VMware vSphere 10.3용 ONTAP 툴 설명서

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

목차

VMware vSphere 10.3용 ONTAP 툴 설명서

릴리스 정보

릴리스 정보

VMware vSphere 10.3용 ONTAP 툴에서 사용할 수 있는 새롭고 향상된 기능에 대해 알아보십시오.

새로운 기능 및 개선 사항의 전체 목록은 을 VMware vSphere 10.3용 ONTAP 툴의 새로운 기능참조하십시오.

VMware vSphere 9용 ONTAP 툴에서 ONTAP Tools 10.3로의 마이그레이션이 올바른 방법인지 자세히 알아보려면 을 참조하십시오VMware vSphere 9용 ONTAP 툴 및 VMware vSphere 10용 ONTAP 툴 기능 비교. 마이그레이션은 VMware vSphere 9.12-D용 ONTAP 툴 및 9.13-D 릴리스에서 VMware vSphere 10.3용 ONTAP 툴로 지원됩니다.

자세한 내용은 를 "VMware vSphere 10.3용 ONTAP 툴 릴리즈 노트"참조하십시오. 릴리스 정보에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

VMware vSphere 10.3용 ONTAP 툴의 새로운 기능

VMware vSphere 10.3용 ONTAP 툴에서 사용할 수 있는 새로운 기능에 대해 알아보십시오.

업데이트	설명
새로운 플랫폼 및 응용 프로그램 버전 지원	VMware vSphere 10.3용 ONTAP 툴은 이제 다음과 같은 플랫폼 및 애플리케이션 버전을 지원합니다. • ONTAP 9.16.0 이상 • VMware vSphere 8.0 U3 • VMware Live Site Recovery 9.0
구현 용이성	이제 단일 노드 클러스터에서 최소 요구 사항으로 VMware vSphere 10.3용 ONTAP 툴을 배포한 다음 고가용성(HA) 또는 다중 노드 배포로 업데이트할 수 있습니다.
원활한 프로비저닝 및 구성	VMware vSphere 10.3용 ONTAP 툴은 Trident와 관련된 종속성을 제거했으며 이제 동적 스토리지 프로비저닝을 사용하여 원활한 프로비저닝 및 구성을 지원합니다.
REST API 인증을 위한 보안 강화	이제 VMware vSphere 10.3용 ONTAP 툴은 CA 서명 인증서에 ONTAP 툴 REST API 및 사용자 인터페이스를 사용하여 보안을 강화합니다.
ASA R2 시스템 지원	VMware vSphere 10.3용 ONTAP 툴은 ASA R2 시스템에서 VMFS 데이터 저장소 프로비저닝을 지원하여 SnapMirror 활성 동기화 및 SRA/VMware 라이브 사이트 복구를 통해 VMFS 데이터 저장소를 보호합니다.
향상된 관찰 가능성	VMware vSphere 10.3용 ONTAP 툴은 VMFS, VVOL 데이터 저장소와 해당 VM에 대한 관측성 메트릭 지원을 확장합니다.

VMware vSphere 9용 ONTAP 툴 및 VMware vSphere 10용 ONTAP 툴 기능 비교

VMware vSphere 9용 ONTAP 툴에서 VMware vSphere 10.1 이상 버전용 ONTAP 툴로 마이그레이션하는 것이 적합한지 알아보십시오. 최신 호환성 정보는 을 "NetApp 상호 운용성 매트릭스 툴"참조하십시오.

피처	**ONTAP** 도구 **9.13**	**ONTAP** 도구 **10.1**	**ONTAP TOOLS 10.2** 이상
주요 가치 제안	향상된 보안, 규정 준수 및 자동화 기능으로 Day 0 ~ Day 2 운영을 간소화하고 단순화합니다	10.x에서 9.x 패리티로 진화하는 ONTAP 도구, 고가용성, 성능 및 확장성 제한 확장	VMFS 및 VVOL용 FC, VMFS-oF/FC, NVMe-oF/TCP만 포함하도록 지원이 확장되었습니다. NetApp SnapMirror의 간편한 사용, vSphere Metro 스토리지 클러스터의 간단한 설정, 3개 사이트 VMware Live Site Recovery 지원
ONTAP 릴리스 자격	ONTAP 9.9.1에서 ONTAP 9.15.1로	ONTAP 9.12.1에서 ONTAP 9.14.1로	ONTAP 툴 10.2 9.14.1, 9.15.1 및 ONTAP 툴 10.3용 9.16.0. ONTAP 툴용 ONTAP 9.12.1 - ONTAP 9.15.1.
VMware 릴리스 지원	vSphere 7.x-8.x VMware SRM(Site Recovery Manager) 8.5에서 VMware Live Site Recovery 9.0으로	vSphere 7.x-8.x VMware SRM(Site Recovery Manager) 8.7에서 VMware Live Site Recovery 9.0으로	vSphere 7.x-8.x VMware SRM(Site Recovery Manager) 8.7에서 VMware Live Site Recovery 9.0으로
프로토콜 지원	NFS 및 VMFS 데이터 저장소: NFS(v3 및 v4.1), VMFS(iSCSI 및 FCP) 데이터 저장소: iSCSI, FCP, NVMe/FC, NFS v3	NFS 및 VMFS 데이터 저장소: NFS(v3 및 v4.1), VMFS(iSCSI) VVol 데이터 저장소: iSCSI, NFS v3	NFS 및 VMFS 데이터 저장소: NFS(v3 및 v4.1), VMFS(iSCSI/FCP/NVMe-oF) 데이터 저장소: iSCSI, FCP, NFS v3
확장성	호스트 및 VM: 호스트 300개, VM 최대 10,000개 데이터 저장소: NFS 600개, VMFS 최대 50개, VVol 최대 250개: 최대 14,000개	호스트 및 VM: 호스트 vVols 600개: 최대 140,000개	호스트 및 VM: 호스트 vVols 600개: 최대 140,000개
관찰 가능성	성능, 용량 및 호스트 규정 준수 대시보드 동적 VM 및 데이터 저장소 보고서	업데이트된 성능, 용량 및 호스트 규정 준수 대시보드 동적 VM 및 데이터 저장소 보고서	업데이트된 성능, 용량 및 호스트 규정 준수 대시보드 동적 VM 및 데이터 저장소 보고서
데이터 보호	VMFS 및 NFS FlexVol에 대한 SRA 복제 VVols SCV 통합 및 백업에 대한 상호 운용이 가능한 복제 기반	iSCSI VMFS 및 NFS v3 데이터 저장소에 대한 SRA 복제	iSCSI VMFS 및 NFS v3 데이터 저장소에 대한 SRA 복제 SMAS 및 VMware Live Site Recovery를 결합한 3개 사이트 보호
VASA Provider 지원	VASA 4.0 를 참조하십시오	VASA 3.0 를 참조하십시오	VASA 3.0 를 참조하십시오

개념

VMware vSphere용 ONTAP 툴 개요

VMware vSphere용 ONTAP 툴은 가상 머신 라이프사이클 관리를 위한 툴 세트입니다. VMware 에코시스템과 통합되어 데이터 저장소 용량 할당 및 가상 시스템에 대한 기본 보호 기능을 제공합니다.

VMware vSphere용 ONTAP 툴은 수평으로 확장 가능한 이벤트 기반 마이크로서비스의 모음으로, OVA(Open Virtual Appliance)로 구축됩니다. 이 릴리즈에서는 REST API와 ONTAP의 통합이 가능합니다.

VMware vSphere용 ONTAP 툴의 구성 요소:

- 기본 보호 및 재해 복구와 같은 가상 시스템 기능
- VM 세부 관리를 위한 VASA 공급자
- 스토리지 정책 기반 관리
- SRA(Storage Replication Adapter)
- SnapMirror 활성 동기화(SMAS)

주요 개념 및 용어

다음 섹션에서는 이 문서에 사용된 핵심 개념과 용어에 대해 설명합니다.

ASA r2 시스템

새로운 NetApp ASA R2 시스템은 통합 하드웨어 및 소프트웨어 솔루션을 제공하여 SAN 전용 고객의 요구 사항에 맞는 간소화된 환경을 제공합니다. "ASA R2 스토리지 시스템에 대해 알아보십시오"..

CA(인증 기관**)**

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

일관성 그룹

정합성 보장 그룹은 단일 유닛으로 관리되는 볼륨의 모음입니다. ONTAP에서 일관성 그룹을 사용하면 여러 볼륨에 걸쳐 있는 애플리케이션 워크로드를 손쉽게 관리하고 보호할 수 있습니다. 에 대해 자세히 "일관성 그룹"알아보십시오.

이중 스택

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

고가용성**(HA)**

클러스터 노드는 무중단 운영을 위해 HA 쌍으로 구성됩니다.

LUN(Logical Unit Number)

LUN은 SAN(Storage Area Network) 내에서 논리 유닛을 식별하는 데 사용되는 번호입니다. 이러한 주소 지정 가능한 디바이스는 일반적으로 SCSI(Small Computer System Interface) 프로토콜 또는 캡슐화된 파생 모델 중 하나를 통해 액세스되는 논리 디스크입니다.

NVMe 네임스페이스 및 서브시스템

NVMe 네임스페이스는 논리 블록으로 포맷될 수 있는 비휘발성 메모리의 양입니다. 네임스페이스는 FC 및 iSCSI 프로토콜을 위한 LUN과 동일하며 NVMe 서브시스템은 igroup과 유사합니다. NVMe 하위 시스템을 이니시에이터와 연결할 수 있으므로 연결된 이니시에이터가 하위 시스템 내의 네임스페이스에 액세스할 수 있습니다.

ONTAP 도구 관리자

ONTAP tools Manager를 사용하면 VMware vSphere 관리자가 관리되는 vCenter Server 인스턴스 및 온보드된 스토리지 백엔드에 대해 ONTAP 툴을 더 효율적으로 제어할 수 있습니다. ONTAP tools Manager는 vCenter Server 인스턴스, 스토리지 백엔드, 인증서, 암호 및 로그 번들 다운로드를 관리하는 데 도움이 됩니다.

OVA(개방형 가상 어플라이언스**)**

OVA는 가상 머신에서 실행해야 하는 가상 어플라이언스 또는 소프트웨어를 패키징하고 배포하는 개방형 표준입니다.

복구 지점 목표**(RPO)**

RPO는 데이터가 백업 또는 복제되는 빈도를 나타내는 척도입니다. 운영 중단 후 비즈니스 운영을 재개하기 위해 데이터를 복구해야 하는 시점을 나타냅니다. 예를 들어 조직의 RPO가 4시간인 경우 재해 시 최대 4시간의 데이터 손실을 허용할 수 있습니다.

SnapMirror 활성 동기화**(SMAS)**

SnapMirror 액티브 동기화를 사용하면 전체 사이트 장애가 발생하더라도 비즈니스 서비스를 계속 운영할 수 있으므로 보조 복사본을 사용하여 애플리케이션을 투명하게 페일오버할 수 있습니다. SnapMirror 활성 동기화로 페일오버를 트리거하려면 수동 개입 또는 사용자 지정 스크립팅이 필요합니다. 자세한 정보 "SnapMirror 활성 동기화".

스토리지 백엔드

스토리지 백엔드는 ESXi 호스트가 가상 머신 파일, 데이터 및 기타 리소스를 저장하는 데 사용하는 기본 스토리지 인프라스트럭처입니다. 스토리지 백엔드를 사용하면 ESXi 호스트가 영구 데이터를 액세스하고 관리할 수 있으므로 가상화 환경에 필요한 스토리지 기능과 성능을 제공할 수 있습니다.

SRA(Storage Replication Adapter)

SRA는 VMware Live Site Recovery 어플라이언스 내부에 설치되는 스토리지 공급업체별 소프트웨어입니다. 이 어댑터를 사용하면 SVM(Storage Virtual Machine) 레벨 및 클러스터 레벨 구성에서 사이트 복구 관리자와 스토리지 컨트롤러 간의 통신이 가능합니다.

스토리지 가상 시스템**(SVM)**

하이퍼바이저에서 실행되는 가상 머신과 마찬가지로 SVM은 물리적 리소스를 추상화하는 논리적 엔터티입니다. SVM은 데이터 볼륨과 클라이언트에 데이터를 제공하는 데 사용되는 하나 이상의 LIF를 포함합니다.

균일 및 비균일 설정

- * 균일 호스트 액세스 * 는 양쪽 사이트의 호스트가 양쪽 사이트의 스토리지 클러스터에 대한 모든 경로에 접속됨을 의미합니다. 크로스 사이트 경로가 거리에 걸쳐 확장됩니다.
- * 비균일 호스트 액세스 * 는 각 사이트의 호스트가 동일한 사이트의 클러스터에만 연결됨을 의미합니다. 사이트 간 경로 및 확장 경로가 연결되지 않았습니다.

> ⓘ 모든 SnapMirror 액티브 동기식 배포에 대해 통일된 호스트 액세스가 지원되며, 비균일 호스트 액세스는 대칭 액티브/액티브 구축에만 지원됩니다.

VMFS(가상 머신 파일 시스템**)**

VMFS는 VMware vSphere 환경에 가상 머신 파일을 저장하도록 특별히 설계된 클러스터 파일 시스템입니다.

가상 볼륨**(VVOL)**

VVOL은 가상 머신에서 사용되는 스토리지에 대한 볼륨 수준 추상화를 제공합니다. 여기에는 여러 가지 이점이 있으며 기존 LUN을 사용하는 대신 사용할 수 있습니다. VVOL 데이터 저장소는 일반적으로 VVOL의 컨테이너 역할을 하는 단일 LUN과 연결됩니다.

VM 스토리지 정책

VM 스토리지 정책은 정책 및 프로필 아래에 vCenter Server에 생성됩니다. VVOL의 경우 NetApp VVols 스토리지 유형 공급자의 규칙을 사용하여 규칙 세트를 생성합니다.

VMware 라이브 사이트 복구

VMware Live Site Recovery는 VMware 가상 환경에 대한 무중단 업무 운영, 재해 복구, 사이트 마이그레이션 및 무중단 테스트 기능을 제공합니다.

VASA(VMware vSphere APIs for Storage Awareness)

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

VMware vSphere Storage API - 어레이 통합**(VAAI)**

VAAI는 VMware vSphere ESXi 호스트와 스토리지 디바이스 간의 통신을 지원하는 API 집합입니다. API에는 호스트에서 스토리지 작업을 스토리지로 오프로드하는 데 사용하는 기본 작업 세트가 포함되어 있습니다. VAAI는 스토리지 집약적인 작업에 대해 상당한 성능 향상을 제공할 수 있습니다.

vSphere Metro 스토리지 클러스터

vMSC(vSphere Metro Storage Cluster)는 확장된 클러스터 구축 환경에서 vSphere를 활성화하고 지원하는 기술입니다. vMSC 솔루션은 NetApp MetroCluster 및 SnapMirror Active Sync(이전의 SMBC)에서 지원됩니다. 이러한 솔루션은 도메인 장애 시 향상된 비즈니스 연속성을 제공합니다. 복원력 모델은 특정한 구성 선택에 따라 달라집니다. 에 대해 자세히 "VMware vSphere Metro 스토리지 클러스터"알아보십시오.

VVOL 데이터 저장소

VVol 데이터 저장소는 VASA Provider에 의해 생성되고 유지되는 VVol 컨테이너의 논리적 데이터 저장소 표현입니다.

제로 **RPO**

RPO는 지정된 시간 동안 허용되는 것으로 간주되는 데이터 손실의 양인 복구 시점 목표를 나타냅니다. RPO가 0이면 데이터 손실이 허용되지 않습니다.

역할 기반 액세스 제어

VMware vSphere 10 RBAC용 **ONTAP** 툴에 대해 알아보십시오

역할 기반 액세스 제어(RBAC)는 조직 내 리소스에 대한 액세스를 제어하기 위한 보안 프레임워크입니다. RBAC는 개별 사용자에게 권한을 할당하는 대신 특정 수준의 권한을 사용하여 역할을 정의하여 관리를 단순화합니다. 정의된 역할이 사용자에게 할당되므로 오류 위험을 줄이고 조직 전체에서 액세스 제어 관리를 간소화할 수 있습니다.

RBAC 표준 모델은 여러 구현 기술 또는 복잡성 증가의 단계로 구성됩니다. 그 결과, 소프트웨어 공급업체와 고객의 요구사항에 따라 실제 RBAC 구축이 비교적 단순 배포에서 매우 복잡한 배포까지 그 범위가 다를 수 있습니다.

RBAC 구성 요소

개략적으로 보면 모든 RBAC 구현에 일반적으로 포함되는 여러 가지 구성 요소가 있습니다. 이러한 구성 요소는 권한 부여 프로세스를 정의하는 과정에서 서로 다른 방식으로 바인딩됩니다.

권한

_privilege_는 허용하거나 거부할 수 있는 작업 또는 기능입니다. 파일을 읽는 기능과 같은 간단한 작업일 수도 있고 특정 소프트웨어 시스템에 특정한 추상적인 작업일 수도 있습니다. REST API 엔드포인트 및 CLI 명령에 대한 액세스를 제한하도록 Privileges를 정의할 수도 있습니다. 모든 RBAC 구현에는 사전 정의된 Privileges가 포함되며 관리자가 사용자 지정 Privileges을 생성할 수도 있습니다.

역할

역할 _ 은(는) 하나 이상의 Privileges을 포함하는 컨테이너입니다. 역할은 일반적으로 특정 작업 또는 직무에 따라 정의됩니다. 사용자에게 역할이 할당되면 역할에 포함된 모든 Privileges가 사용자에게 부여됩니다. 또한 Privileges와 마찬가지로 구현에는 사전 정의된 역할이 포함되며 일반적으로 사용자 지정 역할을 생성할 수 있습니다.

오브젝트

_object_는 RBAC 환경 내에서 식별된 실제 또는 추상 리소스를 나타냅니다. Privileges를 통해 정의된 작업은 연결된 객체에서 또는 관련 객체에서 수행됩니다. 구현에 따라 Privileges 를 개체 형식 또는 특정 개체 인스턴스에 부여할 수 있습니다.

사용자 및 그룹

_Users_는 인증 후 적용된 역할에 할당되거나 연결됩니다. 일부 RBAC 구현에서는 한 번에 하나의 역할만 사용자에게 할당할 수 있는 반면, 한 번에 하나의 역할만 활성 상태일 수 있는 역할도 있습니다. 역할을 _groups_에 할당하면 보안 관리를 더욱 간소화할 수 있습니다.

권한

permission_은 사용자 또는 그룹과 역할을 객체에 바인딩하는 정의입니다. 사용 권한은 계층 구조에서 하위 개체가

선택적으로 상속할 수 있는 계층적 개체 모델에 유용할 수 있습니다.

2개의 RBAC 환경

VMware vSphere 10용 ONTAP 툴을 사용할 때는 두 가지 별개의 RBAC 환경을 고려해야 합니다.

VMware vCenter Server 를 참조하십시오

VMware vCenter Server의 RBAC 구현은 vSphere Client 사용자 인터페이스를 통해 노출된 객체에 대한 액세스를 제한하는 데 사용됩니다. VMware vSphere 10용 ONTAP 툴을 설치할 때 RBAC 환경이 확장되어 ONTAP 툴의 기능을 나타내는 추가 개체가 포함됩니다. 이러한 객체에 대한 액세스는 원격 플러그인을 통해 제공됩니다. 자세한 내용은 을 참조하십시오."vCenter Server RBAC 환경"

ONTAP 클러스터

VMware vSphere 10용 ONTAP 툴은 ONTAP REST API를 통해 ONTAP 클러스터에 연결하여 스토리지 관련 작업을 수행합니다. 스토리지 리소스에 대한 액세스는 인증 중에 제공된 ONTAP 사용자와 연결된 ONTAP 역할을 통해 제어됩니다. 자세한 내용은 을 "ONTAP RBAC 환경" 참조하십시오.

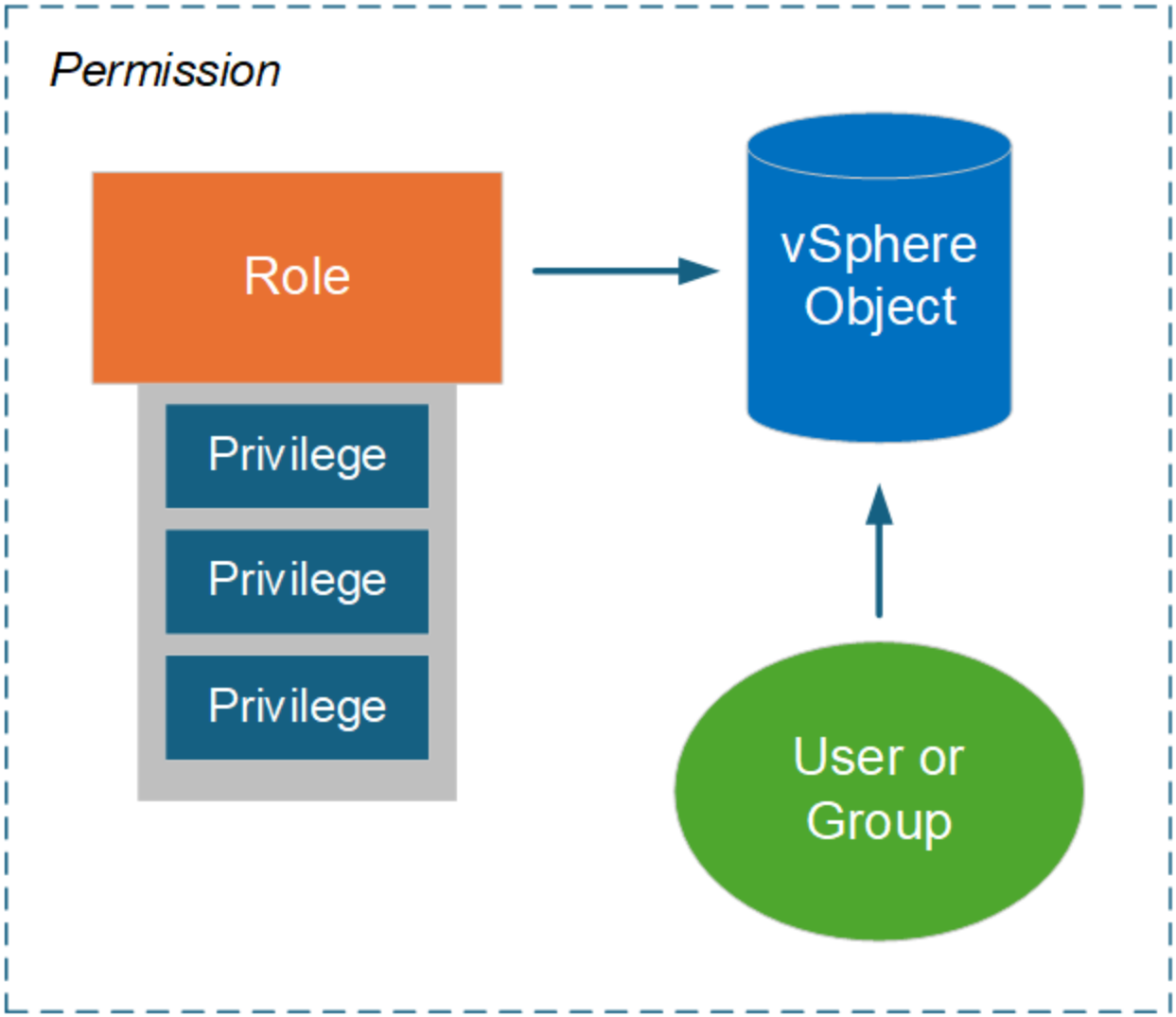
VMware vSphere를 사용하는 RBAC

VMware vSphere 10용 ONTAP 툴을 사용하는 vCenter Server RBAC 환경

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

vCenter Server 사용 권한 그림

권한은 vCenter Server 환경에서 액세스 제어를 적용하기 위한 기반입니다. 권한 정의에 포함된 사용자 또는 그룹이 있는 vSphere 객체에 적용됩니다. 아래 그림에는 vCenter 사용 권한에 대한 개략적인 설명이 나와 있습니다.



vCenter Server 권한의 구성 요소입니다

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

vSphere 객체

사용 권한은 vCenter Server, ESXi 호스트, 가상 머신, 데이터 저장소, 데이터 센터 및 폴더와 같은 vSphere 객체와 연결됩니다. vCenter Server는 객체의 할당된 사용 권한에 따라 객체에 대해 각 사용자 또는 그룹이 수행할 수 있는 작업 또는 작업을 결정합니다. VMware vSphere용 ONTAP 툴과 관련된 작업의 경우 vCenter Server의 루트 또는 루트 폴더 레벨에서 모든 권한이 할당되고 검증됩니다. 자세한 내용은 을 "vCenter Server와 함께 RBAC를 사용합니다" 참조하십시오.

Privileges 및 역할

VMware vSphere 10용 ONTAP 툴과 함께 사용되는 vSphere Privileges에는 두 가지 유형이 있습니다. 이 환경에서 RBAC를 사용하여 작업을 간소화하기 위해 ONTAP 툴은 필요한 기본 및 사용자 지정 Privileges이 포함된 역할을 제공합니다. Privileges에는 다음이 포함됩니다.

- 기본 vCenter Server 권한

  vCenter Server에서 제공하는 Privileges입니다.

- ONTAP 도구별 권한

  VMware vSphere용 ONTAP 툴에 고유한 맞춤형 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. 권한은 연결된 역할의 Privileges를 기반으로 액세스 권한을 부여합니다. 역할은 개별적으로 사용자에게 직접 할당되지 않습니다. 대신 사용자 및 그룹은 더 큰 vCenter Server 권한의 일부로 역할 Privileges를 통해 객체에 대한 액세스 권한을 얻습니다.

VMware vSphere 10용 **ONTAP** 툴과 함께 **vCenter Server RBAC**를 사용하십시오

운영 환경에서 사용하기 전에 vCenter Server를 사용하여 VMware vSphere 10 RBAC를 구축하는 ONTAP 툴의 몇 가지 측면을 고려해야 합니다.

vCenter 역할 및 관리자 계정입니다

vSphere 객체 및 관련 관리 작업에 대한 액세스를 제한하려는 경우 사용자 지정 vCenter Server 역할을 정의하고 사용해야 합니다. 액세스 제한이 필요하지 않은 경우에는 관리자 계정을 대신 사용할 수 있습니다. 각 관리자 계정은 객체 계층의 최상위 레벨에서 관리자 역할을 사용하여 정의됩니다. 이렇게 하면 VMware vSphere 10용 ONTAP 툴에 추가된 개체를 비롯하여 vSphere 객체에 대한 모든 액세스가 가능합니다.

vSphere 객체 계층 구조

vSphere 객체 인벤토리는 계층 구조로 구성됩니다. 예를 들어 다음과 같이 계층 아래로 이동할 수 있습니다.

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

타겟 ESXi 호스트에 대해 검증된 VAAI 플러그인 작업을 제외하고 vSphere 객체 계층에서 모든 권한이 검증됩니다.

VMware vSphere 10용 **ONTAP** 툴에 포함된 역할

vCenter Server RBAC를 사용하여 작업을 간소화하기 위해 VMware vSphere용 ONTAP 툴은 다양한 관리 작업에 맞게 사전 정의된 역할을 제공합니다.

> 필요한 경우 새 사용자 지정 역할을 생성할 수 있습니다. 이 경우 기존 ONTAP 툴 역할 중 하나를 복제하고 필요에 따라 편집해야 합니다. 구성을 변경한 후 영향을 받는 vSphere Client 사용자는 로그아웃했다가 다시 로그인하여 변경 사항을 활성화해야 합니다.

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

VMware vSphere 관리자용 **NetApp ONTAP** 툴

VMware vSphere 관리자 작업을 위한 핵심 ONTAP 툴을 수행하는 데 필요한 모든 기본 vCenter Server Privileges 및 ONTAP 툴 관련 Privileges를 제공합니다.

VMware vSphere 읽기 전용용 **NetApp ONTAP** 툴

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

VMware vSphere 프로비저닝용 **NetApp ONTAP** 툴

에는 스토리지 용량 할당에 필요한 몇 가지 기본 vCenter Server 권한 및 ONTAP 툴별 권한이 나와 있습니다. 다음 작업을 수행할 수 있습니다.

- 새 데이터 저장소를 생성합니다
- 데이터 저장소를 관리합니다

vSphere 오브젝트 및 **ONTAP** 스토리지 백 엔드

두 RBAC 환경이 함께 작동합니다. vSphere Client 인터페이스에서 작업을 수행할 때 vCenter Server에 정의된 ONTAP 툴 역할이 먼저 선택됩니다. vSphere에서 작업을 허용하는 경우 ONTAP 역할 Privileges가 검사됩니다. 이 두 번째 단계는 스토리지 백엔드를 생성 및 구성할 때 사용자에게 할당된 ONTAP 역할에 따라 수행됩니다.

vCenter Server RBAC 작업

vCenter Server Privileges 및 사용 권한으로 작업할 때 고려해야 할 몇 가지 사항이 있습니다.

필요한 권한

VMware vSphere 10 사용자 인터페이스용 ONTAP 툴에 액세스하려면 ONTAP 툴별 _View_권한이 있어야 합니다. 이 권한 없이 vSphere에 로그인하고 NetApp 아이콘을 클릭하면 VMware vSphere용 ONTAP 툴에 오류 메시지가 표시되고 사용자 인터페이스에 액세스할 수 없게 됩니다.

vSphere 객체 계층 구조의 할당 레벨에 따라 액세스할 수 있는 사용자 인터페이스 부분이 결정됩니다. 루트 객체에 보기 권한을 할당하면 NetApp 아이콘을 클릭하여 VMware vSphere용 ONTAP 툴에 액세스할 수 있습니다.

대신 다른 낮은 vSphere 객체 레벨에 View 권한을 할당할 수 있습니다. 그러나 이렇게 하면 액세스하고 사용할 수 있는 VMware vSphere용 ONTAP 툴이 제한됩니다.

권한 할당

vSphere 객체 및 작업에 대한 액세스를 제한하려면 vCenter Server 권한을 사용해야 합니다. vSphere 객체 계층에서 권한을 할당하는 경우 사용자가 수행할 수 있는 VMware vSphere 10 작업에 대한 ONTAP 툴이 결정됩니다.

보다 제한적인 액세스를 정의해야 하는 경우가 아니라면 일반적으로 루트 개체 또는 루트 폴더 수준에서 사용 권한을 할당하는 것이 좋습니다.

VMware vSphere 10용 ONTAP 툴에서 사용할 수 있는 사용 권한은 스토리지 시스템과 같은 사용자 지정 비 vSphere 객체에 적용됩니다. VMware vSphere 루트 객체에 할당할 수 있는 vSphere 객체가 없으므로 가능하면 이러한 권한을 VMware vSphere 루트 객체에 대한 ONTAP 툴에 할당해야 합니다. 예를 들어, VMware vSphere용 ONTAP 툴 "스토리지 시스템 추가/수정/제거" 권한이 포함된 모든 권한은 루트 객체 레벨에서 할당되어야 합니다.

개체 계층 구조에서 상위 수준에서 사용 권한을 정의할 때 자식 개체가 사용 권한을 전달하고 상속하도록 사용 권한을 구성할 수 있습니다. 필요한 경우 상위 개체에서 상속된 사용 권한을 재정의하는 하위 개체에 추가 사용 권한을 할당할 수 있습니다.

사용 권한은 언제든지 수정할 수 있습니다. 권한 내에서 Privileges를 변경하는 경우 권한과 연결된 사용자는

vSphere에서 로그아웃한 후 다시 로그인하여 변경 사항을 활성화해야 합니다.

ONTAP을 사용하는 RBAC

VMware vSphere 10용 ONTAP 툴을 사용하는 ONTAP RBAC 환경

ONTAP는 강력하고 확장 가능한 RBAC 환경을 제공합니다. RBAC 기능을 사용하여 REST API 및 CLI를 통해 노출되는 스토리지 및 시스템 작업에 대한 액세스를 제어할 수 있습니다. 이 환경을 VMware vSphere 10 구축용 ONTAP 툴과 함께 사용하기 전에 이 환경을 잘 아는 것이 좋습니다.

관리 옵션 개요

ONTAP RBAC를 사용할 때는 환경 및 목표에 따라 몇 가지 옵션을 사용할 수 있습니다. 주요 행정 결정의 개요는 다음과 같다. 자세한 내용은 를 "ONTAP 자동화: RBAC 보안 개요" 참조하십시오.

> ONTAP RBAC는 스토리지 환경에 맞게 조정되며 vCenter Server에 제공되는 RBAC 구현보다 더 간단합니다. ONTAP에서는 사용자에게 역할을 직접 할당합니다. ONTAP RBAC에서는 vCenter Server와 함께 사용되는 사용 권한 등 명시적 사용 권한을 구성할 필요가 없습니다.

역할 유형 및 Privileges

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

- 휴식

  나머지 역할은 ONTAP 9.6으로 도입되었으며, REST API를 통해 ONTAP에 액세스하는 사용자에게 일반적으로 적용된다. 이러한 역할에 포함된 Privileges는 ONTAP REST API 끝점에 대한 액세스 및 관련 작업의 측면에서 정의됩니다.

- 기존

  이는 ONTAP 9.6 이전에 포함된 레거시 역할입니다. 계속해서 RBAC의 기본 측면입니다. Privileges는 ONTAP CLI 명령에 대한 액세스 측면에서 정의됩니다.

