역할 기반 액세스 제어

ONTAP tools for VMware vSphere 10.1

NetApp
December 19, 2024

목차

역할 기반 액세스 제어

VMware vSphere용 ONTAP 툴의 역할 기반 액세스 제어 개요

vCenter Server는 vSphere 객체에 대한 액세스를 제어할 수 있는 RBAC(역할 기반 액세스 제어)를 제공합니다. vCenter Server는 역할 및 Privileges를 통해 사용자 및 그룹 권한을 사용하여 인벤토리의 다양한 수준에서 중앙 집중식 인증 및 인증 서비스를 제공합니다. vCenter Server는 RBAC 관리를 위한 5가지 주요 구성 요소:

구성 요소	설명
권한	권한은 vSphere에서 작업을 수행하기 위한 액세스를 설정하거나 거부합니다.
역할	역할에는 하나 이상의 시스템 권한이 포함되며, 여기서 각 권한은 시스템의 특정 개체 또는 개체 유형에 대한 관리 권한을 정의합니다. 사용자에게 역할을 할당하면 사용자는 해당 역할에 정의된 권한의 기능을 상속합니다.
사용자 및 그룹	사용자와 그룹은 AD(Active Directory)에서 역할을 할당할 수 있는 권한에 사용됩니다. vCenter Server에는 사용할 수 있는 고유한 로컬 사용자 및 그룹이 있습니다.
권한	사용 권한을 사용하면 Privileges를 사용자 또는 그룹에 할당하여 vCenter Server 내의 개체를 변경할 수 있습니다. vCenter Server 사용 권한은 ESXi 호스트에 직접 로그인하는 사용자가 아니라 vCenter Server에 로그인하는 사용자에게만 영향을 줍니다.
오브젝트	작업이 수행되는 엔티티입니다. VMware vCenter 객체는 데이터 센터, 폴더, 리소스 풀, 클러스터, 호스트, 및 VM을 지원합니다

작업을 성공적으로 완료하려면 적절한 vCenter Server RBAC 역할이 있어야 합니다. 작업 중에 VMware vSphere용 ONTAP 툴은 사용자의 ONTAP 권한을 확인하기 전에 사용자의 vCenter Server 역할을 확인합니다.

vCenter Server 역할은 VMware vSphere vCenter 사용자용 ONTAP 툴에 적용되며 관리자에게는 적용되지 않습니다. 기본적으로 관리자는 제품에 대한 모든 액세스 권한을 가지며 할당된 역할이 필요하지 않습니다.

사용자 및 그룹은 vCenter Server 역할의 일부가 되어 역할에 액세스할 수 있습니다.

vCenter Server에 대한 역할 할당 및 수정에 대한 주요 사항

vSphere 객체 및 작업에 대한 액세스를 제한하려는 경우에만 vCenter Server 역할을 설정해야 합니다. 그렇지 않으면 관리자로 로그인할 수 있습니다. 이 로그인을 통해 모든 vSphere 객체에 자동으로 액세스할 수 있습니다.

역할을 할당하는 위치에 따라 사용자가 수행할 수 있는 VMware vSphere 작업에 대한 ONTAP 툴이 결정됩니다. 언제든지 하나의 역할을 수정할 수 있습니다. 역할 내의 권한을 변경하는 경우 해당 역할과 연결된 사용자는 로그아웃한 다음 다시 로그인하여 업데이트된 역할을 사용하도록 설정해야 합니다.

VMware vSphere용 ONTAP 툴과 함께 패키지로 제공되는 표준 역할입니다

vCenter Server 권한 및 RBAC를 간편하게 사용할 수 있도록 VMware vSphere용 ONTAP 툴은 VMware vSphere 역할에 사용할 수 있는 표준 ONTAP 툴을 제공합니다. 이 툴을 사용하면 VMware vSphere 작업에 대한 주요 ONTAP 툴을 수행할 수 있습니다. 또한 정보를 볼 수는 있지만 작업을 수행할 수 없는 읽기 전용 역할도 있습니다.

vSphere Client 홈 페이지에서 * 역할 * 을 클릭하여 VMware vSphere 표준 역할용 ONTAP 툴을 볼 수 있습니다. VMware vSphere용 ONTAP 툴이 제공하는 역할을 사용하면 다음 작업을 수행할 수 있습니다.

* 역할 *	* 설명 *
VMware vSphere 관리자용 NetApp ONTAP 툴	VMware vSphere 작업을 위한 일부 ONTAP 툴을 수행하는 데 필요한 모든 기본 vCenter Server 권한 및 ONTAP 툴별 권한을 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

ONTAP tools Manager 관리자 역할이 vCenter Server에 등록되지 않았습니다. 이 역할은 ONTAP 도구 관리자에 따라 다릅니다.

