 정보

vCenter Server 자격 증명을 배포 후 변경한 경우 이 절차를 사용하여 업데이트하십시오.

단계

1. vCenter 서버에서 VASA Provider 콘솔을 엽니다.
2. 유지보수 사용자로 로그인합니다.
3. Enter `2`를 입력하여 시스템 구성 메뉴를 선택합니다.
4. vCenter 자격 증명을 변경하려면 `8`을 입력하십시오.

ONTAP tools에서 인증서 유효성 검사 플래그를 변경합니다

기본적으로 인증서 유효성 검사 플래그는 활성화(true로 설정)되어 있습니다. SAN 인증서 검사를 건너뛰어야 하는 경우 ONTAP 스토리지 백엔드 인증서 유효성 검사 플래그를 false로 설정할 수 있습니다. 이 설정은 vCenter Server 인증서에는 적용되지 않습니다.

시작하기 전에

유지보수 사용자 로그인 자격 증명이 필요합니다.

단계

1. vCenter 서버에서 ONTAP tools 콘솔을 엽니다.
2. 유지보수 사용자로 로그인합니다.
3. Enter `1`를 눌러 애플리케이션 구성 메뉴를 선택합니다.
4. Enter 3 인증서 유효성 검사 플래그를 변경합니다.

유지 관리 콘솔은 인증서 유효성 검사 플래그 상태를 표시하고 변경하도록 안내합니다.

5. 플래그를 켜려면 'y'를 입력하고, 취소하려면 'n'을 입력하세요.

인증서 유효성 검사 플래그를 활성화(true로 설정)하면 ONTAP tools는 모든 스토리지 백엔드가 SAN(Subject Alternative Name)이 포함된 인증서를 사용하는지 확인합니다. 백엔드 중 하나라도 SAN이 없는 인증서를 사용하는 경우 인증서 유효성 검사를 활성화할 수 없습니다. 이 플래그를 활성화하기 전에 모든 스토리지 백엔드가 SAN 기반 인증서를 사용하는지 확인하십시오. 인증서 유효성 검사 플래그를 비활성화(false로 설정)하면 ONTAP tools는 구성된 모든 스토리지 백엔드에 대해 인증서 유효성 검사를 건너뛰니다.

스토리지 백엔드용 **SAN** 기반 인증서를 확인합니다

안전한 통신과 적절한 유효성 검사를 보장하기 위해 모든 스토리지 백엔드가 SAN 기반 인증서를 사용하는지 확인하십시오.

1. ONTAP 관리 인증서에 Subject Alternative Name(SAN) 항목이 포함되어 있는지 확인하십시오.
2. SAN 항목이 ONTAP 관리 IP 주소 또는 DNS 이름 또는 둘 다와 일치하는지 확인하십시오.
3. ONTAP를 온보딩하는 데 사용된 세부 정보가 인증서의 SAN 항목에 있는 IP 주소 또는 DNS 이름과 일치하는지 확인하십시오.

이러한 단계를 따르면 인증서 유효성 검사 문제를 방지하고 ONTAP 시스템이 안전하게 통합되도록 보장할 수 있습니다.

다음 샘플 인증서는 디코딩된 정보를 보여줍니다.

```
HG8u6GK r2JJonWe/kjoKTUnkjuW7feDI747RUuFrthcvTDqhBNWL76jihNp1VX7
v0SDWMAVdecTeU1X/1X3qMxIL+tU4p9SbKVpQw6hjM/zi0LNC784EYIOSQ7qVob
6f21mfP0JHbqs5fLim9NFFUu2DQIDAQA8oQw0jBABgNVHREEEOT43hwShsSHdKXsgI9z
dGkyMjAtdnNpbS1zcjA1MWUtY2OuY2Rs LmdkbC5lbmdsYWJuZKThcPHauY29nt
BgkqhkiG9wQBAQsFAAOCCAQAEEagptz11RN7PLuJUo-SSQExBsF5/3JHr0+sSIMZDzm
4P24kxbQZbfryy68itKGF4LeAid0hgyxc3y9iv4zKlx8SfLNgITnVqAe8'KYNoyD6
IEWppDUE0eVNZIZQjrz9QjUAAF9ifjq8+SKr'lphoXnYYUiM6utvobPMG8cR8Gca
jiLibiMM01K6rD7Ng+7+ydUCAwBQwMDDwdn8+7RIRdKgwqX9QDLegcC5IL5WFLwbMc
2GBv8VM839m0KUAKXSDGwJBZ5nSHQdNi7MU3AES7Nzkv63kGEQJT/5Wr1DmOwlf
osl4qeeeMRigrAbFL6EHMsOMSP0521rtTrJrjBooB22r0tyDA--
-----END CERTIFICATE-----
```

Certificate Information:

- ✓ Common Name: **test.xyz.com**
- ✓ Subject Alternative Names: IP Address: **xxx.xx.xxx.xxx**, **test.xyz.com**
- ✓ Organization: Self-signed-certificate
- ✓ Organization Unit:
- ✓ Locality: N/A
- ✓ State: N/A
- ✓ Country: XX
- ✓ Valid From: March 8, 2026
- ✓ Valid To: March 7, 2028
- ✓ Issuer: **test.xyz.com**, Self-signed-certificate
- ✓ Serial Number: 640c2752bd2c972c5775180070cfdd2120809ee

ONTAP tools 보고서

ONTAP tools for VMware vSphere 플러그인은 가상 머신 및 데이터스토어에 대한 보고서를 제공합니다. vCenter 클라이언트의 바로 가기 섹션에서 NetApp ONTAP tools for VMware vSphere 플러그인 아이콘을 선택하면 사용자 인터페이스가 개요 페이지로 이동합니다. 가상 머신 및 데이터스토어 보고서를 보려면 Reports 탭을 선택하십시오.

가상 머신 보고서는 검색된 가상 머신 목록(ONTAP 스토리지 기반 데이터스토어의 디스크가 하나 이상 있어야 함)과 성능 지표를 보여줍니다. 가상 머신 레코드를 확장하면 디스크 관련 데이터스토어 정보가 모두 표시됩니다.

데이터스토어 보고서에는 ONTAP 스토리지를 사용하는 ONTAP tools for VMware vSphere가 검색하거나 인식한 데이터스토어와 성능 지표가 나열됩니다.

'열 관리' 옵션을 사용하여 여러 열을 숨기거나 표시할 수 있습니다.

가상 머신 관리

ONTAP tools를 사용한 가상 머신 마이그레이션 및 복제 시 고려 사항

ONTAP tools for VMware vSphere는 컴퓨팅 전용(vMotion), 스토리지 전용(Storage vMotion) 및 모든 데이터스토어에 걸친 컴퓨팅 및 스토리지 결합 마이그레이션을 포함하여 모든 주요 유형의 가상 머신 마이그레이션을 지원합니다. 이 항목에서는 기본 데이터스토어 유형에 관계없이 가상 머신의 성공적인 마이그레이션 및 복제를 보장하기 위한 주요 고려 사항과 모범 사례를 설명합니다.

보호된 가상 머신 마이그레이션

보호된 가상 머신을 다음 위치로 마이그레이션할 수 있습니다.

- 다른 ESXi 호스트의 동일한 데이터 저장소
- 동일한 ESXi 호스트에 있는 다른 호환 데이터 저장소
- 다른 ESXi 호스트에 있는 호환 가능한 다른 데이터 저장소

가상 머신을 다른 FlexVol 볼륨으로 마이그레이션하면 시스템은 해당 볼륨의 메타데이터 파일을 가상 머신 정보로 업데이트합니다. 가상 머신을 다른 ESXi 호스트로 마이그레이션하되 스토리지는 동일하게 유지하는 경우, 기본 FlexVol 볼륨의 메타데이터 파일은 수정되지 않습니다.

가상 머신 마이그레이션에 대한 자세한 내용은 Broadcom 설명서를 참조하십시오. "[vSphere 가상 머신 마이그레이션](#)"

보호된 가상 머신 클론 생성

보호된 가상 머신을 다음 위치로 복제할 수 있습니다.

- 복제 그룹을 사용하는 동일한 FlexVol 볼륨의 동일한 컨테이너

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

- 복제 그룹을 사용하는 다른 FlexVol 볼륨의 동일한 컨테이너

복제된 가상 머신이 배치된 FlexVol 볼륨에서 메타데이터 파일이 복제된 가상 머신 세부 정보로 업데이트됩니다.

- 다른 컨테이너 또는 vVols 데이터 저장소

복제된 가상 머신이 배치된 FlexVol 볼륨에서 메타데이터 파일이 가상 머신 세부 정보로 업데이트됩니다.

VMware는 현재 VM 템플릿으로 복제된 가상 머신을 지원하지 않습니다.

보호된 가상 머신의 클론의 클론이 지원됩니다.

자세한 내용은 Broadcom 설명서 "[클론 작업을 위한 가상 머신 생성](#)"를 참조하십시오.

가상 머신 스냅샷

ONTAP tools는 표준 VMware 워크플로를 통해 가상 머신 스냅샷을 지원합니다. 스냅샷은 테스트 및 패치 준비와 같은

사용 사례를 위한 단기 롤백 지점입니다. 스냅샷은 백업 또는 복제 기반 데이터 보호를 대체하는 것이 아닙니다. 스냅샷에서 가상 머신을 장기간 실행하면 불안정성 및 데이터 손실이 발생할 수 있습니다.

지원되는 모든 데이터스토어 유형에서 크래시 일관성 스냅샷(메모리 상태가 없는 스냅샷으로, 가상 머신을 일관된 상태로 다시 시작하는 데 사용할 수 있음)을 생성할 수 있습니다. VMware Tools를 사용하여 캡처하기 전에 메모리 내 데이터를 디스크에 플러시하는 정지 스냅샷도 지원됩니다. 스냅샷 유형 및 동작에 대한 개요는 "[vSphere의 가상 머신 스냅샷 개요](#)"를 참조하십시오.



메모리 스냅샷은 실행 중인 메모리 상태를 캡처하고 가상 머신을 일시적으로 중단시킵니다. ONTAP tools 워크플로에서는 지원되지 않습니다. 가상 머신에 메모리 스냅샷이 있는 경우 ONTAP tools에서 관리하는 일관성 그룹 또는 호스트 클러스터 관계에 가상 머신을 포함하기 전에 삭제해야 합니다.