나머지 역할은 최근에 도입되었지만 전통적인 역할에는 몇 가지 장점이 있습니다. 예를 들어, Privileges가 적용되는 개체를 보다 정확하게 정의하도록 추가 쿼리 매개 변수를 선택적으로 포함할 수 있습니다.

범위

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

역할 정의

ONTAP는 클러스터와 SVM 레벨 모두에서 사전 정의된 역할 세트를 제공합니다. 사용자 지정 역할을 정의할 수도 있습니다.

ONTAP REST 역할을 사용하여 작업합니다

VMware vSphere 10용 ONTAP 툴에 포함된 ONTAP REST 역할을 사용할 때는 몇 가지 사항을 고려해야 합니다.

역할 매핑

기존 역할을 사용하든 REST 역할을 사용하든 모든 ONTAP 액세스는 기본 CLI 명령을 기반으로 결정됩니다. 하지만 REST 역할의 Privileges는 REST API 엔드포인트의 관점에서 정의되기 때문에 ONTAP는 각 REST 역할에 대해 _mapped_trademic 역할을 생성해야 합니다. 따라서 각 REST 역할은 기본적인 기존 역할에 매핑됩니다. 이를 통해 ONTAP는 역할 유형에 관계없이 일관된 방식으로 액세스 제어 결정을 내릴 수 있습니다. 병렬 매핑된 역할은 수정할 수 없습니다.

CLI Privileges를 사용하여 **REST** 역할 정의

ONTAP는 항상 CLI 명령을 사용하여 기본 레벨에서 액세스를 결정하므로 REST 엔드포인트 대신 CLI 명령 Privileges를 사용하여 REST 역할을 표현할 수 있습니다. 이 접근 방식의 한 가지 이점은 기존 역할에서 사용할 수 있는 추가 세분화입니다.

ONTAP 역할을 정의할 때의 관리 인터페이스입니다

ONTAP CLI 및 REST API를 사용하여 사용자와 역할을 생성할 수 있습니다. System Manager 인터페이스와 ONTAP Tools Manager를 통해 사용할 수 있는 JSON 파일을 사용하는 것이 더 편리합니다. 자세한 내용은 을 "VMware vSphere 10용 ONTAP 툴과 함께 ONTAP RBAC를 사용하십시오" 참조하십시오.

VMware vSphere 10용 **ONTAP** 툴과 함께 **ONTAP RBAC**를 사용하십시오

VMware vSphere 10 RBAC를 운영 환경에서 사용하기 전에 ONTAP를 사용하여 구축하는 ONTAP 툴의 여러 측면을 고려해야 합니다.

구성 프로세스 개요

VMware vSphere 10용 ONTAP 툴에는 사용자 지정 역할을 가진 ONTAP 사용자를 생성할 수 있는 지원이 포함되어 있습니다. 이 정의는 ONTAP 클러스터에 업로드할 수 있는 JSON 파일로 패키지됩니다. 사용자를 생성하고 환경 및 보안 요구에 맞게 역할을 조정할 수 있습니다.

주요 구성 단계는 아래에 자세히 설명되어 있습니다. "ONTAP 사용자 역할 및 권한을 구성합니다"자세한 내용은 을 참조하십시오.

1. 준비

ONTAP 툴 관리자와 ONTAP 클러스터 모두에 대한 관리 자격 증명이 있어야 합니다.

2. JSON 정의 파일을 다운로드합니다

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

3. 역할이 있는 **ONTAP** 사용자를 생성합니다

System Manager에 로그인한 후 사용자 및 역할을 생성할 수 있습니다.

1. 왼쪽에서 * Cluster * 를 선택한 다음 * Settings * 를 선택합니다.
2. 아래로 스크롤하여 * 사용자 및 역할 * 을 클릭합니다 -→.
3. 사용자 * 아래에서 * 추가 * 를 선택하고 * 가상화 제품 * 을 선택합니다.
4. 로컬 워크스테이션에서 JSON 파일을 선택하고 업로드합니다.

4. 역할을 구성합니다

역할을 정의하는 과정에서 몇 가지 관리 결정을 내려야 합니다. 자세한 내용은 을 System Manager를 사용하여 역할을 구성합니다참조하십시오.

System Manager를 사용하여 역할을 구성합니다

System Manager로 새로운 사용자 및 역할을 생성하고 JSON 파일을 업로드한 후에는 환경과 요구에 따라 역할을 사용자 지정할 수 있습니다.

핵심 사용자 및 역할 구성

RBAC 정의는 VSC, VASA Provider, SRA의 조합을 포함하여 여러 제품 기능으로 패키지됩니다. RBAC 지원이 필요한 환경 또는 환경을 선택해야 합니다. 예를 들어, 원격 플러그인 기능을 지원하는 역할이 필요한 경우 VSC를 선택합니다. 또한 사용자 이름과 관련 암호도 선택해야 합니다.

권한

Privileges 역할은 ONTAP 스토리지에 필요한 액세스 수준에 따라 4세트로 구성됩니다. 역할의 기반이 되는 Privileges는 다음과 같습니다.

- 탐색

  이 역할을 통해 스토리지 시스템을 추가할 수 있습니다.

- 스토리지 생성

  이 역할을 사용하여 스토리지를 생성할 수 있습니다. 또한 검색 역할과 연결된 모든 Privileges가 포함됩니다.

- 스토리지를 수정합니다

  이 역할을 사용하여 스토리지를 수정할 수 있습니다. 또한 검색 및 스토리지 역할과 연결된 모든 Privileges가 포함됩니다.

- 스토리지 폐기

  이 역할을 사용하면 스토리지를 제거할 수 있습니다. 또한 검색, 스토리지 생성 및 스토리지 역할 수정과 관련된 모든 Privileges도 포함됩니다.

역할이 있는 사용자를 생성합니다

사용자 환경에 대한 구성 옵션을 선택한 후 * 추가 * 를 클릭하면 ONTAP가 사용자 및 역할을 생성합니다. 생성된 역할의 이름은 다음 값을 연결한 것입니다.

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

예

```
OTV_10_VSC_Discovery_Create
```

새 사용자가 "사용자 및 역할" 페이지의 목록에 추가됩니다. HTTP 및 ONTAPI 사용자 로그인 방법이 모두 지원됩니다.

VMware vSphere용 ONTAP 툴의 고가용성

VMware vSphere용 ONTAP 툴은 고가용성(HA) 구성을 지원하여 장애 발생 시 VMware vSphere용 ONTAP 툴의 중단 없는 기능을 지원합니다.

고가용성(HA) 솔루션을 통해 다음과 같은 원인으로 인한 운영 중단으로부터 신속하게 복구할 수 있습니다.

- 호스트 오류입니다

  단일 노드 장애만 지원됩니다.

- 네트워크 오류입니다
- 가상 머신 장애(게스트 OS 장애)
- 응용 프로그램(ONTAP 도구)이 충돌합니다

VMware vSphere용 ONTAP 툴에 고가용성(HA)을 제공하기 위해 추가 구성이 필요하지 않습니다.

VMware vSphere용 ONTAP 툴은 vCenter HA를 지원하지 않습니다.

HA 기능을 활성화하려면 구축 중에 또는 나중에 VMware vSphere VM용 ONTAP 툴에서 CPU 핫 추가 및 메모리 핫 플러그를 활성화해야 합니다.

AutoSupport

AutoSupport는 시스템의 상태를 능동적으로 모니터링하고 NetApp 기술 지원, 내부 지원 조직 및 지원 파트너에게 메시지를 자동으로 보내는 메커니즘입니다.

스토리지 시스템을 처음 구성할 때 AutoSupport가 기본적으로 설정됩니다. AutoSupport는 AutoSupport가 활성화된 후 24시간 후에 기술 지원 부서에 메시지를 보내기 시작합니다.

유지보수 콘솔 옵션 * 애플리케이션 구성 * > * AutoSupport 사용 안 함 * 을 사용하여 AutoSupport을 사용하지 않도록 설정할 수 있습니다. 활성화 상태로 두는 것이 좋습니다. AutoSupport를 활성화하면 문제를 더 빠르게 감지하고 문제를 더 빠르게 해결할 수 있습니다. 시스템은 AutoSupport 정보를 수집하여 AutoSupport가 비활성화된 경우에도 로컬에 저장합니다. 그러나 보고서를 어떤 네트워크에도 보내지 않습니다. 첫 번째 VM의 유지 관리 콘솔을 사용하여 프록시 URL을 제공해야 합니다. 애플리케이션 구성 * > * AutoSupport 프록시 URL 업데이트 * 옵션을 사용하여 프록시 URL을 입력합니다.

ONTAP 도구 관리자 사용자 인터페이스

VMware vSphere용 ONTAP 툴은 여러 vCenter Server 인스턴스를 관리할 수 있는 멀티 테넌트 시스템입니다. ONTAP tools Manager를 사용하면 VMware vSphere 관리자가 관리되는 vCenter Server 인스턴스 및 온보드된 스토리지 백엔드에 대해 ONTAP 툴을 더 효율적으로 제어할 수 있습니다.

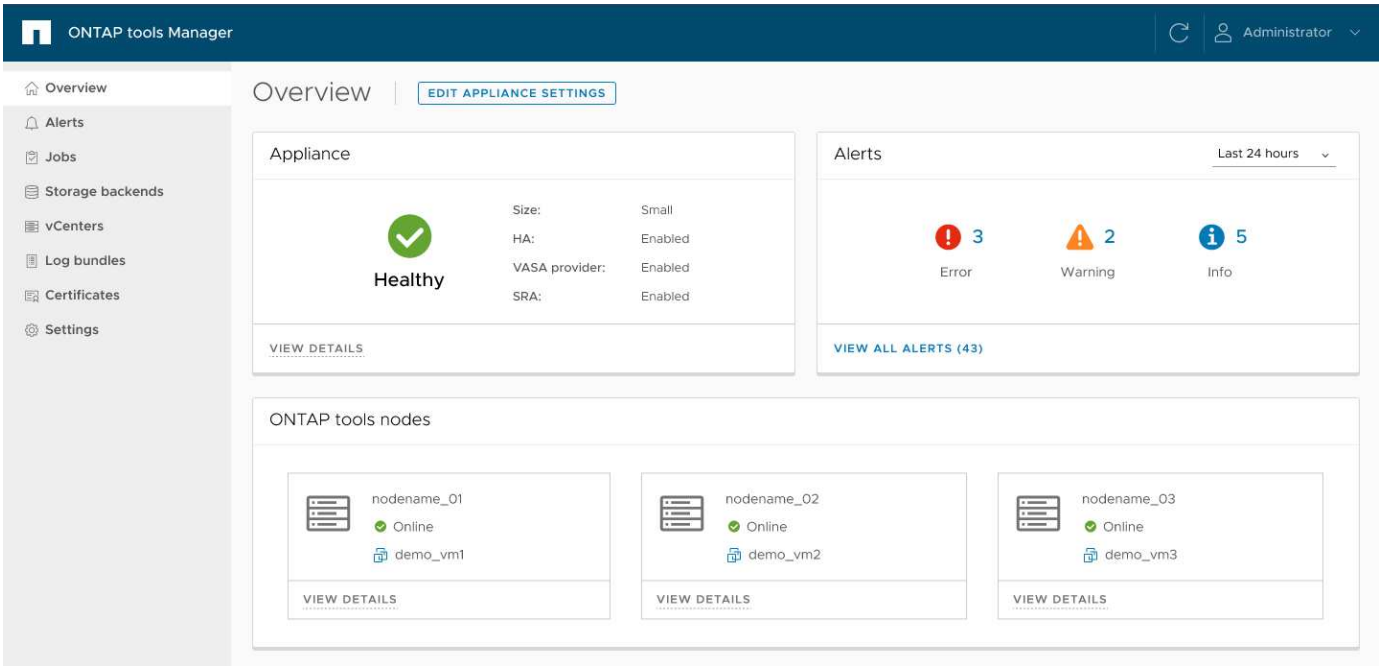
ONTAP Tools Manager는 다음과 같은 기능을 제공합니다.

- vCenter Server 인스턴스 관리 - vCenter Server 인스턴스를 ONTAP 툴에 추가 및 관리합니다.

- 스토리지 백엔드 관리 - ONTAP 스토리지 클러스터를 VMware vSphere용 ONTAP 툴에 추가 및 관리하고 전체적으로 온보딩된 vCenter Server 인스턴스에 매핑합니다.
- 로그 번들 다운로드 - VMware vSphere용 ONTAP 툴에 대한 로그 파일을 수집합니다.
- 인증서 관리 - 자체 서명된 인증서를 사용자 지정 CA 인증서로 변경하고 VASA 공급자 및 ONTAP 툴의 모든 인증서를 갱신하거나 새로 고칩니다.
- 암호 관리 - 사용자의 OVA 응용 프로그램 암호를 재설정합니다.

ONTAP Tools Manager에 액세스하려면 `https://<ONTAPtoolsIP>:8443/virtualization/ui/` 브라우저에서 을 시작하고 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.

ONTAP tools Manager 개요 섹션은 서비스 관리, 노드 크기 확장 및 고가용성(HA) 지원과 같은 어플라이언스 구성을 관리하는 데 도움이 됩니다. 또한 상태, 네트워크 세부 정보, 알림과 같이 노드와 관련된 ONTAP 툴의 전반적인 정보를 모니터링할 수 있습니다.



* 카드 *	* 설명 *
어플라이언스 카드	어플라이언스 카드는 ONTAP 도구 어플라이언스의 전체 상태를 제공합니다. 어플라이언스 구성 세부 정보 및 활성화된 서비스의 상태를 표시합니다. ONTAP 도구 어플라이언스에 대한 자세한 내용을 보려면 * 세부 정보 보기 * 링크를 선택하십시오. 어플라이언스 설정 편집 작업 작업이 진행 중이면 어플라이언스 포틀릿에 작업의 상태 및 세부 정보가 표시됩니다.
경고 카드	경고 카드에는 HA 노드 레벨 경고를 포함하여 ONTAP 툴 경고가 유형별로 나열됩니다. 개수 텍스트(하이퍼링크)를 선택하여 알림 목록을 볼 수 있습니다. 링크는 선택한 유형별로 필터링된 경고 보기 페이지로 연결됩니다.

* 카드 *	* 설명 *
ONTAP 도구 노드 카드	ONTAP tools nodes 카드는 노드 이름, 노드 VM 이름, 상태 및 모든 네트워크 관련 데이터가 있는 노드 목록을 표시합니다. View details * 를 선택하여 선택한 노드와 관련된 추가 세부 정보를 볼 수 있습니다. [참고] 비 HA 설정에서는 하나의 노드만 표시됩니다. HA 설정에서 3개의 노드가 표시됩니다.

VMware vSphere용 ONTAP 툴을 구축합니다

VMware vSphere용 ONTAP 툴을 빠르게 시작합니다

VMware vSphere용 ONTAP 툴을 시작하려면 몇 단계를 거쳐야 합니다. 이 빠른 시작에서는 VMware vSphere용 ONTAP 툴의 초기 설정을 안내합니다.

처음에는 VMware vSphere용 ONTAP 툴을 NFS 및 VMFS 데이터 저장소를 지원하는 핵심 서비스를 제공하는 소규모 단일 노드 구성으로 구축합니다. VVOL 데이터 저장소 및 HA(고가용성)를 사용하도록 구성을 확장해야 하는 경우 이 워크플로를 완료한 후 그렇게 할 수 있습니다. 자세한 내용은 를 "HA 배포 워크플로우"참조하십시오.


배포 계획

vSphere, ONTAP 및 ESXi 호스트 버전이 ONTAP 툴 버전과 호환되는지 확인합니다. 충분한 CPU, 메모리 및 디스크 공간을 할당합니다. 보안 정책에 따라 네트워크 트래픽을 허용하도록 방화벽 또는 기타 보안 어플라이언스를 구성해야 할 수도 있습니다.

vCenter Server가 설치되어 있고 액세스할 수 있는지 확인합니다.

- "상호 운용성 매트릭스 툴"
- "VMware vSphere 구축을 위한 ONTAP 툴 사전 요구 사항"
- "시작하기 전에"


VMware vSphere용 **ONTAP** 툴을 구축합니다

처음에는 NFS 및 VMFS 데이터 저장소를 지원하는 핵심 서비스를 제공하는 소규모 단일 노드 구성으로 VMware vSphere용 ONTAP 툴을 구축합니다. VVOL 데이터 저장소 및 HA(고가용성)를 사용하도록 구성을 확장하려는 경우 이 워크플로를 완료한 후 구성을 확장할 수 있습니다. HA 구성으로 성공적으로 확장하려면 CPU 핫 애드(hot-add) 및 메모리 핫 플러그(memory hot-plug) 옵션이 활성화되어 있는지 확인해야 합니다.

- "VMware vSphere용 ONTAP 툴을 구축합니다"


vCenter Server 인스턴스를 추가합니다

VMware vSphere용 ONTAP 툴에 vCenter Server 인스턴스를 하나 이상 추가하여 vCenter Server 환경에서 가상 데이터 저장소를 구성, 관리 및 보호할 수 있습니다.

- "vCenter Server 인스턴스를 추가합니다"


ONTAP 사용자 역할 및 **Privileges**를 구성합니다

VMware vSphere용 ONTAP 툴과 함께 제공되는 JSON 파일을 사용하여 새로운 사용자 역할과 Privileges를 구성하여 스토리지 백엔드 관리

- "ONTAP 사용자 역할 및 권한을 구성합니다"

5 스토리지 백엔드를 구성합니다

ONTAP 클러스터에 스토리지 백엔드를 추가합니다. vCenter가 관련 SVM과 함께 테넌트 역할을 하는 멀티 테넌시 설정의 경우 ONTAP Tools Manager를 사용하여 클러스터를 추가합니다. 스토리지 백엔드를 vCenter Server와 연결하여 온보드된 vCenter Server 인스턴스에 전역적으로 매핑합니다.

ONTAP 툴의 사용자 인터페이스를 사용하여 클러스터 또는 SVM 자격 증명으로 로컬 스토리지 백엔드를 추가합니다. 이러한 스토리지 백엔드는 단일 vCenter로 제한됩니다. 로컬로 클러스터 자격 증명을 사용할 경우 연결된 SVM이 vCenter에 자동으로 매핑되어 VVOL 또는 VMFS를 관리합니다. ONTAP 툴은 SRA를 포함한 VMFS 관리의 경우 글로벌 클러스터 없이 SVM 자격 증명을 지원합니다.

- "스토리지 백엔드를 추가합니다"
- "스토리지 백엔드를 vCenter Server 인스턴스에 연결합니다"

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

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

- "인증서를 관리합니다"

7 (선택 사항) **SRA** 보호를 활성화합니다

SRA 기능을 사용하여 재해 복구를 구성하고 NFS 또는 VMFS 데이터 저장소를 보호할 수 있습니다.

- "VMware Live Site Recovery 어플라이언스에서 SRA를 구성합니다"

8 (선택 사항) **SnapMirror** 액티브 동기화 보호를 활성화합니다

SnapMirror 활성 동기화에 대한 호스트 클러스터 보호를 관리하도록 VMware vSphere용 ONTAP 툴을 구성합니다. 소스 클러스터와 대상 클러스터와 SVM을 페어링하여 SnapMirror 액티브 동기화 지원 VMFS 데이터 저장소에만 적용됩니다.

- "호스트 클러스터 보호를 사용하여 보호합니다"

9 **VMware vSphere** 구축을 위한 **ONTAP** 툴의 백업 및 복구 설정

장애 발생 시 설정을 복구하는 데 사용할 수 있는 VMware vSphere 설정에 대한 ONTAP 툴 백업 일정을 수립합니다.

- "백업을 생성하고 ONTAP 도구 설정을 복구합니다"

고가용성(HA) 배포 워크플로우

VVOL 데이터 저장소를 사용하는 경우 ONTAP 툴의 초기 구축을 HA(고가용성) 구성으로 확장하고 VASA Provider 서비스를 활성화해야 합니다.

1 배포 확장

VMware vSphere 구성용 ONTAP 툴을 스케일업하여 구축할 때 노드 수를 늘리고 구성을 HA 설정으로 변경할 수 있습니다.

- "VMware vSphere 구성에 대한 ONTAP 툴을 변경합니다"

2 서비스 활성화

VVOL 데이터 저장소를 구성하려면 VASA Provider 서비스를 설정해야 합니다. vCenter에 VASA 공급자를 등록하고 스토리지 정책이 적절한 네트워크 및 스토리지 구성을 포함하여 HA 요구 사항을 충족하는지 확인합니다.

SRA 서비스가 VMware SRM(Site Recovery Manager) 또는 VMware VLSR(Live Site Recovery)에 ONTAP 툴을 사용하도록 설정합니다.

- "VASA Provider 및 SRA 서비스를 설정합니다"

3 인증서를 업그레이드합니다

여러 vCenter Server 인스턴스에서 VVol 데이터 저장소를 사용하는 경우 자체 서명된 인증서를 CA(인증 기관) 서명된 인증서로 업그레이드하십시오.

- "인증서를 관리합니다"

VMware vSphere 구축을 위한 ONTAP 툴 사전 요구 사항

VMware vSphere용 ONTAP 툴을 구축하기 전에 배포 패키지의 공간 요구 사항과 몇 가지 기본적인 호스트 시스템 요구 사항을 숙지해야 합니다.

VMware vSphere용 ONTAP 툴을 VMware vCSA(vCenter Server 가상 어플라이언스)와 함께 사용할 수 있습니다. VMware vSphere용 ONTAP 툴을 ESXi 시스템이 포함된 지원되는 vSphere 클라이언트에 구축해야 합니다.

시스템 요구 사항

- * 노드별 설치 패키지 공간 요구 사항 *
  - 씬 프로비저닝된 설치의 경우 15GB
  - 일반 프로비저닝 설치의 경우 348GB
- * 호스트 시스템 크기 조정 요구 사항 * 배포 크기에 따른 권장 메모리는 아래 표와 같습니다.

* 배포 유형 *	* CPU *	* 메모리(GB) *	* 디스크 공간(GB) 일반 프로비저닝 *
비 HA 소형	9	18	350
HA 미디어가 아닙니다	13	26	350
소규모 HA(3개 노드의 누적)	27	54	1050

HA 중간(3개 노드의 누적)	39	78	1050
HA 대형(3개 노드의 누적)	51	102	1050

최소 스토리지 및 애플리케이션 요구사항

스토리지, 호스트 및 애플리케이션	최소 버전 요구 사항
ONTAP	9.14.1, 9.15.1 및 9.16.0. FAS, ASA A-Series, ASA C-Series, AFF A-Series, AFF C-Series 및 ASA R2와 같은 스토리지 효율성 기술을 보유하고 있습니다.
ESXi 호스트	ESXi 7.0.3을 참조하십시오
vCenter Server입니다	vCenter 7.0U3
VASA 공급자	3.0
OVA 응용 프로그램	10.3

상호 운용성 매트릭스 툴(IMT)에는 지원되는 ONTAP 버전, vCenter Server, ESXi 호스트 및 플러그인 애플리케이션에 대한 최신 정보가 포함되어 있습니다.

"상호 운용성 매트릭스 툴"

VMware vSphere용 ONTAP 툴을 구축하기 위한 구성 제한

다음 표를 참조하여 VMware vSphere용 ONTAP 툴을 구성할 수 있습니다.

* 배포 *	* 유형 *	* VVol 수 *	* 호스트 수 *
HA가 아닙니다	소형(S)	12K 이하	32
HA가 아닙니다	중간(M)	24K 이하	64
고가용성	소형(S)	24K 이하	64
고가용성	중간(M)	5만	128
고가용성	크게(L)	100k 이하	256 [참고] 표에 있는 호스트 수는 여러 vCenter의 총 호스트 수를 보여 줍니다.

VMware vSphere용 ONTAP 툴 - SRA(Storage Replication Adapter)

다음 표에는 VMware vSphere용 ONTAP 툴을 사용하여 VMware 라이브 사이트 복구 인스턴스당 지원되는 수가 나와 있습니다.

* vCenter 배포 크기 *	* 소형 *	* 중간 *
스토리지 기반 복제를 사용하여 보호를 위해 구성된 총 가상 시스템 수입니다	2000	5000
스토리지 기반 복제 보호 그룹의 총 수입니다	250	250
복구 계획당 총 보호 그룹 수입니다	50	50

* **vCenter** 배포 크기 *	* 소형 *	* 중간 *
복제된 데이터 저장소 수입니다	255	255
VM 수입니다	4000	7000

다음 표에는 VMware Live Site Recovery의 수와 VMware vSphere 구축 크기용 ONTAP 툴의 수가 나와 있습니다.

* VMware Live Site Recovery 인스턴스 수 *	* ONTAP 도구 배포 크기 *
최대 4개	작은 크기
4 - 8	중간
8개 이상	대형

자세한 내용은 을 "VMware Live Site Recovery의 운영상의 한계"참조하십시오.

포트 요구 사항

다음 표에는 NetApp에서 사용하는 네트워크 포트와 그 용도가 요약되어 있습니다. 이러한 포트가 열려 있고 시스템 내에서 올바른 작동 및 통신을 위해 액세스할 수 있는지 확인하십시오. 관련 서비스를 위해 이러한 포트의 트래픽이 올바르게 작동할 수 있도록 필요한 네트워크 구성이 준비되어 있는지 확인합니다. 보안 정책에 따라 네트워크 내에서 이 트래픽을 허용하도록 방화벽 또는 기타 보안 어플라이언스를 구성해야 할 수 있습니다.

* 포트 *	* 설명 *
22(TCP)	Ansible은 클러스터 프로비저닝 중의 통신에 이 SSH 포트를 사용합니다. 이 포트는 유지 보수 사용자 암호, 상태 메시지 변경 및 HA 구성의 경우 세 노드 모두에서 값을 업데이트하는 등의 기능에 필요합니다.
443(TCP)	VASA Provider 서비스에 대한 들어오는 통신을 위한 통과 포트입니다. VASA Provider 자체 서명 인증서와 사용자 지정 CA 인증서가 이 포트에서 호스팅됩니다.
8443(TCP)	이 포트는 Swagger 및 Manager 사용자 인터페이스 애플리케이션을 통해 API 설명서를 호스팅합니다.
2379(TCP)	이 포트는 etcd 키 값 저장소에서 키를 가져오거나, 넣거나, 삭제하거나, 감시하는 등의 클라이언트 요청에 대한 기본 포트입니다.
2380(TCP)	이 포트는 etcd가 데이터 복제 및 일관성을 위해 사용하는 raft consensus 알고리즘에 사용되는 etcd 클러스터의 서버 간 통신을 위한 기본 포트입니다.
7472(TCP+UDP)	Prometheus 메트릭 서비스 포트입니다.
7946(TCP+UDP)	이 포트는 Docker의 컨테이너 네트워크 검색에 사용됩니다.
9083(TCP)	이 포트는 VASA Provider 서비스에 대해 내부적으로 사용되는 서비스 포트입니다.
1162(UDP)	SNMP 트랩 패킷 포트입니다.

6443(TCP)	소스: RKE2 에이전트 노드. 대상: REK2 서버 노드. 설명: Kubernetes API
9345(TCP)	소스: RKE2 에이전트 노드. 대상: REK2 서버 노드. 설명: REK2 Supervisor API
8472(TCP+UDP)	플란넬 VXLAN을 사용하는 경우 모든 노드가 UDP 포트 8472를 통해 다른 노드에 연결할 수 있어야 합니다. 소스: 모든 RKE2 노드. 대상: 모든 REK2 노드. 설명: VXLAN과 Canal CNI
10250(TCP)	소스: 모든 RKE2 노드. 대상: 모든 REK2 노드. 설명: Kubelet 메트릭
30000-32767(TCP)	소스: 모든 RKE2 노드. 대상: 모든 REK2 노드. 설명: NodePort 포트 범위입니다
123(TCP)	ntpd는 이 포트를 사용하여 NTP 서버의 검증을 수행합니다.

시작하기 전에....

배포를 진행하기 전에 다음 요구 사항이 충족되는지 확인합니다.

요구 사항	귀하의 상태
vSphere 버전, ONTAP 버전 및 ESXi 호스트 버전은 ONTP 툴 버전과 호환됩니다.	□ 예 □ 아니요
vCenter Server 환경이 설정 및 구성됩니다	□ 예 □ 아니요
브라우저 캐시가 삭제됩니다	□ 예 □ 아니요
상위 vCenter Server 자격 증명이 있습니다	□ 예 □ 아니요
vCenter Server 인스턴스에 대한 로그인 자격 증명이 있으며, 이 자격 증명에는 VMware vSphere용 ONTAP 툴이 등록을 위해 구축 후 에 연결됩니다	□ 예 □ 아니요
인증서가 발급되는 도메인 이름은 사용자 지정 CA 인증서가 필수인 다중 vCenter 배포의 가상 IP 주소에 매핑됩니다.	□ 예 □ 아니요
도메인 이름에 대해 nslookup 검사를 실행하여 도메인이 원하는 IP 주소로 확인되는지 확인했습니다.	□ 예 □ 아니요
인증서는 도메인 이름과 ONTAP 도구 IP 주소를 사용하여 생성됩니다.	□ 예 □ 아니요
ONTAP 툴 애플리케이션 및 내부 서비스는 vCenter Server에서 연결할 수 있습니다.	□ 예 □ 아니요
멀티 테넌트 SVM을 사용하는 경우 각 SVM에 SVM 관리 LIF가 존재합니다.	□ 예 □ 아니요

배포 워크시트

단일 노드 구축에 사용됩니다

다음 워크시트를 사용하여 VMware vSphere 초기 구축을 위한 ONTAP 툴에 대한 필수 정보를 수집합니다. VMware vSphere 초기 구축용 ONTAP 툴:

요구 사항	귀사의 가치
ONTAP 도구 애플리케이션의 IP 주소입니다. ONTAP 도구 웹 인터페이스에 접속하기 위한 IP 주소입니다.	
내부 통신을 위한 ONTAP 도구 가상 IP 주소입니다. 이 IP 주소는 여러 ONTAP 도구 인스턴스가 있는 환경에서 내부 통신에 사용됩니다. 이 IP 주소는 ONTAP 도구 애플리케이션의 IP 주소와 동일해서는 안 됩니다.	
첫 번째 노드의 DNS 호스트 이름입니다	
1차 DNS 서버	
보조 DNS 서버	
DNS 검색 도메인입니다	
첫 번째 노드의 IPv4 주소입니다. 관리 네트워크의 노드 관리 인터페이스에 대한 고유한 IPv4 주소입니다.	
IPv4 주소의 서브넷 마스크입니다	
IPv4 주소의 기본 게이트웨이입니다	
IPv6 주소(선택 사항)	
IPv6 접두사 길이(선택 사항)	
IPv6 주소의 게이트웨이(선택 사항)	

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

고가용성**(HA)** 배포를 위해

단일 노드 배포 요구 사항 외에 HA 배포를 위해 다음과 같은 정보가 필요합니다.

요구 사항	귀사의 가치
1차 DNS 서버	
보조 DNS 서버	
DNS 검색 도메인입니다	
두 번째 노드의 DNS 호스트 이름입니다	
두 번째 노드의 IP 주소입니다	
세 번째 노드의 DNS 호스트 이름입니다	
세 번째 노드의 IP 주소입니다	

네트워크 방화벽 구성

네트워크 방화벽에서 IP 주소에 필요한 포트를 엽니다. ONTAP 툴은 포트 443을 통해 이 LIF에 연결할 수 있어야 합니다. 최신 업데이트는 을 "포트 요구 사항"참조하십시오.

VMware vSphere용 ONTAP 툴을 구축합니다

VMware vSphere 어플라이언스용 ONTAP 툴은 NFS 및 VMFS 데이터 저장소를 지원하는 핵심 서비스를 갖춘 소규모 단일 노드로 구축됩니다.

- 시작하기 전에 *

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

클러스터 내의 모든 호스트가 액세스할 수 있도록 컨텐츠 라이브러리를 공유 데이터 저장소에 저장해야 합니다. 어플라이언스를 HA 구성으로 구성하기 전에 OVA를 저장할 컨텐츠 라이브러리를 생성합니다. 배포 후에는 콘텐츠 라이브러리 서식 파일을 삭제하지 마십시오.

나중에 HA 배포를 활성화하려면 ONTAP 툴을 호스팅하는 가상 시스템을 ESXi 호스트에 직접 배포하지 마십시오. 대신 클러스터 또는 리소스 풀에 배포합니다.

콘텐츠 라이브러리가 없는 경우 다음 단계를 따라 콘텐츠 라이브러리를 만듭니다.

- 콘텐츠 라이브러리 만들기 * 소규모 단일 노드 배포만 사용할 계획이라면 콘텐츠 라이브러리를 만들 필요가 없습니다.
  1. `.zip`에서 VMware vSphere용 ONTAP 툴에 대한 바이너리(*.ova*)와 서명된 인증서가 포함된 파일을 "NetApp Support 사이트" 다운로드합니다.
  2. vSphere Client에 로그인합니다
  3. vSphere Client 메뉴를 선택하고 * Content libraries * 를 선택합니다.
  4. 페이지 오른쪽에서 * 만들기 * 를 선택합니다.
  5. 라이브러리 이름을 지정하고 콘텐츠 라이브러리를 만듭니다.
  6. 만든 콘텐츠 라이브러리로 이동합니다.
  7. 페이지 오른쪽의 * Actions * 를 선택하고 * Import item * 을 선택한 후 OVA 파일을 가져옵니다.