회사에서 VMware vSphere 역할에 대한 표준 ONTAP 툴보다 더 엄격한 역할을 구현해야 하는 경우 VMware vSphere 역할용 ONTAP 툴을 사용하여 새로운 역할을 생성할 수 있습니다.

이 경우 VMware vSphere 역할에 필요한 ONTAP 툴을 클론 생성한 다음 사용자가 필요로 하는 권한만 갖도록 클론 생성된 역할을 편집합니다.

ONTAP 스토리지 백 엔드 및 vSphere 객체에 대한 권한

vCenter Server 권한이 충분하면 VMware vSphere용 ONTAP 툴이 스토리지 백엔드 자격 증명(사용자 이름 및 암호)과 연결된 ONTAP RBAC 권한(ONTAP 역할)을 확인합니다. 해당 스토리지 백엔드에서 VMware vSphere용 ONTAP 툴에 필요한 스토리지 작업을 수행할 수 있는 권한이 있는지 여부를 확인합니다. 올바른 ONTAP Privileges가 있는 경우 스토리지 백엔드에 액세스하고 VMware vSphere 작업에 대한 ONTAP 툴을 수행할 수 있습니다. ONTAP 역할에 따라 스토리지 백엔드에서 수행할 수 있는 VMware vSphere 작업에 대한 ONTAP 툴이 결정됩니다.

vCenter Server 권한의 구성 요소입니다

vCenter Server는 권한이 아닌 권한을 인식합니다. 각 vCenter Server 권한은 세 가지 구성 요소로 구성됩니다.

vCenter Server에는 다음과 같은 구성 요소가 있습니다.

- 하나 이상의 권한(역할)

권한은 사용자가 수행할 수 있는 작업을 정의합니다.

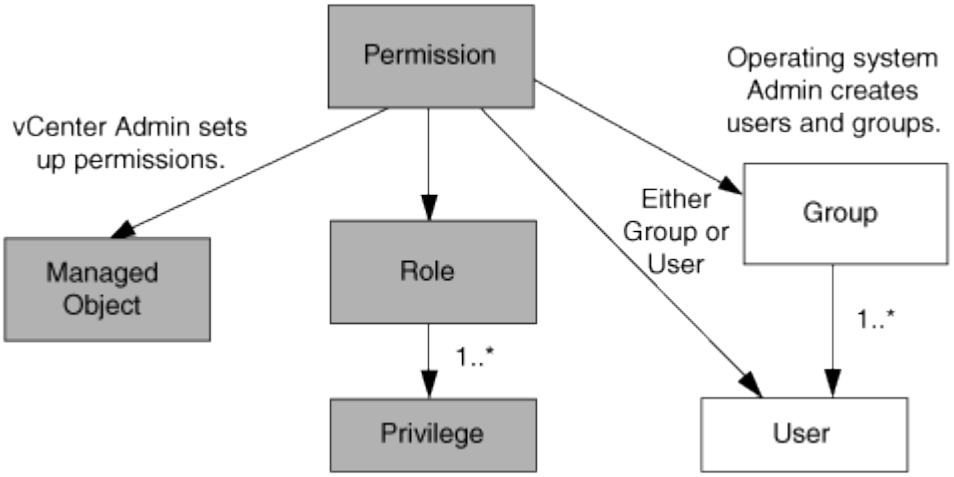
- vSphere 객체입니다

  개체는 작업의 대상입니다.

- 사용자 또는 그룹

  사용자 또는 그룹은 작업을 수행할 수 있는 사용자를 정의합니다.

이 다이어그램에서 회색 상자는 vCenter Server에 있는 구성 요소를 나타내고 흰색 상자는 vCenter Server가 실행 중인 운영 체제에 있는 구성 요소를 나타냅니다.



권한

VMware vSphere용 ONTAP 툴에는 두 가지 유형의 권한이 연결됩니다.

- 기본 vCenter Server 권한

  이러한 권한은 vCenter Server와 함께 제공됩니다.

- ONTAP 도구별 권한

  이러한 권한은 VMware vSphere 작업에 대한 특정 ONTAP 툴에 대해 정의됩니다. VMware vSphere용 ONTAP 툴에만 해당됩니다.

VMware vSphere 작업을 위한 ONTAP 툴에는 ONTAP 툴별 권한과 vCenter Server 기본 권한이 모두 필요합니다. 이러한 권한은 사용자에게 ""역할""을 구성합니다. 권한은 여러 권한을 가질 수 있습니다. 이러한 권한은 vCenter Server에 로그인한 사용자를 위한 것입니다.

VMware vSphere용 ONTAP 툴은 vCenter Server RBAC ONTAP 작업을 간소화하기 위해 VMware vSphere 작업에 필요한 모든 ONTAP 툴과 기본 권한을 포함하는 여러 가지 표준 역할을 제공합니다.