ASA r2 스토리지 시스템에서 가상 머신 스냅샷의 동작은 다른 스토리지 유형과 다릅니다. 스냅샷은 읽기 전용입니다. 가상 머신을 시작하면 VASA Provider는 읽기 전용 스냅샷에서 LUN을 생성하고 IOPS를 활성화합니다. 가상 머신을 끄면 VASA Provider는 LUN을 삭제하고 IOPS를 비활성화합니다.

가상 머신 스냅샷 관리에 대한 자세한 내용은 Broadcom 설명서 "[스냅샷으로 가상 머신 관리](#)"를 참조하십시오.

ONTAP tools에서 가상 머신을 vVols 데이터 저장소로 마이그레이션합니다

NFS 및 VMFS 데이터스토어에서 Virtual Volumes(vVols) 데이터스토어로 가상 머신을 마이그레이션하면 정책 기반 VM 관리 및 기타 vVols 기능을 활용할 수 있습니다. vVols 데이터스토어를 사용하면 증가하는 워크로드 요구 사항을 충족할 수 있습니다.

시작하기 전에

마이그레이션할 가상 머신에서 VASA Provider가 실행 중인지 확인하십시오. VASA Provider가 실행 중인 가상 머신을 vVols 데이터스토어로 마이그레이션하면 vVols 데이터스토어에 있는 가상 머신의 전원을 켜는 것을 포함한 어떠한 관리 작업도 수행할 수 없습니다.

이 작업 정보

NFS 및 VMFS 데이터스토어에서 vVols 데이터스토어로 마이그레이션할 때 vCenter Server는 vStorage VMFS 데이터스토어에서 데이터를 이동할 때는 VAAI(vStorage API for Array Integration) 오프로드를 사용하지만, NFS VMDK 파일에서 이동할 때는 사용하지 않습니다. VAAI 오프로드는 일반적으로 호스트의 부하를 줄여줍니다.

단계

1. 마이그레이션할 가상 머신을 마우스 오른쪽 버튼으로 클릭하고 *마이그레이션*을 선택합니다.
2. *저장 위치만 변경*을 선택한 다음 *다음*을 선택합니다.
3. 마이그레이션할 데이터스토어의 기능과 일치하는 가상 디스크 형식, VM 스토리지 정책 및 vVol 데이터스토어를 선택하십시오.
4. 설정을 검토하고 *완료*를 선택합니다.

ONTAP tools에서 VASA 구성을 정리합니다

VASA 정리 프로세스를 완료하려면 다음 단계를 따르십시오.



VASA 정리 작업을 시작하기 전에 vVols 데이터 저장소를 모두 제거하는 것이 좋습니다.

단계

1. https://OTV_IP:8143/Register.html로 이동하여 플러그인 등록을 해제합니다.
2. vCenter 서버에서 플러그인이 더 이상 사용 가능한 상태가 아닌지 확인하십시오.
3. VMware vSphere VM용 ONTAP tools를 종료합니다.
4. ONTAP tools for VMware vSphere VM을 삭제합니다.

ONTAP tools에서 VM에 데이터 디스크 연결 또는 분리

vSphere의 가상 머신에서 데이터 디스크를 연결하거나 분리하고 스토리지 리소스를 관리하려면 다음 단계를 따르십시오.

가상 머신에 데이터 디스크 연결

가상 머신에 데이터 디스크를 연결하여 스토리지를 추가합니다.

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 선택하십시오.
5. 연결할 디스크를 선택하고 확인 버튼을 선택하십시오.

결과

하드 디스크가 가상 하드웨어 장치 목록에 나타납니다.

가상 머신에서 데이터 디스크 분리

더 이상 필요하지 않은 데이터 디스크를 가상 머신에서 분리하십시오. 디스크는 삭제되지 않으며 ONTAP 스토리지 시스템에 유지됩니다.

단계

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



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

관련 정보

["가상 머신에 새 하드 디스크 추가하기"](#)

["기존 하드 디스크를 가상 머신에 추가"](#)

ONTAP tools에서 스토리지 시스템 및 호스트 검색

ONTAP tools for VMware vSphere가 vSphere Client에서 처음 실행되면 ESXi 호스트, 연결된 LUN 및 NFS 내보내기, 그리고 이러한 리소스를 소유하는 NetApp 스토리지 시스템을 자동으로 검색합니다.

시작하기 전에

- 모든 ESXi 호스트의 전원이 켜져 있고 네트워크에 연결되어 있는지 확인하십시오.
- 검색할 모든 스토리지 가상 머신(SVM)이 실행 중인지 확인하고, 각 클러스터 노드에 사용 중인 스토리지 프로토콜(NFS 또는 iSCSI)에 대해 하나 이상의 데이터 LIF가 구성되어 있는지 확인하십시오.

이 작업 정보

새로운 스토리지 시스템을 검색하거나 기존 시스템을 업데이트하여 최신 용량 및 설정 정보를 얻을 수 있습니다. 또한 스토리지 시스템 액세스를 위한 ONTAP tools for VMware vSphere 자격 증명을 변경할 수도 있습니다.

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

단계

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

확인 대화 상자에서 선택 사항을 확인하십시오.

3. 상태가 'Authentication Failure'인 검색된 스토리지 컨트롤러를 선택하고 작업 > *수정*을 선택합니다.
4. 스토리지 시스템 수정 대화 상자에 필요한 정보를 입력하십시오.
5. Authentication Failure 상태의 모든 스토리지 컨트롤러에 대해 4단계와 5단계를 반복합니다.

검색 프로세스가 완료되면 다음 작업을 수행하십시오.

- 어댑터 설정 열, MPIO 설정 열 또는 NFS 설정 열에 경고 아이콘이 표시되는 호스트에 대해 ONTAP tools for VMware vSphere를 사용하여 ESXi 호스트 설정을 구성하십시오.
- 스토리지 시스템 자격 증명을 제공하십시오.

ONTAP tools를 사용하여 ESXi 호스트 설정 수정

VMware vSphere의 ONTAP tools 대시보드를 사용하여 구성 문제를 식별하고, ESXi 호스트를 선택하고, NetApp 권장 설정을 검토하고 적용하십시오.

시작하기 전에

ESXi 호스트 시스템 포틀릿은 ESXi 호스트 설정 관련 문제를 표시합니다. 문제를 선택하면 호스트 이름 또는 IP 주소를 볼 수 있습니다.

단계

1. vSphere 클라이언트에 로그인합니다.

2. 바로가기 페이지에서 플러그인 섹션 아래에 있는 *NetApp ONTAP tools*를 선택합니다.
3. ONTAP tools for VMware vSphere 플러그인의 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 사용할 호스트를 선택하고 *다음*을 선택합니다.



ESXi 호스트를 확장하면 현재 값을 확인할 수 있습니다.

6. 설정 페이지에서 필요에 따라 권장 값을 선택하십시오.
7. 요약 창에서 값을 확인하고 *완료*를 선택합니다. 최근 작업 패널에서 진행 상황을 확인할 수 있습니다.

관련 정보

["ESXi 호스트 설정 구성"](#)

비밀번호 관리

ONTAP tools Manager 비밀번호 변경

ONTAP tools Manager를 사용하여 관리자 암호를 변경할 수 있습니다.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 화면 오른쪽 상단의 관리자 아이콘을 선택하고 *비밀번호 변경*을 선택합니다.
4. 비밀번호 변경 팝업 창에 기존 비밀번호와 새 비밀번호를 입력합니다. 사용자 인터페이스 화면에 비밀번호 요구 사항이 표시됩니다.
5. 변경 사항을 적용하려면 *변경*을 선택합니다.

ONTAP tools Manager 비밀번호 재설정

ONTAP tools Manager 암호를 잊어버린 경우, ONTAP tools for VMware vSphere 유지 관리 콘솔에서 생성된 재설정 토큰을 사용하여 관리자 액세스 권한을 복원할 수 있습니다.

단계

1. 웹 브라우저를 열고 `https://<ONTAPtoolsIP>:8443/virtualization/ui/` 로 이동하여 ONTAP tools Manager에 액세스합니다.
2. 로그인 페이지에서 *비밀번호 재설정*을 선택합니다.
3. ONTAP tools for VMware vSphere 유지 관리 콘솔을 사용하여 암호 재설정 토큰을 생성합니다.
 - a. vCenter 서버에 로그인하고 유지 관리 콘솔을 엽니다.
 - b. Enter `2`를 눌러 *시스템 구성*을 선택하십시오.
 - c. Enter `3`를 눌러 *maint* 사용자 암호 변경*을 선택합니다.

4. 암호 재설정 대화 상자에서 재설정 토큰, 사용자 이름 및 새 암호를 입력합니다.
5. 자격 증명을 업데이트하려면 *재설정*을 선택하세요.
6. 새 비밀번호를 사용하여 ONTAP tools Manager에 로그인하십시오.

ONTAP tools에서 애플리케이션 사용자 암호 재설정

ONTAP tools for VMware vSphere를 사용하여 vCenter Server에 SRA 및 VASA Provider를 등록하는 데 필요한 애플리케이션 사용자 비밀번호를 재설정하려면 다음 단계를 수행하십시오.

단계

1. 웹 브라우저를 열고 다음 주소로 이동하세요: <https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. ONTAP tools 배포 중에 구성된 관리자 자격 증명을 사용하여 로그인하십시오.
3. 사이드바에서 *설정*을 선택합니다.
4. **VASA/SRA** 자격 증명 페이지에서 *비밀번호 재설정*을 선택하십시오.
5. 새 비밀번호를 입력하고 확인합니다.
6. 새 비밀번호를 적용하려면 *재설정*을 선택합니다.

