



SnapCenter 역할 기반 액세스 제어(RBAC)

SnapCenter Software 4.8

NetApp
January 18, 2024

목차

SnapCenter 역할 기반 액세스 제어(RBAC)	1
RBAC 유형	1
RBAC 권한 및 역할	2
사전 정의된 SnapCenter 역할 및 권한	4

SnapCenter 역할 기반 액세스 제어(RBAC)

RBAC 유형

ONTAP RBAC(역할 기반 액세스 제어) 및 SnapCenter 권한을 사용하여 SnapCenter 관리자는 SnapCenter 리소스에 대한 제어 권한을 다른 사용자 또는 사용자 그룹에 위임할 수 있습니다. 이러한 중앙 관리형 액세스를 통해 애플리케이션 관리자는 위임된 환경 내에서 안전하게 작업할 수 있습니다.

언제든지 역할을 만들고 수정할 수 있으며 사용자에게 리소스 액세스 권한을 추가할 수 있지만 SnapCenter를 처음 설정할 때는 최소한 역할에 Active Directory 사용자 또는 그룹을 추가한 다음 이러한 사용자 또는 그룹에 리소스 액세스 권한을 추가해야 합니다.



SnapCenter를 사용하여 사용자 또는 그룹 계정을 만들 수 없습니다. 운영 체제 또는 데이터베이스의 Active Directory에서 사용자 또는 그룹 계정을 만들어야 합니다.

SnapCenter는 다음과 같은 유형의 역할 기반 액세스 제어를 사용합니다.

- SnapCenter RBAC
- SnapCenter 플러그인 RBAC(일부 플러그인의 경우)
- 애플리케이션 레벨 RBAC
- ONTAP 권한

SnapCenter RBAC

역할 및 권한

SnapCenter에는 권한이 이미 할당된 미리 정의된 역할이 제공됩니다. 이러한 역할에 사용자 또는 사용자 그룹을 할당할 수 있습니다. 새 역할을 만들고 사용 권한 및 사용자를 관리할 수도 있습니다.

- 사용자 또는 그룹에 권한 할당 *

사용자 또는 그룹에 권한을 할당하여 호스트, 스토리지 접속 및 리소스 그룹과 같은 SnapCenter 객체를 액세스할 수 있습니다. SnapCenterAdmin 역할의 권한은 변경할 수 없습니다.

동일한 포리스트 내의 사용자 및 그룹과 다른 포리스트에 속한 사용자에게 RBAC 권한을 할당할 수 있습니다. 포리스트 전체의 중첩된 그룹에 속하는 사용자에게는 RBAC 권한을 할당할 수 없습니다.



사용자 지정 역할을 만드는 경우 SnapCenter 관리자 역할의 모든 권한이 있어야 합니다. 호스트 추가 또는 호스트 제거 등의 일부 권한만 복사하는 경우에는 해당 작업을 수행할 수 없습니다.

인증

사용자는 로그인 시 그래픽 사용자 인터페이스(GUI) 또는 PowerShell cmdlet을 사용하여 인증을 제공해야 합니다. 사용자가 둘 이상의 역할의 구성원인 경우 로그인 자격 증명을 입력한 후 사용할 역할을 지정하라는 메시지가 표시됩니다. 또한 사용자는 API를 실행하기 위한 인증을 제공해야 합니다.

애플리케이션 레벨 RBAC

SnapCenter는 자격 증명을 사용하여 권한이 있는 SnapCenter 사용자에게 응용 프로그램 수준 권한도 있는지 확인합니다.

예를 들어 SQL Server 환경에서 스냅샷 복사본 및 데이터 보호 작업을 수행하려면 적절한 Windows 또는 SQL 자격 증명을 사용하여 자격 증명을 설정해야 합니다. SnapCenter 서버는 두 가지 방법 중 하나를 사용하여 설정된 자격 증명을 인증합니다. ONTAP 스토리지의 Windows 파일 시스템 환경에서 스냅샷 복사본 및 데이터 보호 작업을 수행하려면 SnapCenter 관리자 역할에 Windows 호스트에 대한 관리자 권한이 있어야 합니다.

마찬가지로 Oracle 데이터베이스에서 데이터 보호 작업을 수행하고 데이터베이스 호스트에서 운영 체제(OS) 인증을 사용하지 않도록 설정한 경우 Oracle 데이터베이스 또는 Oracle ASM 자격 증명을 사용하여 자격 증명을 설정해야 합니다. SnapCenter 서버는 작업에 따라 이러한 방법 중 하나를 사용하여 설정된 자격 증명을 인증합니다.

VMware vSphere용 SnapCenter 플러그인 RBAC

VM 일관성 있는 데이터 보호를 위해 SnapCenter VMware 플러그인을 사용하는 경우 vCenter Server는 추가 RBAC 수준을 제공합니다. SnapCenter VMware 플러그인은 vCenter Server RBAC와 Data ONTAP RBAC를 모두 지원합니다.

