VMware vSphere를 사용하는 RBAC

ONTAP tools for VMware vSphere 10

NetApp
August 25, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/ontap-tools-vmware-vsphere-10/concepts/rbac-vcenter-environment.html on August 25, 2025. Always check docs.netapp.com for the latest.

목차

VMware vSphere를 사용하는 RBAC . . . 1
VMware vSphere 10용 ONTAP 툴을 사용하는 vCenter Server RBAC 환경 . . . 1
vCenter Server 사용 권한 그림 . . . 1
vCenter Server 권한의 구성 요소입니다 . . . 2
VMware vSphere 10용 ONTAP 툴과 함께 vCenter Server RBAC를 사용하십시오 . . . 2
vCenter 역할 및 관리자 계정입니다 . . . 2
vSphere 객체 계층 구조 . . . 2
VMware vSphere 10용 ONTAP 툴에 포함된 역할 . . . 3
vSphere 오브젝트 및 ONTAP 스토리지 백 엔드 . . . 3
vCenter Server RBAC 작업 . . . 3

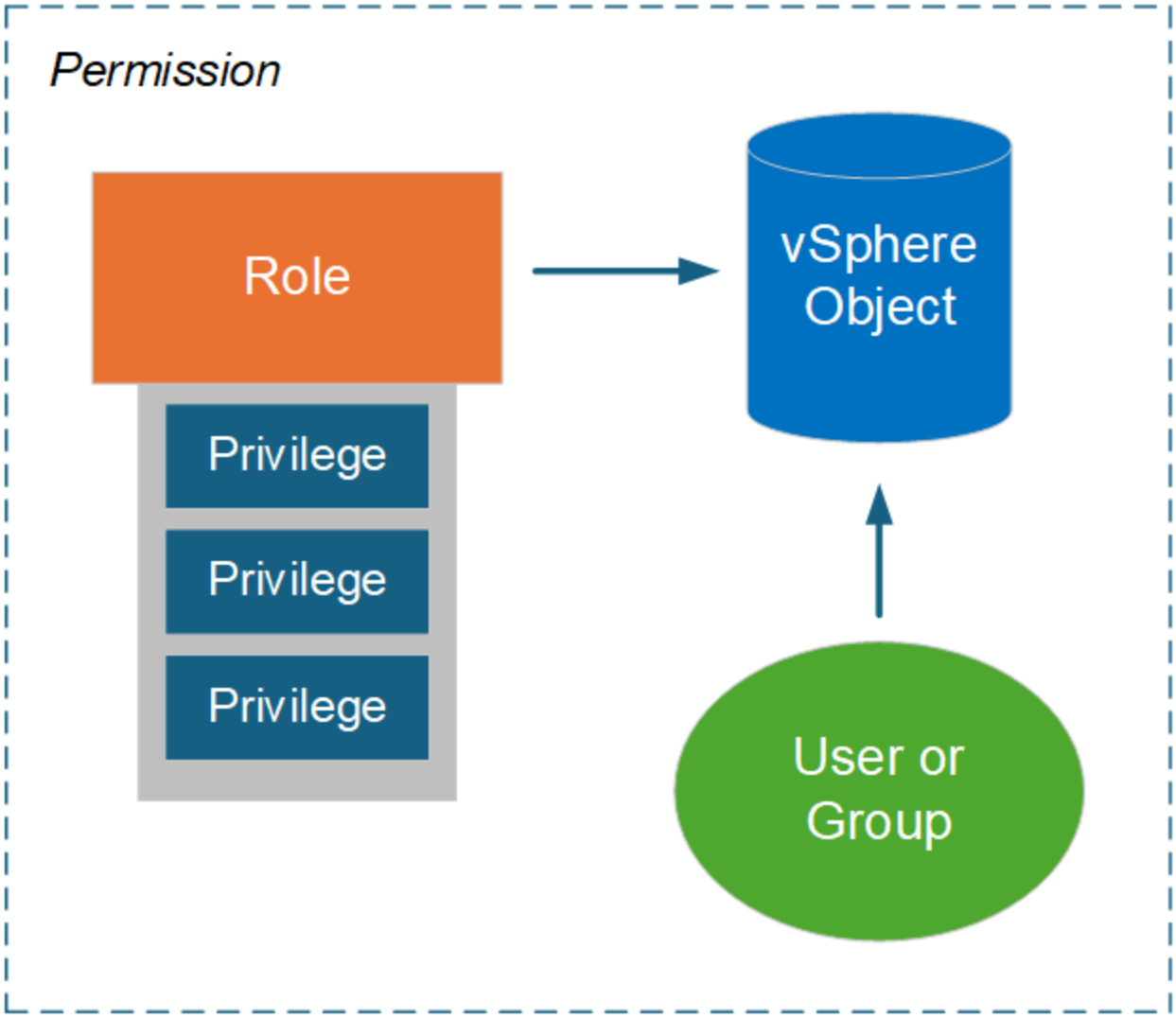
VMware vSphere를 사용하는 RBAC

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

VMware vSphere 10용 ONTAP 툴과 함께 vCenter Server RBAC를 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.

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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