권한 내에서 권한을 변경하면 해당 권한과 연결된 사용자가 로그아웃한 다음 로그인하여 업데이트된 권한을 활성화해야 합니다.

vSphere 객체

사용 권한은 vCenter Server, ESXi 호스트, 가상 머신, 데이터 저장소, 데이터 센터 등의 vSphere 객체와 연결됩니다. 및 폴더. 모든 vSphere 객체에 권한을 할당할 수 있습니다. vSphere 객체에 할당된 권한에 따라 vCenter Server는 해당 객체에 대해 수행할 수 있는 작업을 결정합니다. VMware vSphere 관련 작업에 사용되는 ONTAP 툴의 경우 사용 권한은 루트 폴더 레벨(vCenter Server)에서만 할당되고 검증되며 다른 엔터티에서는 할당되지 않습니다. VAAI 플러그인 작업을 제외하고 관련 ESXi 호스트에 대해 사용 권한이 검증됩니다.

사용자 및 그룹

Active Directory(또는 로컬 vCenter Server 머신)를 사용하여 사용자 및 사용자 그룹을 설정할 수 있습니다. 그런 다음 vCenter Server 권한을 사용하여 이러한 사용자 또는 그룹이 VMware vSphere 작업에 대한 특정 ONTAP 툴을 수행할 수 있도록 액세스 권한을 부여할 수 있습니다.

> 이러한 vCenter Server 사용 권한은 VMware vSphere vCenter 사용자용 ONTAP 툴에 적용되며, VMware vSphere 관리자용 ONTAP 툴에는 적용되지 않습니다. 기본적으로 VMware vSphere 관리자용 ONTAP 툴은 제품에 대한 모든 액세스 권한을 가지며 해당 툴에 할당된 권한이 필요하지 않습니다.

사용자 및 그룹에 할당된 역할이 없습니다. vCenter Server 권한의 일부이기 때문에 역할에 액세스할 수 있습니다.

vCenter Server에 대한 사용 권한을 할당하고 수정합니다

vCenter Server 사용 권한을 사용할 때는 몇 가지 주요 사항을 염두에 두어야 합니다. VMware vSphere 작업을 위한 ONTAP 도구의 성공 여부는 권한이 할당된 위치 또는 권한이 수정된 후 사용자가 수행한 작업에 따라 달라집니다.

권한 할당

vSphere 객체 및 작업에 대한 액세스를 제한하려면 vCenter Server 권한만 설정하면 됩니다. 그렇지 않으면 관리자로 로그인할 수 있습니다. 이 로그인을 통해 모든 vSphere 객체에 자동으로 액세스할 수 있습니다.

권한을 할당하는 위치에 따라 사용자가 수행할 수 있는 VMware vSphere 작업에 대한 ONTAP 툴이 결정됩니다.

작업이 완료되도록 하려면 루트 개체와 같은 상위 수준에서 사용 권한을 할당해야 하는 경우가 있습니다. 이 경우는 작업에 특정 vSphere 객체에 적용되지 않는 권한(예: 작업 추적)이 필요하거나 vSphere가 아닌 객체(예: 스토리지 시스템)에 필요한 권한이 적용되는 경우에 해당합니다.

이러한 경우 사용 권한을 설정하여 자식 엔터티가 사용 권한을 상속할 수 있습니다. 하위 엔티티에 다른 권한을 할당할 수도 있습니다. 자식 엔터티에 할당된 권한은 항상 부모 엔터티로부터 상속된 권한을 재정의합니다. 즉, 자식 엔터티에 권한을 부여하여 루트 개체에 할당되고 자식 엔터티에 의해 상속되는 권한의 범위를 제한할 수 있습니다.

> 회사의 보안 정책에 더 제한적인 권한이 필요한 경우를 제외하고 루트 개체(루트 폴더라고도 함)에 권한을 할당하는 것이 좋습니다.

사용 권한 및 비 vSphere 객체

생성한 권한은 vSphere가 아닌 객체에 적용됩니다. 예를 들어, 스토리지 시스템은 vSphere 객체가 아닙니다. 스토리지 시스템에 권한이 적용되는 경우 해당 권한을 할당할 수 있는 vSphere 객체가 없으므로 VMware vSphere 루트 객체용

ONTAP 툴에 해당 권한이 포함된 권한을 할당해야 합니다.

예를 들어, VMware vSphere용 ONTAP 툴 권한 "스토리지 시스템 추가/수정/건너뛰기"와 같은 권한을 포함하는 모든 권한은 루트 객체 레벨에서 할당되어야 합니다.

권한을 수정합니다

언제든지 하나의 권한을 수정할 수 있습니다.

권한 내에서 권한을 변경하는 경우 해당 권한과 연결된 사용자는 로그아웃한 다음 다시 로그인하여 업데이트된 권한을 활성화해야 합니다.