ONTAP tools 유지 관리 콘솔 암호를 재설정합니다

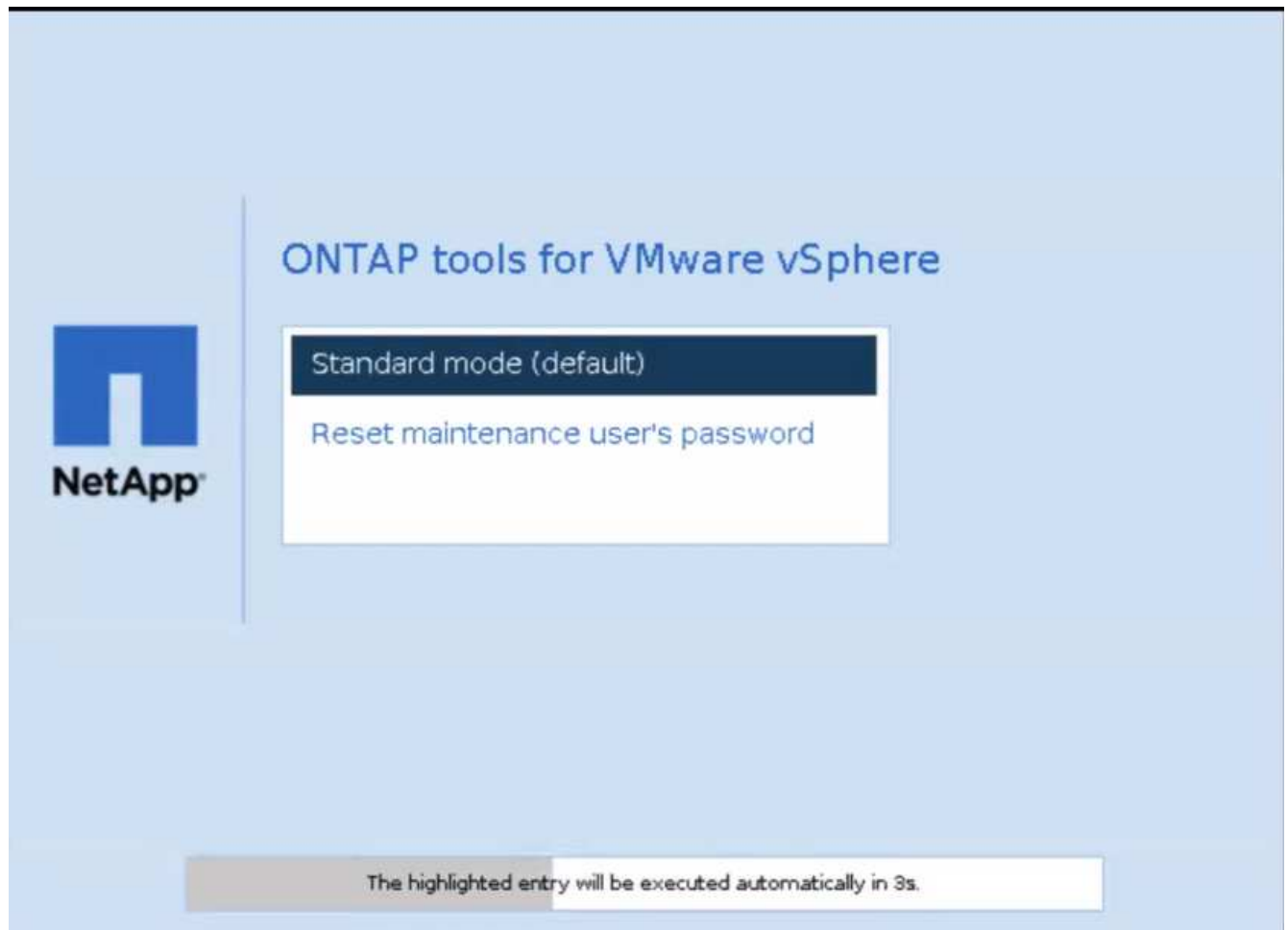
게스트 OS 재시작 작업 중에 GRUB 메뉴에 유지 관리 콘솔 사용자 암호를 재설정하는 옵션이 표시됩니다. 이 옵션을 사용하여 VM의 유지 관리 콘솔 사용자 암호를 업데이트하십시오. 암호를 재설정하면 VM이 재시작되어 새 암호가 설정됩니다. HA 배포 시나리오에서 VM이 재시작되면 나머지 두 VM의 암호도 자동으로 업데이트됩니다.



ONTAP tools for VMware vSphere HA 배포의 경우 ONTAP tools 관리 노드(node1)에서 유지 관리 콘솔 사용자 암호를 변경해야 합니다.

단계

1. vCenter 서버에 로그인합니다.
2. 가상 머신을 마우스 오른쪽 버튼으로 클릭하고 전원 > *게스트 OS 다시 시작*을 선택합니다. 시스템이 다시 시작되면 다음 화면이 나타납니다:



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

3. 유지 관리 사용자 암호 재설정 옵션을 선택합니다. 유지보수 콘솔이 열립니다.
4. 콘솔에서 새 비밀번호를 입력하고 확인하십시오. 세 번 시도할 수 있습니다. 새 비밀번호를 성공적으로 입력하면 시스템이 다시 시작됩니다.
5. 계속하려면 **Enter** 키를 누르십시오. 시스템이 VM의 암호를 업데이트합니다.



가상 머신을 켜면 동일한 GRUB 메뉴가 나타납니다. 하지만 암호 재설정 옵션은 **Restart Guest OS** 옵션과 함께 사용해야 합니다.

호스트 클러스터 보호 관리

ONTAP tools에서 보호된 호스트 클러스터를 수정합니다.

단일 워크플로에서 호스트 클러스터의 보호 설정을 변경할 수 있습니다. 지원되는 변경 사항은 다음과 같습니다.

- 보호된 클러스터에 새 데이터 저장소 또는 호스트를 추가합니다.
- 보호 설정에 새로운 SnapMirror 관계를 추가합니다.
- 보호 설정에서 기존 SnapMirror 관계를 삭제합니다.

- 기존 SnapMirror 관계를 수정합니다.



호스트 클러스터에 대한 보호를 생성, 편집 또는 삭제한 후에는 변경 사항을 반영하기 위해 스토리지 검색을 수행해야 합니다. 스토리지 검색을 수행하지 않으면 주기적인 스토리지 검색이 트리거된 후에 변경 사항이 반영됩니다.

호스트 클러스터 보호 모니터링

보호 대상 호스트 클러스터별로 보호 상태, SnapMirror 관계, 데이터 저장소 및 SnapMirror 상태를 모니터링합니다.

단계

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

보호 열에는 보호 상태를 나타내는 아이콘이 표시됩니다.

3. 아이콘 위에 마우스를 올리면 자세한 내용을 볼 수 있습니다.

새 데이터스토어 또는 호스트 추가

보호된 클러스터에 호스트를 추가하거나 vCenter 사용자 인터페이스를 사용하여 데이터 저장소를 생성합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 보호된 클러스터의 속성을 편집하려면 다음 방법 중 하나를 사용할 수 있습니다.
 - a. **NetApp ONTAP tools** > 보호 > *호스트 클러스터 관계*로 이동하여 클러스터 옆에 있는 줄임표 메뉴를 선택하고 *편집*을 선택하거나
 - b. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools* > *클러스터 보호*를 선택합니다.
3. vCenter 사용자 인터페이스에서 데이터스토어를 생성하면 보호되지 않은 상태로 표시됩니다. 클러스터의 모든 데이터스토어와 해당 보호 상태는 대화 상자에서 확인할 수 있습니다. 보호를 활성화하려면 보호 버튼을 선택하십시오.



vCenter Server 사용자 인터페이스에서 데이터스토어를 생성한 후 개요 페이지에서 *검색*을 선택하여 호스트 클러스터에서 해당 데이터스토어를 보호 후보로 표시합니다. 보호 상태는 다음 주기적인 보호 검색 후에 보호됨으로 업데이트됩니다.

4. 새 ESXi 호스트를 추가하면 보호 상태가 부분적으로 보호됨으로 표시됩니다. SnapMirror 설정에서 점 세 개 메뉴를 선택하고 *편집*을 선택하여 새로 추가된 ESXi 호스트의 근접도를 설정하십시오.



비동기 관계의 경우, 3차 사이트의 대상 SVM을 동일한 인스턴스에 추가할 수 없으므로 ONTAP tools에서 편집이 지원되지 않습니다. 관계 구성을 수정하려면 System Manager 또는 대상 SVM의 CLI를 사용하십시오.

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

ONTAP tools는 vCenter 작업을 생성하며, 최근 작업 패널에서 해당 작업의 진행 상황을 추적할 수 있습니다.

새로운 **SnapMirror** 관계 추가

단계

1. vSphere 클라이언트에 로그인합니다.
2. 보호된 클러스터의 속성을 편집하려면 다음 방법 중 하나를 사용할 수 있습니다.
 - a. **NetApp ONTAP tools** > 보호 > *호스트 클러스터 관계*로 이동하여 클러스터 옆의 줄임표 메뉴를 선택하고 *편집*을 선택하거나
 - b. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools* > *클러스터 보호*를 선택합니다.
3. *관계 추가*를 선택합니다.
4. 새로운 관계를 비동기 또는 **AutomatedFailOverDuplex** 정책 유형으로 추가합니다.
5. *보호*를 선택합니다.

클러스터 보호 창에서 변경 사항을 확인할 수 있습니다.

ONTAP tools는 vCenter 작업을 생성하며, 최근 작업 패널에서 해당 작업의 진행 상황을 추적할 수 있습니다.

기존 **SnapMirror** 관계 삭제

SnapMirror 비동기 관계를 삭제하려면 보조 사이트의 SVM 또는 클러스터가 ONTAP tools for VMware vSphere에 스토리지 백엔드로 추가되어 있어야 합니다. 모든 SnapMirror 관계를 한 번에 삭제할 수는 없습니다. 관계를 삭제하면 해당 관계가 ONTAP 클러스터에서도 제거됩니다. 자동 장애 조치 이중화 SnapMirror 관계를 삭제하면 시스템에서 대상 데이터스토어의 매핑을 해제하고 대상 ONTAP 클러스터에서 일관성 그룹, LUN, 볼륨 및 iGroup을 삭제합니다.

관계를 삭제하면 시스템은 2차 사이트를 다시 스캔하여 매핑되지 않은 LUN을 호스트에서 활성 경로로 제거합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 보호된 클러스터의 속성을 편집하려면 다음 방법 중 하나를 사용할 수 있습니다.
 - a. **NetApp ONTAP tools** > 보호 > *호스트 클러스터 관계*로 이동하여 클러스터 옆의 줄임표 메뉴를 선택하고 *편집*을 선택하거나
 - b. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools* > *클러스터 보호*를 선택합니다.
3. SnapMirror 설정에서 줄임표 메뉴를 선택하고 *삭제*를 선택합니다.
 - 보호된 호스트 클러스터의 비동기 정책 유형 기반 관계를 삭제하는 경우, 3차 스토리지 클러스터에서 스토리지 요소를 수동으로 제거해야 합니다. 스토리지 요소에는 일관성 그룹, 볼륨(ONTAP 시스템의 경우), 스토리지 단위(LUN/네임스페이스) 및 스냅샷이 포함됩니다.
 - 보호 대상 호스트 클러스터의 자동 장애 조치 이중화(AFD) 정책 기반 관계를 삭제하는 경우, 인터페이스에서 직접 2차 스토리지의 관련 스토리지 요소를 제거하도록 선택할 수 있습니다.
 - 자동 장애 조치 이중화(AFD) 정책 기반 관계를 삭제하고 일관성 그룹이 애플리케이션 수준 백업을 위해 계층 구조로 변경된 경우 백업 영향에 대한 경고가 표시됩니다. 계속하려면 확인하십시오. 확인 후 2차 스토리지에서 연결된 스토리지 요소를 삭제하십시오. 삭제하지 않으면 해당 요소가 보조 사이트에 남아 있습니다.