자세한 내용은 "콘텐츠 라이브러리 만들기 및 사용" 블로그 를 참조하십시오.

구축을 진행하기 전에 인벤토리에 있는 클러스터의 DRS(Distributed Resource Scheduler)를 '보존적'으로 설정합니다. 이렇게 하면 설치 중에 VM이 마이그레이션되지 않습니다.

VMware vSphere용 ONTAP 툴은 처음에 비 HA 설정으로 구축됩니다. HA 배포로 확장하려면 CPU 핫 플러그 및 메모리 핫 플러그인을 활성화해야 합니다. 배포 프로세스의 일부로 이 단계를 수행하거나 배포 후 VM 설정을 편집할 수 있습니다.

단계

1. `.zip`에서 VMware vSphere용 ONTAP 툴에 대한 바이너리(*.ova*)와 서명된 인증서가 포함된 파일을 "NetApp Support 사이트" 다운로드합니다. 콘텐츠 라이브러리로 OVA를 가져온 경우 이 단계를 건너뛰고 다음 단계를 진행할 수 있습니다.
2. vSphere 서버에 로그인합니다.
3. OVA를 구축할 리소스 풀, 클러스터 또는 호스트로 이동합니다.

   VMware vSphere 가상 머신용 ONTAP 툴을 관리하는 VVOL 데이터 저장소에 저장하지 마십시오.

4. 콘텐츠 라이브러리 또는 로컬 시스템에서 OVA를 배포할 수 있습니다.

로컬 시스템에서	콘텐츠 라이브러리에서
a. 마우스 오른쪽 단추를 클릭하고 * Deploy OVF template… *.b. URL에서 OVA 파일을 선택하거나 해당 위치를 찾은 후 * Next * 를 선택합니다.	a. 콘텐츠 라이브러리로 이동하여 배포할 라이브러리 항목을 선택합니다. b. * Actions * > * 이 템플릿에서 New VM * 을 선택합니다

5. Select a name and folder * 필드에 가상 머신 이름을 입력하고 위치를 선택합니다.
   - vCenter Server 8.0.3 버전을 사용하는 경우 * 이 가상 시스템의 하드웨어 사용자 정의 * 옵션을 선택합니다. 그러면 * 완료 준비 * 창으로 진행하기 전에 * 하드웨어 사용자 정의 * 라는 추가 단계가 활성화됩니다.
   - vCenter Server 7.0.3 버전을 사용 중인 경우 구축 종료 시 * 다음 단계는 무엇입니까? * 섹션의 단계를 따르십시오.
6. 컴퓨터 리소스를 선택하고 * 다음 * 을 선택합니다. 필요에 따라 배포된 VM의 전원을 자동으로 켜려면 * 확인란을 선택합니다.
7. 템플릿의 세부 정보를 검토하고 * 다음 * 을 선택합니다.
8. 사용권 계약을 읽고 동의한 후 * Next * 를 선택합니다.
9. 구성 및 디스크 형식에 대한 스토리지를 선택하고 * Next * 를 선택합니다.
10. 각 소스 네트워크에 대한 대상 네트워크를 선택하고 * 다음 * 을 선택합니다.
11. Customize template * 창에서 필수 필드를 입력하고 * Next * 를 선택합니다.
    - 이 정보는 설치 중에 검증됩니다. 일치하지 않는 경우 웹 콘솔에 오류 메시지가 나타나고 수정하라는 메시지가 표시됩니다.
    - 호스트 이름은 문자(A-Z, a-z), 숫자(0-9) 및 하이픈(-)을 포함해야 합니다. 이중 스택을 구성하려면 IPv6 주소에 매핑된 호스트 이름을 지정합니다.

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

    - ONTAP 도구 IP 주소는 ONTAP 툴과의 통신을 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.
    - 노드 인터커넥트 IP 주소가 내부 통신에 사용됩니다.
12. vCenter Server 8.0.3 버전을 사용하는 경우 * Customize hardware * 창에서 * CPU hot add * 및 * Memory hot plug * 옵션을 활성화하여 HA 기능을 허용합니다.
13. 완료 준비 * 창에서 세부 정보를 검토하고 * 마침 * 을 선택합니다.

구축 작업이 생성되면 vSphere 작업 표시줄에 진행 상황이 표시됩니다.

14. 작업 완료 후 VM의 전원을 켭니다.

VM의 웹 콘솔에서 설치 진행률을 추적할 수 있습니다.

OVF 양식에 불일치가 있는 경우 대화 상자에 수정 조치가 표시됩니다. 탭 버튼을 사용하여 탐색하고 필요한 내용을 변경한 다음 "확인"을 선택합니다. 문제를 해결하기 위해 세 번 시도할 수 있습니다. 세 번 시도해도 문제가 계속되면 설치 프로세스가 중지되고 새 가상 컴퓨터에서 설치를 다시 시도하는 것이 좋습니다.

다음 단계

vCenter Server 7.0.3과 함께 VMware vSphere용 ONTAP 툴을 배포한 경우 구축 후 다음 단계를 수행합니다.

1. vCenter 클라이언트에 로그인합니다
2. ONTAP 도구 노드의 전원을 끕니다.
3. Inventory * 아래에서 VMware vSphere 가상 머신용 ONTAP 툴로 이동하고 * Edit settings * 옵션을 선택합니다.
4. CPU * 옵션 아래에서 * Enable CPU hot add * 확인란을 선택합니다
5. 메모리 * 옵션에서 * 메모리 핫 플러그 * 에 대해 * 활성화 * 확인란을 선택합니다.

배포 오류 코드입니다

VMware vSphere 구축, 재부팅 및 복구 작업에 대한 ONTAP 툴 중에 오류 코드가 발생할 수 있습니다. 오류 코드는 5자리 길이이며, 처음 두 자리는 문제가 발생한 스크립트를 나타내며, 마지막 세 자리는 해당 스크립트 내의 특정 워크플로를 나타냅니다.

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

이 페이지에 제공된 오류 코드는 참조용으로만 제공됩니다. 오류가 지속되거나 해결 방법이 언급되지 않은 경우 지원 팀에 문의하십시오.

다음 표에는 오류 코드와 해당 파일 이름이 나열되어 있습니다.

* 오류 코드 *	* 스크립트 이름 *
00	firstboot-network-config.pl, 모드 배포
01	firstboot-network-config.pl, 모드 업그레이드
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, 구축, HA
04	firstboot-deploy-otv-ng.pl, 배포, HA가 아닌 타사
05	firstboot-deploy-otv-ng.pl, 재부팅합니다
06	firstboot-deploy-otv-ng.pl, 업그레이드, HA
07	firstboot-deploy-otv-ng.pl, 업그레이드, 비 HA
08	firstboot-otv-recovery.pl

09	post-deploy-upgrade.pl

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

배포 오류 코드	* 워크플로 *	* 해상도 *
050	SSH 키를 생성하지 못했습니다	운영 가상 머신(VM)을 다시 시작합니다.
053	RKE2를 설치하지 못했습니다	다음을 실행하고 기본 VM을 다시 시작하거나 다시 배포합니다: sudo rke2-killall.sh (모든 VM) sudo rke2-uninstall.sh (모든 VM).
054	kubeconfig 설정 실패	재배포
055	레지스트리를 배포하지 못했습니다	레지스트리 창이 있는 경우 Pod가 준비될 때까지 기다린 다음 운영 VM을 다시 시작하거나 다시 배포하십시오.
059	KubeVip 배포에 실패했습니다	구축 중에 제공한 Kubernetes 컨트롤 플레인과 로드 밸런서 IP 주소가 동일한 VLAN에 속하고 사용 가능한 IP 주소인지 확인합니다. 이전 지점이 모두 올바르면 다시 시작합니다. 그렇지 않으면 재배포하십시오.
060	운영자 배치에 실패했습니다	를 다시 시작합니다
061	서비스를 배포하지 못했습니다	NTV-system 네임스페이스에서 get pods, get RS, get svc 등과 같은 기본 Kubernetes 디버깅을 수행하여 자세한 내용과 오류 로그를 확인할 수 있습니다. /var/log/ansible-perl-errors.log 및 /var/log/ansible-run.log 및 redeploy 를 참조하십시오.
062	ONTAP 도구 서비스 배포가 실패했습니다	자세한 내용 및 재배포는 /var/log/ansible-perl-errors.log 오류 로그를 참조하십시오.
065	Swagger 페이지 URL에 연결할 수 없습니다	재배포
066	게이트웨이 인증서에 대한 사후 배포 단계가 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	저널러에 대한 로그 회전을 구성하지 못했습니다	VM이 호스팅되는 호스트와 호환되는 VM 네트워크 설정을 확인합니다. 다른 호스트로 마이그레이션하고 VM을 다시 시작할 수 있습니다.

089	요약 로그 회전 구성 파일의 소유권을 변경하지 못했습니다	운영 VM을 재시작합니다.
096	동적 스토리지 프로비저닝을 설치합니다	-
108	시드 스크립트가 실패했습니다	-

재부팅 오류 코드	* 워크플로 *	* 해상도 *
067	rke2 대기 중 - 서버 시간이 초과되었습니다.	-
101	유지보수/콘솔 사용자 암호를 재설정하지 못했습니다.	-
102	유지보수/콘솔 사용자 암호를 재설정하는 동안 암호 파일을 삭제하지 못했습니다.	-
103	볼트에서 새 유지보수/콘솔 사용자 암호를 업데이트하지 못했습니다.	-
088	저널러에 대한 로그 회전을 구성하지 못했습니다.	VM이 호스팅되는 호스트와 호환되는 VM 네트워크 설정을 확인합니다. 다른 호스트로 마이그레이션하고 VM을 다시 시작할 수 있습니다.
089	요약 로그 회전 구성 파일의 소유권을 변경하지 못했습니다.	VM를 다시 시작합니다.

VMware vSphere용 ONTAP 툴을 구성합니다

vCenter Server 인스턴스를 추가합니다

vCenter Server 인스턴스를 VMware vSphere용 ONTAP 툴에 추가하여 vCenter Server 환경에서 가상 데이터 저장소를 구성, 관리 및 보호할 수 있습니다. 여러 vCenter Server 인스턴스를 추가하는 경우 ONTAP 도구와 각 vCenter Server 간의 보안 통신을 위해 사용자 지정 CA 인증서가 필요합니다.

- 이 작업에 대한 정보 *

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

단계

1. 웹 브라우저를 열고 다음 URL로 이동합니다. `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.
3. vCenter Server 인스턴스를 온보딩하려면 * vCenters * > * Add * 를 선택합니다. vCenter IP 주소 또는 호스트 이름, 사용자 이름, 암호 및 포트 세부 정보를 제공합니다.

> vCenter 인스턴스를 ONTAP 툴에 추가하기 위해 관리자 계정이 필요하지 않습니다. 제한된 권한을 가진 관리자 계정 없이 사용자 지정 역할을 만들 수 있습니다. 자세한 내용은 을 "VMware vSphere 10용 ONTAP 툴과 함께 vCenter Server RBAC를 사용하십시오" 참조하십시오.

ONTAP 툴에 vCenter Server 인스턴스를 추가하면 다음 작업이 자동으로 트리거됩니다.

- vCenter Client 플러그인이 원격 플러그인으로 등록되어 있습니다.
- 플러그인에 대한 사용자 지정 Privileges 및 API는 vCenter Server 인스턴스에 적용됩니다.
- 사용자 지정 역할이 생성되어 사용자를 관리합니다.
- vSphere 사용자 인터페이스에서 플러그인이 바로 가기로 표시됩니다.

vCenter Server 인스턴스에 VASA Provider를 등록합니다

VMware vSphere용 ONTAP 툴을 사용하여 vCenter Server 인스턴스에 VASA Provider를 등록할 수 있습니다. VASA Provider settings 섹션에는 선택한 vCenter Server에 대한 VASA Provider 등록 상태가 표시됩니다. 다중 vCenter 배포에서는 각 vCenter Server 인스턴스에 사용자 지정 CA 인증서가 있는지 확인하세요.

단계

1. vSphere Client에 로그인합니다
2. 플러그인 섹션에서 * 바로 가기 * > * NetApp ONTAP tools * 를 선택합니다.
3. Settings * > * VASA Provider settings * 를 선택합니다. VASA Provider 등록 상태가 등록되지 않음으로 표시됩니다.

4. VASA Provider를 등록하려면 * 등록 * 버튼을 선택합니다.
5. VASA Provider의 이름을 입력하고 VMware vSphere 애플리케이션 사용자 자격 증명을 위한 ONTAP 툴을 제공하고 * 등록 * 을 선택합니다.
6. 등록 및 페이지 새로 고침이 성공하면 등록된 VASA Provider의 상태, 이름 및 버전이 표시됩니다. 등록 후 등록 취소 작업이 활성화됩니다.
    ◦ 완료 후 *

온보딩된 VASA Provider가 vCenter 클라이언트의 VASA Provider 아래에 표시되는지 확인합니다.

단계

1. vCenter Server 인스턴스로 이동합니다.
2. 관리자 자격 증명으로 로그인합니다.
3. 스토리지 공급자 * > * 구성 * 을 선택합니다. 온보드된 VASA Provider가 올바르게 나열되는지 확인합니다.

NFS VAAI 플러그인을 설치합니다

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

시작하기 전에

- "VMware VAAI용 NetApp NFS 플러그인"설치 패키지를 다운로드합니다.
- ESXi 호스트와 vSphere 7.0U3 최신 패치 이상 버전 및 ONTAP 9.14.1 이상 버전이 있는지 확인합니다.
- NFS 데이터 저장소를 마운트합니다.

단계

1. vSphere Client에 로그인합니다.
2. 플러그인 섹션에서 * 바로 가기 * > * NetApp ONTAP tools * 를 선택합니다.
3. Settings * > * NFS VAAI Tools * 를 선택합니다.
4. VAAI 플러그인이 vCenter Server에 업로드되면 * Existing version * 섹션에서 * Change * 를 선택합니다. VAAI 플러그인이 vCenter Server에 업로드되지 않은 경우 * 업로드 * 버튼을 선택합니다.
5. 파일을 찾아 선택하고 `.vib` * 업로드 * 를 선택하여 ONTAP 도구에 파일을 업로드합니다.
6. ESXi 호스트에 설치 * 를 선택하고 NFS VAAI 플러그인을 설치할 ESXi 호스트를 선택한 다음 * 설치 * 를 선택합니다.

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

7. 설치 후 ESXi 호스트를 수동으로 다시 시작합니다.

    VMware 관리자가 ESXi 호스트를 다시 시작하면 VMware vSphere용 ONTAP 툴이 NFS VAAI 플러그인을 자동으로 감지하고 사용하도록 설정합니다.

다음 단계

NFS VAAI 플러그인을 설치하고 ESXi 호스트를 재부팅한 후에는 VAAI 복사 오프로드에 대한 올바른 NFS 내보내기 정책을 구성해야 합니다. NFS 환경에서 VAAI를 구성할 때는 다음 요구 사항을 고려하여 내보내기 정책 규칙을 구성하십시오.

- NFSv4 호출을 허용하려면 관련 ONTAP 볼륨이 필요합니다.
- 루트 사용자는 루트로 유지되어야 하고 NFSv4는 모든 접합 상위 볼륨에서 허용되어야 합니다.
- VAAI 지원 옵션은 관련 NFS 서버에서 설정해야 합니다.

절차에 대한 자세한 내용은 "VAAI 복사 오프로드에 대한 올바른 NFS 내보내기 정책을 구성합니다" KB 문서 를 참조하십시오.

관련 정보

"VMware vStorage over NFS 지원"

"NFSv4.0을 사용하거나 사용하지 않도록 설정합니다"

"NFSv4.2에 대한 ONTAP 지원"

ESXi 호스트 설정을 구성합니다

ESXi 서버 다중 경로 및 시간 초과 설정을 구성하면 운영 경로에 장애가 발생할 경우 백업 스토리지 경로로 원활하게 전환할 수 있으므로 고가용성 및 데이터 무결성을 보장할 수 있습니다.

ESXi 서버 다중 경로 및 시간 초과 설정을 구성합니다

VMware vSphere용 ONTAP 툴은 ESXi 호스트 다중 경로 설정과 NetApp 스토리지 시스템에 가장 적합한 HBA 시간 초과 설정을 확인하고 설정합니다.

- 이 작업에 대한 정보 *

구성 및 시스템 로드에 따라 이 프로세스에는 시간이 오래 걸릴 수 있습니다. 작업 진행률이 Recent Tasks(최근 작업) 패널에 표시됩니다.

단계

1. VMware vSphere Web Client 홈 페이지에서 * 호스트 및 클러스터 * 를 선택합니다.
2. 호스트를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools * > * Update host data * 를 선택합니다.
3. VMware vSphere Web Client의 바로 가기 페이지에서 플러그인 섹션에서 * NetApp ONTAP tools * 를 선택합니다.
4. VMware vSphere용 ONTAP 툴의 개요(대시보드)에서 * ESXi 호스트 규정 준수 * 카드로 이동합니다.
5. 권장 설정 적용 * 링크를 선택합니다.
6. 권장 호스트 설정 적용 * 창에서 NetApp 권장 설정에 따라 업데이트할 호스트를 선택하고 * 다음 * 을 선택합니다.

   ESXi 호스트를 확장하여 현재 값을 볼 수 있습니다.

7. 설정 페이지에서 필요한 권장 값을 선택합니다.

8. 요약 창에서 값을 확인하고 * Finish * 를 선택합니다. 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

ESXi 호스트 값을 설정합니다

VMware vSphere용 ONTAP 툴을 사용하면 ESXi 호스트에서 시간 초과 및 기타 값을 설정하여 최상의 성능과 성공적인 페일오버를 보장할 수 있습니다. VMware vSphere용 ONTAP 툴 세트는 내부 NetApp 테스트를 기반으로 합니다.

ESXi 호스트에서 다음 값을 설정할 수 있습니다.

HBA/CNA 어댑터 설정

다음 매개 변수를 기본값으로 설정합니다.

- Disk.QFullSampleSize 를 참조하십시오
- Disk.QFullThreshold를 참조하십시오
- Emulex FC HBA 시간 초과
- QLogic FC HBA 시간 초과

MPIO 설정

MPIO 설정은 NetApp 스토리지 시스템에 대한 기본 경로를 정의합니다. 또한 사용 가능한 경로 중 최적화된 경로를 결정하고(상호 연결 케이블을 통과하는 최적화되지 않은 경로와 비교) 기본 경로를 이러한 경로 중 하나로 설정합니다.

고성능 환경에서 또는 단일 LUN 데이터 저장소를 사용하여 성능을 테스트하는 경우 기본 IOPS 설정인 1000에서 값 1로 라운드 로빈(VMW_PSP_RR) PSP(경로 선택 정책)의 로드 밸런싱 설정을 변경하는 것이 좋습니다.

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

NFS 설정

매개 변수	이 값을 다음으로 설정…
NET.TcpipHeapSize	32
net.TcpipHeapMax	1024MB
NFS.MaxVolumes	256
NFS41.MaxVolumes를 참조하십시오	256
NFS.MaxQueueDepth입니다	128 이상
NFS.HeartbeatMaxFailures 를 참조하십시오	10
NFS.HeartbeatFrequency 를 선택합니다	12
NFS.HeartbeatTimeout	5

ONTAP 사용자 역할 및 권한을 구성합니다

VMware vSphere 및 ONTAP System Manager용 ONTAP 툴과 함께 제공되는 JSON 파일을

사용하여 스토리지 백엔드 관리를 위한 새로운 사용자 역할 및 권한을 구성할 수 있습니다.

시작하기 전에

- VMware vSphere용 ONTAP 툴에서 _\https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip_을 사용하여 ONTAP 권한 파일을 다운로드해야 합니다.
- 을 사용하여 ONTAP 도구에서 ONTAP Privileges 파일을 다운로드해야 `https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip` 합니다.

> 사용자는 클러스터 또는 스토리지 가상 머신(SVM) 레벨에서 직접 생성할 수 있습니다. user_roles.json 파일을 사용하지 않고 사용자를 생성할 수도 있습니다. 생성한 경우 SVM 레벨에서 최소 권한 세트가 있어야 합니다.

- 스토리지 백엔드에 대한 관리자 권한으로 로그인해야 합니다.

단계

1. 다운로드한 _\https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip_file의 압축을 풉니다.
2. 클러스터의 클러스터 관리 IP 주소를 사용하여 ONTAP System Manager에 액세스합니다.
3. admin Privileges를 사용하여 클러스터에 로그인합니다. 사용자를 구성하려면 다음 단계를 수행하십시오.
   a. 클러스터 ONTAP 툴 사용자를 구성하려면 * 클러스터 * > * 설정 * > * 사용자 및 역할 * 창을 선택합니다.
   b. SVM ONTAP 툴 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 * ONTAP 권한 JSON 파일을 선택하여 업로드합니다.

      Product(제품) 필드는 자동으로 채워집니다.

   f. 제품 기능 드롭다운 메뉴에서 필요한 기능을 선택합니다.

      역할 * 필드는 선택한 제품 기능에 따라 자동으로 채워집니다.

   g. 필요한 사용자 이름과 암호를 입력합니다.
   h. 사용자에게 필요한 Privileges(검색, 스토리지 생성, 스토리지 수정, 스토리지 제거, NAS/SAN 역할)를 선택한 다음 * 추가 * 를 선택합니다.

새 역할 및 사용자가 추가되며 구성한 역할 아래에서 자세한 권한을 볼 수 있습니다.

SVM 애그리게이트 매핑 요구사항

데이터 저장소 프로비저닝에 SVM 사용자 자격 증명을 사용하기 위해 VMware vSphere용 내부 ONTAP 툴은 데이터 저장소 POST API에 지정된 애그리게이트에 볼륨을 생성합니다. ONTAP에서는 SVM 사용자 자격 증명을 사용하여 SVM의 매핑되지 않은 애그리게이트에 볼륨을 생성할 수 없습니다. 이 문제를 해결하려면 여기에서 설명하는 대로 ONTAP REST API 또는 CLI를 사용하여 SVM을 애그리게이트와 매핑해야 합니다.

REST API:

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

ONTAP CLI:

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

ONTAP 사용자 및 역할을 수동으로 생성합니다

JSON 파일을 사용하지 않고 수동으로 사용자 및 역할을 생성하려면 이 섹션의 지침을 따르십시오.

1. 클러스터의 클러스터 관리 IP 주소를 사용하여 ONTAP System Manager에 액세스합니다.
2. admin Privileges를 사용하여 클러스터에 로그인합니다.
   a. 클러스터 ONTAP 툴 역할을 구성하려면 * 클러스터 * > * 설정 * > * 사용자 및 역할 * 창을 선택합니다.
   b. 클러스터 SVM ONTAP 툴 역할을 구성하려면 * 스토리지 SVM * > * 설정 * > * 사용자 및 역할 * 창을 선택합니다
3. 역할 생성:
   a. 역할 * 표 아래에서 * 추가 * 를 선택합니다.
   b. 역할 이름 * 및 * 역할 속성 * 세부 정보를 입력합니다.

      REST API 경로 * 및 드롭다운에서 각 액세스 권한을 추가합니다.

   c. 필요한 모든 API를 추가하고 변경 사항을 저장합니다.
4. 사용자 생성:
   a. 사용자 * 표에서 * 추가 * 를 선택합니다.
   b. 사용자 추가 * 대화 상자에서 * 시스템 관리자 * 를 선택합니다.
   c. 사용자 이름 * 을 입력합니다.
   d. 위의 * 역할 생성 * 단계에서 생성한 옵션에서 * 역할 * 을 선택합니다.
   e. 액세스 권한을 부여할 응용 프로그램과 인증 방법을 입력합니다. ONTAPI 및 HTTP는 필수 응용 프로그램이며 인증 유형은 * Password * 입니다.
   f. 사용자의 * 비밀번호 * 를 설정하고 사용자를 * 저장 * 합니다.

관리자가 아닌 전역 범위 클러스터 사용자에게 필요한 최소 권한 목록입니다

사용자 JSON 파일을 사용하지 않고 생성된 관리자가 아닌 전역 범위 클러스터 사용자에게 필요한 최소 권한은 이 섹션에 나와 있습니다. 클러스터가 로컬 범위에 추가되는 경우 JSON 파일을 사용하여 사용자를 생성하는 것이 좋습니다. VMware vSphere용 ONTAP 툴에는 ONTAP에서 프로비저닝하기 위한 읽기 권한만 있으면 되기

때문입니다.

API 사용:

API를 참조하십시오	액세스 수준	에 사용됩니다
/api/클러스터	읽기 전용	클러스터 구성 검색
/api/cluster/licensing/licenses 를 선택합니다	읽기 전용	라이센스 확인 - 프로토콜별 라이센스
/api/cluster/nodes를 사용합니다	읽기 전용	플랫폼 유형 검색
/api/security/accounts	읽기 전용	권한 검색
/API/보안/역할	읽기 전용	권한 검색
/api/스토리지/애그리게이트	읽기 전용	데이터 저장소/볼륨 프로비저닝 중 애그리게이트 공간 검사
/api/storage/cluster 를 선택합니다	읽기 전용	클러스터 수준 공간 및 효율성 데이터를 가져오는 데 사용됩니다
/api/스토리지/디스크	읽기 전용	Aggregate에 연결된 Disks를 가져옵니다
/api/스토리지/QoS/정책	읽기/생성/수정	QoS 및 VM 정책 관리
/api/svm/sSVM	읽기 전용	클러스터가 로컬로 추가된 경우 SVM 구성을 가져옵니다.
/api/network/ip/interfaces 를 참조하십시오	읽기 전용	스토리지 백엔드 추가 - 관리 LIF 범위가 클러스터/SVM으로 식별됩니다

VMware vSphere ONTAP API 기반 클러스터 범위 사용자를 위한 **ONTAP** 툴을 생성합니다

데이터 저장소에 장애가 발생한 경우 패치 작업 및 자동 롤백을 수행하려면 Privileges를 검색, 생성, 수정 및 폐기해야 합니다. 이러한 모든 Privileges가 함께 제공되지 않으면 워크플로 중단 및 정리 문제가 발생합니다.

VMware vSphere ONTAP API 기반 사용자용 ONTAP 툴을 생성하여 검색, 스토리지 생성, 스토리지 수정, 스토리지 제거 Privileges를 통해 검색을 시작하고 ONTAP 툴 워크플로우를 관리할 수 있습니다.

위에서 언급한 모든 Privileges를 사용하여 클러스터 범위 사용자를 생성하려면 다음 명령을 실행합니다.

