



RBAC 보안 ONTAP automation

NetApp
January 12, 2026

목차

RBAC 보안	1
ONTAP REST API를 사용한 RBAC 보안 개요	1
ONTAP 역할	1
역할 매핑 및 ONTAP 처리	2
RBAC 발전 요약	2
ONTAP REST API에서 역할 및 사용자와 함께 작업합니다	2
관리 액세스	2
역할 정의	3
권한	4
기본 제공 역할 요약	5
역할 유형 비교	5

RBAC 보안

ONTAP REST API를 사용한 RBAC 보안 개요

ONTAP에는 강력하고 확장 가능한 RBAC(역할 기반 액세스 제어) 기능이 포함되어 있습니다. REST API 및 CLI를 통해 노출된 리소스에 대한 사용자의 액세스를 제어하는 역할을 각 계정에 다르게 할당할 수 있습니다. 이 역할은 다양한 ONTAP 사용자에게 대해 서로 다른 수준의 관리 액세스를 정의합니다.



ONTAP RBAC 기능은 계속 확장되고 ONTAP 9.11.1(및 후속 릴리스)로 크게 향상되었습니다. ["RBAC 발전 요약"](#) 자세한 내용은 및 ["ONTAP REST API의 새로운 기능"](#) 를 참조하십시오.

ONTAP 역할

역할은 사용자가 수행할 수 있는 작업을 집합적으로 정의하는 권한 집합입니다. 각 권한은 특정 액세스 경로 및 관련 액세스 수준을 식별합니다. 역할은 사용자 계정에 할당되며 액세스 제어 결정을 내릴 때 ONTAP에 의해 적용됩니다.

역할 유형

역할에는 두 가지 유형이 있습니다. ONTAP이 발전함에 따라 다양한 환경에 맞게 조정되고 도입되었습니다.



각 유형의 역할을 사용할 때 장단점이 있습니다. 을 참조하십시오 ["역할 유형 비교"](#) 를 참조하십시오.

유형	설명
휴식	나머지 역할은 ONTAP 9.6으로 도입되었으며, REST API를 통해 ONTAP에 액세스하는 사용자에게 일반적으로 적용된다. REST 역할을 생성하면 기존의 _mapping_role이 자동으로 생성됩니다.
기존	이는 ONTAP 9.6 이전에 포함된 레거시 역할입니다. ONTAP CLI 환경에 도입되었으며 RBAC 보안의 기본 요소로 계속 사용됩니다.

범위

모든 역할에는 해당 역할이 정의 및 적용되는 범위 또는 컨텍스트가 있습니다. 범위는 특정 역할이 사용되는 위치와 방법을 결정합니다.



ONTAP 사용자 계정에도 사용자 정의 및 사용 방법을 결정하는 유사한 범위가 있습니다.

범위	설명
클러스터	클러스터 범위가 있는 역할은 ONTAP 클러스터 레벨에 정의되어 있습니다. 클러스터 레벨 사용자 계정과 연결되어 있습니다.
SVM	SVM 범위를 갖는 역할은 특정 데이터 SVM에 대해 정의됩니다. 동일한 SVM의 사용자 계정에 할당됩니다.

역할 정의의 소스

ONTAP 역할은 두 가지 방법으로 정의할 수 있습니다.

역할 소스	설명
맞춤형	ONTAP 관리자는 사용자 지정 역할을 만들 수 있습니다. 이러한 역할은 특정 환경 및 보안 요구 사항에 맞게 조정할 수 있습니다.
내장	맞춤형 역할을 통해 더 많은 유연성을 제공할 뿐만 아니라, 클러스터 및 SVM 레벨에서 모두 사용할 수 있는 기본 제공 역할 세트가 있습니다. 이러한 역할은 미리 정의되어 있으며 일반적인 관리 작업에 사용할 수 있습니다.