ONTAP tools는 vCenter 작업을 생성하며, 최근 작업 패널에서 해당 작업의 진행 상황을 추적할 수 있습니다.

기존 SnapMirror 관계 수정

SnapMirror 비동기 관계를 수정하려면 보조 사이트 SVM 또는 클러스터가 ONTAP tools for VMware vSphere의 스토리지 백엔드로 추가되어 있는지 확인하십시오. 자동 장애 조치 이중화 SnapMirror 관계의 경우 균일 구성의 경우 호스트 근접성을 업데이트하거나 비균일 구성의 경우 호스트 액세스를 업데이트할 수 있습니다. 비동기 및 자동 장애 조치 이중화 정책 유형 간 변경은 지원되지 않습니다. 클러스터에서 새로 검색된 호스트에 대한 근접성 또는 액세스 설정을 구성할 수 있습니다.



기존 SnapMirror 비동기 관계는 편집할 수 없습니다.

단계

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

ONTAP tools는 vCenter 작업을 생성합니다. 최근 작업 패널에서 진행 상황을 추적합니다.

ONTAP tools에서 호스트 클러스터 보호 제거

호스트 클러스터 보호를 제거하면 데이터 저장소가 보호되지 않은 상태가 됩니다.

단계

1. 보호된 호스트 클러스터 목록을 보려면 * NetApp ONTAP tools* > 보호 > *호스트 클러스터 관계*로 이동하십시오.

이 페이지에서는 보호 대상 호스트 클러스터, 보호 상태, SnapMirror 관계 및 상태를 모니터링할 수 있습니다. 일관성 그룹을 선택하여 용량, 연결된 데이터 저장소 및 하위 그룹을 볼 수 있습니다.

2. 호스트 클러스터 보호 창에서 클러스터 옆에 있는 점 세 개 메뉴를 선택하고 *보호 제거*를 선택합니다.
 - SnapMirror 비동기 관계만 있는 호스트 클러스터에서 보호 기능을 제거하는 경우 스토리지 요소를 수동으로 삭제해야 합니다. 스토리지 요소에는 일관성 그룹, 볼륨(ONTAP 시스템의 경우), 스토리지 단위(LUN) 및 스냅샷이 포함됩니다.
 - 자동 장애 조치 이중화 기반 SnapMirror 정책 관계와 비계층 일관성 그룹만 있는 호스트 클러스터에서 보호를 제거하면 동일한 화면에서 직접 2차 스토리지의 연결된 스토리지 요소를 삭제할 수 있습니다.
 - SnapMirror 정책과 백업용 계층적 일관성 그룹이 모두 적용된 호스트 클러스터에서 보호 기능을 제거하면 백업에 미치는 영향에 대한 경고가 표시됩니다. 계속하려면 확인을 클릭하십시오. 확인 후 2차 스토리지에서 연결된 스토리지 요소를 삭제하십시오. 삭제하지 않으면 스토리지 요소가 보조 사이트에 남아 있습니다.

ONTAP tools 설정 복구

ONTAP tools for VMware vSphere 10.5부터 백업 기능이 기본적으로 활성화되어 있습니다.

ONTAP tools for VMware vSphere 가상 머신을 배포하는 데이터 저장소에 백업 파일이 저장됩니다. ONTAP tools의 IP 주소(점은 밑줄로 대체되고 *OTV_backup* 접미사가 붙음)로 이름이 지정된 폴더에는 가장 최근의 백업 파일 두 개 (*OTV_backup_1.tar.enc* 및 *OTV_backup_2.tar.enc*)와 최신 백업 이름이 포함된 정보 파일(*OTV_backup_info.txt*)이 저장됩니다.

새 가상 머신이 동일한 ONTAP tools IP 주소를 사용하고 활성화된 서비스, 노드 크기 및 HA 모드를 포함하여 초기 시스템 구성과 일치하는지 확인하십시오.

단계

1. 원래 가상 머신의 데이터 저장소에서 백업 파일을 로컬 시스템으로 다운로드하십시오.
 - a. 저장소 섹션으로 이동하여 가상 머신의 백업 파일이 포함된 데이터 저장소를 선택하십시오.
 - b. 파일 섹션을 선택합니다.
 - c. 필요한 백업 디렉토리를 다운로드하십시오.
2. 기존 가상 머신의 전원을 끄십시오. 그런 다음, 원래 배포에 사용했던 것과 동일한 OVA 파일을 사용하여 새 가상 머신을 배포하십시오.
3. vCenter 서버에서 유지 관리 콘솔을 엽니다.
4. 유지보수 사용자로 로그인합니다.
5. Enter `4`를 입력하여 *지원 및 진단*을 선택합니다.
6. `2`를 입력하여 원격 진단 액세스 활성화 옵션을 선택하고 진단 액세스에 사용할 새 암호를 생성하십시오.
7. 다운로드한 디렉토리에서 백업 파일을 선택하십시오. 최신 백업을 확인하려면 *OTV_backup_info.txt* 파일을 참조하십시오.
8. 다음 명령어를 사용하여 백업 파일을 새 가상 머신으로 전송하십시오. 메시지가 나타나면 진단 암호를 입력하십시오.

```
scp <OTV_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 마십시오.

9. 백업 파일 전송이 완료되면 진단 셸에 로그인하여 다음 명령을 실행하십시오.

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

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

복구가 완료되면 ONTAP tools가 서비스와 vCenter 개체를 복원합니다.

ONTAP 도구를 제거합니다

ONTAP tools for VMware vSphere를 제거하면 도구에 저장된 모든 데이터가 삭제됩니다.

단계

1. ONTAP tools for VMware vSphere 관리형 데이터스토어에서 모든 가상 머신을 제거하거나 이동합니다.
 - 가상 머신을 제거하려면 다음을 참조하십시오 ["가상 머신 및 가상 머신 템플릿 제거 및 재등록"](#)
 - 관리되지 않는 데이터 저장소로 이동하려면 다음을 참조하십시오 ["Storage vMotion으로 가상 머신을 마이그레이션하는 방법"](#)
2. ["데이터 저장소 삭제"](#) ONTAP tools for VMware vSphere에서 생성되었습니다.
3. VASA 공급자를 활성화한 경우 ONTAP 도구에서 설정 > **VASA** 공급자 설정 > *등록 해제*를 선택하여 모든 vCenter 서버에서 VASA 공급자의 등록을 해제하십시오.
4. vCenter Server 인스턴스에서 모든 스토리지 백엔드를 연결 해제합니다. ["vCenter Server 인스턴스와 스토리지 백엔드 연결을 해제합니다."](#)을 참조하십시오.
5. 모든 스토리지 백엔드를 삭제합니다. ["스토리지 백엔드 관리"](#)을 참조하십시오.
6. VMware Live Site Recovery에서 SRA 어댑터를 제거합니다.
 - a. 포트 5480을 사용하여 VMware Live Site Recovery 어플라이언스 관리 인터페이스에 admin으로 로그인하십시오.
 - b. *Storage Replication Adapters*를 선택하십시오.
 - c. 해당 SRA 카드를 선택하고 드롭다운 메뉴에서 *삭제*를 선택합니다.
 - d. 어댑터 삭제 결과를 확인한 후 *삭제*를 선택합니다.
7. ONTAP tools for VMware vSphere에 온보딩된 vCenter 서버 인스턴스를 삭제하십시오. ["vCenter Server 인스턴스 관리"](#)을 참조하십시오.
8. vCenter Server에서 ONTAP tools for VMware vSphere VM의 전원을 끄고 VM을 삭제합니다.

다음 단계는 무엇입니까?

["FlexVol 볼륨 제거"](#)

ONTAP tools 제거 후 FlexVol 볼륨 제거

VMware 배포를 위한 ONTAP tools for VMware에 전용 ONTAP 클러스터를 사용하는 경우 사용되지 않는 FlexVol 볼륨이 많이 생성됩니다. VMware vSphere용 ONTAP tools for VMware를 제거한 후 성능 저하를 방지하려면 FlexVol 볼륨을 삭제해야 합니다.

단계

1. ONTAP tools 관리 노드 VM에서 VMware vSphere용 ONTAP tools 배포 유형을 확인합니다. 다음 명령을 실행하여 배포 유형을 확인하십시오. `cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocol`

iSCSI 배포 환경이라면 igroup도 삭제해야 합니다.
2. FlexVol 볼륨 목록을 가져옵니다. `kubect! describe persistentvolumes | grep internalName | awk -F='{' '{print $2}'`

3. vCenter Server에서 VM을 제거합니다. 을(를) 참조하십시오. ["가상 머신 및 가상 머신 템플릿 제거 및 재등록"](#)
4. FlexVol 볼륨을 삭제합니다. 자세한 내용은 ["FlexVol 볼륨 삭제"](#)을 참조하십시오. 볼륨을 삭제하려면 CLI 명령에 정확한 FlexVol 볼륨 이름을 입력하십시오.
5. iSCSI 배포 시 ONTAP 스토리지 시스템에서 SAN igroup을 삭제하십시오. 을(를) 참조하십시오. ["SAN 이니시에이터 및 igroup 보기 및 관리"](#)

ONTAP tools for VMware vSphere 업그레이드

VMware vSphere 10.x용 ONTAP tools에서 10.5으로 업그레이드

ONTAP tools for VMware vSphere 10.3 또는 10.4에서 10.5로 업그레이드할 수 있습니다. 하지만 ONTAP tools 10.0, 10.1 또는 10.2에서 10.5로 업그레이드하려면 먼저 10.3 또는 10.4로 업그레이드한 후 10.5로 진행해야 합니다.



- ASA r2 시스템의 경우, 추가 스토리지 가용성 영역(SAZ)을 설정하기 전에 VMware vSphere용 ONTAP tools를 10.5로, ONTAP을 9.16.1로 업그레이드해야 합니다.
- ONTAP tools for VMware vSphere 10.3 또는 10.4에서 10.5으로의 업그레이드가 실패하면 롤백할 수 없습니다. 설정을 복원하려면 낮은 RPO 또는 스냅샷 복구를 사용하십시오. ONTAP tools for VMware vSphere 10.2 이하 버전의 경우, 설정을 복원하려면 zero-RPO를 사용하십시오.

시작하기 전에

- 모든 노드가 활성화되어 있는지 확인하십시오.
- ONTAP 시스템 인증서와 온보딩된 vCenter 인증서의 유효 기간이 최소 5일 이상인지 확인하십시오. 인증서가 더 빨리 만료되면 업그레이드가 실패합니다.
- 모든 노드에 100GB 용량의 다섯 번째 디스크가 있는지 확인하십시오.
- 노드 구성이 아래 표의 사양과 일치하는지 확인하십시오.

배포 유형	노드당 CPU(Core)	노드당 메모리(GB)	노드당 디스크 공간(GB)	총 CPU(코어)	메모리(GB)	총 디스크 공간(GB)
비HA 소형	9	18	350	9	18	350
비-HA 중간	13	26	350	13	26	350
HA Small	9	18	350	27	54	1050
HA Medium	13	26	350	39	78	1050
HA Large	17	34	350	51	102	1050

- CPU와 RAM에 대한 핫 플러그인이 활성화되어 있는지 확인하십시오.
- 낮은 RPO 백업을 활성화하고 vCenter 클라이언트 인터페이스에 백업이 하나 이상 표시되는지 확인하십시오. 업그레이드 전에 백업 폴더를 다운로드하십시오.
- 낮은 RPO 백업을 권장합니다. 하지만 비 HA 배포에서는 업그레이드 전에 ONTAP tools 가상 머신의 정지된 스냅샷을 생성할 수 있습니다.

백업 및 복구에 대한 자세한 내용은 "[백업 설정 편집](#)" 및 "[ONTAP tools 설정 복구](#)"를 참조하십시오.

단계

1. ONTAP tools for VMware vSphere 업그레이드 ISO를 콘텐츠 라이브러리에 업로드합니다.
2. 기본 VM 페이지에서 작업 > *설정 편집*을 선택합니다. 기본 VM 이름을 확인하려면 다음을 수행합니다.
 - a. 모든 노드에서 진단 셀 활성화

b. 다음 명령을 실행합니다.