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

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

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

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

```
/api/protocols/nvme/subsystem-maps -access all

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

또한 ONTAP 버전 9.16.0 이상의 경우 다음 명령을 실행합니다.

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

VMware vSphere ONTAP API 기반 **SVM** 범위 사용자를 위한 **ONTAP** 툴을 생성합니다

모든 Privileges을 사용하여 SVM 범위 사용자를 생성하려면 다음 명령을 실행합니다.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
/api/support/ems/application-logs -access read_create -vserver <vserver-
name>

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
-access readonly -vserver <vserver-name>

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

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

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

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

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

또한 ONTAP 버전 9.16.0 이상의 경우 다음 명령을 실행합니다.

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

위에서 생성한 API 기반 역할을 사용하여 새 API 기반 사용자를 생성하려면 다음 명령을 실행합니다.

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

예:

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

계정의 잠금을 해제하려면 관리 인터페이스에 대한 액세스를 활성화하려면 다음 명령을 실행합니다.

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

예:

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

VMware vSphere 10.1 사용자용 ONTAP 툴을 10.3 사용자로 업그레이드합니다

VMware vSphere 10.1 사용자용 ONTAP 툴이 json 파일을 사용하여 생성된 클러스터 범위 사용자인 경우, admin 사용자를 사용하여 ONTAP CLI에서 다음 명령을 실행하여 10.3 릴리즈로 업그레이드하십시오.

제품 기능:

- VSC
- VSC 및 VASA 공급자
- VSC 및 SRA
- VSC, VASA 공급자 및 SRA:

클러스터 Privileges:

security login role create -role <existing-role-name> -cmdddirname "vserver NVMe namespace show" -access all

_security login role create -role <existing-role-name> -cmdddirname "vserver NVMe subsystem show" -access all _

_security login role create -role <existing-role-name> -cmdddirname "vserver NVMe 서브시스템 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> -cmdddirname "vserver NVMe 하위 시스템 호스트 추가*" -access all*

security login role create -role <existing-role-name> -cmddirname "vserver NVMe 하위 시스템 맵 *add" -access all*

_security login role create -role <existing-role-name> -cmdddirname "vserver NVMe namespace delete" -access all _

security login role create -role <existing-role-name> -cmdddirname "vserver NVMe 하위 시스템 삭제*" -access all*

security login role create -role <existing-role-name> -cmdddirname "vserver NVMe 하위 시스템 호스트 제거*" -access all*

security login role create -role <existing-role-name> -cmdddirname "vserver NVMe 하위 시스템 맵 제거*" -access all*

VMware vSphere 10.1 사용자용 ONTAP 툴이 json 파일을 사용하여 생성된 SVM 범위 사용자인 경우, admin 사용자를 사용하여 ONTAP CLI에서 다음 명령을 실행하여 10.3 릴리즈로 업그레이드하십시오.

SVM Privileges:

security login role create -role <existing-role-name> -cmdddirname "vserver NVMe namespace show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmdddirname "vserver NVMe subsystem show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmdddirname "vserver NVMe 하위 시스템 *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> -cmdddirname "vserver NVMe 하위 시스템 호스트 추가*" -access all -vserver <vserver-name>*

_security login role create -role <existing-role-name> -cmddirname "vserver NVMe 서브시스템 맵 add" -access all -vserver <vserver-name> _

_security login role create -role <existing-role-name> -cmdddirname "vserver NVMe namespace delete" -access all -vserver <vserver-name> _

security login role create -role <existing-role-name> -cmdddirname "vserver NVMe 하위 시스템 삭제*" -access all -vserver <vserver-name>*

security login role create -role <existing-role-name> -cmdddirname "vserver NVMe 하위 시스템 호스트 제거*" -access all -vserver <vserver-name>*

security login role create -role <existing-role-name> -cmdddirname "vserver NVMe 하위 시스템 맵 제거*" -access all -vserver <vserver-name>*

command_vserver NVMe namespace show_and_vserver NVMe subsystem show_를 기존 역할에 추가하면 다음 명령이 추가됩니다.

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

스토리지 백엔드를 추가합니다

스토리지 백엔드를 추가하면 ONTAP 클러스터를 온보딩할 수 있습니다.

- 이 작업에 대한 정보 *

vCenter가 관련 SVM과 함께 테넌트 역할을 하는 멀티테넌시 설정의 경우 ONTAP Tools Manager를 사용하여 클러스터를 추가합니다. 스토리지 백엔드를 vCenter Server와 연결하여 온보드된 vCenter Server 인스턴스에 전역적으로 매핑합니다. vCenter 테넌트가 원하는 SVM(Storage Virtual Machine)을 온보딩해야 합니다. 이를 통해

SVM 사용자는 VVOL 데이터 저장소를 프로비저닝할 수 있습니다. SVM을 사용하여 vCenter에서 스토리지를 추가할 수 있습니다.

ONTAP 툴의 사용자 인터페이스를 사용하여 클러스터 또는 SVM 자격 증명으로 로컬 스토리지 백엔드를 추가합니다. 이러한 스토리지 백엔드는 단일 vCenter로 제한됩니다. 로컬로 클러스터 자격 증명을 사용할 경우 연결된 SVM이 vCenter에 자동으로 매핑되어 VVOL 또는 VMFS를 관리합니다. ONTAP 툴은 SRA를 포함한 VMFS 관리의 경우 글로벌 클러스터 없이 SVM 자격 증명을 지원합니다.

ONTAP 도구 관리자 사용

멀티 테넌트 설정에서 스토리지 백엔드 클러스터를 글로벌 및 SVM을 로컬에서 추가하여 SVM 사용자 자격 증명을 사용할 수 있습니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.
3. 측면 표시줄에서 * Storage Backend * 를 선택합니다.
4. 스토리지 백엔드를 추가하고 서버 IP 주소 또는 FQDN, 사용자 이름 및 암호 세부 정보를 제공합니다.

   IPv4 및 IPv6 주소 관리 LIF가 지원됩니다.

vSphere Client 사용자 인터페이스 사용

vSphere Client 사용자 인터페이스를 통해 스토리지 백엔드를 구성할 때는 VVol 데이터 저장소에서 SVM 사용자를 직접 추가할 수 없습니다.

1. vSphere Client에 로그인합니다.
2. 바로 가기 페이지의 플러그인 섹션에서 * NetApp ONTAP tools * 를 선택합니다.
3. 측면 표시줄에서 * Storage Backend * 를 선택합니다.
4. 스토리지 백엔드를 추가하고 서버 IP 주소, 사용자 이름, 암호 및 포트 세부 정보를 제공합니다.

   SVM 사용자를 직접 추가하기 위해 클러스터 기반 자격 증명, IPv4 및 IPv6 주소 관리 LIF를 추가하거나 SVM 관리 LIF에 SVM 기반 자격 증명을 제공할 수 있습니다.

다음 단계

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

스토리지 백엔드를 **vCenter Server** 인스턴스에 연결합니다

스토리지 백엔드를 vCenter Server에 연결하여 스토리지 백엔드와 온보딩된 vCenter Server 인스턴스 간의 매핑을 전체적으로 생성합니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.
3. 사이드바에서 vCenter를 선택합니다.
4. 스토리지 백엔드에 연결할 vCenter Server 인스턴스에 대해 세로 줄임표를 선택합니다.
5. 드롭다운에서 스토리지 백엔드를 선택하여 vCenter Server 인스턴스를 필요한 스토리지 백엔드와 연결합니다.

네트워크 액세스를 구성합니다

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

단계

1. vSphere Client에 로그인합니다.
2. 플러그인 섹션 아래의 바로 가기 페이지에서 * NetApp ONTAP tools * 를 선택합니다.
3. ONTAP 도구의 왼쪽 창에서 * 설정 * > * 네트워크 액세스 관리 * > * 편집 * 으로 이동합니다.

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

4. 저장 * 을 선택합니다.

데이터 저장소를 생성합니다

호스트 클러스터 레벨에서 데이터 저장소를 생성하면 데이터 저장소가 생성되고 대상의 모든 호스트에 마운트되며, 현재 사용자에게 실행 권한이 있는 경우에만 작업이 활성화됩니다.

VVOL 데이터 저장소를 생성합니다

VMware vSphere 10.3용 ONTAP 툴부터 공간 효율성을 얇은 VVOL으로 ASA R2 시스템에 VVOL 데이터 저장소를 생성할 수 있습니다. VASA Provider는 컨테이너와 원하는 프로토콜 엔드포인트를 생성하는 동시에 VVOL 데이터 저장소를 생성합니다. 이 컨테이너에는 백업 볼륨이 없습니다.

시작하기 전에

- 루트 애그리게이트가 SVM에 매핑되지 않도록 합니다.
- VASA Provider가 선택한 vCenter에 등록되어 있는지 확인합니다.
- ASA R2 스토리지 시스템에서 SVM 사용자를 위해 SVM을 애그리게이트에 매핑해야 합니다.

단계

1. vSphere Client에 로그인합니다.
2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools * > * Create Datastore * 를 선택합니다.
3. VVols * Datastore type * 을 선택합니다.
4. Datastore name * 및 * Protocol * 정보를 입력합니다.

   ASA R2 시스템은 VVOL을 위해 iSCSI 및 FC 프로토콜을 지원합니다.

5. 데이터 저장소를 생성할 스토리지 VM을 선택합니다.
6. 고급 옵션 * 에서 NFS 프로토콜에 대한 사용자 지정 내보내기 정책 또는 iSCSI 및 FC 프로토콜에 대한 사용자 지정 이니시에이터 그룹 이름을 선택합니다.

   ASA R2 스토리지 시스템 유형 SVM에서는 데이터 저장소가 논리적 컨테이너일 뿐이므로 스토리지 유닛(LUN/네임스페이스)이 생성되지 않습니다.

7. Storage attributes * 창에서 새 볼륨을 생성하거나 기존 볼륨을 사용할 수 있습니다. 그러나 이 두 가지 유형의 볼륨을 결합하여 VVol 데이터 저장소를 만들 수는 없습니다.

   새 볼륨을 생성할 때 데이터 저장소에서 QoS를 사용하도록 설정할 수 있습니다. 기본적으로 LUN 생성 요청마다 하나의 볼륨이 생성됩니다. 이 단계는 ASA R2 스토리지 시스템을 사용하는 VVol 데이터 저장소에는 적용되지 않습니다.

8. 요약 * 창에서 선택 항목을 검토하고 * 마침 * 을 선택합니다.

NFS 데이터 저장소를 생성합니다

VMware NFS(Network File System) 데이터 저장소는 NFS 프로토콜을 사용하여 네트워크를 통해 ESXi 호스트를 공유 스토리지 디바이스에 연결합니다. NFS 데이터 저장소는 VMware vSphere 환경에서 일반적으로 사용되며 사용 편의성과 유연성과 같은 여러 가지 이점을 제공합니다.

단계

1. vSphere Client에 로그인합니다.
2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools * > * Create datastore * 를 선택합니다.
3. Datastore type * 필드에서 NFS를 선택합니다.

4. Name and protocol * 창에 데이터스토어 이름, 크기 및 프로토콜 정보를 입력합니다. 고급 옵션에서 * Datastore cluster * 및 * Kerberos authentication * 을 선택합니다.

   Kerberos 인증은 NFS 4.1 프로토콜을 선택한 경우에만 사용할 수 있습니다.

5. Storage * 창에서 * Platform * 및 * Storage VM * 을 선택합니다.
6. 필요한 경우 고급 옵션에서 * 사용자 지정 내보내기 정책 * 을 선택하되 권장하지는 않습니다. 사용하는 경우 vCenter에서 모든 객체에 대해 검색을 실행해야 합니다.

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

   - 고급 옵션에서 플랫폼 드롭다운에서 성능 또는 용량을 선택한 경우에만 * 비대칭 * 전환 버튼이 표시됩니다.
   - 플랫폼 드롭다운에서 * any * 옵션을 선택하면 플랫폼 또는 비대칭 플래그와 상관없이 vCenter의 일부인 SVM을 볼 수 있습니다.

7. Storage Attributes * 창에서 볼륨 생성을 위한 집계를 선택합니다. 고급 옵션에서 필요에 따라 * Space Reserve * 및 * Enable QoS * 를 선택합니다.
8. Summary * 창에서 선택 항목을 검토하고 * Finish * 를 선택합니다.

NFS 데이터 저장소는 모든 호스트에 생성되고 마운트됩니다.

VMFS 데이터 저장소를 생성합니다

VMFS(Virtual Machine File System)는 VMware vSphere 환경에 가상 머신 파일을 저장하는 클러스터 파일 시스템입니다. VMFS를 사용하면 여러 ESXi 호스트가 동일한 가상 머신 파일을 동시에 액세스할 수 있으므로 vMotion 및 High Availability 같은 기능을 사용할 수 있습니다.

보호된 클러스터에서 다음을 수행합니다.

- VMFS 데이터 저장소만 생성할 수 있습니다. VMFS 데이터 저장소를 보호된 클러스터에 추가하면 데이터 저장소가 자동으로 보호됩니다.
- 하나 이상의 보호된 호스트 클러스터가 있는 데이터 센터에는 데이터 저장소를 생성할 수 없습니다.
- 상위 호스트 클러스터가 "Automated Failover Duplex policy" 유형(uniform/non-uniform config)으로 보호되는 경우 ESXi 호스트에서 데이터 저장소를 생성할 수 없습니다.
- VMFS 데이터 저장소는 비동기식 관계로 보호되는 ESXi 호스트에서만 생성할 수 있습니다. "Automated Failover Duplex" 정책으로 보호되는 호스트 클러스터의 일부인 ESXi 호스트에서는 데이터 저장소를 생성하고 마운트할 수 없습니다.

시작하기 전에

- ONTAP 스토리지 측에서 각 프로토콜에 대해 서비스와 LIF를 사용하도록 설정합니다.
- ASA R2 스토리지 시스템의 SVM 사용자를 위해 SVM을 애그리게이트로 매핑합니다.
- NVMe/TCP 프로토콜을 사용하는 경우 ESXi 호스트를 구성합니다.
  a. 를 검토합니다 "VMware 호환성 가이드 를 참조하십시오"

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

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

c. NIC 공급업체 사양에 따라 NVMe/TCP용 ESXi NIC를 구성합니다.

d. VMware vSphere 7 릴리즈를 사용하는 경우 VMware 사이트의 지침에 따라 "NVMe over TCP 어댑터에 대한 VMkernel 바인딩을 구성합니다" NVMe/TCP 포트 바인딩을 구성합니다. VMware vSphere 8 릴리즈를 사용하는 경우 에 따라 "ESXi에서 TCP를 통한 NVMe 구성" NVMe/TCP 포트 바인딩을 구성합니다.

e. VMware vSphere 7 릴리즈의 경우 페이지의 지침에 따라 "NVMe over RDMA 또는 NVMe over TCP 소프트웨어 어댑터를 활성화합니다" NVMe/TCP 소프트웨어 어댑터를 구성합니다. VMware vSphere 8 릴리즈의 경우, 에 따라 "소프트웨어 NVMe over RDMA 또는 NVMe over TCP 어댑터를 추가합니다" NVMe/TCP 소프트웨어 어댑터를 구성합니다.

f. "스토리지 시스템 및 호스트를 검색합니다"ESXi 호스트에서 작업을 실행합니다. 자세한 내용은 을 "vSphere 8.0 업데이트 1 및 VMFS 데이터 저장소용 ONTAP 9.13.1을 사용하여 NVMe/TCP를 구성하는 방법"참조하십시오.

- NVMe/FC 프로토콜을 사용하는 경우 다음 단계를 수행하여 ESXi 호스트를 구성합니다.

a. ESXi 호스트에서 NVMe-oF(NVMe over Fabrics)를 사용하도록 설정합니다.

b. SCSI 조닝을 완료합니다.

c. ESXi 호스트와 ONTAP 시스템이 물리적 계층과 논리적 계층에 연결되어 있는지 확인합니다.

FC 프로토콜을 위해 ONTAP SVM을 구성하려면 을 참조하십시오 "FC용 SVM 구성".

VMware vSphere 8.0에서 NVMe/FC 프로토콜 사용에 대한 자세한 내용은 을 참조하십시오 "ONTAP가 있는 ESXi 8.x용 NVMe-oF 호스트 구성".

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

단계

1. vSphere Client에 로그인합니다.
2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools * > * Create Datastore * 를 선택합니다.
3. VMFS 데이터 저장소 유형을 선택합니다.
4. Name and Protocol * 창에 데이터 저장소 이름, 크기 및 프로토콜 정보를 입력합니다. 새 데이터 저장소를 기존 VMFS 데이터 저장소 클러스터에 추가하기로 선택한 경우 고급 옵션 에서 데이터 저장소 클러스터 선택기를 선택합니다.
5. 스토리지 * 창에서 스토리지 VM을 선택합니다. 필요한 경우 * 고급 옵션 * 섹션에 * 사용자 지정 이니시에이터 그룹 이름 * 을 입력합니다. 데이터 저장소에 대해 기존 igroup을 선택하거나 사용자 지정 이름으로 새로운 igroup을 생성할 수 있습니다.

   NVMe/FC 또는 NVMe/TCP 프로토콜을 선택하면 새 네임스페이스 서브시스템이 생성되고 네임스페이스 매핑에 사용됩니다. 네임스페이스 하위 시스템은 데이터 저장소 이름이 포함된 자동 생성 이름을 사용하여 생성됩니다. 저장소* 창의 고급 옵션에 있는 * 사용자 지정 네임스페이스 하위 시스템 이름 * 필드에서 네임스페이스 하위 시스템의 이름을 바꿀 수 있습니다.

6. storage attributes * 창에서 다음을 수행합니다.

a. 드롭다운 옵션에서 * Aggregate * 를 선택합니다.

ASA R2 스토리지 시스템의 경우 * Aggregate * 옵션은 ASA R2 스토리지가 Disaggregated 스토리지이므로 표시되지 않습니다. ASA R2 스토리지 시스템 유형의 SVM을 선택하면 스토리지 특성 페이지에 QoS 활성화 옵션이 표시됩니다.

b. 선택한 프로토콜에 따라 씬 유형의 공간 예비 공간을 사용하여 스토리지 유닛(LUN/네임스페이스)이 생성됩니다.

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

ASA R2 스토리지 유형에서 볼륨 생성 또는 선택은 스토리지 유닛 생성(LUN/네임스페이스)에 적용할 수 없습니다. 따라서 이러한 옵션은 표시되지 않습니다.

NVMe/FC 또는 NVMe/TCP 프로토콜을 사용하여 VMFS 데이터 저장소를 생성하려면 기존 볼륨을 사용할 수 없으며 새 볼륨을 생성해야 합니다.

7. Summary * 창에서 데이터 저장소 세부 정보를 검토하고 * Finish * 를 선택합니다.

보호된 클러스터에 데이터 저장소를 생성하는 경우 "데이터 저장소가 보호된 클러스터에 마운트되어 있습니다."라는 읽기 전용 메시지가 표시됩니다.

결과

VMFS 데이터 저장소는 모든 호스트에 생성되고 마운트됩니다.

데이터 저장소와 가상 머신을 보호합니다

호스트 클러스터 보호를 사용하여 보호합니다

VMware vSphere용 ONTAP 툴은 호스트 클러스터의 보호를 관리합니다. 선택한 SVM에 속하고 클러스터의 하나 이상의 호스트에 마운트된 모든 데이터 저장소는 호스트 클러스터에서 보호됩니다.

시작하기 전에

다음 필수 구성 요소가 충족되는지 확인합니다.

- 호스트 클러스터에는 하나의 SVM의 데이터 저장소만 있습니다.
- 호스트 클러스터에 마운트된 데이터 저장소는 클러스터 외부의 호스트에 마운트해서는 안 됩니다.
- 호스트 클러스터에 마운트된 모든 데이터 저장소는 iSCSI/FC 프로토콜을 사용하는 VMFS 데이터 저장소여야 합니다. NVMe/FC 및 NVMe/TCP 프로토콜을 사용하는 VVol, NFS 또는 VMFS 데이터 저장소는 지원되지 않습니다.
- 호스트 클러스터에 마운트된 데이터 저장소를 형성하는 FlexVol/LUN이 기존 CG(정합성 보장 그룹)의 일부가 아니어야 합니다.
- 호스트 클러스터에 마운트된 데이터 저장소를 형성하는 FlexVol/LUN이 기존 SnapMirror 관계에 있으면 안 됩니다.
- 호스트 클러스터에는 데이터 저장소가 하나 이상 있어야 합니다.

단계

1. vSphere Client에 로그인합니다
2. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools * > * Protect Cluster * 를 선택합니다.
3. 클러스터 보호 창에서 데이터 저장소 유형 및 소스 VM(스토리지 가상 머신) 세부 정보가 자동으로 채워집니다. Datastores 링크를 선택하여 보호된 데이터 저장소를 봅니다.
4. 정합성 보장 그룹 이름 * 을 입력합니다.
5. 관계 추가 * 를 선택합니다.
6. SnapMirror 관계 추가 * 창에서 * 대상 스토리지 VM * 및 * 정책 * 유형을 선택합니다.

   정책 유형은 Asynchronous 또는 AutomatedFailOverDuplex 일 수 있습니다.

   SnapMirror 관계를 AutomatedFailOverDuplex 유형 정책으로 추가하는 경우 VMware vSphere용 ONTAP 툴이 구축된 동일한 vCenter에 타겟 스토리지 VM을 스토리지 백엔드로 추가해야 합니다.

   AutomatedFailOverDuplex 정책 유형에는 균일하고 균일하지 않은 호스트 구성이 있습니다. uniform host configuration * 토글 버튼을 선택하면 호스트 이니시에이터 그룹 구성이 타겟 사이트에 암시적으로 복제됩니다. 자세한 내용은 을 "주요 개념 및 용어"참조하십시오.

7. 비균일한 호스트 구성을 사용하도록 선택한 경우 해당 클러스터 내의 각 호스트에 대한 호스트 액세스(소스/타겟)를 선택합니다.
8. 추가 * 를 선택합니다.

9. protect cluster * 창에서 생성 작업 중에는 보호된 클러스터를 편집할 수 없습니다. 삭제하고 보호를 다시 추가할 수 있습니다. Modify host cluster protection(호스트 클러스터 보호 수정) 작업 중에는 편집 옵션을 사용할 수 있습니다. 줄임표 메뉴 옵션을 사용하여 관계를 편집하거나 삭제할 수 있습니다.
10. protect * 버튼을 선택합니다.

    vCenter 작업이 작업 ID 세부 정보와 함께 생성되며 진행 상황이 Recent Tasks 패널에 표시됩니다. 이 작업은 비동기 작업이며 사용자 인터페이스는 요청 제출 상태만 표시하고 작업이 완료될 때까지 기다리지 않습니다.

11. 보호된 호스트 클러스터를 보려면 * NetApp ONTAP tools * > * 보호 * > * 호스트 클러스터 관계 * 로 이동하십시오.

SRA 보호를 사용하여 보호합니다

SRA를 활성화하여 데이터 저장소를 보호합니다

VMware vSphere용 ONTAP 툴은 SRA 기능을 사용하여 재해 복구를 구성할 수 있는 옵션을 제공합니다.

시작하기 전에

- vCenter Server 인스턴스를 설정하고 ESXi 호스트를 구성해야 합니다.
- VMware vSphere용 ONTAP 툴을 배포해야 합니다.
- `.tar.gz`에서 SRA Adapter 파일을 다운로드해야 "NetApp Support 사이트" 합니다.
- 소스 및 대상 ONTAP 클러스터에서 SRA 워크플로우를 실행하기 전에 생성된 동일한 사용자 지정 SnapMirror 일정이 있어야 합니다.

단계

1. URL:을 사용하여 VMware Live Site Recovery 어플라이언스 관리 인터페이스에 로그인한 `https://:<srm_ip>:5480` 다음 VMware VMware Live Site Recovery 어플라이언스 관리 인터페이스의 스토리지 복제 어댑터로 이동합니다.
2. 새 어댑터 * 를 선택합니다.
3. SRA 플러그인용 _.tar.gz_installer를 VMware Live Site Recovery에 업로드합니다.
4. 어댑터를 다시 검색하여 VMware Live Site Recovery Storage Replication Adapters 페이지에서 세부 정보가 업데이트되었는지 확인합니다.

SAN 및 NAS 환경에 대해 SRA 구성

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

SAN 환경에 대한 SRA 구성

시작하기 전에

보호된 사이트와 복구 사이트에 다음 프로그램이 설치되어 있어야 합니다.

- VMware 라이브 사이트 복구

VMware Live Site Recovery 설치에 대한 설명서는 VMware 사이트에 있습니다.

"VMware Live Site Recovery에 대해 알아보십시오"

- SRA

  어댑터는 VMware Live Site Recovery에 설치됩니다.

단계

1. 운영 ESXi 호스트가 보호 사이트의 운영 스토리지 시스템에 있는 LUN에 연결되어 있는지 확인합니다.
2. LUN이 `ostype` 운영 스토리지 시스템에서 _vmware_로 설정된 igroup에 있는지 확인합니다.
3. 복구 사이트의 ESXi 호스트가 SVM(스토리지 가상 머신)에 대한 iSCSI 연결이 적절한지 확인합니다. 보조 사이트 ESXi 호스트는 보조 사이트 스토리지에 액세스할 수 있어야 하며 운영 사이트 ESXi 호스트는 운영 사이트 스토리지에 액세스할 수 있어야 합니다.

   이 작업은 ESXi 호스트에 SVM에 로컬 LUN이 연결되어 있는지 확인하거나 SVM `iscsi show initiators`에서 명령을 실행하여 수행할 수 있습니다. ESXi 호스트에서 매핑된 LUN에 대한 LUN 액세스를 확인하여 iSCSI 접속을 확인합니다.

NAS 환경에 대한 **SRA** 구성

시작하기 전에

보호된 사이트와 복구 사이트에 다음 프로그램이 설치되어 있어야 합니다.

- VMware 라이브 사이트 복구

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

  "VMware Live Site Recovery에 대해 알아보십시오"

- SRA

  어댑터는 VMware Live Site Recovery 및 SRA 서버에 설치됩니다.

단계

1. 보호 사이트의 데이터 저장소에 vCenter Server에 등록된 가상 머신이 포함되어 있는지 확인합니다.
2. 보호 사이트의 ESXi 호스트에서 NFS 엑스포트 볼륨을 SVM(스토리지 가상 머신)에서 마운트했는지 확인합니다.
3. Array Manager 마법사를 사용하여 VMware Live Site Recovery에 어레이를 추가할 때 NFS 내보내기가 있는 IP 주소, 호스트 이름 또는 FQDN과 같은 유효한 주소가 * NFS 주소 * 필드에 지정되었는지 확인합니다.
4. `ping`복구 사이트의 각 ESXi 호스트에서 명령을 사용하여 SVM에서 NFS 내보내기를 제공하는 데 사용되는 IP 주소를 액세스할 수 있는 VMkernel 포트가 호스트에 있는지 확인합니다.

확장성이 높은 환경에 맞게 **SRA**를 구성합니다

확장성이 높은 환경에서 최적으로 수행되도록 SRA(Storage Replication Adapter)의 권장 설정에 따라 스토리지 시간 초과 간격을 구성해야 합니다.

저장소 공급자 설정

확장 환경에 대해 VMware Live Site Recovery에서 다음 시간 초과 값을 설정해야 합니다.

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

`StorageProvider.autoResignatureMode`옵션을 활성화해야 합니다.

저장소 공급자 설정 수정에 대한 자세한 내용은 을 "저장소 공급자 설정을 변경합니다" 참조하십시오.

저장소 설정

시간 초과에 도달하면 `storage.commandTimeout` 및 의 값을 `storage.maxConcurrentCommandCnt` 더 높은 값으로 늘립니다.

지정된 시간 제한 간격이 최대값입니다. 최대 시간 초과에 도달할 때까지 기다릴 필요가 없습니다. 대부분의 명령이 설정된 최대 시간 제한 간격 내에 완료됩니다.

SAN Provider 설정을 수정하는 방법은 을 "저장소 설정을 변경합니다" 참조하십시오.

VMware Live Site Recovery 어플라이언스에서 SRA를 구성합니다

VMware Live Site Recovery 어플라이언스를 구축한 후에는 VMware Live Site Recovery 어플라이언스에 SRA를 구성해야 합니다. SRA 구성이 성공하면 VMware Live Site Recovery 어플라이언스가 SRA와 통신하여 재해 복구 관리를 수행할 수 있습니다. VMware Live Site Recovery 어플라이언스와 SRA 간의 통신을 활성화하려면 VMware vSphere 자격 증명(IP 주소)용 ONTAP 툴을 VMware Live Site Recovery 어플라이언스에 저장해야 합니다.

시작하기 전에

에서 _tar.gz_파일을 다운로드해야 "NetApp Support 사이트" 합니다.

- 이 작업에 대한 정보 *

VMware Live Site Recovery 어플라이언스에서 SRA를 구성하면 SRA 자격 증명이 VMware Live Site Recovery 어플라이언스에 저장됩니다.

단계

1. VMware Live Site Recovery 어플라이언스 화면에서 * Storage Replication Adapter * > * New Adapter * 를

선택합니다.

2. VMware Live Site Recovery에 _.tar.gz_파일을 업로드합니다.
3. putty를 사용하여 관리자 계정을 사용하여 VMware Live Site Recovery 어플라이언스에 로그인합니다.
4. 다음 명령을 사용하여 루트 사용자로 전환합니다. `su root`
5. 명령을 `cd /var/log/vmware/srm` 실행하여 로그 디렉토리로 이동합니다.
6. 로그 위치에 명령을 입력하여 SRA에서 사용하는 Docker ID를 가져옵니다. `docker ps -l`
7. 컨테이너 ID에 로그인하려면 명령을 입력합니다. `docker exec -it -u srm <container id> sh`
8. 다음 명령을 사용하여 VMware vSphere용 ONTAP 툴을 사용하여 VMware 라이브 사이트 복구를 구성합니다.
   `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>'`

   Perl 스크립트가 암호의 특수 문자를 입력의 구분 기호로 읽지 않도록 하려면 암호 값을 작은따옴표로 묶어야 합니다.

   애플리케이션 사용자 이름 및 암호는 ONTAP 도구 배포 중에 설정됩니다. VASA Provider/SRA 등록에 필요합니다.

9. 어댑터를 다시 검색하여 VMware Live Site Recovery Storage Replication Adapters 페이지에서 세부 정보가 업데이트되었는지 확인합니다.

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

SRA 자격 증명을 업데이트합니다

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

시작하기 전에

항목에서 언급한 단계를 실행했어야 "VMware Live Site Recovery 어플라이언스에서 SRA 구성"합니다.

단계

1. 다음 명령을 실행하여 VMware Live Site Recovery 시스템 폴더 캐시된 ONTAP tools 사용자 이름 암호를 삭제합니다.
   a. `sudo su <enter root password>`
   b. `docker ps`
   c. `docker exec -it <container_id> sh`
   d. `cd conf/`
   e. `rm -rf *`
2. Perl 명령을 실행하여 새 자격 증명으로 SRA를 구성합니다.
   a. `cd ..`

b. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>` 암호 값을 따옴표로 묶어야 합니다.

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

보호 및 복구 사이트를 구성합니다

보호 사이트에서 가상 머신 그룹을 보호하려면 보호 그룹을 만들어야 합니다.

보호 그룹을 구성합니다

시작하기 전에

소스 사이트와 타겟 사이트가 모두 다음에 대해 구성되어 있는지 확인해야 합니다.

- 동일한 버전의 VMware Live Site Recovery가 설치되었습니다
- 가상 머신
- 페어링된 보호 및 복구 사이트
- 소스 및 대상 데이터 저장소를 해당 사이트에 마운트해야 합니다

단계

1. vCenter Server에 로그인한 다음 * Site Recovery * > * Protection Groups * 를 선택합니다.
2. 보호 그룹 * 창에서 * 새로 만들기 * 를 선택합니다.
3. 보호 그룹의 이름과 설명을 지정하고 * 다음 * 을 선택합니다.
4. Type * 필드에서 * Type 필드 옵션… * 을 NFS 및 VMFS 데이터 저장소에 대한 데이터 저장소 그룹(스토리지 기반 복제)으로 선택합니다. 복제가 활성화된 SVM에 대한 장애 도메인은 더 이상 없습니다. 피어링만 구축되며 문제가 없는 SVM이 표시됩니다.
5. Replication Groups 탭에서 설정된 스토리지 페어 또는 구성한 가상 머신이 있는 복제 그룹을 선택한 후 * Next * 를 선택합니다.

   복제 그룹의 모든 가상 머신이 보호 그룹에 추가됩니다.

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

보호 사이트와 복구 사이트 페어링

vSphere Client를 사용하여 생성한 보호 사이트와 복구 사이트를 페어링하여 SRA(Storage Replication Adapter)가 스토리지 시스템을 검색할 수 있도록 설정해야 합니다.

시작하기 전에

- 보호 사이트와 복구 사이트에 VMware Live Site Recovery가 설치되어 있어야 합니다.
- 보호 사이트와 복구 사이트에 SRA가 설치되어 있어야 합니다.

단계

1. vSphere Client 홈 페이지에서 * Site Recovery * 를 두 번 클릭하고 * Sites * 를 선택합니다.
2. 오브젝트 * > * 작업 * > * 페어 사이트 * 를 선택합니다.
3. 사이트 복구 관리자 서버 페어링 * 대화 상자에서 보호된 사이트의 플랫폼 서비스 컨트롤러 주소를 입력한 후 * 다음 * 을 선택합니다.
4. vCenter Server 선택 섹션에서 다음을 수행합니다.
   a. 보호 사이트의 vCenter Server가 페어링하는 데 일치하는 후보로 나타나는지 확인합니다.
   b. SSO 관리 자격 증명을 입력한 다음 * Finish * 를 선택합니다.
5. 메시지가 표시되면 * 예 * 를 선택하여 보안 인증서를 수락합니다.

결과

보호된 사이트와 복구 사이트가 모두 개체 대화 상자에 나타납니다.

보호 및 복구 사이트 리소스를 구성합니다

네트워크 매핑을 구성합니다

보호 사이트에서 복구 사이트의 적절한 리소스로 각 리소스를 매핑할 수 있도록 두 사이트의 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 연결해야 합니다.

단계

1. vCenter Server에 로그인하고 * Site Recovery * > * Sites * 를 선택합니다.
2. 보호된 사이트를 선택하고 * 관리 * 를 선택합니다.
3. 관리 탭에서 * 네트워크 매핑 * > * 신규 * 를 선택하여 새 네트워크 매핑을 생성합니다.
4. 네트워크 매핑 만들기 마법사에서 다음을 수행합니다.
   a. 이름이 일치하는 네트워크에 대한 매핑 자동 준비 * 를 선택하고 * 다음 * 을 선택합니다.
   b. 보호 및 복구 사이트에 필요한 데이터 센터 개체를 선택하고 * 매핑 추가 * 를 선택합니다.
   c. 매핑을 성공적으로 생성한 후 * 다음 * 을 선택합니다.
   d. 역방향 매핑을 생성하기 위해 이전에 사용된 오브젝트를 선택한 후 * Finish * 를 선택합니다.

결과

네트워크 매핑 페이지에는 보호된 사이트 리소스와 복구 사이트 리소스가 표시됩니다. 사용자 환경의 다른 네트워크에 대해서도 동일한 단계를 수행할 수 있습니다.

폴더 매핑을 구성합니다

보호 사이트와 복구 사이트의 폴더를 매핑하여 폴더 간 통신을 활성화해야 합니다.

시작하기 전에

보호 사이트와 복구 사이트를 연결해야 합니다.

단계

1. vCenter Server에 로그인하고 * Site Recovery * > * Sites * 를 선택합니다.
2. 보호된 사이트를 선택하고 * 관리 * 를 선택합니다.
3. 관리 탭에서 * 폴더 매핑 * > * 폴더 * 아이콘을 선택하여 새 폴더 매핑을 생성합니다.
4. 폴더 매핑 생성 마법사에서 다음을 수행합니다.
   a. 이름이 일치하는 폴더에 대한 매핑 자동 준비 * 를 선택하고 * 다음 * 을 선택합니다.
   b. 보호 및 복구 사이트에 필요한 데이터 센터 개체를 선택하고 * 매핑 추가 * 를 선택합니다.
   c. 매핑을 성공적으로 생성한 후 * 다음 * 을 선택합니다.
   d. 역방향 매핑을 생성하기 위해 이전에 사용된 오브젝트를 선택한 다음 * 마침 * 을 선택합니다.

결과

폴더 매핑 페이지에는 보호된 사이트 리소스와 복구 사이트 리소스가 표시됩니다. 사용자 환경의 다른 네트워크에 대해서도 동일한 단계를 수행할 수 있습니다.

리소스 매핑을 구성합니다

가상 시스템이 하나의 호스트 그룹 또는 다른 그룹으로 페일오버되도록 구성되도록 보호 사이트 및 복구 사이트에 리소스를 매핑해야 합니다.

시작하기 전에

보호 사이트와 복구 사이트를 연결해야 합니다.

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

단계

1. vCenter Server에 로그인하고 * Site Recovery * > * Sites * 를 선택합니다.
2. 보호된 사이트를 선택하고 * 관리 * 를 선택합니다.
3. 관리 탭에서 * 리소스 매핑 * > * 신규 * 를 선택하여 새 리소스 매핑을 생성합니다.
4. 리소스 매핑 생성 마법사에서 다음을 수행합니다.
   a. 일치하는 이름의 리소스에 대한 매핑 자동 준비 * 를 선택하고 * 다음 * 을 선택합니다.
   b. 보호 및 복구 사이트에 필요한 데이터 센터 개체를 선택하고 * 매핑 추가 * 를 선택합니다.
   c. 매핑을 성공적으로 생성한 후 * 다음 * 을 선택합니다.
   d. 역방향 매핑을 생성하기 위해 이전에 사용된 오브젝트를 선택한 다음 * 마침 * 을 선택합니다.

결과

리소스 매핑 페이지에는 보호된 사이트 리소스와 복구 사이트 리소스가 표시됩니다. 사용자 환경의 다른 네트워크에 대해서도 동일한 단계를 수행할 수 있습니다.

자리 표시자 데이터 저장소를 구성합니다

보호된 가상 머신(VM)의 복구 사이트에서 vCenter 인벤토리에 위치를 보관하도록 자리 표시자 데이터 저장소를 구성해야 합니다. 자리 표시자 VM이 작고 수백 킬로바이트 이하만 사용하기 때문에 자리 표시자 데이터 저장소는 크기가 클 필요가 없습니다.

시작하기 전에

- 보호 사이트와 복구 사이트를 연결해야 합니다.
- 리소스 매핑을 구성해야 합니다.

단계

1. vCenter Server에 로그인하고 * Site Recovery * > * Sites * 를 선택합니다.
2. 보호된 사이트를 선택하고 * 관리 * 를 선택합니다.
3. 관리 탭에서 * 자리 표시자 데이터 저장소 * > * 신규 * 를 선택하여 새 자리 표시자 데이터 저장소를 생성합니다.
4. 적절한 데이터 저장소를 선택하고 * OK * 를 선택합니다.

   자리 표시자 데이터 저장소는 로컬 또는 원격일 수 있으며 복제해서는 안 됩니다.

5. 3-5단계를 반복하여 복구 사이트에 대한 자리 표시자 데이터 저장소를 구성합니다.

Array Manager를 사용하여 **SRA**를 구성합니다

VMware Live Site Recovery의 Array Manager 마법사를 사용하여 SRA(스토리지 복제 어댑터)를 구성하여 VMware Live Site Recovery와 SVM(스토리지 가상 머신) 간의 상호 작용을 지원할 수 있습니다.

시작하기 전에

- VMware Live Site Recovery에서 보호된 사이트와 복구 사이트를 페어링해야 합니다.
- 어레이 관리자를 구성하기 전에 온보드된 스토리지를 구성해야 합니다.
- 보호된 사이트와 복구 사이트 간에 SnapMirror 관계를 구성하고 복제해야 합니다.
- 멀티테넌시를 사용하도록 SVM 관리 LIF를 활성화해야 합니다.

SRA는 클러스터 수준 관리 및 SVM 수준 관리를 지원합니다. 클러스터 레벨에서 스토리지를 추가하면 클러스터의 모든 SVM을 검색하고 작업을 수행할 수 있습니다. SVM 레벨에서 스토리지를 추가할 경우 해당 SVM만 관리할 수 있습니다.

단계

1. VMware Live Site Recovery에서 * Array Managers * > * Add Array Manager * 를 선택합니다.
2. VMware Live Site Recovery의 스토리지를 설명하는 다음 정보를 입력합니다.

   a. Display Name* 필드에 어레이 관리자를 식별할 이름을 입력하십시오.

b. SRA Type * 필드에서 * ONTAP * 용 NetApp 스토리지 복제 어댑터를 선택합니다.

c. 클러스터 또는 SVM에 연결할 정보를 입력합니다.

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

> 스토리지 관리자를 구성할 때는 VMware vSphere용 ONTAP 툴에서 스토리지 시스템을 온보딩하는 데 사용된 스토리지 시스템에 대해 동일한 접속(IP 주소)을 사용해야 합니다. 예를 들어, 어레이 관리자 구성이 SVM 범위인 경우 VMware vSphere용 ONTAP 툴에 있는 스토리지를 SVM 레벨에서 추가해야 합니다.

d. 클러스터에 연결하려면 SVM 이름 * 필드에 SVM 이름을 입력합니다.

이 필드를 비워 둘 수도 있습니다.

e. Volume include list *(볼륨 포함 목록 *) 필드에 검색할 볼륨을 입력합니다.

보호 사이트의 소스 볼륨 및 복구 사이트의 복제된 대상 볼륨을 입력할 수 있습니다.

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

f. * (선택 사항) * * Volume exclude list *(볼륨 제외 목록 *) 필드에 검색에서 제외할 볼륨을 입력합니다.

보호 사이트의 소스 볼륨 및 복구 사이트의 복제된 대상 볼륨을 입력할 수 있습니다.

예를 들어 volume_dst_vol1_과 SnapMirror 관계에 있는 volume_src_vol1_을 제외하려면 보호된 사이트 필드에 _src_vol1_를 지정하고 복구 사이트 필드에 _dst_vol1_를 지정해야 합니다.

3. 다음 * 을 선택합니다.
4. Array Manager 추가 창 하단에 어레이가 검색되어 표시되는지 확인하고 * Finish * 를 선택합니다.

적절한 SVM 관리 IP 주소와 자격 증명을 사용하여 복구 사이트에 대해 동일한 단계를 수행할 수 있습니다. Add Array Manager 마법사의 Enable Array Pairs 화면에서 올바른 스토리지 쌍이 선택되었는지 확인하고 사용할 준비가 되었음을 표시해야 합니다.

복제된 스토리지 시스템을 확인합니다

SRA(Storage Replication Adapter)를 구성한 후 보호 사이트와 복구 사이트가 성공적으로 페어링되었는지 확인해야 합니다. 복제된 스토리지 시스템은 보호 사이트와 복구 사이트 모두에서 검색할 수 있어야 합니다.

- 시작하기 전에 *
- 스토리지 시스템을 구성해야 합니다.
- VMware Live Site Recovery 어레이 관리자를 사용하여 보호 사이트와 복구 사이트를 페어링해야 합니다.
- SRA에 대한 테스트 페일오버 작업 및 페일오버 작업을 수행하기 전에 FlexClone 라이센스 및 SnapMirror 라이센스를 활성화해야 합니다.
- 소스 사이트와 대상 사이트에 동일한 SnapMirror 정책 및 일정이 있어야 합니다.

단계

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

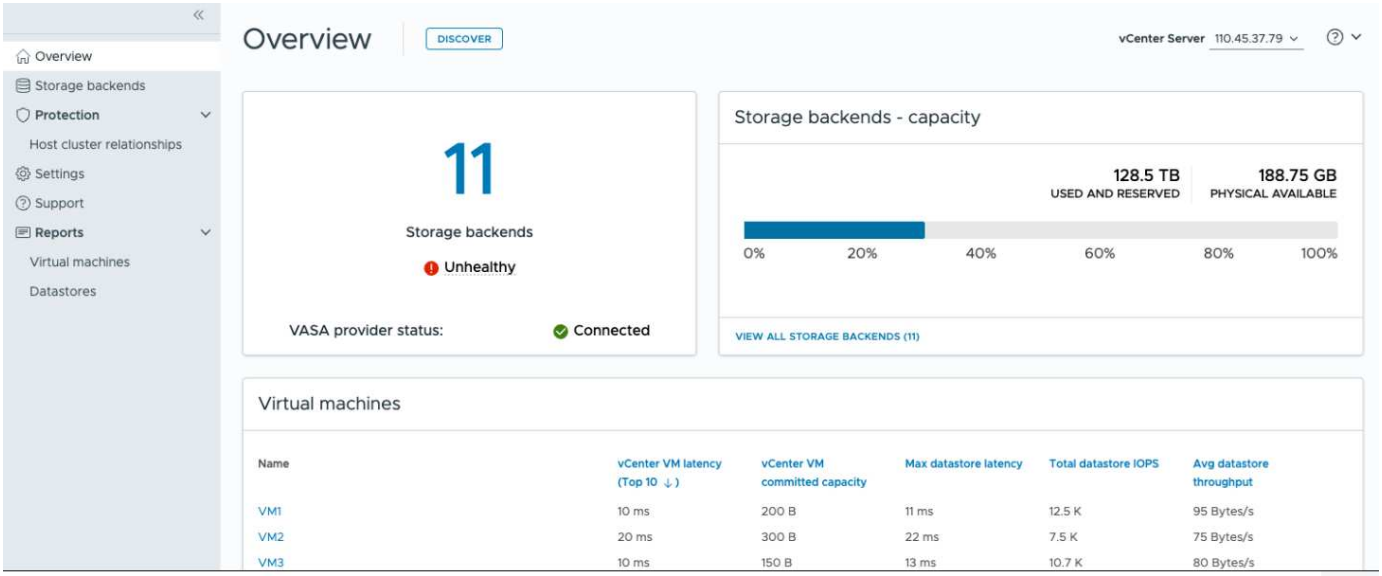
   보호 사이트 및 복구 사이트에서 상태가 ""Enabled""로 설정된 스토리지 시스템을 검색해야 합니다.

VMware vSphere용 ONTAP 툴을 관리합니다

VMware vSphere용 ONTAP 툴 대시보드 개요

vCenter Client의 바로 가기 섹션에서 VMware vSphere 플러그인용 ONTAP 툴 아이콘을 선택하면 사용자 인터페이스에서 개요 페이지로 이동합니다. 이 페이지는 VMware vSphere 플러그인용 ONTAP 툴에 대한 요약을 제공하는 대시보드 역할을 합니다.

ELM(Enhanced Linked Mode Setup)의 경우 vCenter Server 선택 드롭다운이 나타나고 원하는 vCenter Server를 선택하여 관련 데이터를 볼 수 있습니다. 이 드롭다운은 플러그인의 다른 모든 목록 보기에 사용할 수 있습니다. 한 페이지에서 선택한 vCenter Server는 플러그인의 탭 간에 계속 유지됩니다.



개요 페이지에서 * Discovery * 작업을 실행할 수 있습니다. 검색 작업은 vCenter 레벨에서 검색을 실행하여 새로 추가되거나 업데이트된 스토리지 백엔드, 호스트, 데이터 저장소 및 보호 상태/관계를 감지합니다. 예약된 검색을 기다리지 않고도 필요에 따라 엔터티 검색을 실행할 수 있습니다.

작업 버튼은 검색 작업을 수행할 수 있는 권한이 있는 경우에만 활성화됩니다.

검색 요청이 제출되면 Recent Tasks(최근 작업) 패널에서 작업 진행 상황을 추적할 수 있습니다.

대시보드에는 시스템의 다양한 요소를 보여 주는 여러 카드가 있습니다. 다음 표는 다양한 카드와 카드를 나타냅니다.

* 카드 *	* 설명 *
상태	상태 카드에는 스토리지 백엔드 수와 스토리지 백엔드 및 VASA Provider의 전체 상태가 표시됩니다. 모든 스토리지 백엔드 상태가 정상이면 스토리지 백엔드 상태가 * 정상 * 으로 표시되고 스토리지 백엔드 중 하나에 문제가 있는 경우 * 비정상 * 으로 표시됩니다(알 수 없음/도달할 수 없음/성능 저하 상태). 툴 팁을 선택하여 스토리지 백엔드의 상태 세부 정보를 엽니다. 자세한 내용을 보려면 임의의 스토리지 백엔드를 선택할 수 있습니다. * Other VASA Provider states * 링크는 vCenter Server에 등록된 VASA Provider의 현재 상태를 표시합니다.

스토리지 백엔드 - 용량	이 카드는 선택한 vCenter Server 인스턴스에 대해 모든 스토리지 백엔드의 집계된 사용 용량 및 사용 가능한 용량을 보여 줍니다. ASA R2 스토리지 시스템의 경우 용량 데이터가 분리된 시스템으로 표시되지 않습니다.
가상 머신	이 카드는 성능 메트릭별로 정렬된 상위 10개 VM을 보여 줍니다. 머리글을 선택하여 선택한 메트릭에 대해 상위 10개의 VM을 오름차순 또는 내림차순으로 정렬할 수 있습니다. 카드의 정렬 및 필터링 변경 사항은 브라우저 캐시를 변경하거나 지울 때까지 유지됩니다.
데이터 저장소	이 카드는 성능 메트릭별로 정렬된 상위 10개 데이터 저장소를 보여 줍니다. 머리글을 선택하여 선택한 메트릭에 대한 상위 10개 데이터 저장소를 오름차순 또는 내림차순으로 정렬할 수 있습니다. 카드의 정렬 및 필터링 변경 사항은 브라우저 캐시를 변경하거나 지울 때까지 유지됩니다. 데이터 저장소 유형 드롭다운에서 데이터 저장소 유형을 선택할 수 있습니다(NFS, VMFS 또는 VVol).
ESXi 호스트 규정 준수 카드	이 카드는 설정 그룹/범주별로 권장되는 NetApp 호스트 설정과 관련된 모든 ESXi 호스트(선택한 vCenter에 대한) 설정의 전체 규정 준수 상태를 표시합니다. 권장 설정 적용 * 링크를 선택하여 권장 설정을 적용할 수 있습니다. 호스트의 준수 상태를 선택하여 호스트 목록을 볼 수 있습니다.

ONTAP 도구 관리자 사용자 인터페이스

VMware vSphere용 ONTAP 툴은 여러 vCenter Server 인스턴스를 관리할 수 있는 멀티 테넌트 시스템입니다. ONTAP tools Manager를 사용하면 VMware vSphere 관리자가 관리되는 vCenter Server 인스턴스 및 온보드된 스토리지 백엔드에 대해 ONTAP 툴을 더 효율적으로 제어할 수 있습니다.

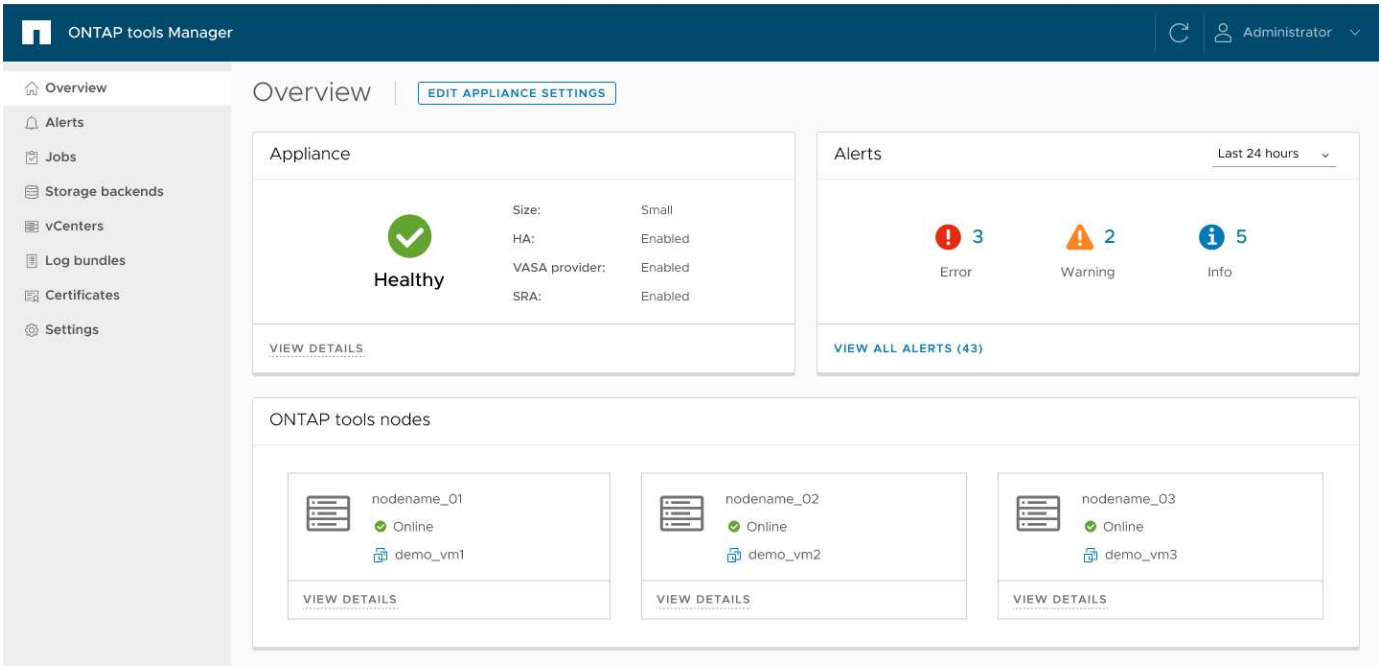
ONTAP Tools Manager는 다음과 같은 기능을 제공합니다.

- vCenter Server 인스턴스 관리 - vCenter Server 인스턴스를 ONTAP 툴에 추가 및 관리합니다.
- 스토리지 백엔드 관리 - ONTAP 스토리지 클러스터를 VMware vSphere용 ONTAP 툴에 추가 및 관리하고 전체적으로 온보딩된 vCenter Server 인스턴스에 매핑합니다.
- 로그 번들 다운로드 - VMware vSphere용 ONTAP 툴에 대한 로그 파일을 수집합니다.
- 인증서 관리 - 자체 서명된 인증서를 사용자 지정 CA 인증서로 변경하고 VASA 공급자 및 ONTAP 툴의 모든 인증서를 갱신하거나 새로 고칩니다.
- 암호 관리 - 사용자의 OVA 응용 프로그램 암호를 재설정합니다.

ONTAP Tools Manager에 액세스하려면 `https://<ONTAPtoolsIP>:8443/virtualization/ui/` 브라우저에서 을 시작하고 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.

ONTAP tools Manager 개요 섹션은 서비스 관리, 노드 크기 확장 및 고가용성(HA) 지원과 같은 어플라이언스 구성을 관리하는 데 도움이 됩니다. 또한 상태, 네트워크 세부 정보, 알림과 같이 노드와 관련된 ONTAP 툴의 전반적인 정보를

모니터링할 수 있습니다.



* 카드 *	* 설명 *
어플라이언스 카드	어플라이언스 카드는 ONTAP 도구 어플라이언스의 전체 상태를 제공합니다. 어플라이언스 구성 세부 정보 및 활성화된 서비스의 상태를 표시합니다. ONTAP 도구 어플라이언스에 대한 자세한 내용을 보려면 * 세부 정보 보기 * 링크를 선택하십시오. 어플라이언스 설정 편집 작업 작업이 진행 중이면 어플라이언스 포틀릿에 작업의 상태 및 세부 정보가 표시됩니다.
경고 카드	경고 카드에는 HA 노드 레벨 경고를 포함하여 ONTAP 툴 경고가 유형별로 나열됩니다. 개수 텍스트(하이퍼링크)를 선택하여 알림 목록을 볼 수 있습니다. 링크는 선택한 유형별로 필터링된 경고 보기 페이지로 연결됩니다.
ONTAP 도구 노드 카드	ONTAP tools nodes 카드는 노드 이름, 노드 VM 이름, 상태 및 모든 네트워크 관련 데이터가 있는 노드 목록을 표시합니다. View details * 를 선택하여 선택한 노드와 관련된 추가 세부 정보를 볼 수 있습니다. [참고] 비 HA 설정에서는 하나의 노드만 표시됩니다. HA 설정에서 3개의 노드가 표시됩니다.

VMware vSphere용 ONTAP 도구의 igroups 및 내보내기 정책 이해

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

VMware vSphere 9.x용 ONTAP 도구에서 igroup은 vCenter의 각 데이터스토어가 단일 igroup과 연결되는 플랫 구조로 생성 및 관리되었습니다. 이 모델은 여러 데이터스토어에서 igroup의 유연성과 재사용성을 제한했습니다.

VMware vSphere 10.x용 ONTAP 도구는 중첩 igroup을 도입하여 vCenter의 각 데이터스토어가 상위 igroup과 연결되고, 각 호스트는 해당 상위 igroup 아래의 하위 igroup에 연결됩니다. VMware 여러 데이터스토어에서 재사용할 수 있도록 사용자 정의 이름으로 사용자 지정 상위 igroup을 정의하여 igroup을 더욱 유연하고 상호 연결된 방식으로 관리할 수 있습니다. vSphere용 ONTAP 도구에서 LUN과 데이터스토어를 효과적으로 관리하려면 igroup 워크플로우를 이해하는 것이 필수적입니다. 다음 예와 같이 워크플로우에 따라 다양한 igroup 구성이 생성됩니다.

언급된 이름은 예시 목적으로만 사용되었으며 실제 igroup 이름을 나타내는 것이 아닙니다. ONTAP 도구에서 관리하는 igroup은 "otv_" 접두사를 사용합니다. 사용자 지정 igroup에는 원하는 이름을 지정할 수 있습니다.

기간	설명
DS<숫자>	데이터 저장소
iqn<숫자>	초기자 IQN
호스트<번호>	호스트 MoRef
lun<숫자>	LUN ID입니다
<DSName>Igroup<번호>	기본(ONTAP 도구 관리) 상위 igroup
<호스트-모어>그룹<번호>	어린이 i그룹
CustomIgroup<숫자>	사용자 정의 사용자 정의 상위 igroup
ClassicIgroup<숫자>	ONTAP 도구 9.x 버전에서 사용되는 igroup입니다.

예시 **1:**

하나의 이니시에이터로 단일 호스트에 데이터 저장소 생성

작업 흐름: [생성] DS1(lun1): host1(iqn1)

- 결과 *:
- DS1Igroup:
  - host1Igroup → (iqn1: lun1)

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

예시 **2:**

기존 데이터 저장소를 추가 호스트에 마운트합니다.

워크플로: [마운트] DS1(lun1): host2(iqn2)

- 결과 *:
- DS1Igroup:
  - host1Igroup → (iqn1: lun1)
  - host2Igroup → (iqn2: lun1)

자식 igroup host2Igroup이 생성되어 기존 부모 igroup DS1Igroup에 추가됩니다.

예시 **3:**

호스트에서 데이터 저장소 마운트 해제

워크플로: [마운트 해제] DS1(lun1): 호스트1(iqn1)

- 결과 *:
- DS1Igroup:
  - host2Igroup → (iqn2: lun1)

host1Igroup이 계층 구조에서 제거됩니다. 자식 igroup은 명시적으로 삭제되지 않습니다. 삭제는 다음 두 가지 조건에서 발생합니다. • LUN이 매핑되지 않은 경우 ONTAP 시스템은 자식 igroup을 삭제합니다. • 예약된 정리 작업을 통해 LUN 매핑이 없는 불안정한 자식 igroup을 제거합니다. 이러한 시나리오는 ONTAP 도구에서 관리하는 igroup에만 적용되며, 사용자 지정 igroup에는 적용되지 않습니다.

예시 **4:**

데이터 저장소 삭제

작업 흐름: [삭제] DS1(lun1): host2(iqn2)

- 결과 *:
- DS1Igroup:
  - host2Igroup → (iqn2: lun1)

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

예시 **5:**

사용자 정의 부모 igroup 아래에 여러 데이터 저장소 만들기

작업 흐름:

- [생성] DS2(lun2): host1(iqn1), host2(iqn2)
- [생성] DS3(lun3): host1(iqn1), host3(iqn3)
- 결과 *:
- CustomIgroup1:
  - host1Igroup → (iqn1: lun2, lun3)
  - host2Igroup → (iqn2: lun2)
  - host3Igroup → (iqn3: lun3)

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

예시 **6:**

사용자 정의 상위 igroup에 있는 하나의 데이터 저장소를 삭제합니다.

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

- 결과 *:

- CustomIgroup1:
  - host1Igroup → (iqn1: lun3)
  - host3Igroup → (iqn3: lun3)
- CustomIgroup1은 재사용되지 않더라도 삭제되지 않습니다.
- LUN이 매핑되지 않으면 ONTAP 시스템은 host2Igroup을 삭제합니다.
- host1Igroup은 DS3의 lun3에 매핑되어 있으므로 삭제되지 않습니다. 사용자 지정 igroup은 재사용 상태와 관계없이 삭제되지 않습니다.

예시 **7:**

vVols 데이터 저장소 확장(볼륨 추가)

작업 흐름:

확장 전:

[확장] DS4(lun4): host4(iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

확장 후:

[확장] DS4(lun4, lun5): host4(iqn4)

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

새로운 LUN이 생성되어 기존 자식 igroup host4Igroup에 매핑됩니다.

예시 **8:**

vVols 데이터 저장소 축소(볼륨 제거)

작업 흐름:

수축 전:

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

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

수축 후:

[축소] DS4(lun4): host4(iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

지정된 LUN(lun5)이 자식 igroup에서 매핑 해제됩니다. igroup은 매핑된 LUN이 하나 이상 있는 한 활성 상태로 유지됩니다.

예시 **9:**

ONTAP 도구 9에서 10으로 마이그레이션(igroup 정규화)

- 워크플로 *

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

이전 전:

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

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

마이그레이션 후:

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

마이그레이션 중:

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

이를 통해 계층적 모델을 준수할 수 있습니다.

관련 항목

"Igroup 정보"

엑스포트 정책

내보내기 정책은 VMware vSphere용 ONTAP 도구에서 NFS 데이터 저장소에 대한 액세스를 제어합니다. 이 정책은 데이터 저장소에 액세스할 수 있는 클라이언트와 해당 클라이언트가 가진 권한을 정의합니다. 내보내기 정책은 ONTAP 시스템에서 생성 및 관리되며, NFS 데이터 저장소와 연결하여 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.

VMware vSphere용 ONTAP 도구에서 NFS 데이터스토어를 생성할 때 기존 내보내기 정책을 선택하거나 새 정책을 생성할 수 있습니다. 내보내기 정책은 데이터스토어에 적용되어 권한이 있는 클라이언트만 액세스할 수 있도록 합니다.

새 ESXi 호스트에 NFS 데이터스토어를 마운트하면 VMware vSphere용 ONTAP 도구가 호스트의 IP 주소를 데이터스토어와 연결된 기존 내보내기 정책에 추가합니다. 이를 통해 새 호스트는 새 내보내기 정책을 생성하지 않고도 데이터스토어에 액세스할 수 있습니다.

ESXi 호스트에서 NFS 데이터스토어를 삭제하거나 마운트 해제하면 ONTAP Tools for VMware vSphere가 내보내기 정책에서 호스트의 IP 주소를 제거합니다. 다른 호스트에서 해당 내보내기 정책을 사용하지 않으면 해당 정책은 삭제됩니다. NFS 데이터스토어를 삭제하면 ONTAP Tools for VMware vSphere는 다른 데이터스토어에서 재사용되지 않는 경우 해당 데이터스토어와 연결된 내보내기 정책을 제거합니다. 내보내기 정책이 재사용되면 호스트 IP 주소는 그대로 유지되고 변경되지 않습니다. 데이터스토어를 삭제하면 내보내기 정책은 호스트 IP 주소 할당을 해제하고 기본 내보내기 정책을 할당하여 ONTAP 시스템이 필요한 경우 해당 정책에 액세스할 수 있도록 합니다.

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

관련 항목

"엑스포트 정책을 생성합니다"

VMware vSphere 서비스에 대해 ONTAP 툴을 사용하도록 설정합니다

Manager: ONTAP Tools Manager를 사용하여 VASA 공급자, VVol 구성 가져오기, SRA(재해 복구)와 같은 서비스를 지원합니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.
3. 개요 섹션에서 * 어플라이언스 설정 편집 * 을 선택합니다.
4. 서비스 * 섹션에서 필요에 따라 VASA Provider, VVol 구성 가져오기, SRA(재해 복구) 등의 옵션 서비스를 활성화할 수 있습니다.

   서비스를 처음 설정할 때는 VASA Provider 및 SRA 자격 증명을 생성해야 합니다. vCenter Server에서 VASA Provider 및 SRA 서비스를 등록하거나 설정하는 데 사용됩니다.

   선택적 서비스를 비활성화하기 전에 ONTAP 툴로 관리되는 vCenter Server에서 해당 서비스를 사용하지 않도록 하십시오.

   Allow import of vVols configuration * 옵션은 VASA Provider 서비스가 활성화된 경우에만 표시됩니다. 이 옵션을 사용하면 ONTAP 툴 9.x에서 ONTAP 툴 10.3으로 VVol 데이터를 마이그레이션할 수 있습니다.

VMware vSphere 구성에 대한 ONTAP 툴을 변경합니다

ONTAP Tools Manager를 사용하여 VMware vSphere용 ONTAP 툴을 확장하여 구축 시 노드 수를 늘리거나 구성을 고가용성(HA) 설정으로 변경합니다. VMware vSphere 어플라이언스용 ONTAP 툴은 처음에 단일 노드 비 HA 구성으로 구축됩니다.

- 시작하기 전에 *
- OVA 템플릿의 OVA 버전이 노드 1과 동일한지 확인합니다. 노드 1은 VMware vSphere OVA용 ONTAP 툴이 처음 구축되는 기본 노드입니다.
- CPU 핫 애드 및 메모리 핫 플러그가 활성화되어 있는지 확인합니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.
3. 개요 섹션에서 * 어플라이언스 설정 편집 * 을 선택합니다.
4. Configuration * 섹션에서 필요에 따라 노드 크기를 늘릴 수 있도록 스케일업하고 HA 구성을 활성화할 수 있습니다.

변경하려면 vCenter Server 자격 증명이 필요합니다.

ONTAP 도구가 HA 구성으로 되어 있으면 콘텐츠 라이브러리 세부 정보를 변경할 수 있습니다. 새 편집 제출에 대한 암호를 다시 입력해야 합니다.

VMware vSphere용 ONTAP 툴에서는 노드 크기만 늘릴 수 있고 노드 크기를 줄일 수는 없습니다. HA가 아닌 설정에서는 중간 규모 구성만 지원됩니다. HA 설정에서는 중간 규모 및 대규모 구성이 지원됩니다.

5. HA 전환 버튼을 사용하여 HA 구성을 활성화합니다. HA 설정 * 페이지에서 다음을 확인합니다.
   - 컨텐츠 라이브러리는 ONTAP 툴 노드 VM이 실행되는 동일한 vCenter Server에 속합니다. vCenter Server 자격 증명은 어플라이언스 변경 사항을 확인하기 위해 OVA 템플릿을 다운로드하고 다운로드하는 데 사용됩니다.
   - ONTAP 툴을 호스팅하는 가상 시스템은 ESXi 호스트에 직접 구축되지 않습니다. VM은 클러스터 또는 리소스 풀에 배포해야 합니다.

     HA 구성이 활성화되면 HA가 아닌 단일 노드 구성으로 되돌릴 수 없습니다.