자세한 내용은 을 참조하십시오 "[VMware vSphere용 SnapCenter 플러그인 RBAC](#)"

ONTAP 권한

스토리지 시스템에 액세스하는 데 필요한 권한이 있는 vsadmin 계정을 생성해야 합니다.

계정을 만들고 권한을 할당하는 방법에 대한 자세한 내용은 을 참조하십시오 "[최소 권한으로 ONTAP 클러스터 역할을 생성합니다](#)"

RBAC 권한 및 역할

SnapCenter RBAC(역할 기반 액세스 제어)를 사용하여 역할을 만들고 해당 역할에 권한을 할당한 다음 사용자 또는 사용자 그룹을 역할에 할당할 수 있습니다. 따라서 SnapCenter 관리자는 중앙에서 관리되는 환경을 만들 수 있고, 애플리케이션 관리자는 데이터 보호 작업을 관리할 수 있습니다. SnapCenter에는 몇 가지 미리 정의된 역할 및 권한이 제공됩니다.

SnapCenter 역할

SnapCenter에는 다음과 같은 사전 정의된 역할이 제공됩니다. 이러한 역할에 사용자와 그룹을 할당하거나 새 역할을 만들 수 있습니다.

사용자에게 역할을 할당하면 SnapCenter 관리자 역할을 할당하지 않는 한 해당 사용자와 관련된 작업만 작업 페이지에 표시됩니다.

- 애플리케이션 백업 및 클론 관리
- 백업 및 클론 뷰어
- 인프라 관리자
- SnapCenter서버

VMware vSphere 역할용 SnapCenter 플러그인

VM, VMDK 및 데이터 저장소의 VM 일관성 있는 데이터 보호를 관리하기 위해 VMware vSphere용 SnapCenter 플러그인을 통해 vCenter에서 다음 역할이 생성됩니다.

- SCV 관리자
- SCV 보기
- SCV 백업
- SCV 복원
- SCV 게스트 파일 복원

자세한 내용은 을 참조하십시오 "[VMware vSphere 사용자를 위한 SnapCenter 플러그인의 RBAC 유형](#)"

* 모범 사례: * VMware vSphere 운영을 위한 SnapCenter 플러그인에 대해 하나의 ONTAP 역할을 생성한 후 필요한 모든 권한을 할당하는 것이 좋습니다.

SnapCenter 권한

SnapCenter는 다음과 같은 권한을 제공합니다.

- 리소스 그룹
- 정책
- 백업
- 호스트
- 스토리지 연결
- 복제
- 프로비저닝(Microsoft SQL 데이터베이스에만 해당)
- 대시보드
- 보고서
- 복원
 - 전체 볼륨 복원(사용자 지정 플러그인에만 해당)
- 리소스

관리자가 아닌 경우 리소스 검색 작업을 수행하려면 관리자에게 플러그인 권한이 필요합니다.

- 플러그인 설치 또는 제거



플러그인 설치 권한을 활성화할 경우 읽기 및 업데이트를 사용하도록 호스트 권한도 수정해야 합니다.

- 마이그레이션
- 마운트(Oracle 데이터베이스에만 해당)

- 마운트 해제(Oracle 데이터베이스에만 해당)
- 작업 모니터

작업 모니터 권한을 사용하면 다른 역할의 구성원이 할당된 모든 개체에 대한 작업을 볼 수 있습니다.

사전 정의된 SnapCenter 역할 및 권한

SnapCenter에는 미리 정의된 역할이 제공되며 각 역할에는 이미 설정된 사용 권한이 있습니다. 역할 기반 액세스 제어(RBAC)를 설정 및 관리할 때 이러한 사전 정의된 역할을 사용하거나 새 역할을 생성할 수 있습니다.

SnapCenter에는 다음과 같은 사전 정의된 역할이 포함되어 있습니다.

- SnapCenter 관리자 역할
- 앱 백업 및 클론 관리자 역할
- 백업 및 클론 뷰어 역할
- 인프라 관리자 역할

사용자를 역할에 추가할 때는 스토리지 가상 시스템(SVM) 통신을 지원하기 위해 StorageConnection 권한을 할당하거나 SVM을 사용할 수 있도록 SVM을 사용자에게 할당해야 합니다. 스토리지 연결 권한을 사용하면 SVM 연결을 생성할 수 있습니다.

예를 들어, SnapCenter 관리자 역할을 가진 사용자는 SVM 연결을 생성하여 앱 백업 및 클론 관리 역할을 가진 사용자에게 할당할 수 있습니다. 이 역할은 기본적으로 SVM 연결을 생성하거나 편집할 권한이 없습니다. SVM이 연결되지 않으면 사용자는 백업, 클론 복제 또는 복원 작업을 완료할 수 없습니다.

SnapCenter 관리자 역할

SnapCenter 관리자 역할에는 모든 권한이 활성화되어 있습니다. 이 역할에 대한 권한은 수정할 수 없습니다. 사용자 및 그룹을 역할에 추가하거나 제거할 수 있습니다.