역할 매핑 및 ONTAP 처리

사용 중인 ONTAP 릴리즈에 따라 전체 또는 거의 모든 REST API 호출이 하나 이상의 CLI 명령에 매핑됩니다. REST 역할을 만들면 기존 또는 레거시 역할도 만들어집니다. 이 * Mapped * 기존 역할은 해당 CLI 명령을 기반으로 하며 조작하거나 변경할 수 없습니다.



역 역할 매핑은 지원되지 않습니다. 즉, 기존 역할을 생성해도 해당 REST 역할은 발생하지 않습니다.

RBAC 발전 요약

기존 역할은 모든 ONTAP 9 릴리즈에 포함됩니다. 나머지 역할은 나중에 소개되었으며 아래 설명과 같이 발전했습니다.

ONTAP 9.6

REST API는 ONTAP 9.6과 함께 도입되었습니다. 나머지 역할도 이 릴리즈에 포함되어 있습니다. 또한 REST 역할을 생성하면 이에 상응하는 기존 역할도 생성됩니다.

ONTAP 9.7 ~ 9.10.1

9.7에서 9.10.1까지의 각 ONTAP 릴리즈에는 REST API의 향상된 기능이 포함되어 있습니다. 예를 들어, 각 릴리즈마다 다른 REST 엔드포인트가 추가되었습니다. 그러나 두 역할 유형의 생성 및 관리는 별개였습니다. 또한 ONTAP 9.10.1은 리소스 검증된 엔드포인트인 스냅샷 REST 엔드포인트 `"/api/storage/volumes/{vol.uuid}/snapshots"`에 대한 REST RBAC 지원을 추가했습니다.

ONTAP 9.11.1

이 릴리즈에서는 REST API를 사용하여 기존 역할을 구성 및 관리할 수 있는 기능이 추가되었습니다. REST 역할에 대한 추가 액세스 레벨도 추가되었습니다.

ONTAP REST API에서 역할 및 사용자와 함께 작업합니다

기본적인 RBAC 기능을 이해한 후에는 ONTAP 역할 및 사용자 작업을 시작할 수 있습니다.



을 참조하십시오 ["RBAC 워크플로"](#) ONTAP REST API를 사용하여 역할을 생성하고 사용하는 방법의 예를 참조하십시오.

관리 액세스

REST API 또는 명령줄 인터페이스를 통해 ONTAP 역할을 생성하고 관리할 수 있습니다. 액세스 세부 정보는 아래에 설명되어 있습니다.

REST API

RBAC 역할 및 사용자 계정으로 작업할 때 사용할 수 있는 여러 엔드포인트가 있습니다. 표의 처음 4개는 역할을 만들고 관리하는 데 사용됩니다. 마지막 두 가지는 사용자 계정을 만들고 관리하는 데 사용됩니다.



온라인으로 ONTAP에 액세스할 수 있습니다 ["API 참조입니다"](#) API 사용 방법의 예를 포함한 자세한 내용은 설명서를 참조하십시오.

엔드포인트	설명
<code>/security/roles'</code>	이 끝점을 사용하면 새 REST 역할을 만들 수 있습니다. ONTAP 9.11.1부터 기존 역할을 만들 수도 있습니다. 이 경우 ONTAP는 입력 매개 변수를 기반으로 역할 유형을 결정합니다. 정의된 역할 목록을 검색할 수도 있습니다.
<code>/security/roles/{owner.UUID}/{name}'</code>	특정 클러스터 또는 SVM 범위 역할을 검색하거나 삭제할 수 있습니다. UUID 값은 역할이 정의된 SVM(클러스터 또는 데이터 SVM)을 식별합니다. 이름 값은 역할의 이름입니다.
<code>/security/roles/{owner.UUID}/{name}/Privileges'</code>	이 끝점을 사용하면 특정 역할에 대한 권한을 구성할 수 있습니다. 기본 제공 역할은 검색할 수 있지만 업데이트할 수는 없습니다. 자세한 내용은 ONTAP 릴리스의 API 참조 설명서를 참조하십시오.
<code>/security/roles/{owner.UUID}/{name}/Privileges/[path]'</code>	특정 권한에 대한 액세스 수준 및 선택적 쿼리 값을 검색, 수정 및 삭제할 수 있습니다. 자세한 내용은 ONTAP 릴리스의 API 참조 설명서를 참조하십시오.
<code>/security/accounts'</code>	이 엔드포인트를 사용하면 새 클러스터 또는 SVM 범위 사용자 계정을 생성할 수 있습니다. 계정이 작동하기 전에 몇 가지 유형의 정보를 포함시키거나 추가해야 합니다. 정의된 사용자 계정 목록을 검색할 수도 있습니다.
<code>/security/accounts/{owner.UUID}/{name}'</code>	특정 클러스터 또는 SVM 범위 사용자 계정을 검색, 수정, 삭제할 수 있습니다. UUID 값은 사용자가 정의된 SVM(클러스터 또는 데이터 SVM)을 식별합니다. 이름 값은 계정의 이름입니다.