```
grep sourceHost /opt/netapp/meta/ansible_vars.yaml
```

3. 편집 설정 창의 **CD/DVD** 드라이브 필드에서 *콘텐츠 라이브러리 ISO 파일*을 선택하십시오.
4. ISO 파일을 선택하고, **CD/DVD** 드라이브 필드의 연결됨 확인란을 선택한 다음 *확인*을 클릭합니다.
5. vCenter 서버에서 ONTAP tools 콘솔을 엽니다.
6. 유지보수 사용자로 로그인합니다.
7. **2***를 입력하여 ***System Configuration** 메뉴를 선택하십시오.
8. **6***을 입력하여 *업그레이드 옵션을 선택합니다.
9. 메시지가 표시되면 vCenter 자격 증명을 제공하십시오. 이는 ONTAP tools가 호스팅되는 vCenter 인스턴스입니다.

ONTAP 도구를 두 개의 vCenter Server 토폴로지(어플라이언스가 하나의 vCenter 인스턴스에서 호스팅되고 다른 인스턴스를 관리하는 경우)에서 사용하는 경우, ONTAP 도구를 호스팅하는 vCenter 인스턴스에 제한된 역할을 할당할 수 있습니다. OVF 템플릿 배포에 필요한 권한만 있는 전용 vCenter 사용자 및 역할을 생성할 수 있습니다. 자세한 내용은 "[ONTAP tools for VMware vSphere 10에 포함된 역할](#)"에 나열된 역할을 참조하십시오.

ONTAP tools로 관리할 vCenter 인스턴스의 경우, vCenter 사용자 계정에 관리자 권한이 있는지 확인하십시오.

업그레이드 과정에서 온보딩된 스토리지 백엔드 인증서 중 SAN(Subject Alternative Name) 항목이 누락된 경우, 누락된 SAN을 나타내는 메시지가 표시됩니다. SAN 유효성 검사를 하지 않고 업그레이드를 진행하더라도 보안 위험이 발생할 수 있으므로 권장하지 않습니다.

10. 업그레이드 시 다음 작업이 자동으로 수행됩니다.
 - a. 게이트웨이 인증서는 1년 유효기간으로 갱신됩니다. 기존 SRA 어댑터를 제거하고 새 10.5 어댑터를 업로드하면 SRA 인증서의 유효기간이 10년에서 1년으로 변경됩니다.
 - b. 원격 플러그인이 업그레이드되었습니다.
 - c. ONTAP 및 vCenter Server 인증서가 검증되어 ONTAP tools에 추가됩니다
 - d. 백업이 활성화되었습니다.

다음 단계

ONTAP tools for VMware vSphere 10.5으로 업그레이드한 후:

- 시스템 알림을 모니터링하고 게이트웨이 인증서가 1년 후 만료되기 전에 갱신할 계획을 세우십시오.
- ONTAP tools 10.4 또는 10.3 SRA 어댑터를 제거하고 10.5 SRA 어댑터 tar 파일을 업로드하십시오.
- SRA 어댑터 tar 파일을 업로드한 후 설치 명령을 실행하십시오. 그런 다음 SRA 어댑터를 다시 스캔하여 VMware Site Recovery Storage Replication Adapters 페이지를 업데이트하십시오.

업그레이드 후에는 다음을 수행할 수 있습니다.

- 관리자 사용자 인터페이스에서 서비스 비활성화
- 고가용성(HA) 구성이 아닌 상태에서 고가용성(HA) 구성으로 전환하기
- 비HA 소규모 구성을 비HA 중규모로, 또는 HA 중규모 또는 대규모 구성으로 확장합니다.

관련 정보

"[ONTAP tools for VMware vSphere 9.xx에서 10.5으로 마이그레이션](#)"

ONTAP tools 업그레이드 오류 코드

ONTAP tools for VMware vSphere 업그레이드 작업 중 오류 코드가 발생할 수 있습니다. 오류 코드는 5자리 숫자로 구성되며, 앞의 두 자리는 문제가 발생한 스크립트를 나타내고, 뒤의 세 자리는 해당 스크립트 내의 특정 워크플로를 나타냅니다.

모든 오류 로그는 문제를 쉽게 추적하고 해결할 수 있도록 ansible-perl-errors.log 파일에 기록됩니다. 이 로그 파일에는 오류 코드와 실패한 Ansible 작업이 포함됩니다.



이 페이지에 제공된 오류 코드는 참고용일 뿐입니다. 오류가 계속 발생하거나 해결 방법이 제시되지 않은 경우 지원팀에 문의하십시오.

다음 표에는 오류 코드와 해당 파일 이름이 나열되어 있습니다.

오류 코드	스크립트 이름
00	firstboot-network-config.pl, mode deploy
01	firstboot-network-config.pl, 업그레이드 모드
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, 비HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

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

업그레이드 오류 코드	워크플로우	해결 방법
052	ISO 파일은 현재 버전과 동일하거나 현재 버전보다 두 단계 위의 버전일 수 있습니다.	현재 버전에서 업그레이드하려면 호환되는 ISO 버전을 사용하십시오.
068	데비안 패키지 롤백이 실패했습니다.	RPO가 0이거나 스냅샷 기반 복구를 사용하고 업그레이드를 재시도하십시오.
069	파일 복원에 실패했습니다	RPO가 0이거나 스냅샷 기반 복구를 사용하고 업그레이드를 재시도하십시오.
070	백업 삭제 실패	-
071	Kubernetes 클러스터가 정상적이지 않습니다.	-

업그레이드 오류 코드	워크플로우	해결 방법
074	ISO 마운트에 실패했습니다.	/var/log/upgrade-run.log 파일을 확인하고 업그레이드를 다시 시도하십시오.
075	업그레이드 사전 검사에 실패했습니다	업그레이드를 다시 시도하십시오.
076	레지스트리 업그레이드에 실패했습니다	RPO가 0이거나 스냅샷 기반 복구를 사용하고 업그레이드를 재시도하십시오.
077	레지스트리 롤백이 실패했습니다.	RPO가 0이거나 스냅샷 기반 복구를 사용하고 업그레이드를 재시도하십시오.
078	운영자 업그레이드에 실패했습니다	RPO가 0이거나 스냅샷 기반 복구를 사용하고 업그레이드를 재시도하십시오.
079	운영자 롤백이 실패했습니다	RPO가 0이거나 스냅샷 기반 복구를 사용하고 업그레이드를 재시도하십시오.
080	서비스 업그레이드가 실패했습니다.	RPO가 0이거나 스냅샷 기반 복구를 사용하고 업그레이드를 재시도하십시오.
081	서비스 롤백이 실패했습니다	RPO가 0이거나 스냅샷 기반 복구를 사용하고 업그레이드를 재시도하십시오.
082	컨테이너에서 이전 이미지를 삭제하지 못했습니다.	RPO가 0이거나 스냅샷 기반 복구를 사용하고 업그레이드를 재시도하십시오.
083	백업 삭제에 실패했습니다	RPO가 0이거나 스냅샷 기반 복구를 사용하고 업그레이드를 재시도하십시오.
084	JobManager를 프로덕션으로 되돌리는 작업이 실패했습니다.	업그레이드를 복구/완료하려면 다음 단계를 수행하십시오. 1. 진단 셸을 활성화합니다. 2. 다음 명령을 실행합니다. <code>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade 3. /var/log/post-deploy-upgrade.log에서 로그를 확인합니다.</code>
087	업그레이드 후 단계에 실패했습니다.	업그레이드를 복구/완료하려면 다음 단계를 수행하십시오. 1. 진단 셸을 활성화합니다. 2. <code>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</code> 명령을 실행합니다. 3. /var/log/post-deploy-upgrade.log에서 로그를 확인합니다.

업그레이드 오류 코드	워크플로우	해결 방법
088	journald에 대한 로그 로테이션 구성에 실패했습니다.	VM이 호스팅되는 호스트와 호환되는 VM 네트워크 설정을 확인하십시오. VM을 다른 호스트로 마이그레이션한 후 다시 시작해 볼 수 있습니다.
089	요약 로그 순환 설정 파일의 소유권 변경에 실패했습니다.	업그레이드를 다시 시도하십시오.
095	OS 업그레이드 실패	OS 업그레이드에 대한 복구는 없습니다. ONTAP tools 서비스가 업그레이드되고 새로운 Pod가 실행될 예정입니다.
096	동적 스토리지 프로비저너 설치	업그레이드 로그를 확인하고 업그레이드를 다시 시도하십시오.
097	업그레이드를 위한 서비스 제거에 실패했습니다.	RPO가 0이거나 스냅샷 기반 복구를 사용하고 업그레이드를 재시도하십시오.
098	ntv-system에서 동적 스토리지 프로비저너 네임스페이스로 dockercréd secret을 복사하는 데 실패했습니다.	업그레이드 로그를 확인하고 업그레이드를 다시 시도하십시오.
099	새 HDD 추가에 대한 유효성 검사에 실패했습니다.	고가용성(HA) 구성의 경우 모든 노드에 새 HDD를 추가하고, 비고가용성(non-HA) 구성의 경우 하나의 노드에 추가합니다.
109	영구 볼륨 데이터 백업에 실패했습니다.	업그레이드 로그를 확인하고 업그레이드를 다시 시도하십시오.
110	영구 볼륨 데이터 복원에 실패했습니다.	RPO가 0이거나 스냅샷 기반 복구를 사용하고 업그레이드를 재시도하십시오.
111	RKE2의 etcd 타임아웃 매개변수 업데이트에 실패했습니다.	업그레이드 로그를 확인하고 업그레이드를 다시 시도하십시오.
112	동적 스토리지 프로비저너 제거에 실패했습니다	-
113	보조 노드의 리소스 새로 고침에 실패했습니다.	업그레이드 로그를 확인하고 업그레이드를 다시 시도하십시오.
104	보조 노드 재시작에 실패했습니다.	노드를 하나씩 수동으로 재시작합니다.
100	커널 롤백이 실패했습니다	-
051	동적 스토리지 프로비저너 업그레이드가 실패했습니다	업그레이드 로그를 확인하고 업그레이드를 다시 시도하십시오.
056	마이그레이션 백업 삭제에 실패했습니다.	NA

업그레이드 오류 코드	워크플로우	해결 방법
090	스토리지 백엔드 및 vCenter에 대한 인증서 유효성 검사가 실패했습니다.	업그레이드 로그와 /var/log/cert_validation_error.log의 로그 파일을 확인하고 업그레이드를 다시 시도하십시오.

업그레이드 오류 코드	워크플로우	해결 방법
114	MongoDB 컬렉션의 내부 인증서 업데이트가 실패했습니다	업그레이드가 오류 코드 114와 함께 실패하는 경우 다음 단계를 수행하십시오. 1. 운영 노드에서 업그레이드 ISO에 연결하고 진단 셀을 활성화하십시오. 2. SSH 세션에서 운영 노드에 ISO를 마운트합니다. <pre>sudo mount /dev/cdrom sudo mount -o loop,ro /dev/cdrom/APPLIANCE_UPGRADE.bin /upgrade</pre> 3. Debian 패키지 설치: <pre>sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vplatform.deb sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vpupgrader.deb sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vmware-tools.deb</pre> 4. 빌드 정보 파일을 복사합니다. <pre>sudo cp /upgrade/APPLIANCE_BUILD /</pre> 5. 진단 셀을 활성화하고 다음을 실행하여 컬렉션에 인증서를 추가합니다.



ONTAP tools for VMware vSphere 10.3부터는 제로 RPO가 지원되지 않습니다.

자세히 알아보기 "버전 10.0에서 10.1로 업그레이드가 실패한 경우 ONTAP tools for VMware vSphere를 복원하는 방법"

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