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

   대부분의 입력 옵션은 워크플로우의 용이성을 위해 노드 1 네트워크 세부 정보로 미리 채워져 있습니다. 그러나 마법사의 마지막 페이지로 이동하기 전에 입력 데이터를 편집할 수 있습니다. 첫 번째 노드에서 IPv6 주소가 활성화된 경우에만 다른 두 노드에 대해 IPv6 주소 세부 정보를 입력할 수 있습니다.

   ESXi 호스트에 ONTAP 툴 VM이 하나만 포함되어 있는지 확인합니다. 입력은 다음 창으로 이동할 때마다 검증됩니다.

7. 요약 * 섹션의 세부 사항을 검토하고 변경 사항을 * 저장 * 하십시오.

다음 단계

개요 * 페이지에는 배포 상태가 표시됩니다. 작업 ID를 사용하여 작업 보기에서 어플라이언스 설정 편집 작업 상태를 추적할 수도 있습니다.

HA 구축에 실패하고 새 노드의 상태가 'New'로 표시되면 HA 활성화 작업을 다시 시도하기 전에 vCenter에서 새 VM을 삭제합니다.

왼쪽 패널의 * Alerts * 탭에는 VMware vSphere용 ONTAP 툴에 대한 경고가 표시됩니다.

데이터 저장소를 관리합니다

NFS 및 VMFS 데이터 저장소를 마운트합니다

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

이 작업에 대해

- vSphere Client 버전 및 선택한 데이터 저장소 유형에 따라 일부 마우스 오른쪽 버튼 클릭 작업이 해제되거나 사용할 수 없습니다.
  - vSphere Client 8.0 이상 버전을 사용하는 경우 마우스 오른쪽 버튼 클릭 옵션 중 일부가 표시되지 않습니다.
  - vSphere 7.0U3에서 vSphere 8.0 버전까지 옵션이 표시되더라도 작업이 비활성화됩니다.
- 호스트 클러스터가 균일한 구성으로 보호되는 경우 데이터 저장소 마운트 옵션이 비활성화됩니다.

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 데이터 저장소를 마운트하려면 마우스 오른쪽 버튼을 클릭하고 * NetApp ONTAP tools * > * Mount Datastores * 를 선택합니다.
4. 마운트할 데이터 저장소를 선택하고 * Mount * 를 선택합니다.

다음 단계

최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

NFS 및 VMFS 데이터 저장소를 마운트 해제합니다

데이터 저장소 마운트 해제 작업은 ESXi 호스트에서 NFS 또는 VMFS 데이터 저장소를 마운트 해제합니다. 데이터 저장소 마운트 해제 작업은 VMware vSphere용 ONTAP 툴로 검색되거나 관리되는 NFS 및 VMFS 데이터 저장소에 대해 설정됩니다.

단계

1. vSphere Client에 로그인합니다
2. NFS 또는 VMFS 데이터 저장소 객체를 마우스 오른쪽 버튼으로 클릭하고 * Unmount datastore * 를 선택합니다.

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

3. 데이터 저장소를 마운트 해제할 ESXi 호스트를 하나 이상 선택합니다.

   모든 호스트에서 데이터 저장소를 마운트 해제할 수 없습니다. 사용자 인터페이스에서 데이터 저장소 삭제 작업을 대신 사용할 것을 제안합니다.

4. Unmount * 버튼을 선택합니다.

   데이터 저장소가 보호된 호스트 클러스터의 일부인 경우 경고 메시지가 표시됩니다.

보호된 데이터 저장소가 마운트 해제되면 기존 보호 설정이 부분적으로 보호될 수 있습니다. "보호된 호스트 클러스터를 수정합니다"전체 보호를 활성화하려면 을 참조하십시오.

다음 단계

최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

VVOL 데이터 저장소를 마운트합니다

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

단계

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

최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

NFS 및 VMFS 데이터 저장소의 크기를 조정합니다

데이터 저장소의 크기를 조정하면 가상 시스템 파일의 스토리지를 늘릴 수 있습니다. 인프라 요구사항의 변화에 따라 데이터 저장소의 크기를 변경할 수 있습니다.

- 이 작업에 대한 정보 *

NFS 및 VMFS 데이터 저장소의 크기만 늘릴 수 있습니다. NFS 및 VMFS 데이터 저장소의 일부인 FlexVol 볼륨은 기존 크기 이하로 줄일 수 없지만 최대 120% 확장할 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 데이터 저장소를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools * > * Resize datastore * 를 선택합니다.
4. 크기 조정 대화 상자에서 데이터 저장소의 새 크기를 지정하고 * OK * 를 선택합니다.

VVOL 데이터 저장소를 확장합니다

vCenter 객체 보기에서 데이터 저장소 객체를 마우스 오른쪽 버튼으로 클릭하면 VMware vSphere용 ONTAP 툴 지원 작업이 플러그인 섹션 아래에 표시됩니다. 데이터 저장소의 유형과 현재 사용자 권한에 따라 특정 작업이 설정됩니다.

VVols 데이터 저장소 확장 작업은 ASA R2 기반 VVols 데이터 저장소에 적용할 수 없습니다.

단계

1. vSphere Client 홈 페이지에서 * 호스트 및 클러스터 * 를 선택합니다.
2. 탐색 창에서 데이터 저장소가 포함된 데이터 센터를 선택합니다.

3. 데이터 저장소를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools * > * Add storage to datastore * 를 선택합니다.
4. Create 또는 Select Volumes * 창에서 새 볼륨을 생성하거나 기존 볼륨에서 선택할 수 있습니다. 사용자 인터페이스는 쉽게 설명할 수 있습니다. 원하는 대로 지침을 따릅니다.
5. Summary * 창에서 선택 사항을 검토하고 * Expand * 를 선택합니다. 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

VVOL 데이터 저장소를 축소합니다

데이터 저장소 삭제 작업은 선택한 데이터 저장소에 VVol이 없을 때 데이터 저장소를 삭제합니다.

ASA R2 기반 VVols 데이터 저장소에 대해서는 VVOL 데이터 저장소 축소 작업이 지원되지 않습니다.

단계

1. vSphere Client 홈 페이지에서 * 호스트 및 클러스터 * 를 선택합니다.
2. 탐색 창에서 데이터 저장소가 포함된 데이터 센터를 선택합니다.
3. VVOL 데이터 저장소를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools * > * Remove storage from datastore * 를 선택합니다.
4. VVol이 없는 볼륨을 선택하고 * Remove * 를 선택합니다.

   VVol이 상주하는 볼륨을 선택하는 옵션은 비활성화됩니다.

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

데이터 저장소를 삭제합니다

데이터 저장소에서 스토리지 제거 작업은 vCenter Server에서 VMware vSphere가 검색하거나 관리되는 VVol 데이터 저장소용 모든 ONTAP 툴에서 지원됩니다. 이 작업을 통해 VVOL 데이터 저장소에서 볼륨을 제거할 수 있습니다.

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

vCenter Server의 VMware vSphere용 ONTAP 툴에서 데이터 저장소 삭제 작업은 다음과 같습니다.

- VVOL 컨테이너를 마운트 해제합니다.
- igroup을 정리합니다. igroup을 사용하고 있지 않으면 igroup에서 iqn을 제거합니다.
- VVol 컨테이너를 삭제합니다.
- Flex 볼륨을 스토리지 배열에 그대로 둡니다.

vCenter Server의 ONTAP 도구에서 NFS, VMFS 또는 VVOL 데이터 저장소를 삭제하려면 다음 단계를 따르십시오.

단계

1. vSphere Client에 로그인합니다
2. 호스트 시스템 또는 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools * > * Delete datastore * 를 선택합니다.

   해당 데이터 저장소를 사용하는 가상 시스템이 있는 경우 데이터 저장소를 삭제할 수 없습니다. 데이터 저장소를 삭제하기 전에 가상 머신을 다른 데이터 저장소로 이동해야 합니다. 데이터 저장소가 보호된 호스트 클러스터에 속한 경우 볼륨 삭제 확인란을 선택할 수 없습니다.

   a. NFS 또는 VMFS 데이터 저장소의 경우 데이터 저장소를 사용 중인 VM 목록이 포함된 대화 상자가 나타납니다.
   b. VMFS 데이터 저장소가 ASA R2 시스템에서 생성되고 보호 대상인 경우 데이터 저장소를 삭제하기 전에 보호 해제를 수행해야 합니다.
   c. VVols 데이터 저장소의 경우 데이터 저장소 삭제 작업은 연결된 VVol이 없는 경우에만 데이터 저장소를 삭제합니다. 데이터 저장소 삭제 대화 상자에는 ONTAP 클러스터에서 볼륨을 삭제하는 옵션이 제공됩니다.
   d. ASA R2 시스템 기반 VVol 데이터 저장소의 경우 백업 볼륨을 삭제하는 확인란은 적용되지 않습니다.
3. ONTAP 스토리지에서 백업 볼륨을 삭제하려면 * Delete volumes on ONTAP cluster * 를 선택합니다.

   보호된 호스트 클러스터에 속하는 VMFS 데이터 저장소에 대한 ONTAP 클러스터의 볼륨은 삭제할 수 없습니다.

데이터 저장소에 대한 **ONTAP** 스토리지 뷰

VMware vSphere용 ONTAP 툴은 구성 탭에 데이터 저장소와 해당 볼륨에 대한 ONTAP 스토리지의 뷰를 보여 줍니다.

단계

1. vSphere Client에서 데이터 저장소로 이동합니다.
2. 오른쪽 창에서 * Configure * 탭을 선택합니다.
3. NetApp ONTAP tools *> * ONTAP 스토리지 * 를 선택합니다. 데이터 저장소 유형에 따라 보기가 변경됩니다. 자세한 내용은 아래 표를 참조하십시오.

* 데이터 저장소 유형 *	* 사용 가능한 정보 *
NFS 데이터 저장소	스토리지 세부 정보 * 페이지에는 스토리지 백엔드, 집계 및 볼륨 정보가 포함되어 있습니다. NFS 세부 정보 페이지에는 NFS 데이터 저장소와 관련된 데이터가 포함되어 있습니다.
VMFS 데이터 저장소	스토리지 세부 정보 * 페이지에는 스토리지 백엔드, 집계 및 볼륨 정보가 포함되어 있습니다. lun details * 페이지에는 LUN과 관련된 데이터가 포함되어 있습니다. Namespace details * 페이지에는 VMFS 데이터 저장소가 NVMe/TCP 또는 NVMe/FC 프로토콜을 사용할 때 네임스페이스와 관련된 데이터가 포함되어 있습니다. ASA R2 스토리지 시스템 기반 데이터 저장소의 경우 볼륨 및 애그리게이트 세부 정보가 표시되지 않습니다.

VVOL 데이터 저장소	모든 볼륨을 나열합니다. ONTAP storage 창에서 스토리지를 확장하거나 제거할 수 있습니다. 이 보기는 ASA R2 시스템 기반 VVol 데이터 저장소에 대해 지원되지 않습니다.

가상 머신 스토리지 뷰

스토리지 보기에는 가상 시스템에서 생성된 VVol 목록이 표시됩니다.

이 보기는 VMware vSphere 관리 VVOL 데이터 저장소와 관련된 디스크가 마운트된 하나 이상의 ONTAP 툴이 있는 VM에 적용됩니다.

단계

1. vSphere Client에서 가상 머신으로 이동합니다.
2. 오른쪽 창에서 * Monitor * 탭을 선택합니다.
3. NetApp ONTAP tools * > * 스토리지 * 를 선택합니다. 오른쪽 창에 * Storage * 세부 정보가 나타납니다. VM에 있는 VVol 목록을 볼 수 있습니다.

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

스토리지 임계값 관리

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

단계:

1. vSphere Client에 로그인합니다
2. 바로 가기 페이지의 플러그인 섹션에서 * NetApp ONTAP tools * 를 선택합니다.
3. ONTAP 도구의 왼쪽 창에서 * 설정 * > * 임계값 설정 * > * 편집 * 으로 이동합니다.
4. Edit Threshold * 창에서 * 거의 다 찼음 * 및 * 전체 * 필드에 원하는 값을 입력하고 * Save * 를 선택합니다. 숫자를 권장 값으로 재설정할 수 있습니다. 이 값은 거의 가득 찬 경우 80이고 가득 찬 경우 90입니다.

스토리지 백엔드 관리

스토리지 백엔드는 ESXi 호스트가 데이터 스토리지에 사용하는 시스템입니다.

스토리지를 검색합니다

스토리지 세부 정보를 업데이트하기 위해 예약된 검색을 기다리지 않고 필요 시 스토리지 백엔드 검색을 실행할 수 있습니다.

다음 단계에 따라 스토리지 백엔드를 검색합니다.

단계

1. vSphere Client에 로그인합니다
2. 바로 가기 페이지의 플러그인 섹션에서 * NetApp ONTAP tools * 를 선택합니다.
3. ONTAP 도구의 왼쪽 창에서 * Storage Backend * 로 이동하여 스토리지 백엔드를 선택합니다.
4. 수직 타원 메뉴를 선택하고 * 스토리지 검색 * 을 선택합니다

최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

스토리지 백엔드를 수정합니다

이 섹션의 단계에 따라 스토리지 백엔드를 수정합니다.

1. vSphere Client에 로그인합니다
2. 바로 가기 페이지의 플러그인 섹션에서 * NetApp ONTAP tools * 를 선택합니다.
3. ONTAP 도구의 왼쪽 창에서 * Storage Backend * 로 이동하여 스토리지 백엔드를 선택합니다.
4. 수직 타원 메뉴를 선택하고 * 수정 * 을 선택하여 자격 증명 또는 포트 이름을 수정합니다. 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

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

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.
3. 사이드바에서 스토리지 백엔드를 선택합니다.
4. 수정할 스토리지 백엔드를 선택합니다.
5. 수직 타원 메뉴를 선택하고 * 수정 * 을 선택합니다.
6. 자격 증명 또는 포트를 수정할 수 있습니다. 스토리지 백엔드를 수정하려면 * Username * 및 * Password * 를 입력하십시오.

저장소 백엔드를 제거합니다

스토리지 백엔드를 제거하기 전에 스토리지 백엔드에 연결된 모든 데이터 저장소를 삭제해야 합니다. 스토리지 백엔드를 제거하려면 다음 단계를 수행하십시오.

1. vSphere Client에 로그인합니다
2. 바로 가기 페이지의 플러그인 섹션에서 * NetApp ONTAP tools * 를 선택합니다.
3. ONTAP 도구의 왼쪽 창에서 * Storage Backend * 로 이동하여 스토리지 백엔드를 선택합니다.
4. 수직 타원 메뉴를 선택하고 * 제거 * 를 선택합니다. 스토리지 백엔드에 데이터 저장소가 포함되어 있지 않은지 확인합니다. 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

ONTAP 툴 관리자를 사용하여 글로벌 ONTAP 클러스터에 대해 제거 작업을 수행할 수 있습니다.

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.

3. 측면 표시줄에서 * Storage Backend * 를 선택합니다.
4. 제거할 스토리지 백엔드를 선택합니다
5. 수직 타원 메뉴를 선택하고 * 제거 * 를 선택합니다.

스토리지 백엔드를 드릴다운합니다

스토리지 백엔드 페이지에 모든 스토리지 백엔드가 나열됩니다. 클러스터 아래의 개별 하위 SVM이 아니라 추가한 스토리지 백엔드에서 스토리지 검색, 수정 및 제거할 수 있습니다.

스토리지 백엔드에서 상위 클러스터 또는 하위 클러스터를 선택하면 구성 요소의 전체 요약을 볼 수 있습니다. 상위 클러스터를 선택하면 검색 스토리지, 수정 및 제거 작업을 수행할 수 있는 작업 드롭다운이 표시됩니다.

요약 페이지는 다음과 같은 세부 정보를 제공합니다.

- 스토리지 백엔드의 상태입니다
- 용량 정보입니다
- VM에 대한 기본 정보입니다
- 네트워크의 IP 주소 및 포트와 같은 네트워크 정보 하위 SVM의 경우 정보는 상위 스토리지 백엔드와 동일합니다.
- 스토리지 백엔드에 대해 허용 및 제한된 권한입니다. 하위 SVM의 경우 정보는 상위 스토리지 백엔드와 동일합니다. 권한은 클러스터 기반 스토리지 백엔드에만 표시됩니다. SVM을 스토리지 백엔드로 추가하면 권한 정보가 표시되지 않습니다.
- ASA R2 클러스터 드릴다운 뷰에는 SVM 또는 클러스터에 대해 Disaggregated 속성이 "true"로 설정된 경우 로컬 계층 탭이 포함되지 않습니다.
- ASA R2 SVM 시스템의 경우 용량 포틀릿이 표시되지 않습니다. 용량 포털은 SVM 또는 클러스터에 대해 분리된 속성이 "true"로 설정된 경우에만 필요합니다.
- ASA R2 SVM 시스템의 경우 기본 정보 섹션에 플랫폼 유형이 표시됩니다.

인터페이스 탭은 인터페이스에 대한 자세한 정보를 제공합니다.

로컬 계층 탭에는 집계 목록에 대한 자세한 정보가 표시됩니다.

vCenter Server 인스턴스를 관리합니다

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

vCenter Server 인스턴스로 스토리지 백엔드를 분리합니다

vCenter Server 목록 페이지에는 연결된 스토리지 백엔드 수가 표시됩니다. 각 vCenter Server 인스턴스에는 스토리지 백엔드에 연결하거나 연결을 해제하는 옵션이 있습니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.

3. 사이드바에서 필요한 vCenter Server 인스턴스를 선택합니다.
4. 스토리지 백엔드와 연결하거나 분리할 vCenter Server에 대해 세로 줄임표를 선택합니다.
5. 스토리지 백엔드 분리 * 를 선택합니다.

vCenter Server 인스턴스를 수정합니다

vCenter Server 인스턴스를 수정하려면 다음 단계를 따르십시오.

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.
3. 사이드바에서 해당 vCenter Server 인스턴스를 선택합니다
4. 수정할 vCenter Server에 대해 수직 타원을 선택하고 * Modify * 를 선택합니다.
5. vCenter Server 인스턴스 세부 정보를 수정하고 * Modify * 를 선택합니다.

vCenter Server 인스턴스를 제거합니다

vCenter Server에 연결된 모든 스토리지 백엔드를 제거한 후 제거해야 합니다.

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.
3. 사이드바에서 해당 vCenter Server 인스턴스를 선택합니다
4. 제거할 vCenter Server에 대해 수직 타원을 선택하고 * Remove * 를 선택합니다.

> vCenter Server 인스턴스를 제거하면 더 이상 애플리케이션에서 해당 인스턴스를 유지 관리할 수 없습니다.

ONTAP 툴에서 vCenter Server 인스턴스를 제거하면 다음 작업이 자동으로 수행됩니다.

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

인증서를 관리합니다

구축 중에 기본적으로 ONTAP 툴 및 VASA Provider에 대해 자체 서명된 인증서가 생성됩니다. ONTAP 도구 관리자 인터페이스를 사용하여 인증서를 갱신하거나 사용자 지정 CA로 업그레이드할 수 있습니다. 다중 vCenter 배포에서는 사용자 지정 CA 인증서가 필수입니다.

시작하기 전에

- 인증서가 발급된 도메인 이름을 가상 IP 주소에 매핑해야 합니다.
- 도메인 이름에 대해 nslookup 검사를 실행하여 도메인이 원하는 IP 주소로 확인되는지 확인합니다.

- 인증서는 도메인 이름과 부하 분산 장치 IP 주소를 사용하여 만들어야 합니다.

로드 밸런서 IP 주소는 FQDN(정규화된 도메인 이름)에 매핑되어야 합니다. 인증서에는 제목 또는 제목 대체 이름의 로드 밸런서 IP 주소에 매핑된 동일한 FQDN이 포함되어야 합니다.

CA에서 서명한 인증서에서 자체 서명된 인증서로 전환할 수 없습니다.

ONTAP 도구 인증서를 업그레이드합니다

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

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.
3. 인증서를 갱신하려면 * 인증서 * > * ONTAP tools * > * 갱신 * 을 선택합니다.

   인증서가 만료되었거나 만료 날짜가 임박한 경우 인증서를 갱신할 수 있습니다. 인증서 유형이 CA 서명일 때 갱신 옵션을 사용할 수 있습니다. 팝업 창에서 서버 인증서, 개인 키, 루트 CA 및 중간 인증서 세부 정보를 제공합니다.

   ⓘ 인증서가 갱신될 때까지 시스템이 오프라인 상태가 되고 ONTAP 도구 관리자 인터페이스에서 로그아웃됩니다.

4. 자체 서명 인증서를 사용자 지정 CA 인증서로 업그레이드하려면 * 인증서 * > * ONTAP tools * > * CA로 업그레이드 * 옵션을 선택합니다.
   a. 팝업 창에서 서버 인증서, 서버 인증서 개인 키, 루트 CA 인증서 및 중간 인증서 파일을 업로드합니다.
   b. 이 인증서를 생성한 도메인 이름을 입력하고 인증서를 업그레이드합니다.

   ⓘ 업그레이드가 완료될 때까지 시스템이 오프라인 상태가 되고 ONTAP 도구 관리자 인터페이스에서 로그아웃됩니다.

VASA Provider 인증서를 업그레이드합니다

VMware vSphere용 ONTAP 툴은 VASA Provider에 대한 자체 서명 인증서와 함께 구축됩니다. 이 옵션을 사용하면 VVol 데이터 저장소에 대해 하나의 vCenter Server 인스턴스만 관리할 수 있습니다. 여러 vCenter Server 인스턴스를 관리하고 이러한 인스턴스에서 VVol 기능을 활성화하려면 자체 서명된 인증서를 사용자 지정 CA 인증서로 변경해야 합니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.
3. 인증서를 갱신하려면 * 인증서 * > * VASA 공급자 * 또는 * ONTAP 툴 * > * 갱신 * 을 선택합니다.
4. 인증서 * > * VASA 공급자 * 또는 * ONTAP 툴 * > * CA로 업그레이드 * 를 선택하여 자체 서명된 인증서를 사용자 지정 CA 인증서로 업그레이드합니다.
   a. 팝업 창에서 서버 인증서, 서버 인증서 개인 키, 루트 CA 인증서 및 중간 인증서 파일을 업로드합니다.
   b. 이 인증서를 생성한 도메인 이름을 입력하고 인증서를 업그레이드합니다.

업그레이드가 완료될 때까지 시스템이 오프라인 상태가 되고 ONTAP 도구 관리자 인터페이스에서 로그아웃됩니다.

VMware vSphere 유지 관리 콘솔용 ONTAP 툴에 액세스할 수 있습니다

VMware vSphere 유지 관리 콘솔용 ONTAP 툴 개요

ONTAP 툴의 유지보수 콘솔을 사용하여 애플리케이션, 시스템 및 네트워크 구성을 관리할 수 있습니다. 관리자 암호 및 유지보수 암호를 변경할 수 있습니다. 또한 지원 번들을 생성하고, 다양한 로그 수준을 설정하고, TLS 구성을 확인 및 관리하고, 원격 진단을 시작할 수 있습니다.

유지 관리 콘솔에 액세스하려면 VMware vSphere용 ONTAP 툴을 구축한 후 VMware 툴을 설치해야 합니다. `maint`구축 중에 구성한 사용자 이름과 암호로 를 사용하여 ONTAP 도구의 유지 관리 콘솔에 로그인해야 합니다. 유지 관리 또는 루트 로그인 콘솔에서 파일을 편집할 때는 * nano * 를 사용해야 합니다.

`diag`원격 진단을 활성화하는 동안 사용자의 암호를 설정해야 합니다.

유지 관리 콘솔에 액세스하려면 구축된 VMware vSphere용 ONTAP 툴의 * Summary * 탭을 사용해야 합니다. 을  선택하면 유지보수 콘솔이 시작됩니다.

* 콘솔 메뉴 *	* 옵션 *
애플리케이션 구성	1. 서버 상태 요약을 표시합니다 2. VASA Provider Services 및 SRA Services에 대한 로그 수준을 변경합니다 3. AutoSupport를 비활성화합니다 4. AutoSupport 프록시 URL을 업데이트합니다
시스템 구성	1. 가상 머신을 재부팅합니다 2. 가상 머신을 종료합니다 3. '성자' 사용자 암호를 변경합니다 4. 시간대를 변경합니다 5. 새 NTP 서버를 추가합니다 6. jail 디스크 크기 증가(/jail) 7. 업그레이드 8. VMware Tools를 설치합니다

네트워크 구성	1. IP 주소 설정을 표시합니다 2. 도메인 이름 검색 설정을 표시합니다 3. 도메인 이름 검색 설정을 변경합니다 4. 정적 경로를 표시합니다 5. 정적 경로를 변경합니다 6. 변경 사항을 커밋합니다 7. 호스트에 Ping을 보냅니다 8. 기본 설정을 복원합니다
지원 및 진단	1. 진단 셸에 액세스합니다 2. 원격 진단 액세스를 활성화합니다 3. 백업을 위한 vCenter 자격 증명을 제공합니다 4. 백업을 수행합니다

원격 진단 액세스를 구성합니다

diag 사용자에 대해 SSH 액세스를 사용하도록 VMware vSphere용 ONTAP 툴을 구성할 수 있습니다.

시작하기 전에

vCenter Server 인스턴스에 대해 VASA Provider 확장을 설정해야 합니다.

- 이 작업에 대한 정보 *

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

- SSH의 활성화당 하나의 로그인 계정만 허용됩니다.
- 다음 중 하나가 발생하면 diag 사용자 계정에 대한 SSH 액세스가 비활성화됩니다.
  - 시간이 만료됩니다.

    로그인 세션은 다음 날 자정까지만 유효합니다.
  - SSH를 사용하여 diag 사용자로 다시 로그인합니다.

단계

1. vCenter Server에서 콘솔을 열고 VASA Provider로 이동합니다.
2. 유지보수 사용자로 로그인합니다.
3. 를 `4` 입력하여 지원 및 진단 을 선택합니다.
4. 를 `2` 입력하여 원격 진단 액세스 활성화 를 선택합니다.
5. `y`원격 진단 액세스를 활성화하려면 Confirmation(확인) 대화 상자에 를 입력합니다.

6. 원격 진단 액세스를 위한 암호를 입력합니다.

다른 노드에서 **SSH**를 시작합니다

업그레이드하기 전에 다른 노드에서 SSH를 시작해야 합니다.

시작하기 전에

vCenter Server 인스턴스에 대해 VASA Provider 확장을 설정해야 합니다.

- 이 작업에 대한 정보 *

업그레이드 전에 각 노드에서 이 절차를 수행하십시오.

단계

1. vCenter Server에서 콘솔을 열고 VASA Provider로 이동합니다.
2. 유지보수 사용자로 로그인합니다.
3. 를 `4` 입력하여 지원 및 진단 을 선택합니다.
4. `1`Access diagnostic shell(진단 쉘 액세스)을 선택하려면
5. `y`계속하려면 를 입력하십시오.
6. *sudo systemctl restart ssh* 명령을 실행합니다.

vCenter Server 및 **ONTAP** 자격 증명을 업데이트합니다

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

시작하기 전에

유지보수 사용자 로그인 자격 증명이 있어야 합니다.

- 이 작업에 대한 정보 *

구축 후 vCenter Server, ONTAP 또는 데이터 LIF에 대한 자격 증명을 변경한 경우에는 다음 절차를 사용하여 자격 증명을 업데이트해야 합니다.

단계

1. vCenter Server에서 콘솔을 열고 VASA Provider로 이동합니다.
2. 유지보수 사용자로 로그인합니다.
3. 를 `2` 입력하여 시스템 구성 메뉴를 선택합니다.
4. ONTAP 자격 증명을 변경하려면 를 `9` 입력합니다.
5. vCenter 자격 증명을 변경하려면 를 `10` 입력합니다.

ONTAP 도구 보고서

VMware vSphere용 ONTAP 툴 플러그인은 가상 머신 및 데이터 저장소에 대한 보고서를

제공합니다. vCenter Client의 바로 가기 섹션에서 VMware vSphere 플러그인용 NetApp ONTAP 툴 아이콘을 선택하면 사용자 인터페이스에서 개요 페이지로 이동합니다. Reports 탭을 선택하여 가상 머신과 데이터 저장소 보고서를 봅니다.

가상 머신 보고서에는 검색된 가상 머신(ONTAP 스토리지 기반 데이터 저장소로부터 하나 이상의 디스크가 있어야 함) 목록이 성능 메트릭과 함께 표시됩니다. VM 레코드를 확장하면 모든 디스크 관련 데이터 저장소 정보가 표시됩니다.

Datastores 보고서는 모든 유형의 ONTAP 스토리지 백엔드에서 프로비저닝된 VMware vSphere 관리 데이터 저장소에 대해 검색되거나 인식된 ONTAP 툴 목록을 성능 메트릭과 함께 표시합니다.

열 관리 옵션을 사용하여 다른 열을 숨기거나 표시할 수 있습니다.

로그 파일을 수집합니다

VMware vSphere용 ONTAP 툴에 대한 로그 파일은 ONTAP Tools Manager 사용자 인터페이스에서 사용할 수 있는 옵션을 통해 수집할 수 있습니다. 기술 지원 부서에서 문제 해결을 위해 로그 파일을 수집하도록 요청할 수 있습니다.

ONTAP Tools Manager에서 로그를 생성하는 데는 모든 vCenter Server 인스턴스에 대한 모든 로그가 포함됩니다. vCenter 클라이언트 사용자 인터페이스에서 로그를 생성하는 작업은 선택한 vCenter Server에 대해 범위가 지정됩니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.
3. 사이드바에서 * 로그 번들 * 을 선택합니다.

   이 작업은 몇 분 정도 걸릴 수 있습니다.
4. 로그 파일을 생성하려면 * Generate * 를 선택하십시오.
5. 로그 번들의 레이블을 입력하고 * Generate * 를 선택합니다.

   tar.gz 파일을 다운로드하여 기술 지원 부서에 보내십시오.

vCenter 클라이언트 사용자 인터페이스를 사용하여 로그 번들을 생성하려면 다음 단계를 수행하십시오.

단계

1. vSphere Client에 로그인합니다
2. vSphere Client 홈 페이지에서 * Support * > * Log bundle * > * Generate * 로 이동합니다.
3. 로그 번들 레이블을 제공하고 로그 번들을 생성합니다. 파일이 생성되면 다운로드 옵션을 볼 수 있습니다. 다운로드하는 데 시간이 걸릴 수 있습니다.

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

가상 머신 관리

가상 머신의 마이그레이션 또는 클론 생성 고려 사항

데이터 센터에서 기존 가상 머신을 마이그레이션할 때 고려해야 할 몇 가지 사항을 알고 있어야 합니다.

보호된 가상 시스템을 마이그레이션합니다

보호된 가상 시스템을 다음으로 마이그레이션할 수 있습니다.

- 다른 ESXi 호스트에서 동일한 VVol 데이터 저장소
- 동일한 ESXi 호스트에서 서로 다른 호환되는 VVol 데이터 저장소
- 다른 ESXi 호스트에서 서로 다른 호환되는 VVol 데이터 저장소

가상 머신이 다른 FlexVol 볼륨으로 마이그레이션되면 해당 메타데이터 파일도 가상 머신 정보로 업데이트됩니다. 가상 머신이 동일한 스토리지이지만 다른 ESXi 호스트로 마이그레이션되면 기본 FlexVol 볼륨 메타데이터 파일이 수정되지 않습니다.

보호된 가상 머신의 클론을 생성합니다

보호된 가상 컴퓨터를 다음 컴퓨터에 클론 복제할 수 있습니다.

- 복제 그룹을 사용하는 동일한 FlexVol 볼륨의 동일한 컨테이너입니다

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

- 복제 그룹을 사용하는 다른 FlexVol 볼륨의 동일한 컨테이너입니다

  클론 생성된 가상 머신이 배치되는 FlexVol 볼륨에서는 메타데이터 파일이 클론 생성된 가상 머신 세부 정보로 업데이트됩니다.

- 컨테이너 또는 VVOL 데이터 저장소가 서로 다릅니다

  클론 생성된 가상 머신이 배치되는 FlexVol 볼륨에서는 메타데이터 파일이 업데이트된 가상 머신 세부 정보를 가져옵니다.

VMware는 현재 VM 템플릿에 복제된 가상 머신을 지원하지 않습니다.

보호된 가상 머신의 클론 복제가 지원됩니다.

자세한 내용은 을 "클론 생성을 위한 가상 머신 생성" 참조하십시오.

가상 머신 스냅샷

현재 메모리가 없는 가상 머신 스냅샷만 지원됩니다. 가상 머신에 메모리가 있는 스냅샷이 있는 경우 가상 머신이 보호 대상으로 고려되지 않습니다.

또한 메모리 스냅샷이 있는 보호되지 않는 가상 머신을 보호할 수 없습니다. 이 릴리즈에서는 가상 머신에 대한 보호를 활성화하기 전에 메모리 스냅샷을 삭제해야 합니다.

ASA R2 스토리지 유형이 있는 Windows VM의 경우 가상 머신의 스냅샷을 생성하면 읽기 전용 스냅샷이 됩니다. VM에 대한 전원 호출 시 VASA Provider는 읽기 전용 스냅샷을 사용하여 LUN을 생성한 다음 IOPS를 사용하도록 설정합니다. 전원 끄기 요청 중에 VASA Provider는 생성된 LUN을 삭제한 다음 IOPS를 비활성화합니다.

NFS 및 VMFS 데이터 저장소를 사용하는 가상 시스템을 VVol 데이터 저장소로 마이그레이션합니다

NFS 및 VMFS 데이터 저장소에서 가상 머신을 VVol(Virtual Volumes) 데이터 저장소로 마이그레이션하여 정책 기반 VM 관리 및 기타 VVol 기능을 활용할 수 있습니다. VVol 데이터 저장소를 사용하면 증가하는 워크로드 요구사항을 충족할 수 있습니다.

시작하기 전에

마이그레이션할 가상 시스템에서 VASA Provider가 실행되고 있지 않은지 확인합니다. VASA Provider를 실행하는 가상 머신을 VVol 데이터 저장소로 마이그레이션할 경우, VVOL 데이터 저장소에 있는 가상 머신의 전원을 켜는 것을 포함하여 관리 작업을 수행할 수 없습니다.

- 이 작업에 대한 정보 *

NFS 및 VMFS 데이터 저장소에서 VVol 데이터 저장소로 마이그레이션할 때 vCenter Server는 VMFS 데이터 저장소에서 데이터를 이동할 때 VAAI(vStorage APIs for Array Integration) 오프로드를 사용하지만 NFS VMDK 파일에서는 데이터를 이동할 때 사용합니다. VAAI 오프로드는 일반적으로 호스트의 부하를 줄입니다.

단계

1. 마이그레이션할 가상 머신을 마우스 오른쪽 버튼으로 클릭하고 * Migrate * 를 선택합니다.
2. Change storage only * 를 선택하고 * Next * 를 선택합니다.
3. 마이그레이션할 데이터 저장소의 기능과 일치하는 가상 디스크 형식, VM 스토리지 정책 및 VVOL 데이터 저장소를 선택합니다.
4. 설정을 검토하고 * Finish * 를 선택합니다.

VASA 정리

이 섹션의 단계를 사용하여 VASA 정리를 수행합니다.

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

단계

1. https://OTV_IP:8143/Register.html로 이동하여 플러그인 등록을 취소합니다
2. vCenter Server에서 플러그인을 더 이상 사용할 수 없는지 확인합니다.
3. VMware vSphere VM용 ONTAP 툴을 종료합니다.
4. VMware vSphere VM용 ONTAP 툴을 삭제합니다.

스토리지 시스템 및 호스트를 검색합니다

vSphere 클라이언트에서 VMware vSphere용 ONTAP 툴을 처음 실행하면 ONTAP 툴이 ESXi 호스트, 해당 LUN 및 NFS 내보내기, 그리고 해당 LUN 및 내보내기를 소유한 NetApp 스토리지

시스템을 검색합니다.

시작하기 전에

- 모든 ESXi 호스트의 전원이 켜져 있고 연결되어 있어야 합니다.
- 검색할 모든 SVM(스토리지 가상 머신)이 실행되고 있어야 하며, 각 클러스터 노드에는 사용 중인 스토리지 프로토콜(NFS 또는 iSCSI)에 대해 하나 이상의 데이터 LIF가 구성되어 있어야 합니다.
- 이 작업에 대한 정보 *

언제든지 새 스토리지 시스템을 발견하거나 기존 스토리지 시스템에 대한 정보를 업데이트하여 최신 용량 및 구성 정보를 얻을 수 있습니다. VMware vSphere용 ONTAP 툴이 스토리지 시스템에 로그인하는 데 사용하는 자격 증명을 수정할 수도 있습니다.

스토리지 시스템을 검색하는 동안 VMware vSphere용 ONTAP 툴은 vCenter Server 인스턴스에서 관리하는 ESXi 호스트에서 정보를 수집합니다.

단계

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

   확인 * 대화 상자에서 선택 사항을 확인합니다.

3. 상태인 검색된 스토리지 컨트롤러를 `Authentication Failure` 선택하고 * Actions * > * Modify * 를 선택합니다.
4. 스토리지 시스템 수정 * 대화 상자에 필요한 정보를 입력합니다.
5. `Authentication Failure`상태가 인 모든 스토리지 컨트롤러에 대해 4단계와 5단계를 반복합니다.

검색 프로세스가 완료되면 다음 작업을 수행합니다.

- VMware vSphere용 ONTAP 툴을 사용하여 어댑터 설정 열, MPIO 설정 열 또는 NFS 설정 열에 경고 아이콘을 표시하는 호스트의 ESXi 호스트 설정을 구성합니다.
- 스토리지 시스템 자격 증명을 제공합니다.

ONTAP 툴을 사용하여 ESXi 호스트 설정을 수정합니다

VMware vSphere용 ONTAP 툴의 대시보드를 사용하여 ESXi 호스트 설정을 편집할 수 있습니다.

시작하기 전에

ESXi 호스트 설정에 문제가 있는 경우 대시보드의 ESXi 호스트 시스템 포틀릿에 문제가 표시됩니다. 문제를 선택하여 문제가 발생한 ESXi 호스트의 호스트 이름 또는 IP 주소를 볼 수 있습니다.

단계

1. vSphere Client에 로그인합니다
2. 바로 가기 페이지의 플러그인 섹션에서 * NetApp ONTAP tools * 를 선택합니다.
3. VMware vSphere 플러그인용 ONTAP 툴의 개요(대시보드)에서 * ESXi 호스트 규정 준수 * 포틀릿으로

이동합니다.

4. 권장 설정 적용 * 링크를 선택합니다.
5. Apply recommended host settings * 창에서 NetApp 권장 호스트 설정을 준수할 호스트를 선택하고 * Next * 를 선택합니다.

   ESXi 호스트를 확장하여 현재 값을 볼 수 있습니다.

6. 설정 페이지에서 필요한 권장 값을 선택합니다.
7. 요약 창에서 값을 확인하고 * Finish * 를 선택합니다. 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

   ◦ 관련 정보 *

"ESXi 호스트 설정을 구성합니다"

암호 관리

ONTAP 도구 관리자 암호를 변경합니다

ONTAP 도구 관리자를 사용하여 관리자 암호를 변경할 수 있습니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.
3. 화면 오른쪽 상단 모서리에 있는 * 관리자 * 아이콘을 선택하고 * 암호 변경 * 을 선택합니다.
4. 암호 변경 팝업 창에서 이전 암호와 새 암호 세부 정보를 입력합니다. 암호 변경에 대한 제한은 사용자 인터페이스 화면에 표시됩니다.
5. 변경 사항을 적용하려면 * 변경 * 을 선택하십시오.

ONTAP 도구 관리자 암호를 재설정합니다

ONTAP 툴 관리자 암호를 잊은 경우 VMware vSphere 유지 관리 콘솔용 ONTAP 툴에서 생성된 토큰을 사용하여 관리자 자격 증명을 재설정할 수 있습니다.

단계

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

   관리자 암호를 재설정하려면 VMware vSphere 유지 보수 콘솔용 ONTAP 툴을 사용하여 재설정 토큰을 생성해야 합니다.

   a. vCenter Server에서 유지 관리 콘솔을 엽니다
   b. '2'를 입력하여 시스템 구성 옵션을 선택합니다

c. '이전' 사용자 암호를 변경하려면 '3'을 입력하십시오.

3. 암호 변경 팝업 창에서 암호 재설정 토큰, 사용자 이름 및 새 암호 세부 정보를 입력합니다.
4. 변경 사항을 적용하려면 * 재설정 * 을 선택하십시오. 암호 재설정에 성공하면 새 암호를 사용하여 로그인할 수 있습니다.

응용 프로그램 사용자 암호를 재설정합니다

애플리케이션 사용자 암호는 vCenter Server에 대한 SRA 및 VASA Provider 등록에 사용됩니다.

단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 구축 중에 제공한 VMware vSphere 관리자 자격 증명용 ONTAP 툴을 사용하여 로그인합니다.
3. 측면 표시줄에서 * 설정 * 을 선택합니다.
4. VASA/SRA 자격 증명 * 화면에서 * 암호 재설정 * 을 선택합니다.
5. 새 암호를 입력하고 새 암호 입력을 확인합니다.
6. 변경 사항을 적용하려면 * 재설정 * 을 선택하십시오.

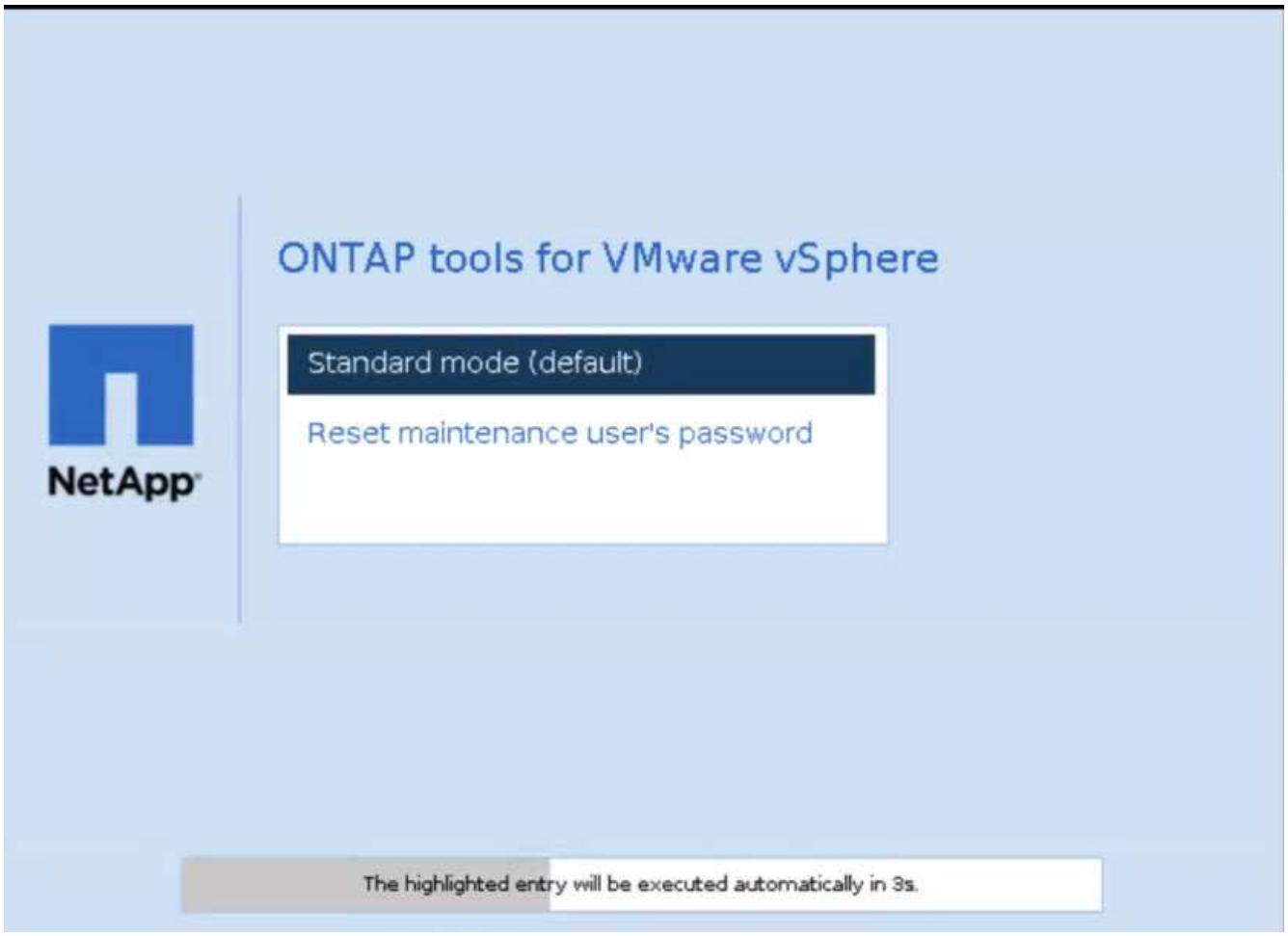
유지보수 콘솔 사용자 암호를 재설정합니다

게스트 OS 재시작 작업 중에 grub 메뉴에 유지 관리 콘솔 사용자 암호를 재설정하는 옵션이 표시됩니다. 이 옵션은 해당 VM에 있는 유지 관리 콘솔 사용자 암호를 업데이트하는 데 사용됩니다. 암호 재설정이 완료되면 VM이 다시 시작되어 새 암호를 설정합니다. HA 구축 시나리오에서 VM을 다시 시작한 후 다른 2개의 VM에서 암호가 자동으로 업데이트됩니다.

VMware vSphere HA 배포를 위한 ONTAP 도구의 경우 첫 번째 노드(node1)에서 유지 관리 콘솔 사용자 비밀번호를 변경해야 합니다.

단계

1. vCenter Server에 로그인합니다
2. VM을 마우스 오른쪽 버튼으로 클릭하고 * Power * > * Restart Guest OS * 를 선택합니다. 시스템을 다시 시작하는 동안 다음 화면이 나타납니다.



5초 이내에 옵션을 선택할 수 있습니다. 아무 키나 눌러 진행 과정을 중지하고 GRUB 메뉴를 고정합니다.

3. 유지 관리 사용자 암호 재설정 * 옵션을 선택합니다. 유지 관리 콘솔이 열립니다.
4. 콘솔에서 새 암호 세부 정보를 입력합니다. 암호를 재설정하려면 새 암호와 새 암호 다시 입력 세부 정보가 일치해야 합니다. 올바른 암호를 입력할 수 있는 기회는 세 번 있습니다. 새 암호를 성공적으로 입력한 후 시스템이 다시 시작됩니다.
5. Enter 키를 눌러 계속합니다. 암호가 VM에서 업데이트됩니다.

VM의 전원을 켜는 동안에도 동일한 GRUB 메뉴가 나타납니다. 그러나 * Restart Guest OS * 옵션에만 암호 재설정 옵션을 사용해야 합니다.

호스트 클러스터 보호 관리

보호된 호스트 클러스터를 수정합니다

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

- 보호된 클러스터에 새 데이터 저장소 또는 호스트를 추가합니다.
- 보호 설정에 새 SnapMirror 관계를 추가합니다.

- 보호 설정에서 기존 SnapMirror 관계를 삭제합니다.
- 기존 SnapMirror 관계 수정

호스트 클러스터 보호를 모니터링합니다

호스트 클러스터 보호 상태를 모니터링하려면 다음 절차를 따르십시오. 보호 상태, SnapMirror 관계, 데이터 저장소 및 해당 SnapMirror 상태와 함께 모든 보호 호스트 클러스터를 모니터링할 수 있습니다.

단계

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

   보호 열 아래의 아이콘은 보호 상태를 나타냅니다

3. 자세한 내용을 보려면 아이콘 위에 마우스를 올려 놓으십시오.

새 데이터 저장소 또는 호스트를 추가합니다

새로 추가된 데이터 저장소나 호스트를 보호하려면 다음 절차를 따르십시오. vCenter 기본 사용자 인터페이스를 사용하여 보호된 클러스터에 새 호스트를 추가하거나 호스트 클러스터에 새 데이터 저장소를 생성할 수 있습니다.

단계

1. vSphere Client에 로그인합니다
2. 보호된 클러스터의 속성을 편집하려면 다음 중 하나를 수행합니다
   a. NetApp ONTAP tools * > * 보호 * > * 호스트 클러스터 관계 * 로 이동한 후 클러스터에 대한 줄임표 메뉴를 선택하고 * 편집 * 또는 을 선택합니다
   b. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools * > * Protect Cluster * 를 선택합니다.
3. vCenter 기본 사용자 인터페이스에서 데이터 저장소를 생성한 경우 해당 데이터 저장소가 보호되지 않음으로 표시됩니다. 사용자 인터페이스는 클러스터의 모든 데이터 저장소와 보호 상태를 대화 상자에 표시합니다. 완벽한 보호를 활성화하려면 * 보호 * 버튼을 선택하십시오.
4. 새 ESXi 호스트를 추가한 경우 보호 상태가 부분적으로 보호됨 으로 표시됩니다. SnapMirror 설정에서 줄임표 메뉴를 선택하고 * 편집 * 을 선택하여 새로 추가된 ESXi 호스트의 근접성을 설정합니다.

   비동기식 유형 관계의 경우 3차 사이트의 타겟 SVM을 동일한 ONTAP 툴 인스턴스에 추가할 수 없으므로 편집 작업이 지원되지 않습니다. 그러나 타겟 SVM의 시스템 관리자 또는 CLI를 사용하여 관계 구성을 변경할 수 있습니다.

5. 필요한 사항을 변경한 후 * 저장 * 을 선택합니다.
6. Protect Cluster * 창에서 변경 사항을 확인할 수 있습니다.

vCenter 작업이 생성되고 * Recent task * 패널에서 진행 상황을 추적할 수 있습니다.

새 **SnapMirror** 관계를 추가합니다

단계

1. vSphere Client에 로그인합니다
2. 보호된 클러스터의 속성을 편집하려면 다음 중 하나를 수행합니다
   a. NetApp ONTAP tools * > * 보호 * > * 호스트 클러스터 관계 * 로 이동한 후 클러스터에 대한 줄임표 메뉴를 선택하고 * 편집 * 또는 을 선택합니다
   b. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools * > * Protect Cluster * 를 선택합니다.
3. 관계 추가 * 를 선택합니다.
4. 새 관계를 * Asynchronous * 또는 * AutomatedFailOverDuplex * 정책 유형으로 추가합니다.
5. protect * 를 선택합니다.

   Protect Cluster * 창에서 변경 사항을 확인할 수 있습니다.

vCenter 작업이 생성되고 * Recent task * 패널에서 진행 상황을 추적할 수 있습니다.

기존 **SnapMirror** 관계를 삭제합니다

비동기식 SnapMirror 관계를 삭제하려면 VMware vSphere용 ONTAP 툴에 2차 사이트 SVM 또는 클러스터를 스토리지 백엔드로 추가해야 합니다. 모든 SnapMirror 관계를 삭제할 수 없습니다. 관계를 삭제하면 ONTAP 클러스터의 해당 관계도 제거됩니다. AutomatedFailOverDuplex SnapMirror 관계를 삭제하면 대상의 데이터 저장소가 매핑 해제되고 일관성 그룹, LUN, 볼륨 및 igroup이 대상 ONTAP 클러스터에서 제거됩니다.

관계를 삭제하면 보조 사이트에 대한 재검사가 트리거되어 매핑되지 않은 LUN이 호스트에서 활성 경로로 제거됩니다.

단계

1. vSphere Client에 로그인합니다
2. 보호된 클러스터의 속성을 편집하려면 다음 중 하나를 수행합니다
   a. NetApp ONTAP tools * > * 보호 * > * 호스트 클러스터 관계 * 로 이동한 후 클러스터에 대한 줄임표 메뉴를 선택하고 * 편집 * 또는 을 선택합니다
   b. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools * > * Protect Cluster * 를 선택합니다.
3. SnapMirror 설정 아래에서 줄임표 메뉴를 선택하고 * 삭제 * 를 선택합니다.

vCenter 작업이 생성되고 * Recent task * 패널에서 진행 상황을 추적할 수 있습니다.

기존 **SnapMirror** 관계 수정

비동기식 SnapMirror 관계를 수정하려면 VMware vSphere용 ONTAP 툴에 2차 사이트 SVM 또는 클러스터를 스토리지 백엔드로 추가해야 합니다. AutomatedFailOverDuplex SnapMirror 관계인 경우 구성이 균일한 경우 호스트 근접성을 수정할 수 있고 구성이 균일하지 않은 경우 호스트 액세스를 수정할 수 있습니다. Asynchronous 및 AutomatedFailOverDuplex 정책 유형은 상호 변경할 수 없습니다. 클러스터에서 새로 검색된 호스트에 대한 근접성 또는 액세스를 설정할 수 있습니다.

ⓘ 기존의 비동기식 SnapMirror 관계는 편집할 수 없습니다.

단계

1. vSphere Client에 로그인합니다
2. 보호된 클러스터의 속성을 편집하려면 다음 중 하나를 수행합니다
   a. NetApp ONTAP tools * > * 보호 * > * 호스트 클러스터 관계 * 로 이동한 후 클러스터에 대한 줄임표 메뉴를 선택하고 * 편집 * 또는 을 선택합니다
   b. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools * > * Protect Cluster * 를 선택합니다.
3. AutomatedFailoOverDuplex 정책 유형을 선택한 경우 호스트 근접 또는 호스트 액세스 세부 정보를 추가합니다.
4. 보호 * 버튼을 선택합니다.

vCenter 작업이 생성되고 * Recent task * 패널에서 진행 상황을 추적할 수 있습니다.

호스트 클러스터 보호를 제거합니다

호스트 클러스터 보호를 제거하면 데이터 저장소가 보호되지 않는 상태가 됩니다.

단계

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

   이 페이지에서는 보호 상태, SnapMirror 관계 및 해당 SnapMirror 상태와 함께 보호 호스트 클러스터를 모니터링할 수 있습니다.

2. Host cluster protection * 창에서 클러스터에 대한 줄임표 메뉴를 선택한 다음 * Remove protection * 을 선택합니다.

AutoSupport를 비활성화합니다

스토리지 시스템을 처음으로 구성할 경우 AutoSupport가 기본적으로 사용하도록 설정됩니다. 활성화 후 24시간 후에 기술 지원 부서에 메시지를 보냅니다. AutoSupport를 비활성화하면 더 이상 사전 지원 및 모니터링을 받을 수 없습니다.

AutoSupport를 사용하도록 설정하는 것이 좋습니다. 문제 감지 및 해결 시간을 단축할 수 있습니다. 시스템이 AutoSupport 정보를 수집하여 로컬에 저장합니다. 비활성화된 경우에도 마찬가지입니다.

단계

1. vCenter Server에서 유지 관리 콘솔을 엽니다.
2. 유지보수 사용자로 로그인합니다.
3. 1을 입력하여 * 애플리케이션 구성 * 을 선택합니다.
4. 3을 입력하여 * AutoSupport 비활성화 * 를 선택합니다.
5. 확인 대화 상자에 y 를 입력합니다.

AutoSupport 프록시 URL을 업데이트합니다

프록시 서버가 네트워크 액세스 제어 또는 보안 조치에 사용되는 시나리오에서 AutoSupport 프록시 URL을 업데이트하여 AutoSupport 기능이 올바르게 작동하는지 확인합니다. AutoSupport 데이터를 적절한 프록시를 통해 라우팅하여 안전한 전송 및 규정 준수를 보장합니다.

단계

1. vCenter Server에서 유지 관리 콘솔을 엽니다.
2. 유지보수 사용자로 로그인합니다.
3. 1을 입력하여 * 애플리케이션 구성 * 을 선택합니다.
4. 4를 입력하여 * AutoSupport 프록시 URL 업데이트 * 를 선택합니다.
5. 프록시 URL을 입력합니다.

백업을 생성하고 설정을 복구합니다

VMware vSphere 10.3용 ONTAP 툴은 동적 스토리지 프로비저닝을 사용하므로 제로 RPO를 달성할 수 없습니다. 하지만 거의 0에 가까운 RPO를 달성할 수 있습니다. RPO가 0에 가까우려면 설정 백업을 생성하고 새 가상 시스템에서 복원해야 합니다.

백업을 생성하고 백업 파일을 다운로드합니다

단계

1. vCenter Server에서 유지 관리 콘솔을 엽니다.
2. 유지보수 사용자로 로그인합니다.
3. 를 4 입력하여 * 지원 및 진단 * 을 선택합니다.
4. Enter 키를 눌러 3 * 시스템 백업 활성화 * 옵션을 선택합니다.
5. HA가 아닌 경우 ONTAP 툴 가상 머신을 구축할 vCenter 자격 증명을 입력합니다.
6. 5-60분 사이의 백업 빈도 값을 입력합니다.
7. Enter * 를 누릅니다

   이렇게 하면 백업이 생성되며 정기적으로 가상 머신의 데이터 저장소로 백업을 푸시합니다.

8. 백업에 액세스하려면 스토리지 섹션으로 이동하여 가상 머신의 데이터 저장소를 선택합니다
9. 파일 * 섹션을 선택합니다.

   파일 섹션에서 디렉토리를 볼 수 있습니다. 디렉토리 이름은 ONTAP 도구 IP 주소이며, 여기서 점(.)은 _backup_으로 접미사가 붙은 밑줄로 바뀝니다.

10. 자세한 백업 정보를 보려면 * Files * > * Download * 에서 backup_info.txt 파일을 다운로드하십시오.

복구

설정을 복구하려면 기존 가상 머신의 전원을 끄고 초기 구축에 사용된 OVA를 사용하여 새 가상 머신을 구축합니다.

새 가상 머신에 동일한 ONTAP 툴 IP 주소(로드 밸런서 IP)를 사용해야 하며 서비스 사용, 노드 크기, HA 모드 등의 시스템 구성은 초기 구축과 동일해야 합니다.

백업 파일에서 설정을 복구하려면 다음 단계를 수행하십시오.

1. vCenter Server에서 유지 관리 콘솔을 엽니다.
2. 유지보수 사용자로 로그인합니다.
3. 를 4 입력하여 * 지원 및 진단 * 을 선택합니다.
4. Enter 키를 2 눌러 * 원격 진단 액세스 활성화 * 옵션을 선택하고 진단 액세스에 사용할 새 암호를 만듭니다.
5. 다운로드된 디렉토리에서 백업 하나를 선택합니다. 마지막 백업 파일 이름은 _backup_info.txt_file에 기록됩니다.
6. 아래 명령을 실행하여 백업을 새 가상 머신에 복사하고 메시지가 표시되면 진단 암호를 입력합니다.

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

> ⓘ 명령에 언급된 대상 경로 및 파일 이름(/home/diag/system_recovery.tar.enc)을 변경하지 마십시오.

7. 백업 파일이 복사되면 진단 셸에 로그인하고 다음 명령을 실행합니다.

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

로그는 _/var/log/post-deploy-upgrade.log_file에 기록됩니다.

8. 성공적으로 복구되면 서비스 및 vCenter 객체가 복구됩니다.

VMware vSphere용 ONTAP 툴을 제거합니다

VMware vSphere용 ONTAP 툴을 제거하면 툴의 데이터가 모두 삭제됩니다.

단계

1. VMware vSphere에서 관리하는 데이터 저장소용 ONTAP 툴에서 모든 가상 머신을 제거하거나 이동합니다.
   - 가상 머신을 제거하려면 을 참조하십시오 "VM 및 VM 템플릿을 제거하고 다시 등록합니다"
   - 관리되지 않는 데이터 저장소로 이동하려면 을 참조하십시오 "마이그레이션"
2. "데이터 저장소를 삭제합니다" VMware vSphere용 ONTAP 툴에 생성되었습니다.
3. VASA 공급자를 설정한 경우 ONTAP 툴에서 * Settings * > * VASA Provider settings * > * Unregister * 를 선택하여 모든 vCenter 서버에서 VASA Provider 등록을 취소합니다.
4. vCenter Server 인스턴스에서 모든 스토리지 백엔드의 연결을 해제합니다. 을 "vCenter Server 인스턴스로 스토리지 백엔드를 분리합니다"참조하십시오.

5. 모든 스토리지 백엔드를 삭제합니다. 을 "스토리지 백엔드 관리"참조하십시오.
6. VMware Live Site Recovery에서 SRA 어댑터 제거:
   a. 포트 5480을 사용하여 VMware Live Site Recovery 어플라이언스 관리 인터페이스에 admin으로 로그인합니다.
   b. Storage Replication Adapters * 를 선택합니다.
   c. 해당 SRA 카드를 선택하고 드롭다운 메뉴에서 * Delete * 를 선택합니다.
   d. 어댑터 삭제 결과를 알고 있는지 확인하고 * 삭제 * 를 선택합니다.
7. VMware vSphere용 ONTAP 툴에 온보딩된 vCenter 서버 인스턴스를 삭제합니다. 을 "vCenter Server 인스턴스를 관리합니다"참조하십시오.
8. vCenter Server에서 VMware vSphere VM용 ONTAP 툴의 전원을 끄고 VM을 삭제합니다.

다음 단계

"FlexVol 볼륨을 제거합니다"

FlexVol 볼륨을 제거합니다

VMware 배포용 ONTAP 툴용 전용 ONTAP 클러스터를 사용하면 사용되지 않은 FlexVol 볼륨이 여러 개 생성됩니다. VMware vSphere용 ONTAP 툴을 제거한 후에는 성능에 미치는 영향을 방지하기 위해 FlexVol 볼륨을 제거해야 합니다.

단계

1. 첫 번째 노드 VM에서 VMware vSphere 배포 유형에 대한 ONTAP 도구를 확인합니다.

   _cat/opt/netapp/meta/Ansible_vars.yaml | grep-i 프로토콜 _

   iSCSI를 구축할 경우 igroup도 삭제해야 합니다.

2. FlexVol 볼륨 목록을 가져옵니다.

   kubectl persistentvolumes|grep internalName|awk-F'='{print$2}' 을(를) 설명합니다

3. vCenter Server에서 VM을 제거합니다. 을 "VM 및 VM 템플릿을 제거하고 다시 등록합니다"참조하십시오.
4. ONTAP System Manager에서 FlexVol 볼륨을 삭제합니다. 을 "FlexVol 볼륨을 삭제합니다"참조하십시오. 볼륨을 삭제하려면 CLI 명령에서 FlexVol 볼륨의 정확한 이름을 지정하십시오.
5. iSCSI 구축 시 ONTAP 스토리지 시스템에서 SAN igroup을 삭제합니다. 을 "SAN 이니시에이터 및 igroup을 보고 관리합니다"참조하십시오.

VMware vSphere용 ONTAP 툴을 업그레이드합니다

VMware vSphere 10.x용 ONTAP 툴을 10.3로 업그레이드하십시오

업그레이드는 HA 및 비 HA 구현 모두에서 지원됩니다. 지원되는 업그레이드 경로는 다음과 같습니다.

VMware vSphere 10.1 및 10.2 구성에 대한 ONTAP 툴 활용	VMware vSphere 10.3 구성을 위한 ONTAP 툴
비 HA 소형	HA가 아닌 고급 소형
HA 미디어가 아닙니다	비 HA 및 고급 매체
고급 소형	HA가 아닌 고급 소형
고급 미디어	비 HA 및 고급 매체
HA 소규모	HA 소규모
HA 중간 규모	HA 중간 규모
HA 대규모	HA 대규모

VMware vSphere 10.1 및 10.2용 ONTAP 툴에서 10.3으로 업그레이드할 수 있습니다. ONTAP 도구 10.0에서 10.3으로 직접 업그레이드할 수 없습니다.

- 시작하기 전에 *

HA가 아닌 업그레이드의 경우 ONTAP 도구 VM의 전원을 끄고 HA 업그레이드의 경우 가상 머신(VM) 설정을 변경하기 전에 첫 번째 노드의 전원을 끕니다.

- 서비스 데이터가 VM에 로컬로 저장되므로 각 노드에 100GB 하드 디스크를 추가합니다.
- 배포 종류에 따라 전원이 꺼진 VM의 CPU 및 메모리를 변경합니다. CPU 및 RAM에 대한 핫 플러그인을 활성화합니다.

10.3 배포 유형	노드당 **CPU(**코어	노드당 메모리**(GB)**입니다	노드당 디스크 공간**(GB)**입니다	총 **CPU(**코어**)**	메모리**(GB)**	총 디스크 공간**(GB)**
비 HA 소형	9	18	350	9	18	350
HA가 아닌 중간	13	26	350	13	26	350
HA 소규모	9	18	350	27	54	1050
HA 중간	13	26	350	39	78	1050
HA 대규모	17	34	350	51	102	1050

- 변경이 완료된 후 VM의 전원을 켜고 서비스가 실행 상태가 될 때까지 기다립니다.
- HA 배포의 경우 리소스를 변경하고 CPU 및 RAM용 핫 플러그인을 활성화하고 두 번째 노드와 세 번째 노드에

100GB 하드 디스크를 추가합니다. 이러한 노드를 재부팅할 필요가 없습니다.

- ONTAP tools 10.1 또는 10.2를 사용하여 어플라이언스를 로컬 경로로 배포한 경우 업그레이드하기 전에 스냅샷을 중지해야 합니다.

VMware vSphere 10.0용 ONTAP 도구에서 10.1로 업그레이드하는 경우 업그레이드 작업을 진행하기 전에 다음 단계를 완료해야 합니다.

- 진단 활성화 *
  1. vCenter Server에서 콘솔을 열고 ONTAP 툴을 엽니다.
  2. 유지보수 사용자로 로그인합니다.
  3. 4 * 를 입력하여 * 지원 및 진단 * 을 선택합니다.
  4. 2 * 를 입력하여 * 원격 진단 액세스 활성화 * 를 선택합니다.
  5. y * 를 입력하여 선택한 암호를 설정합니다.
  6. 사용자가 'DIAG'로, 이전 단계에서 설정한 암호를 사용하여 터미널/putty에서 VM IP 주소에 로그인합니다.
- MongoDB 백업 *

다음 명령을 실행하여 MongoDB 백업을 수행합니다.

- kN Exec-IT NTV-mongodb-0 sh-kn은 kubectl-n NTV-system의 별칭입니다.
- 포드 안에서 _env | grep mongodb_root_password_command 를 실행합니다.
- run_exit_command 를 실행하여 포드에서 나오십시오.
- run_kn exec ntv-mongodb-0—mongodump -u root -p mongodb_root_password—archive=/tmp/mongodb-backup.gz - -gzip_command 를 실행하여 위의 명령에서 설정한 Mongo_root_password를 대체합니다.
- run_kn CP NTV-mongodb-0:/tmp/mongodb-backup.gz./mongodb-backup.gz_command를 실행하여 위의 명령을 사용하여 생성된 MongoDB 백업을 Pod에서 호스트로 복사합니다.
- 모든 볼륨의 Quaise 스냅샷을 촬영합니다 *
- 'kn Get PVC' 명령을 실행하고 명령 출력을 저장합니다.
- 다음 방법 중 하나를 사용하여 모든 볼륨의 스냅샷을 하나씩 생성합니다.
  - CLI에서 *volume snapshot create -vserver <vserver_name> -volume <volume_name> -snapshot <snapshot_name>* 명령을 실행합니다
  - ONTAP 시스템 관리자 사용자 인터페이스의 검색 표시줄에서 볼륨을 이름으로 검색한 다음 이름을 선택하여 해당 볼륨을 엽니다. 스냅샷으로 이동하여 해당 볼륨의 스냅샷을 추가합니다.
- vCenter에서 VMware vSphere VM용 ONTAP 툴의 스냅샷 생성(HA 구축 시 VM 3개, 비 HA 구축 시 VM 1개) *
- vSphere Client 사용자 인터페이스에서 VM을 선택합니다.
- 스냅샷 탭으로 이동하여 * 스냅샷 촬영 * 버튼을 선택합니다. VM의 일시 중지된 스냅샷을 생성합니다. 자세한 내용은 을 "가상 시스템의 스냅샷을 생성합니다" 참조하십시오.

업그레이드를 수행하기 전에 앞에 "generate-support-bundle-job"이라는 접두사가 있는 완료된 Pod를 로그 번들에서 삭제하십시오. 지원 번들 생성이 진행 중인 경우 완료될 때까지 기다린 다음 Pod를 삭제하십시오.

모든 업그레이드 유형의 경우 100GB HDD(하드 디스크 드라이브)를 추가해야 합니다. HDD를 추가하려면 다음 작업을 수행하십시오.

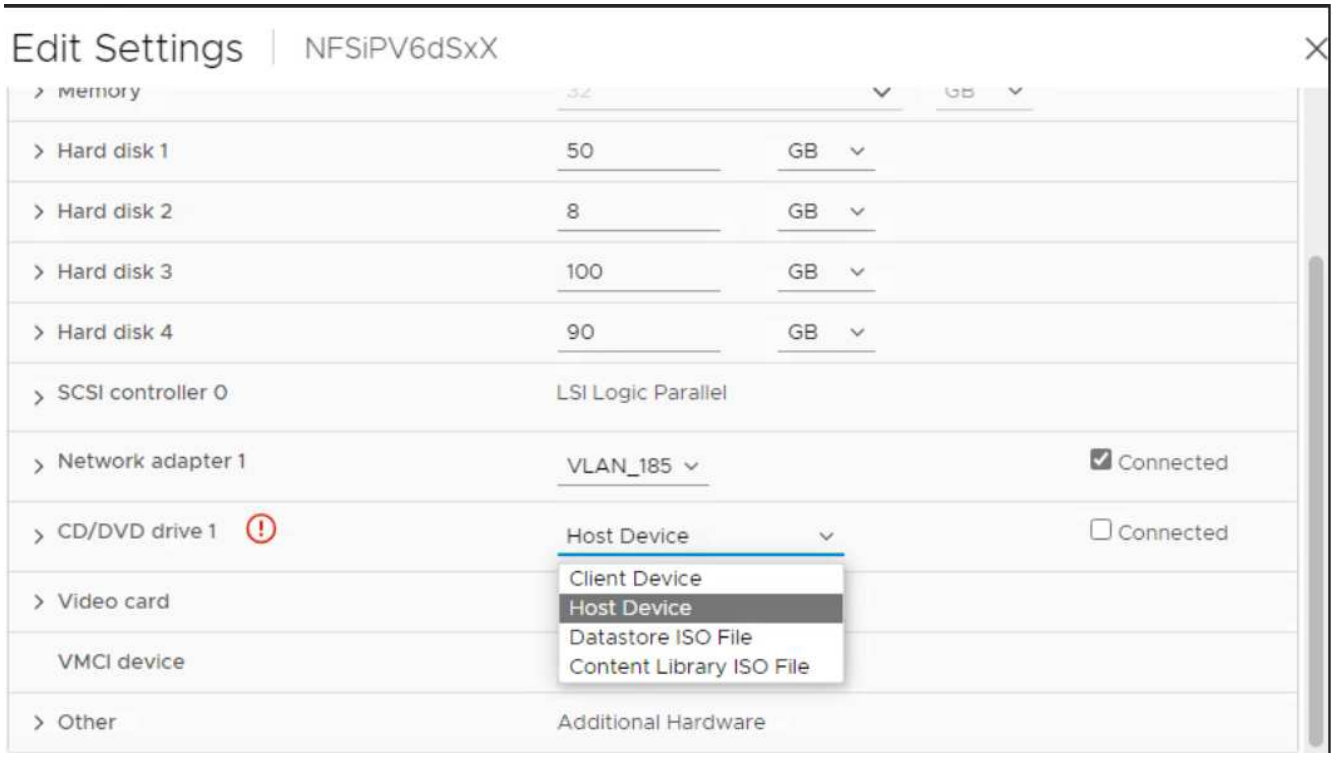
1. 단일 노드 구성의 VM을 선택하거나 HA 구성의 VM 3개 모두를 선택합니다.
2. VM을 마우스 오른쪽 버튼으로 클릭하고 * Add New Device * > * Hard Disk * 를 선택합니다
3. 새 하드 디스크 * 필드에 100GB HDD를 추가합니다.
4. 적용 * 을 선택합니다

하드 디스크를 추가한 후 각 구성에 대한 VM 리소스를 업데이트하고 기본 VM을 다시 시작합니다.

새 HDD가 생성됩니다. Dynamic Storage Provisioner는 이 HDD를 사용하여 볼륨을 생성하거나 복제합니다.

단계

1. VMware vSphere용 ONTAP 툴을 컨텐츠 라이브러리로 업그레이드합니다.
2. 기본 VM 페이지에서 작업 > *설정 편집*을 선택합니다. 기본 VM 이름을 식별하려면:
   a. 모든 노드에서 진단 셸을 활성화합니다.
   b. 다음 명령을 실행하세요.
   `grep sourceHost /opt/netapp/meta/ansible_vars.yaml`
3. 편집 설정 창의 * CD/DVD 드라이브 * 필드에서 콘텐츠 라이브러리 ISO 파일을 선택합니다.
4. ISO 파일을 선택하고 * 확인 * 을 선택합니다. CD/DVD 드라이브 * 필드에서 연결됨 확인란을 선택합니다.



5. vCenter Server에서 콘솔을 열고 ONTAP 툴을 엽니다.
6. 유지보수 사용자로 로그인합니다.
7. 3 * 을 입력하여 System Configuration 메뉴를 선택합니다.
8. 7 * 을 입력하여 업그레이드 옵션을 선택합니다.
9. 를 업그레이드하면 다음 작업이 자동으로 수행됩니다.
   a. 인증서 업그레이드

b. 원격 플러그인 업그레이드

VMware vSphere 10.3용 ONTAP 툴로 업그레이드한 후 다음을 수행할 수 있습니다.

- 관리자 사용자 인터페이스에서 서비스를 비활성화합니다
- 비 HA 설정에서 HA 설정으로 이동합니다
- HA가 아닌 소규모 구성을 HA가 아닌 매체 또는 HA 매체 또는 대규모 구성으로 확장합니다.
- HA가 아닌 업그레이드의 경우 ONTAP 툴 VM을 재부팅하여 변경 사항을 반영합니다. HA를 업그레이드하는 경우 첫 번째 노드를 재부팅하여 노드의 변경 사항을 반영합니다.
- 완료 후 *

VMware vSphere용 ONTAP 툴의 이전 릴리스에서 10.3으로 업그레이드한 후 SRA 어댑터를 다시 검색하여 VMware 라이브 사이트 복구 스토리지 복제 어댑터 페이지에 세부 정보가 업데이트되는지 확인합니다.

성공적으로 업그레이드한 후 다음 절차에 따라 ONTAP에서 Trident 볼륨을 수동으로 삭제합니다.

VMware vSphere 10.1 또는 10.2용 ONTAP 툴이 비 HA 소형 또는 중형(로컬 경로) 구성인 경우에는 이러한 단계가 필요하지 않습니다.

1. vCenter Server에서 콘솔을 열고 ONTAP 툴을 엽니다.
2. 유지보수 사용자로 로그인합니다.
3. 4 * 를 입력하여 * 지원 및 진단 * 메뉴를 선택합니다.
4. Access diagnostics shell * 옵션을 선택하려면 * 1 * 을 입력합니다.
5. 다음 명령을 실행합니다

