



개념

ONTAP tools for VMware vSphere 105

NetApp

July 24, 2026

목차

개념.....	1
ONTAP 도구에 대해 알아보세요.....	1
ONTAP 도구의 주요 개념 및 용어.....	1
역할 기반 액세스 제어(RBAC).....	4
ONTAP 도구 RBAC에 대해 알아보십시오.....	4
VMware vSphere를 사용한 RBAC.....	6
ONTAP를 사용한 RBAC.....	12

개념

ONTAP 도구에 대해 알아보세요

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

ONTAP tools for VMware vSphere은 다음을 지원합니다:

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

VMware용 ONTAP tools for VMware의 고가용성

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

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

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

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



ONTAP tools for VMware vSphere는 vCenter HA를 지원하지 않습니다.

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

ONTAP 도구의 주요 개념 및 용어

다음 절에서는 문서에서 사용된 주요 개념과 용어를 설명합니다.

인증 기관(CA)

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

일관성 그룹

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

듀얼 스택

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

고가용성(HA)

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

논리 유닛 번호(LUN)

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

NVMe 네임스페이스 및 서브시스템

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

ONTAP tools Manager

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

Open Virtual Appliance(OVA)

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

복구 시점 목표(RPO)

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

SnapMirror 액티브 동기화

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

스토리지 백엔드

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

글로벌 클러스터(스토리지 백엔드)

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

로컬 스토리지 백엔드

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

스토리지 복제 어댑터(SRA)

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

스토리지 가상 머신(SVM)

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

균일한 구성과 불균일한 구성

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



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

가상 머신 파일 시스템(VMFS)

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

가상 볼륨(vVols)

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

VM 스토리지 정책

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

VMware Live Site Recovery

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

VMware vSphere APIs for Storage Awareness(VASA)

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

VMware vSphere Storage APIs - Array Integration(VAAI)

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

vSphere Metro 스토리지 클러스터

vSphere Metro Storage Cluster(vMSC)는 확장 클러스터 배포 환경에서 vSphere를 지원하고 활성화하는 아키텍처입니다. vMSC 솔루션은 NetApp MetroCluster 및 SnapMirror active sync(이전 SMBC)에서 지원됩니다. 이러한 솔루션은 도메인 장애 발생 시 향상된 비즈니스 연속성을 제공합니다. 복원력 모델은 사용자의 특정 구성 선택에 따라 달라집니다. 자세한 내용은 "[VMware vSphere Metro 스토리지 클러스터](#)"를 참조하십시오.

vVols 데이터스토어

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

제로 RPO

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

역할 기반 액세스 제어(RBAC)