```
`/var/log/otvng/pos
t-deploy-
upgrade.log`에서
로그를 확인하십시오.
```

6. 노드를 재부팅합니다.

```
sudo bash
/home/maint/scripts
/vault_decrypt.sh
cd
/home/maint/rke2-pb
sudo ansible-
playbook site.yaml
--tags
restart_nodes
--skip-tags
debian_upgrade,kern
el_upgrade,rescan_s
csi_bus,source_iso,
eject_upgrade,mount
Iso,upgradeNodes,re
gistryUpg,deleteOld
Images,wait,checkRe
achability,delete_o
tv_cr,uninstall_tri
dent,del_trident_im
ages,refresh_resour
ces,ntp_configure,n
tpd_uninstall
```

7. 업그레이드 후 단계를 수행하십시오.

ONTAP tools for VMware vSphere 9.xx를 10.5으로 마이그레이션

ONTAP tools for VMware vSphere 9.xx에서 10.5으로 마이그레이션

NetApp ONTAP tools for VMware vSphere 설정을 버전 9.xx에서 10.5로 이전하려면 버전 간 주요 제품 업데이트 및 개선 사항으로 인해 마이그레이션 프로세스가 필요합니다.

ONTAP tools for VMware vSphere 9.12D1, 9.13D2 및 9.13P2 릴리스에서 ONTAP tools for VMware vSphere 10.5으로 마이그레이션할 수 있습니다.

설정에 NFS 및 VMFS 데이터 저장소가 있고 vVols 데이터 저장소가 없는 경우 ONTAP tools 9.xx를 제거하고 ONTAP tools 10.5를 구축하기만 하면 됩니다. 그러나 설정에 vVols 데이터 저장소가 포함된 경우 VASA Provider 및 SRA를 마이그레이션하는 프로세스를 거쳐야 합니다.

다음 표는 이 두 가지 시나리오에서 마이그레이션 프로세스를 간략하게 설명합니다.

설정에 vVols 데이터스토어가 있는 경우	설정에 NFS 및 VMFS 데이터스토어만 포함된 경우
단계: 1. " VASA Provider 마이그레이션 " 2. " VM 스토리지 정책 생성 "	단계: 1. 사용자 환경에서 ONTAP tools 9.xx를 제거합니다. " 환경에서 OTV 9.xx를 제거하는 방법 " NetApp 기술 자료 문서를 참조하십시오. 2. " ONTAP tools for VMware vSphere 10.5 배포 및 구성 " 3. " SRA 업데이트 " 4. " VM 스토리지 정책 생성 "



ONTAP tools for VMware vSphere 9.xx에서 10.5으로 마이그레이션한 후, ONTAP tools 10.5은 NVMe-oF 프로토콜을 VMFS 데이터스토어에서만 지원하기 때문에 NVMe/FC 프로토콜을 사용하는 vVols 데이터스토어가 작동하지 않게 됩니다.

VASA Provider를 마이그레이션하고 ONTAP tools에서 SRA를 업데이트합니다.

이 섹션의 단계에 따라 VASA Provider를 ONTAP tools for VMware vSphere 9.xx에서 ONTAP tools for VMware vSphere 10.5로 마이그레이션하고 VMware Live Site Recovery 어플라이언스의 Storage Replication Adapter(SRA)를 업데이트하십시오.

VASA Provider 마이그레이션 단계

1. 기존 ONTAP tools for VMware vSphere에서 Derby PORT 1527을 활성화하려면 루트 사용자를 활성화하고 SSH를 통해 CLI에 로그인하십시오. 그런 다음 다음 명령을 실행하십시오.

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. VMware vSphere용 ONTAP tools 10.5 OVA를 배포합니다.

3. 마이그레이션할 vCenter Server 인스턴스를 ONTAP tools for VMware vSphere 10.5 릴리스에 추가하십시오. 자세한 내용은 ["vCenter Server 인스턴스 추가"](#)를 참조하십시오.

4. **"VASA Provider 활성화"** ONTAP tools for VMware vSphere 10.5의 서비스입니다.

5. vCenter 서버 API를 사용하여 ONTAP 도구 플러그인의 스토리지 백엔드를 로컬로 온보딩합니다. 자세한 내용은 ["vSphere 클라이언트 인터페이스를 사용하여 스토리지 백엔드 추가"](#)를 참조하십시오.

6. REST API 요청을 인증하기 위한 액세스 토큰을 획득하십시오. 다음 예제를 참조하여 변수 값을 사용자 환경에 맞게 변경하십시오.

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

```
curl --request POST \
  --location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/vcenter-
login" \
  --header "Content-Type: application/json" \
  --header "Accept: */*" \
  -d '{"username": "$MYUSER", "password": "$MYPASSWORD", "vcenter
hostname": "$MYVCENTER"}'
```

응답에 포함된 액세스 토큰을 복사하여 저장하십시오.

성공 메시지를 찾습니다.
Completed post 10.5
upgrade steps.

7. 마이그레이션을 위해 Swagger 또는 Postman에서 다음 API를 실행하십시오.

9. ISO를 꺼냅니다.

```
curl -X POST
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migra
tion-jobs`
```

다음 URL을 통해 Swagger에 액세스할 수 있습니다: [https://\\$FQDN_IP_PORT/](https://$FQDN_IP_PORT/) 예를 들어:
<https://10.67.25.33:8443/>.

```
/dev/cdrom
sudo eject
/dev/cdrom
```

10. 운영 노드를 재부팅합니다.

```
sudo reboot -f
```

HTTP 메서드 및 엔드포인트

이 REST API 호출은 다음 메서드와 엔드포인트를 사용합니다.

HTTP 방식	경로
POST	/api/v1

처리 유형

비동기

Curl 예시

```
curl -X POST 'https://<OTV-NG-IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs' \
--header 'x-auth: <auth_token>' \
--header 'Content-Type: application/json' \
--data '{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxxx",
    "password": "*****"
  },
  "database_password": "*****"
}'
```

다른 릴리스 마이그레이션을 위한 요청 본문:

```
{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxxx",
    "password": "*****"
  }
}
```

JSON 출력 예시

시스템에서 작업 객체가 반환됩니다. 다음 단계에서 사용할 작업 식별자를 저장하십시오.

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

8. Swagger에서 상태를 확인하려면 다음 URI를 사용하십시오.