```
sudo python3 /home/maint/scripts/ontap_cleanup.py
```

6. ONTAP 사용자 이름과 암호를 입력합니다

이렇게 하면 VMware vSphere 10.1/10.2용 ONTAP 툴에 사용된 ONTAP의 Trident 볼륨이 모두 삭제됩니다.

- 관련 정보 *

"VMware vSphere 9.x용 ONTAP 툴에서 10.3로 마이그레이션합니다"

업그레이드 오류 코드입니다

VMware vSphere 업그레이드 작업용 ONTAP 툴 중에 오류 코드가 발생할 수 있습니다. 오류 코드는 5자리 길이이며, 처음 두 자리는 문제가 발생한 스크립트를 나타내며, 마지막 세 자리는 해당 스크립트 내의 특정 워크플로를 나타냅니다.

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

이 페이지에 제공된 오류 코드는 참조용으로만 제공됩니다. 오류가 지속되거나 해결 방법이 언급되지 않은 경우 지원 팀에 문의하십시오.

다음 표에는 오류 코드와 해당 파일 이름이 나열되어 있습니다.

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

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

* 업그레이드 오류 코드 *	* 워크플로 *	* 해상도 *
068	데비안 패키지 롤백에 실패했습니다	제로 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하십시오.
069	파일을 복원하지 못했습니다	제로 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하십시오.
070	백업을 삭제하지 못했습니다	-
071	Kubernetes 클러스터가 정상 상태가 아닙니다	-
074	ISO 마운트에 실패했습니다	/var/log/upgrade-run.log 를 확인하고 업그레이드를 다시 시도하십시오.
075	업그레이드 사전 검사가 실패했습니다	업그레이드를 다시 시도하십시오.
076	레지스트리를 업그레이드하지 못했습니다	제로 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하십시오.
077	레지스트리 롤백에 실패했습니다	제로 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하십시오.
078	운영자를 업그레이드하지 못했습니다	제로 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하십시오.

079	운영자 롤백에 실패했습니다	제로 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하십시오.
080	서비스를 업그레이드하지 못했습니다	제로 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하십시오.
081	서비스 롤백에 실패했습니다	제로 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하십시오.
082	컨테이너에서 이전 이미지를 삭제하지 못했습니다	제로 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하십시오.
083	백업을 삭제하지 못했습니다	제로 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하십시오.
084	JobManager를 프로덕션으로 다시 변경하지 못했습니다	아래 단계에 따라 업그레이드를 복구/완료하십시오. 1. 진단 셸 2를 활성화합니다. _sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade_3 명령을 실행합니다. /var/log/post-deploy-upgrade.log 에서 로그를 확인합니다
087	업그레이드 후 단계가 실패했습니다.	업그레이드를 복구/완료하려면 다음 단계를 수행하십시오. 1. 진단 셸 2를 활성화합니다. run_sudo perl/home/maint/scripts/post-deploy-upgrade.pl --postupgrade_command 3. /var/log/post-deploy-upgrade.log 에서 로그를 확인합니다
088	저널러에 대한 로그 회전을 구성하지 못했습니다	VM이 호스팅되는 호스트와 호환되는 VM 네트워크 설정을 확인합니다. VM을 다른 호스트로 마이그레이션하고 다시 시작할 수 있습니다.
089	요약 로그 회전 구성 파일의 소유권을 변경하지 못했습니다	업그레이드를 다시 시도하십시오.
093	동적 스토리지 프로비저닝을 수행하지 못했습니다	업그레이드를 다시 시도하십시오.
094	동적 스토리지 프로비저닝 롤백에 실패했습니다	업그레이드를 다시 시도하십시오.
095	OS를 업그레이드하지 못했습니다	OS 업그레이드를 위한 복구 기능이 없습니다. ONTAP 툴 서비스가 업그레이드되고 새 Pod가 실행됩니다.
096	동적 스토리지 프로비저닝을 설치합니다	업그레이드 로그를 확인하고 업그레이드를 다시 시도하십시오.

097	업그레이드를 위한 서비스를 제거하지 못했습니다	제로 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하십시오.
098	NTV-system에서 동적 스토리지 프로비저닝 네임스페이스로 dockercredd 암호를 복사하지 못했습니다	업그레이드 로그를 확인하고 업그레이드를 다시 시도하십시오.
099	새 HDD 추가를 확인하지 못했습니다	HA의 경우 모든 노드에, HA가 아닌 구축 시 단일 노드에 새 HDD를 추가합니다.
108	시드 스크립트가 실패했습니다	-
109	영구 볼륨 데이터를 백업하지 못했습니다	업그레이드 로그를 확인하고 업그레이드를 다시 시도하십시오.
110	영구 볼륨 데이터를 복원하지 못했습니다	제로 RPO 또는 스냅샷 기반 복구를 사용하고 업그레이드를 다시 시도하십시오.
111	RKE2에 대한 etcd 시간 초과 매개 변수를 업데이트하지 못했습니다	업그레이드 로그를 확인하고 업그레이드를 다시 시도하십시오.
112	동적 스토리지 프로비저닝을 제거하지 못했습니다	-
113	보조 노드의 리소스를 새로 고치지 못했습니다	업그레이드 로그를 확인하고 업그레이드를 다시 시도하십시오.

VMware vSphere 10.3용 ONTAP 툴은 제로 RPO를 지원합니다.

에 대해 자세히 알아보십시오 "버전 10.0에서 10.1로 업그레이드하지 못한 경우 VMware vSphere용 ONTAP 툴을 복원하는 방법"

VMware vSphere 9.xx용 ONTAP 툴을 10.3으로 마이그레이션합니다

VMware vSphere 9.xx용 ONTAP 툴에서 10.3로 마이그레이션합니다

VMware vSphere용 NetApp ONTAP 도구를 버전 9.xx에서 10.x로 옮기려면 버전 전반에 걸쳐 중요한 제품 업데이트와 개선 사항이 적용되므로 마이그레이션 프로세스가 필요합니다.

VMware vSphere 9.12D1 및 9.13D2 릴리즈용 ONTAP 툴에서 10.3으로 마이그레이션할 수 있습니다.

설정에 NFS 및 VMFS 데이터 저장소가 있고 vVols 데이터 저장소가 없는 경우 ONTAP Tools 9.xx를 제거하고 ONTAP Tools 10.x를 배포하면 됩니다. 하지만 설정에 vVols 데이터 저장소가 포함된 경우 VASA Provider와 SRA를 마이그레이션하는 과정을 거쳐야 합니다.

다음 표에서는 두 가지 시나리오에서의 마이그레이션 프로세스를 간략하게 설명합니다.

설정에 **vVols** 데이터 저장소가 있는 경우	설정에 **NFS** 및 **VMFS** 데이터 저장소만 포함된 경우
단계: 1. "VASA 공급자 마이그레이션" 2. "VM 스토리지 정책 생성"	단계: 1. 환경에서 ONTAP 도구 9.xx를 제거합니다. 다음을 참조하세요. "환경에서 OTV 9.xx를 제거하는 방법" NetApp 기술 자료 문서. 2. "VMware vSphere 10.3에 대한 ONTAP 도구 배포 및 구성" 3. "SRA를 업데이트합니다" 4. "VM 스토리지 정책 생성"

VMware vSphere 9.xx용 ONTAP 툴에서 10.3로 마이그레이션한 후 NVMe/FC 프로토콜을 사용하는 VVOL 데이터 저장소가 작동하지 않게 됩니다. ONTAP 툴 10.3는 VMFS 데이터 저장소에서만 NVMe-oF 프로토콜을 지원하기 때문입니다.

VASA 공급자를 마이그레이션하고 SRA를 업데이트합니다.

VASA 공급자를 마이그레이션하는 단계

1. VMware vSphere용 기존 ONTAP 툴에서 더비 포트 1527을 활성화하려면 루트 사용자를 활성화하고 SSH를 통해 CLI에 로그인합니다. 그런 다음 다음 다음 명령을 실행합니다.

   ```
   iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
   ```

2. VMware vSphere 10.3용 ONTAP 툴용 OVA 구축
3. VMware vSphere 10.3 릴리즈용 ONTAP 툴로 마이그레이션할 vCenter Server 인스턴스를 추가합니다. 자세한 내용은 을 "vCenter Server 인스턴스를 추가합니다" 참조하십시오.
4. ONTAP 도구 플러그인을 위한 vCenter 서버 API에서 로컬로 스토리지 백엔드를 온보딩합니다.
5. Swagger 또는 Postman에서 다음 API를 실행하여 마이그레이션하십시오.

   CURL-X POST 를 누릅니다 https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migration-jobs

Swagger는 다음 URL을 통해 액세스할 수 있습니다. "https://$FQDN_IP_PORT/,: https://10.67.25.33:8443/.

HTTP 메서드 및 끝점

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

* HTTP 메서드 *	* 경로 *
게시	/api/v1 을 참조하십시오

◦ 처리 유형 *

비동기식

◦ 컬링 예제 *

curl -X POST 'https://<OTV-NG-IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs' \ --header 'x-auth: <인증 토큰>' \ --header '콘텐츠 유형: application/json' \ --data '{ "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "username": "xxxxx", "password": "" }, "database_password": "" }'

다른 릴리스 마이그레이션에 대한 요청 본문:

{ "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "username": "xxxxx", "password": "*" } }

◦ JSON 출력 예 *

작업 객체가 반환됩니다. 다음 단계에서 사용할 작업 식별자를 저장해야 합니다.

{"id":123,"migration_id":"d50073ce-35b4-4c51-9d2e-4ce66f802c35","status":"running"}

6. Swagger에서 다음 URI를 사용하여 상태를 확인합니다.