ONTAP 툴에 필요한 VMware vSphere 작업에 필요한 권한

VMware vSphere 작업에 사용되는 ONTAP 툴이 다르면 VMware vSphere용 ONTAP 툴과 기본 vCenter Server 권한에 대해 서로 다른 권한을 조합해야 합니다.

VMware vSphere GUI용 ONTAP 툴에 액세스하려면 올바른 vSphere 객체 수준에서 제품 수준의 ONTAP 툴별 보기 권한이 할당되어 있어야 합니다. 이 권한 없이 로그인하면 VMware vSphere용 ONTAP Tools에서 NetApp 아이콘을 클릭하면 오류 메시지가 표시되고 ONTAP 툴에 액세스할 수 없습니다.

보기 * 권한에서 VMware vSphere용 ONTAP 툴에 액세스할 수 있습니다. 이 권한을 사용하여 VMware vSphere용 ONTAP 툴 내에서 작업을 수행할 수 없습니다. VMware vSphere 작업에 대한 ONTAP 툴을 수행하려면 해당 작업에 대한 올바른 ONTAP 툴과 기본 vCenter Server 권한이 있어야 합니다.

할당 수준은 UI에서 볼 수 있는 부분을 결정합니다. 루트 객체(폴더)에 보기 권한을 할당하면 NetApp 아이콘을 클릭하여 VMware vSphere용 ONTAP 툴을 시작할 수 있습니다.

보기 권한을 다른 vSphere 객체 레벨에 할당할 수 있지만, 이렇게 하면 보고 사용할 수 있는 VMware vSphere 메뉴에 대한 ONTAP 툴이 제한됩니다.

루트 개체는 보기 권한이 포함된 권한을 할당하는 데 권장되는 장소입니다.

VMware vSphere용 ONTAP 툴에 대해 권장되는 ONTAP 역할

VMware vSphere 및 역할 기반 액세스 제어(RBAC)에 대한 ONTAP 툴로 작업하기 위해 권장되는 여러 ONTAP 역할을 설정할 수 있습니다. 이러한 역할에는 VMware vSphere 작업을 위해 ONTAP 툴에서 실행되는 스토리지 작업을 수행하는 데 필요한 ONTAP 권한이 포함됩니다.

새로운 사용자 역할을 생성하려면 ONTAP를 실행하는 스토리지 시스템의 관리자로 로그인해야 합니다. ONTAP 시스템 관리자 9.8P1 이상을 사용하여 ONTAP 역할을 생성할 수 있습니다.

각 ONTAP 역할에는 역할의 자격 증명을 구성하는 연결된 사용자 이름 및 암호 쌍이 있습니다. 이러한 자격 증명을 사용하여 로그인하지 않으면 해당 역할과 연결된 스토리지 작업에 액세스할 수 없습니다.

보안 조치로서 VMware vSphere 관련 ONTAP 역할에 대한 ONTAP 툴은 계층적으로 정렬됩니다. 즉, 첫 번째 역할이 가장 제한적이며 VMware vSphere 스토리지 작업을 위한 가장 기본적인 ONTAP 툴 세트와 관련된 권한만 가집니다. 다음 역할에는 자체 권한 및 이전 역할과 연결된 모든 권한이 포함됩니다. 각 추가 역할은 지원되는 스토리지 작업과 관련하여 덜 제한적입니다.

다음은 VMware vSphere용 ONTAP 툴을 사용할 때 권장되는 ONTAP RBAC 역할 중 일부입니다. 이러한 역할을 생성한 후 가상 시스템 프로비저닝과 같이 스토리지와 관련된 작업을 수행해야 하는 사용자에게 역할을 할당할 수 있습니다.

* 역할 *	* 권한 *
탐색	이 역할을 통해 스토리지 시스템을 추가할 수 있습니다.
스토리지 생성	이 역할을 사용하여 스토리지를 생성할 수 있습니다. 이 역할에는 검색 역할과 연결된 모든 권한도 포함됩니다.
스토리지 수정	이 역할을 사용하여 스토리지를 수정할 수 있습니다. 이 역할에는 검색 역할 및 스토리지 생성 역할과 연결된 모든 권한도 포함됩니다.
스토리지 폐기	이 역할을 사용하면 스토리지를 제거할 수 있습니다. 이 역할에는 검색 역할, 스토리지 생성 역할 및 스토리지 수정 역할과 연결된 모든 권한도 포함됩니다.

VMware vSphere용 ONTAP 툴을 사용하는 경우에는 PBM(정책 기반 관리) 역할도 설정해야 합니다. 이 역할을 통해 스토리지 정책을 사용하여 스토리지를 관리할 수 있습니다. 이 역할을 수행하려면 "Discovery" 역할도 설정해야 합니다.