앱 백업 및 클론 관리자 역할

App Backup and Clone Admin 역할에는 애플리케이션 백업 및 클론 관련 작업에 대한 관리 작업을 수행하는 데 필요한 권한이 있습니다. 이 역할에는 호스트 관리, 프로비저닝, 스토리지 접속 관리 또는 원격 설치에 대한 권한이 없습니다.

권한	활성화됨	생성	읽기	업데이트	삭제
리소스 그룹	해당 없음	예	예	예	예
정책	해당 없음	예	예	예	예
백업	해당 없음	예	예	예	예
호스트	해당 없음	예	예	예	예

권한	활성화됨	생성	읽기	업데이트	삭제
스토리지 연결	해당 없음	아니요	예	아니요	아니요
복제	해당 없음	예	예	예	예
프로비저닝	해당 없음	아니요	예	아니요	아니요
대시보드	예	해당 없음	해당 없음	해당 없음	해당 없음
보고서	예	해당 없음	해당 없음	해당 없음	해당 없음
복원	예	해당 없음	해당 없음	해당 없음	해당 없음
리소스	예	예	예	예	예
플러그인 설치 /제거	아니요	해당 없음		해당 없음	해당 없음
마이그레이션	아니요	해당 없음	해당 없음	해당 없음	해당 없음
마운트	예	예	해당 없음	해당 없음	해당 없음
마운트 해제하다	예	예	해당 없음	해당 없음	해당 없음
전체 볼륨 복원	아니요	아니요	해당 없음	해당 없음	해당 없음
작업 모니터	예	해당 없음	해당 없음	해당 없음	해당 없음

백업 및 클론 뷰어 역할

백업 및 클론 뷰어 역할에는 모든 권한에 대한 읽기 전용 보기가 있습니다. 또한 이 역할에는 대시보드 검색, 보고 및 액세스에 대한 사용 권한이 설정되어 있습니다.

권한	활성화됨	생성	읽기	업데이트	삭제
리소스 그룹	해당 없음	아니요	예	아니요	아니요
정책	해당 없음	아니요	예	아니요	아니요
백업	해당 없음	아니요	예	아니요	아니요
호스트	해당 없음	아니요	예	아니요	아니요

권한	활성화됨	생성	읽기	업데이트	삭제
스토리지 연결	해당 없음	아니요	예	아니요	아니요
복제	해당 없음	아니요	예	아니요	아니요
프로비저닝	해당 없음	아니요	예	아니요	아니요
대시보드	예	해당 없음	해당 없음	해당 없음	해당 없음
보고서	예	해당 없음	해당 없음	해당 없음	해당 없음
복원	아니요	아니요	해당 없음	해당 없음	해당 없음
리소스	아니요	아니요	예	예	아니요
플러그인 설치 /제거	아니요	해당 없음	해당 없음	해당 없음	해당 없음
마이그레이션	아니요	해당 없음	해당 없음	해당 없음	해당 없음
마운트	예	해당 없음	해당 없음	해당 없음	해당 없음
마운트 해제하다	예	해당 없음	해당 없음	해당 없음	해당 없음
전체 볼륨 복원	아니요	해당 없음	해당 없음	해당 없음	해당 없음
작업 모니터	예	해당 없음	해당 없음	해당 없음	해당 없음

인프라 관리자 역할

인프라 관리자 역할에는 호스트 관리, 스토리지 관리, 프로비저닝, 리소스 그룹, 원격 설치 보고서, 대시보드에 액세스합니다.

권한	활성화됨	생성	읽기	업데이트	삭제
리소스 그룹	해당 없음	예	예	예	예
정책	해당 없음	아니요	예	예	예
백업	해당 없음	예	예	예	예
호스트	해당 없음	예	예	예	예

권한	활성화됨	생성	읽기	업데이트	삭제
스토리지 연결	해당 없음	예	예	예	예
복제	해당 없음	아니요	예	아니요	아니요
프로비저닝	해당 없음	예	예	예	예
대시보드	예	해당 없음	해당 없음	해당 없음	해당 없음
보고서	예	해당 없음	해당 없음	해당 없음	해당 없음
복원	예	해당 없음	해당 없음	해당 없음	해당 없음
리소스	예	예	예	예	예
플러그인 설치 /제거	예	해당 없음	해당 없음	해당 없음	해당 없음
마이그레이션	아니요	해당 없음	해당 없음	해당 없음	해당 없음
마운트	아니요	해당 없음	해당 없음	해당 없음	해당 없음
마운트 해제하다	아니요	해당 없음	해당 없음	해당 없음	해당 없음
전체 볼륨 복원	아니요	아니요	해당 없음	해당 없음	해당 없음
작업 모니터	예	해당 없음	해당 없음	해당 없음	해당 없음

저작권 정보

Copyright © 2024 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.