```
curl
https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID>?
includeSubJobsAndTasks=true
```

작업을 완료한 후 마이그레이션 보고서를 검토합니다. 이 보고서는 작업 데이터에 포함되며 작업 응답에서 액세스할 수 있습니다.

7. vCenter Server에 VMware vSphere 스토리지 공급자용 ONTAP 도구를 추가합니다. "VASA Provider를 등록합니다" VMware vSphere용 ONTAP 도구 사용.
8. "VASA Provider를 설정합니다" VMware vSphere 10.3용 ONTAP 툴에 대한 서비스입니다.
9. 유지 관리 콘솔에서 VMware vSphere 스토리지 공급자용 ONTAP 툴 9.10/9.11/9.12/9.13 VASA Provider 서비스를 중지합니다.

   VASA Provider를 삭제하지 마십시오.

   이전 VASA Provider가 중지되면 vCenter Server가 VMware vSphere용 ONTAP 툴로 페일오버됩니다. 모든 데이터 저장소와 VM에 액세스할 수 있으며 VMware vSphere용 ONTAP 툴을 통해 제공됩니다.

10. VMware vSphere 9.xxx용 ONTAP 툴에서 마이그레이션된 NFS 및 VMFS 데이터 저장소는 데이터 저장소 검색 작업이 트리거된 후에만 VMware vSphere 10.3용 ONTAP 툴에 표시됩니다. 이 작업은 완료하는 데 최대 30분이 걸릴 수 있습니다. VMware vSphere 플러그인 사용자 인터페이스 페이지의 ONTAP 도구 개요 페이지에 데이터 저장소가 표시되는지 확인하세요.
11. Swagger 또는 Postman에서 다음 API를 사용하여 패치 마이그레이션을 수행합니다.

HTTP 메서드 및 끝점

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

* HTTP 메서드 *	* 경로 *
패치	/api/v1 을 참조하십시오

◦ 처리 유형 *

비동기식

◦ 컬링 예제 *

curl-X 패치 https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/84dr73bd-9173-65r7-w345-8ufdbb887d43

◦ JSON 출력 예 *

작업 객체가 반환됩니다. 다음 단계에서 사용할 작업 식별자를 저장해야 합니다.

{"id":123,"migration_id":"d50073ce-35b4-4c51-9d2e-4ce66f802c35","status":"running"}

패치 작업을 위한 요청 본문이 비어 있습니다.

UUID는 마이그레이션 후 API에 대한 응답으로 반환된 마이그레이션 UUID입니다.

패치 마이그레이션 API를 실행한 후에는 모든 VM이 스토리지 정책을 준수합니다.

다음 단계

마이그레이션을 완료하고 ONTAP 툴 10.3를 vCenter Server에 등록한 후 다음 단계를 수행합니다.

- 검색 * 이 완료될 때까지 기다리면 모든 호스트에서 인증서가 자동으로 새로 고쳐집니다.
- 데이터 저장소 및 가상 머신 작업을 시작하기 전에 충분한 시간을 둡니다. 필요한 대기 기간은 구성에 포함된 호스트, 데이터 저장소 및 가상 머신의 수에 따라 달라집니다. 기다리지 않으면 간헐적인 작동 오류가 발생할 수 있습니다.

업그레이드 후 가상 머신의 규정 준수 상태가 오래된 경우 다음 단계를 사용하여 스토리지 정책을 다시 적용합니다.

1. 데이터 저장소로 이동하고 * Summary * > * VM Storage policies * 를 선택합니다.

   VM 스토리지 정책 준수 * 에서 규정 준수 상태는 * 업데이트 안 됨 * 으로 표시됩니다.

2. 스토리지 VM 정책과 해당 VM을 선택합니다

3. 적용 * 을 선택합니다

   VM 저장소 정책 준수 * 의 규정 준수 상태가 이제 준수 상태로 표시됩니다.

관련 정보

- "VMware vSphere 10 RBAC용 ONTAP 툴에 대해 알아보십시오"
- "VMware vSphere 10.x용 ONTAP 툴을 10.3로 업그레이드하십시오"

스토리지 복제 어댑터(SRA)를 업데이트하는 단계

시작하기 전에

복구 계획에서 보호 사이트는 VM이 현재 실행 중인 위치를 나타내고, 복구 사이트는 VM이 복구될 위치를 나타냅니다. SRM 인터페이스는 보호 사이트와 복구 사이트에 대한 세부 정보와 함께 복구 계획의 상태를 표시합니다. 복구 계획에서 CLEANUP(정리) 및 REPROTECT(재보호) 버튼은 비활성화되어 있지만, TEST(테스트) 및 RUN(실행) 버튼은 활성화되어 있습니다. 이는 사이트가 데이터 복구를 위해 준비되었음을 나타냅니다. SRA를 마이그레이션하기 전에 한 사이트는 보호 상태이고 다른 사이트는 복구 상태인지 확인하십시오.

> 페일오버가 완료되었지만 재보호가 보류 중인 경우에는 마이그레이션을 시작하지 마십시오. 마이그레이션을 진행하기 전에 재보호 프로세스가 완료되었는지 확인합니다. 테스트 페일오버가 진행 중인 경우 테스트 페일오버를 정리하고 마이그레이션을 시작합니다.

1. 다음 단계에 따라 VMware 사이트 복구에서 VMware vSphere 9.xx용 ONTAP 툴 SRA 어댑터를 삭제합니다.
   a. VMware Live Site Recovery 구성 관리 페이지로 이동합니다
   b. 스토리지 복제 어댑터 * 섹션으로 이동합니다.
   c. 줄임표 메뉴에서 * Reset configuration * 을 선택합니다.
   d. 줄임표 메뉴에서 * 삭제 * 를 선택합니다.
2. 보호 사이트와 복구 사이트 모두에서 다음 단계를 수행합니다.
   a. 의 단계에 따라 VMware vSphere 10.3 SRA 어댑터용 ONTAP 툴을 설치합니다"VMware Live Site Recovery 어플라이언스에서 SRA를 구성합니다".
   b. VMware Live Site Recovery 사용자 인터페이스 페이지에서 * 스토리지 검색 * 및 * 디바이스 검색 * 작업을 수행하고 디바이스가 마이그레이션 전과 동일하게 표시되는지 확인합니다.

REST API를 사용하여 자동화

VMware vSphere 10 REST API용 ONTAP 툴에 대해 알아보십시오

VMware vSphere 10용 ONTAP 툴은 가상 머신 라이프사이클 관리를 위한 툴 세트입니다. 이 솔루션에는 자동화 프로세스의 일부로 사용할 수 있는 강력한 REST API가 포함되어 있습니다.

REST 웹 서비스 기반

REST(Representational State Transfer)는 웹 서비스 API 설계를 비롯한 분산 웹 애플리케이션을 만드는 스타일입니다. 서버 기반 리소스를 노출하고 상태를 관리하기 위한 일련의 기술을 구축합니다.

리소스 및 상태 표시

리소스는 REST 웹 서비스 애플리케이션의 기본 구성 요소입니다. REST API를 설계할 때 두 가지 중요한 초기 작업이 있습니다.

- 시스템 또는 서버 기반 리소스를 식별합니다
- 리소스 상태 및 관련 상태 전환 작업을 정의합니다

클라이언트 응용 프로그램은 잘 정의된 메시지 흐름을 통해 리소스 상태를 표시하고 변경할 수 있습니다.

HTTP 메시지

HTTP(Hypertext Transfer Protocol)는 웹 서비스 클라이언트와 서버에서 리소스에 대한 메시지를 교환하기 위해 사용하는 프로토콜입니다. 일반 작업 생성, 읽기, 업데이트 및 삭제 작업을 기반으로 한 CRUD 모델을 따릅니다. HTTP 프로토콜에는 응답 상태 코드뿐만 아니라 요청 및 응답 헤더가 포함됩니다.

JSON 데이터 형식

사용할 수 있는 메시지 형식은 여러 가지지만 가장 많이 사용되는 옵션은 JSON(JavaScript Object Notation)입니다. JSON은 단순 데이터 구조를 일반 텍스트로 표시하기 위한 업계 표준이며 리소스와 원하는 작업을 설명하는 상태 정보를 전송하는 데 사용됩니다.

보안

REST API에서는 보안이 중요한 요소입니다. 네트워크를 통해 HTTP 트래픽을 보호하는 데 사용되는 TLS(Transport Layer Security) 프로토콜 외에도 VMware vSphere 10 REST API용 ONTAP 툴은 인증에 액세스 토큰을 사용합니다. 액세스 토큰을 획득하여 이후 API 호출에 사용해야 합니다.

비동기 요청 지원

VMware vSphere 10 REST API용 ONTAP 툴은 대부분의 요청을 동기식으로 수행하며 작업이 완료되면 상태 코드를 반환합니다. 또한 완료하는 데 시간이 오래 걸리는 작업에 대한 비동기 프로세싱도 지원합니다.

ONTAP 도구 관리자 환경

ONTAP 도구 관리자 환경에는 몇 가지 측면을 고려해야 합니다.

가상 머신

VMware vSphere 10용 ONTAP 툴은 vSphere 원격 플러그인 아키텍처를 사용하여 구축됩니다. REST API 지원을

포함한 소프트웨어가 별도의 가상 머신에서 실행됩니다.

ONTAP 도구 **IP** 주소입니다

VMware vSphere 10용 ONTAP 툴은 가상 머신의 기능에 대한 게이트웨이를 제공하는 단일 IP 주소를 표시합니다. 초기 구성 중에 주소를 제공해야 하며 내부 로드 밸런서 구성 요소에 할당됩니다. 이 주소는 Swagger 문서 페이지 및 REST API에 직접 액세스할 뿐만 아니라 ONTAP 도구 관리자 사용자 인터페이스에서 사용됩니다.

REST API 2개

ONTAP 클러스터에는 VMware vSphere 10 REST API용 ONTAP 툴 외에도 자체 REST API가 있습니다. ONTAP 툴 관리자는 ONTAP REST API를 클라이언트로 사용하여 스토리지 관련 작업을 수행한다. 이 두 가지 API는 별개이며 구별된다는 점을 명심해야 합니다. 자세한 내용은 을 "ONTAP 자동화"참조하십시오.

VMware vSphere 10 REST API용 ONTAP 툴 구현 세부 정보입니다

REST에서 일반적인 기술 세트와 모범 사례를 설정하지만 각 API의 정확한 구현은 설계 선택에 따라 다를 수 있습니다. 그리고 VMware vSphere 10 REST API용 ONTAP 툴의 설계 방법을 숙지한 후에 사용해야 합니다.

REST API에는 vCenter 및 Aggregate와 같은 몇 가지 리소스 범주가 포함되어 있습니다. 자세한 내용은 를 "API 참조 "참조하십시오.

REST API 액세스 방법

ONTAP 툴 로드 밸런서 IP 주소와 포트를 통해 VMware vSphere 10 REST API용 ONTAP 툴에 액세스할 수 있습니다. 전체 URL에는 다음과 같은 여러 부분이 있습니다.

- ONTAP 도구 IP 주소 및 포트
- API 버전
- 자원 범주
- 특정 리소스

초기 구성 중에 IP 주소를 구성해야 하며 포트는 항상 8443입니다. 또한 VMware vSphere 10용 특정 ONTAP 툴의 경우 URL의 첫 번째 부분은 일정합니다. 끝점마다 자원 범주와 특정 자원만 다릅니다.

아래 예제의 IP 주소 및 포트 값은 예시용입니다. 환경에 맞게 이러한 값을 변경해야 합니다.

인증 서비스 액세스 예