```
curl
`https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobId
>?includeSubJobsAndTasks=true`
```

이전 단계에서 마이그레이션 작업으로부터 반환된 'id' 값을 사용하십시오. 작업이 완료되면 작업 응답에서 마이그레이션 보고서를 검토하십시오.

9. VASA Provider를 ONTAP tools for VMware vSphere에 등록합니다. 지침은 "[VASA Provider 등록](#)"을 참조하십시오.
10. VASA Provider 등록을 확인하십시오:
 - a. vSphere Client에서 vCenter Server로 이동합니다.
 - b. 구성 > *스토리지 공급자*를 선택합니다.
 - c. 이전 단계에서 등록한 VASA Provider가 온라인 상태인지 확인하십시오.
11. 다음 단계를 사용하여 VMware vSphere 스토리지 공급자 9.10/9.11/9.12/9.13 VASA Provider 서비스에 대한 ONTAP tools for VMware vSphere를 중지하십시오.
 - a. ONTAP tools 9.x에서 웹 콘솔을 엽니다.
 - b. 유지보수 콘솔에 액세스합니다.
 - c. `1`를 눌러 애플리케이션 구성 메뉴를 선택하십시오.
 - d. `5`를 입력하여 VASA Provider 및 SRA 서비스를 중지하십시오.
 - e. vSphere Client에서 vCenter Server로 이동한 다음 **Configure** > *Storage Providers*를 선택합니다.
 - f. ONTAP tools 9.x용 오프라인 VASA Provider를 선택하고 *Remove*를 선택합니다.

기존 VASA Provider가 중지되면 vCenter Server가 ONTAP tools for VMware vSphere로 페일오버됩니다. 모든 데이터스토어와 VM은 ONTAP tools for VMware vSphere에서 액세스 가능하며 제공됩니다.
12. 마이그레이션된 NFS 및 VMFS 데이터스토어는 데이터스토어 검색 작업(최대 30분 소요)이 완료된 후 ONTAP tools for VMware vSphere 10.5에 나타납니다. 개요 페이지에서 데이터스토어의 표시 여부를 확인하십시오.
13. Swagger 또는 Postman에서 다음 API를 사용하여 패치 마이그레이션을 수행하십시오.

HTTP 메서드 및 엔드포인트

이 REST API 호출은 다음 메서드와 엔드포인트를 사용합니다.

HTTP 방식	경로
PATCH	/api/v1

처리 유형

비동기

Swagger에서 다음 URI를 사용하십시오.

```
curl -X PATCH
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_id>/migration-jobs/<migration_id>`
```

HTTP 메서드 및 엔드포인트

이 REST API 호출은 다음 메서드와 엔드포인트를 사용합니다.

HTTP 방식	경로
PATCH	/api/v1

처리 유형

비동기

Swagger에서 다음 URI를 사용하십시오.

```
curl -X PATCH
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_id>/migration-jobs/<migration_id>`
```

Curl 예시

```
curl -X PATCH
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/d50073ce-35b4-4c51-9d2e-4ce66f802c35`
```

JSON 출력 예시

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```



7단계에서 반환된 'migration_id' 값을 PATCH API 호출에서 <migration_id>로 사용합니다. 패치 작업의 경우 요청 본문은 비어 있습니다.



UUID는 post-migrate API에 대한 응답으로 반환되는 마이그레이션 UUID입니다.

패치 마이그레이션 API를 실행한 후 모든 VM이 스토리지 정책을 준수합니다.

다음 단계

마이그레이션을 완료하고 ONTAP tools 10.5를 vCenter Server에 등록한 후 다음 단계를 따르십시오.

- *검색*이 완료될 때까지 기다리면 시스템이 모든 호스트의 인증서를 자동으로 갱신합니다.
- 데이터 저장소 및 가상 머신 작업을 시작하기 전에 잠시 기다리십시오. 대기 시간은 호스트, 데이터 저장소 및 가상 머신 수에 따라 달라집니다. 기다리지 않고 작업을 시작하면 간헐적인 오류가 발생할 수 있습니다.

업그레이드 후 가상 머신의 규정 준수 상태가 최신 상태가 아닌 경우 다음 단계를 사용하여 스토리지 정책을 다시 적용하십시오.

1. 데이터 저장소로 이동하여 요약 > *VM 스토리지 정책*을 선택합니다.
2. 시스템에서 **VM** 스토리지 정책 준수 상태가 *최신 상태가 아님*으로 표시됩니다.
3. 스토리지 VM 정책과 해당 VM을 선택합니다.
4. *적용*을 선택합니다.
5. **VM** 스토리지 정책 준수 항목의 준수 상태가 준수로 표시됩니다.

관련 정보

- ["ONTAP tools for VMware vSphere 10 RBAC에 대해 알아보기"](#)
- ["VMware vSphere 10.x용 ONTAP tools에서 10.5으로 업그레이드"](#)

스토리지 복제 어댑터(SRA) 업데이트 단계

시작하기 전에

복구 계획에서 보호 사이트는 현재 VM이 실행 중인 위치를 나타내고, 복구 사이트는 VM이 복구될 위치를 나타냅니다. VMware Live Site Recovery 어플라이언스 인터페이스는 보호 사이트와 복구 사이트에 대한 세부 정보와 함께 복구 계획의 상태를 표시합니다. 복구 계획에서 CLEANUP 및 REPROTECT 버튼은 비활성화되어 있고 TEST 및 RUN 버튼은 활성화된 상태입니다. 이는 해당 사이트가 데이터 복구를 위해 준비되었음을 나타냅니다. SRA를 마이그레이션하기 전에 한 사이트는 보호 상태이고 다른 사이트는 복구 상태인지 확인하십시오.



페일오버가 완료되었지만 재보호가 보류 중인 경우 마이그레이션을 시작하지 마십시오. 마이그레이션을 진행하기 전에 재보호 프로세스가 완료되었는지 확인하십시오. 테스트 페일오버가 진행 중인 경우 테스트 페일오버를 정리하고 마이그레이션을 시작하십시오.

1. VMware Site Recovery에서 VMware vSphere 9.xx용 ONTAP tools SRA 어댑터를 삭제하려면 다음 단계를 따르십시오.
2. VMware Live Site Recovery 구성 관리 페이지로 이동합니다.
 - a. **Storage Replication Adapter** 섹션으로 이동하세요.
 - b. 줄임표 메뉴에서 *구성 재설정*을 선택합니다.
 - c. 줄임표 메뉴에서 *삭제*를 선택합니다.
3. 보호 사이트와 복구 사이트 모두에서 다음 단계를 수행하십시오.
 - a. "ONTAP tools for VMware vSphere 서비스 활성화"
 - b. "VMware Live Site Recovery 어플라이언스에서 SRA 구성"의 단계에 따라 VMware vSphere 10.5 SRA 어댑터용 ONTAP tools for VMware vSphere를 구성하십시오.
 - c. VMware Live Site Recovery 인터페이스에서 어레이 검색 및 *장치 검색*을 실행합니다. 마이그레이션 전과 같이 장치가 표시되는지 확인합니다.

REST API를 사용하여 자동화

ONTAP 도구 REST API에 대해 알아보십시오

ONTAP tools for VMware vSphere 10은 가상 머신 수명 주기 관리를 위한 도구 모음입니다. 여기에는 자동화 프로세스의 일부로 사용할 수 있는 강력한 REST API가 포함되어 있습니다.

REST 웹 서비스 기반

REST(Representational State Transfer)는 웹 서비스 API 설계 등 분산 웹 애플리케이션 개발을 위한 표준 스타일입니다. 서버 기반 리소스를 노출하고 해당 리소스의 상태를 관리하기 위한 일련의 기술을 정의합니다.

리소스 및 상태 표현

리소스는 REST 웹 서비스 애플리케이션의 기본 구성 요소입니다. REST API를 설계할 때 중요한 초기 작업 두 가지가 있습니다.

- 시스템 또는 서버 기반 리소스를 식별합니다.
- 리소스 상태 및 관련 상태 전환 작업을 정의합니다.

클라이언트 애플리케이션은 잘 정의된 메시지 흐름을 통해 리소스 상태를 표시하고 변경할 수 있습니다.

HTTP 메시지

HTTP(Hypertext Transfer Protocol)는 웹 서비스 클라이언트와 서버가 리소스에 대한 메시지를 교환하는 데 사용되는 프로토콜입니다. 생성(Create), 읽기(Read), 업데이트(Update), 삭제>Delete)라는 일반적인 작업을 기반으로 하는 CRUD 모델을 따릅니다. HTTP 프로토콜에는 요청 및 응답 헤더와 응답 상태 코드가 포함됩니다.

JSON 데이터 형식

다양한 메시지 형식이 있지만 가장 널리 사용되는 형식은 JavaScript Object Notation(JSON)입니다. JSON은 간단한 데이터 구조를 일반 텍스트로 표현하기 위한 업계 표준이며, 리소스와 원하는 동작을 설명하는 상태 정보를 전송하는 데 사용됩니다.

보안

보안은 REST API의 중요한 측면입니다. 네트워크를 통해 전송되는 HTTP 트래픽을 보호하는 데 사용되는 전송 계층 보안(TLS) 프로토콜 외에도, ONTAP tools for VMware vSphere 10 REST API는 인증을 위해 액세스 토큰을 사용합니다. 액세스 토큰을 획득하여 이후 API 호출에 사용해야 합니다.

비동기 요청 지원

ONTAP tools for VMware vSphere 10 REST API는 대부분의 요청을 동기적으로 처리하며, 작업이 완료되면 상태 코드를 반환합니다. 또한 완료하는 데 시간이 오래 걸리는 작업의 경우 비동기 처리도 지원합니다.

ONTAP tools Manager 환경

ONTAP tools Manager 환경에서 고려해야 할 몇 가지 측면이 있습니다.

가상 머신

ONTAP tools for VMware vSphere 10은 vSphere 원격 플러그인 아키텍처를 사용하여 배포됩니다. REST API 지원을 포함한 이 소프트웨어는 별도의 가상 머신에서 실행됩니다.

ONTAP tools IP 주소

ONTAP tools for VMware vSphere 10은 가상 머신의 기능에 대한 게이트웨이를 제공하는 단일 IP 주소를 노출합니다. 초기 구성 중에 해당 주소를 제공해야 하며, 이 주소는 내부 로드 밸런서 구성 요소에 할당됩니다. 이 주소는 ONTAP 도구 관리자 사용자 인터페이스에서 사용될 뿐만 아니라 Swagger 문서 페이지 및 REST API에 직접 액세스하는 데에도 사용됩니다.

두 개의 REST API

ONTAP tools for VMware vSphere 10 REST API 외에도 ONTAP 클러스터 자체에 REST API가 있습니다. ONTAP tools Manager는 ONTAP REST API를 클라이언트로 사용하여 스토리지 관련 작업을 수행합니다. 이 두 API는 서로 별개이며 구별된다는 점을 유념해야 합니다. 자세한 내용은 "[ONTAP 자동화](#)"를 참조하십시오.

ONTAP tools REST API 구현 세부 정보

REST는 공통된 기술과 모범 사례를 제시하지만, 각 API의 정확한 구현 방식은 설계 선택에 따라 달라질 수 있습니다. 따라서 ONTAP tools for VMware vSphere 10 REST API 설계 방식을 숙지한 후에 사용해야 합니다.

REST API에는 vCenters 및 애그리게이트와 같은 여러 리소스 범주가 포함되어 있습니다. 자세한 내용은 "[API 참조](#)"를 검토하십시오.

REST API에 액세스하는 방법

ONTAP tools for VMware vSphere 10 REST API는 포트와 함께 ONTAP tools IP 주소를 통해 액세스할 수 있습니다. 전체 URL은 다음과 같은 여러 부분으로 구성됩니다.

- ONTAP tools IP 주소 및 포트
- API 버전
- 리소스 카테고리
- 특정 리소스

초기 설정 시 IP 주소를 구성해야 하며, 포트는 8443으로 고정됩니다. URL의 앞부분은 각 ONTAP tools for VMware vSphere 10 인스턴스에서 동일하며, 엔드포인트 간에 리소스 범주와 특정 리소스만 변경됩니다.



아래 예시의 IP 주소와 포트 값은 설명 목적으로만 제시된 것입니다. 실제 사용 환경에 맞게 이 값을 변경해야 합니다.

인증 서비스에 액세스하는 예시

`https://10.61.25.34:8443/virtualization/api/v1/auth/login`

이 URL은 POST 방식을 사용하여 액세스 토큰을 요청하는 데 사용할 수 있습니다.

vCenter 서버 목록을 표시하는 예시

`https://10.61.25.34:8443/virtualization/api/v1/vcenters`

이 URL을 사용하면 GET 메서드를 통해 정의된 vCenter 서버 인스턴스 목록을 요청할 수 있습니다.

HTTP 세부 정보

ONTAP tools for VMware vSphere 10 REST API는 HTTP 및 관련 매개변수를 사용하여 리소스 인스턴스 및 컬렉션에 대한 작업을 수행합니다. HTTP 구현에 대한 자세한 내용은 아래에 나와 있습니다.

HTTP 메서드

REST API에서 지원하는 HTTP 메서드 또는 동사는 아래 표에 나와 있습니다.

방법	CRUD	설명
GET	읽기	리소스 인스턴스 또는 컬렉션의 객체 속성을 검색합니다. 컬렉션과 함께 사용할 경우 목록 작업으로 간주됩니다.
POST	생성	입력 매개변수를 기반으로 새로운 리소스 인스턴스를 생성합니다.
PUT	업데이트	제공된 JSON 요청 본문을 사용하여 전체 리소스 인스턴스를 업데이트합니다. 사용자가 수정할 수 없는 주요 값은 유지됩니다.
PATCH	업데이트	요청에서 선택한 변경 사항들을 리소스 인스턴스에 적용하도록 요청합니다.
삭제	삭제	기존 리소스 인스턴스를 삭제합니다.

요청 및 응답 헤더

다음 표는 REST API에서 사용되는 가장 중요한 HTTP 헤더를 요약한 것입니다.

헤더	유형	사용 참고 사항
수락	요청	이는 클라이언트 애플리케이션이 허용할 수 있는 콘텐츠 유형입니다. 유효한 값에는 <code>*/*</code> 또는 <code>application/json</code> 이 포함됩니다.
x-auth	요청	클라이언트 애플리케이션을 통해 요청을 보낸 사용자를 식별하는 액세스 토큰이 포함되어 있습니다.
Content-Type	응답	서버에서 <code>Accept</code> 요청 헤더를 기반으로 반환된 값입니다.

HTTP 상태 코드

REST API에서 사용되는 HTTP 상태 코드는 다음과 같습니다.

코드	의미	설명
200	OK	새로운 리소스 인스턴스를 생성하지 않는 호출의 경우 성공을 나타냅니다.
201	생성됨	리소스 인스턴스에 대한 고유 식별자를 가진 객체가 성공적으로 생성되었습니다.
202	수락됨	요청이 승인되었으며, 해당 요청을 처리하기 위한 백그라운드 작업이 생성되었습니다.
204	콘텐츠 없음	요청은 성공했지만 반환된 콘텐츠가 없습니다.
400	잘못된 요청	요청 입력값이 인식되지 않거나 부적절합니다.
401	무단	해당 사용자는 권한이 없으므로 인증해야 합니다.

코드	의미	설명
403	금지됨	권한 오류로 인해 액세스가 거부되었습니다.
404	찾을 수 없음	요청에서 참조한 리소스가 존재하지 않습니다.
409	충돌	객체가 이미 존재하므로 객체를 생성하지 못했습니다.
500	내부 오류	서버에서 일반적인 내부 오류가 발생했습니다.

인증

REST API에 대한 클라이언트 인증은 액세스 토큰을 사용하여 수행됩니다. 토큰 및 인증 프로세스의 주요 특징은 다음과 같습니다.

- 클라이언트는 ONTAP tools Manager 관리자 자격 증명(사용자 이름 및 비밀번호)을 사용하여 토큰을 요청해야 합니다.
- 토큰은 JSON 웹 토큰(JWT) 형식으로 구성됩니다.
- 각 토큰은 60분 후에 만료됩니다.
- 클라이언트의 API 요청에는 `x-auth` 요청 헤더에 토큰이 포함되어야 합니다.

"첫 번째 REST API 호출"을 참조하여 액세스 토큰을 요청하고 사용하는 예시를 확인하십시오.

동기 및 비동기 요청

대부분의 REST API 호출은 빠르게 완료되므로 동기적으로 실행됩니다. 즉, 요청이 완료되면 상태 코드(예: 200)를 반환합니다. 완료하는 데 시간이 더 오래 걸리는 요청은 백그라운드 작업을 사용하여 비동기적으로 실행됩니다.

비동기적으로 실행되는 API 호출 후 서버는 HTTP 상태 코드 202를 반환합니다. 이는 요청이 수락되었지만 아직 완료되지 않았음을 나타냅니다. 백그라운드 작업을 조회하여 성공 또는 실패 여부를 포함한 상태를 확인할 수 있습니다.

비동기 처리는 데이터 저장소 및 vVol 작업과 같은 여러 유형의 장시간 실행 작업에 사용됩니다. 자세한 내용은 Swagger 페이지의 REST API 작업 관리자 범주를 참조하십시오.

첫 번째 ONTAP tools REST API 호출

curl을 사용하여 API 호출을 실행하면 ONTAP tools for VMware vSphere 10 REST API를 시작할 수 있습니다.

시작하기 전에

curl 예제에 필요한 정보와 매개변수를 검토해야 합니다.

필수 정보

다음에 필요합니다:

- ONTAP tools for VMware vSphere 10 IP 주소 또는 FQDN 및 포트
- ONTAP tools Manager 관리자 자격 증명(사용자 이름 및 비밀번호)

매개변수 및 변수

아래의 curl 예제에는 Bash 스타일 변수가 포함되어 있습니다. 이러한 변수는 Bash 환경에서 설정하거나 명령을 실행하기 전에 수동으로 업데이트할 수 있습니다. 변수를 설정하면 셸은 각 명령이 실행되기 전에 해당 값으로 대체합니다. 변수에 대한 설명은 아래 표를 참조하십시오.

변수	설명
\$FQDN_IP_PORT	ONTAP tools Manager의 정규화된 도메인 이름 또는 IP 주소와 포트 번호입니다.
\$MYUSER	ONTAP tools Manager 계정의 사용자 이름입니다.
\$MYPASSWORD	ONTAP tools Manager 사용자 이름과 연결된 비밀번호입니다.
\$ACCESS_TOKEN	ONTAP tools Manager에서 발급한 액세스 토큰입니다.

다음은 Linux CLI에서 변수를 설정하고 표시하는 방법을 보여주는 명령과 출력입니다.