ONTAP 도구 RBAC에 대해 알아보십시오

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

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

RBAC 구성 요소

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

Privileges

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

역할

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

객체

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

사용자 및 그룹

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

권한

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

두 개의 RBAC 환경

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

VMware vCenter Server

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

ONTAP 클러스터

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

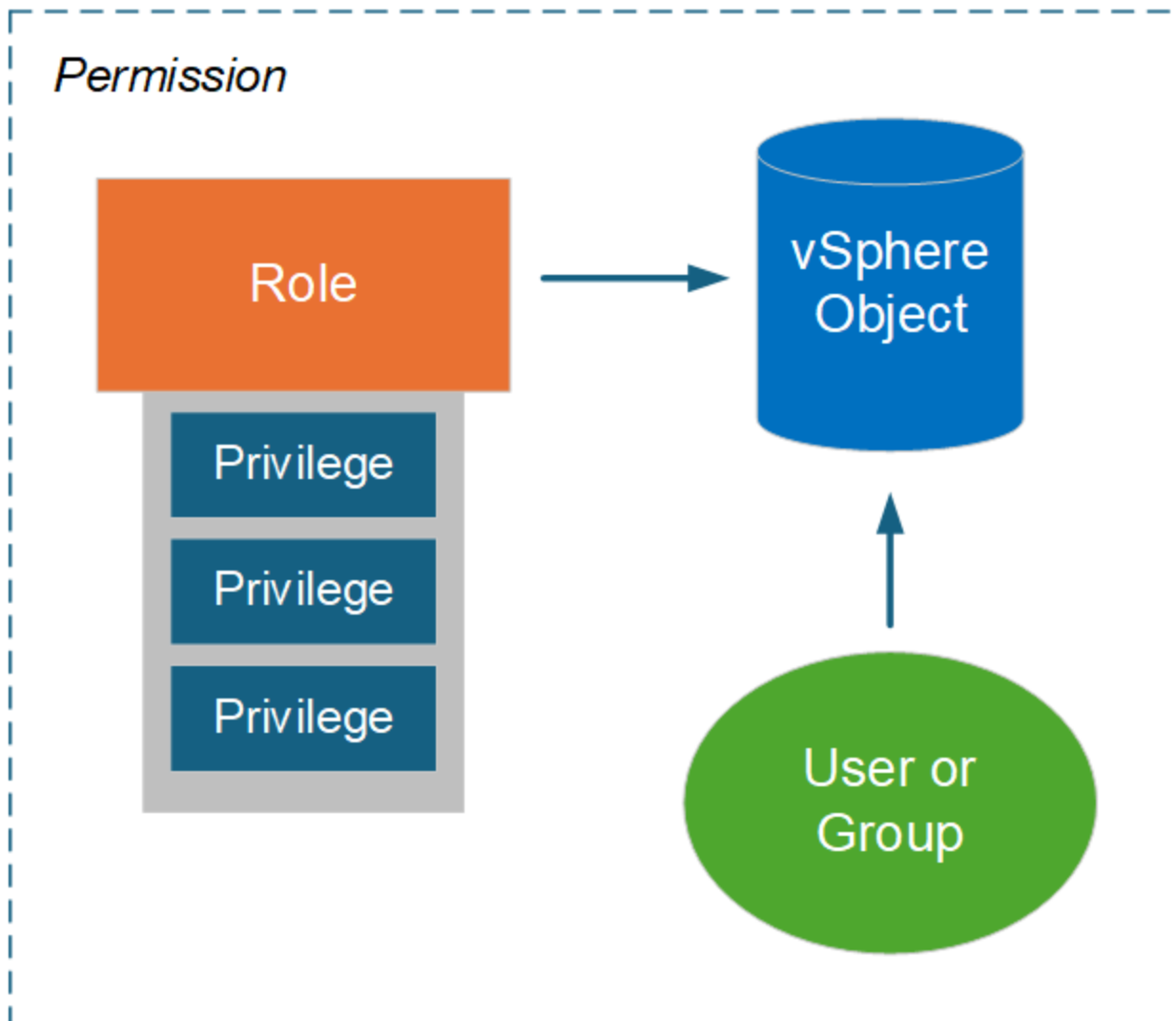
VMware vSphere를 사용한 RBAC

vCenter Server RBAC가 ONTAP 도구와 연동되는 방식

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

vCenter Server 권한 그림

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



vCenter Server 권한의 구성 요소

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

vSphere 객체

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

Privileges 및 역할

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

- 네이티브 vCenter Server Privileges

vCenter Server에서 제공하는 Privileges는 다음과 같습니다.

- ONTAP tools별 Privileges

이는 ONTAP tools for VMware vSphere에 고유한 사용자 지정 Privileges입니다.

사용자 및 그룹

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

vCenter Server RBAC의 ONTAP tools 관련 고려 사항

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

vCenter 역할 및 관리자 계정

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

vSphere 객체 계층 구조

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

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

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

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



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

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

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

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

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

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

아래에 설명된 바와 같이 미리 정의된 세 가지 역할이 있습니다.

NetApp ONTAP tools for VMware vSphere 관리자

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

NetApp ONTAP tools for VMware vSphere 읽기 전용

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

NetApp ONTAP tools for VMware vSphere 프로비저닝

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

- 새 데이터스토어 생성
- 데이터 저장소 관리

vSphere 객체 및 ONTAP 스토리지 백엔드

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

vCenter Server RBAC 작업

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

필수 권한

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

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

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

권한 할당

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



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

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

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

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

ONTAP를 사용한 RBAC

ONTAP RBAC가 ONTAP tools와 연동되는 방식

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

관리 옵션 개요

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



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

역할 및 권한 유형

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

- REST

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

- 전통적인

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

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

범위

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

역할 정의

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

ONTAP REST 역할 사용

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

역할 매핑

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

CLI Privileges를 사용하여 REST 역할 정의하기

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

ONTAP 역할 정의 시 관리 인터페이스

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

ONTAP tools에 대한 ONTAP RBAC 고려 사항

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

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

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

1. 준비

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

2. JSON 정의 파일을 다운로드합니다.

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

3. 역할을 가진 ONTAP 사용자 생성

System Manager에 로그인한 후 사용자 및 역할을 생성할 수 있습니다.

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

4. 역할 구성

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

System Manager를 사용하여 역할 구성

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

핵심 사용자 및 역할 구성

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

Privileges

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

- 검색

이 역할을 통해 스토리지 시스템을 추가할 수 있습니다.

- 스토리지 생성

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

- 저장소 수정

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

- 스토리지 삭제

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

역할을 부여하여 사용자를 생성합니다.

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

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

예

OTV_10_VSC_Discovery_Create

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

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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