```
https://10.61.25.34:8443/virtualization/api/v1/auth/login
```

이 URL은 POST 메서드를 사용하여 액세스 토큰을 요청하는 데 사용할 수 있습니다.

vCenter Server를 나열하는 예입니다

```
https://10.61.25.34:8443/virtualization/api/v1/vcenters
```

이 URL은 Get 메서드를 사용하여 정의된 vCenter Server 인스턴스의 목록을 요청하는 데 사용할 수 있습니다.

HTTP 세부 정보입니다

VMware vSphere 10 REST API용 ONTAP 툴은 HTTP 및 관련 매개 변수를 사용하여 리소스 인스턴스 및 컬렉션에 대해 작동합니다. HTTP 구현에 대한 자세한 내용은 아래에 나와 있습니다.

HTTP 메서드

REST API가 지원하는 HTTP 메서드 또는 동사는 아래 표에 나와 있습니다.

방법	CRUD	설명
가져오기	읽기	리소스 인스턴스 또는 컬렉션의 개체 속성을 검색합니다. 이 작업은 컬렉션과 함께 사용할 때 목록 작업으로 간주됩니다.
게시	생성	입력 매개 변수를 기반으로 새 리소스 인스턴스를 만듭니다.
를 누릅니다	업데이트	제공된 JSON 요청 본문으로 전체 리소스 인스턴스를 업데이트합니다. 사용자가 수정할 수 없는 키 값은 유지됩니다.
패치	업데이트	요청에 대해 선택한 변경 사항을 리소스 인스턴스에 적용하도록 요청합니다.
삭제	삭제	기존 리소스 인스턴스를 삭제합니다.

요청 및 응답 헤더

다음 표에는 REST API와 함께 사용되는 가장 중요한 HTTP 헤더가 요약되어 있습니다.

머리글	유형	사용 참고 사항
수락	요청하십시오	클라이언트 응용 프로그램에서 허용할 수 있는 콘텐츠 유형입니다. 유효한 값에는 '\ */ * ' OR `application/json`이 포함됩니다.
X - 인증	요청하십시오	클라이언트 응용 프로그램을 통해 요청을 실행하는 사용자를 식별하는 액세스 토큰이 포함되어 있습니다.
Content-Type(콘텐츠 유형)	응답	요청 헤더에 따라 서버에서 `Accept` 반환됩니다.

HTTP 상태 코드입니다

REST API에서 사용하는 HTTP 상태 코드는 다음과 같다.

코드	의미	설명
200	좋습니다	새 리소스 인스턴스를 만들지 않는 호출의 성공 여부를 나타냅니다.
201	작성됨	리소스 인스턴스에 대한 고유 식별자를 사용하여 개체가 생성되었습니다.
202	수락됨	요청이 수락되었으며 요청을 수행하기 위한 백그라운드 작업이 생성되었습니다.
204	콘텐츠가 없습니다	반환된 콘텐츠가 없지만 요청이 성공했습니다.
400	잘못된 요청입니다	요청 입력이 인식되지 않거나 부적절합니다.
401	권한이 없습니다	사용자에게 권한이 없으므로 인증을 받아야 합니다.
403	금지됨	인증 오류로 인해 액세스가 거부되었습니다.

코드	의미	설명
404	찾을 수 없습니다	요청에서 참조되는 리소스가 없습니다.
409	충돌	개체가 이미 있으므로 개체를 만들지 못했습니다.
500	내부 오류입니다	서버에서 일반적인 내부 오류가 발생했습니다.

인증

REST API에 대한 클라이언트 인증은 액세스 토큰을 사용하여 수행됩니다. 토큰 및 인증 프로세스의 관련 특징은 다음과 같습니다.

- 클라이언트는 ONTAP 도구 관리자 관리자 자격 증명(사용자 이름 및 암호)을 사용하여 토큰을 요청해야 합니다.
- 토큰은 JSON 웹 토큰(JWT)으로 포맷됩니다.
- 각 토큰은 60분 후에 만료됩니다.
- 클라이언트의 API 요청은 요청 헤더에 토큰을 포함해야 `x-auth` 합니다.

액세스 토큰을 요청하고 사용하는 예는 을 "첫 번째 REST API 호출"참조하십시오.

동기 및 비동기 요청

대부분의 REST API 호출은 빠르게 완료되므로 동기식으로 실행됩니다. 즉, 요청이 완료된 후 상태 코드(예: 200)를 반환합니다. 백그라운드 작업을 사용하여 비동기적으로 실행하는 데 시간이 오래 걸리는 요청

비동기적으로 실행되는 API 호출을 실행한 후 서버는 202 HTTP 상태 코드를 반환합니다. 이는 요청이 수락되었지만 아직 완료되지 않았음을 나타냅니다. 백그라운드 작업을 쿼리하여 성공 또는 실패를 포함하여 상태를 확인할 수 있습니다.

비동기식 처리는 데이터 저장소 및 VVOL 작업을 포함하여 여러 유형의 장기 실행 작업에 사용됩니다. 자세한 내용은 Swagger 페이지에서 REST API의 작업 관리자 범주를 참조하십시오.

VMware vSphere 10 REST API 호출용 첫 번째 ONTAP 툴

curl을 사용하여 API 호출을 실행하여 VMware vSphere 10 REST API용 ONTAP 툴을 시작할 수 있습니다.

시작하기 전에

curl 예제에 필요한 정보와 매개변수를 검토해야 합니다.

필수 정보입니다

다음이 필요합니다.

- VMware vSphere 10 IP 주소 또는 FQDN 및 포트용 ONTAP 툴
- ONTAP 도구 관리자 자격 증명(사용자 이름 및 암호)

매개 변수 및 변수

아래에 제시된 컬에는 Bash 스타일 변수가 포함됩니다. 이러한 변수는 Bash 환경에서 설정하거나 명령을 실행하기

전에 수동으로 업데이트할 수 있습니다. 변수를 설정하면 셸이 실행되기 전에 각 명령으로 값을 대체합니다. 변수는 아래 표에 설명되어 있습니다.

변수	설명
$FQDN_IP_port	포트 번호와 함께 ONTAP 도구 관리자의 정규화된 도메인 이름 또는 IP 주소입니다.
$MYUSER	ONTAP 도구 관리자 계정의 사용자 이름입니다.
$MYPASSWORD	ONTAP 도구 관리자 사용자 이름과 연결된 암호입니다.
$access_token입니다	ONTAP 도구 관리자가 발급한 액세스 토큰.

Linux CLI에서의 다음 명령 및 출력은 변수를 설정하고 표시하는 방법을 보여줍니다.

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

1단계: 액세스 토큰을 획득합니다

REST API를 사용하려면 액세스 토큰을 얻어야 합니다. 액세스 토큰을 요청하는 방법의 예는 다음과 같습니다. 환경에 적합한 값으로 대체해야 합니다.

```
curl --request POST \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/login” \
--header "Content-Type: application/json" \
--header "Accept: */*" \
-d "{"username": "$MYUSER", "password": "$MYPASSWORD"}"
```

응답에 제공된 액세스 토큰을 복사하고 저장합니다.

2단계: REST API 호출을 실행합니다

액세스 토큰이 있으면 curl을 사용하여 REST API 호출을 실행할 수 있습니다. 첫 번째 단계에서 획득한 액세스 토큰을 포함합니다.

컬의 예

```
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 포함됩니다.

VMware vSphere 10 REST API용 ONTAP 툴에 대한 API 참조입니다

VMware vSphere 10 REST API 참조용 ONTAP 툴에는 모든 API 호출에 대한 자세한 정보가 포함되어 있습니다. 이 참조는 자동화 애플리케이션을 개발할 때 유용합니다.

Swagger 사용자 인터페이스를 통해 VMware vSphere 10 REST API용 ONTAP 툴 설명서에 온라인으로 액세스할 수 있습니다. 포트뿐만 아니라 VMware vSphere 10 게이트웨이 서비스용 ONTAP 툴의 IP 주소 또는 FQDN이 필요합니다.

단계

1. 브라우저에 변수에 대해 적절한 IP 주소와 포트 조합을 대체할 다음 URL을 입력하고 * Enter * 키를 누릅니다.

   `https://$FQDN_IP_PORT/`

   ◦ 예 *

   `https://10.61.25.33:8443/`

2. 개별 API 호출의 예로, 아래로 스크롤하여 * vCenters * 범주로 이동한 후 끝점 옆에 있는 * Get * 을 선택합니다 `/virtualization/api/v1/vcenters`

법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

"https://www.netapp.com/company/legal/copyright/"

상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

"https://www.netapp.com/company/legal/trademarks/"

특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

개인 정보 보호 정책

"https://www.netapp.com/company/legal/privacy-policy/"

오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이센스에 대한 정보를 제공합니다.

"VMware vSphere 10.3용 ONTAP 툴에 대한 고지 사항"