```
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 발급받아야 합니다. 액세스 토큰을 요청하는 방법의 예시는 아래와 같습니다. 사용 환경에 맞게 값을 적절히 바꿔 사용하십시오.

```
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"}'
```

응답에 제공된 액세스 토큰을 복사하여 저장하십시오.

2단계: REST API 호출 실행

액세스 토큰을 얻은 후에는 curl을 사용하여 REST API 호출을 실행할 수 있습니다. 첫 번째 단계에서 얻은 액세스 토큰을 포함하십시오.

Curl 예제

```
curl --request GET \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/vcenters" \
--header "Accept: */*" \
--header "x-auth: $ACCESS_TOKEN"
```

JSON 응답에는 ONTAP tools Manager에 구성된 VMware vCenter 인스턴스 목록이 포함되어 있습니다.

ONTAP tools REST API 참조

ONTAP tools for VMware vSphere 10 REST API 참조에는 모든 API 호출에 대한 세부 정보가 포함되어 있습니다. 이 참조는 자동화 애플리케이션 개발 시 유용합니다.

Swagger 사용자 인터페이스를 통해 ONTAP tools for VMware vSphere 10 REST API 설명서에 온라인으로 액세스할 수 있습니다. ONTAP tools for VMware vSphere 10 게이트웨이 서비스의 IP 주소 또는 FQDN과 포트 번호가 필요합니다.

단계

1. 다음 URL을 브라우저에 입력하고 변수에 해당하는 IP 주소와 포트 조합을 대체한 후 **Enter** 키를 누르십시오.

```
https://$FQDN_IP_PORT/
```

예

```
https://10.61.25.33:8443/
```

2. 개별 API 호출의 예시를 보려면 아래로 스크롤하여 **vCenters** 카테고리를 찾고 엔드포인트 옆에 있는 *GET*을 선택하십시오. /virtualization/api/v1/vcenters

법적 고지

법적 고지사항은 저작권 표시, 상표, 특허 등에 대한 접근을 제공합니다.

저작권

["https://www.netapp.com/company/legal/copyright/"](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/"](https://www.netapp.com/company/legal/trademarks/)

특허

NetApp이 소유한 특허의 현재 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/"](https://www.netapp.com/company/legal/privacy-policy/)

오픈 소스

고지 파일에는 NetApp 소프트웨어에 사용된 타사 저작권 및 라이선스에 대한 정보가 포함되어 있습니다.

["ONTAP tools for VMware vSphere 10.5 관련 공지"](#)

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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