명령줄 인터페이스입니다

관련 ONTAP CLI 명령어는 다음과 같다. 모든 명령은 클러스터 수준에서 관리자 계정을 통해 액세스합니다.

명령	설명
보안 로그인	사용자 로그인을 만들고 관리하는 데 필요한 명령이 들어 있는 디렉토리입니다.
보안 로그인 REST 역할	사용자 로그인과 관련된 REST 역할을 생성하고 관리하는 데 필요한 명령이 들어 있는 디렉토리입니다.
'보안 로그인 역할	이 디렉터리는 사용자 로그인과 관련된 기존 역할을 만들고 관리하는 데 필요한 명령이 들어 있는 디렉토리입니다.

역할 정의

나머지 역할과 기존 역할은 일련의 특성을 통해 정의됩니다.

소유자 및 범위

역할은 ONTAP 클러스터 또는 클러스터 내의 특정 데이터 SVM에서 소유할 수 있습니다. 또한 소유자는 역할의 범위를 암시적으로 결정합니다.

고유한 이름입니다

모든 역할은 범위 내에서 고유한 이름을 가져야 합니다. 클러스터 역할의 이름은 ONTAP 클러스터 수준에서 고유해야 하며 SVM 역할은 특정 SVM 내에서 고유해야 합니다.



새로운 REST 역할의 이름은 기존 역할과 REST 역할 사이에서 고유해야 합니다. REST 역할을 생성하면 이름이 같은 새로운 기존 `_mapping_role`도 생성되기 때문입니다.

권한 집합

모든 역할에는 하나 이상의 권한이 포함됩니다. 각 권한은 특정 리소스 또는 명령과 연결된 액세스 레벨을 식별합니다.

권한

역할에는 하나 이상의 권한이 포함될 수 있습니다. 각 권한 정의는 튜플이며 특정 리소스 또는 작업에 대한 액세스 수준을 설정합니다.

리소스 경로입니다

리소스 경로는 REST 엔드포인트 또는 CLI 명령/명령 디렉토리 경로로 식별됩니다.

REST 엔드포인트

API 끝점이 REST 역할의 대상 리소스를 식별했습니다.

CLI 명령

CLI 명령은 기존 역할의 타겟을 식별합니다. 명령 디렉토리를 지정할 수도 있습니다. 그러면 ONTAP CLI 계층에 모든 다운스트림 명령이 포함됩니다.

액세스 수준

액세스 수준은 특정 리소스 경로 또는 명령에 대한 역할의 액세스 유형을 정의합니다. 액세스 수준은 사전 정의된 키워드 집합을 통해 식별됩니다. 세 가지 액세스 수준이 ONTAP 9.6에 도입되었습니다. 기존 역할과 REST 역할 모두에 사용할 수 있습니다. 또한 ONTAP 9.11.1을 사용하여 세 가지 새로운 액세스 수준이 추가되었습니다. 이러한 새로운 액세스 수준은 REST 역할에만 사용할 수 있습니다.



액세스 수준은 CRUD 모델을 따릅니다. REST에서는 기본 HTTP 메서드(POST, GET, 패치, 삭제)를 기반으로 합니다. 해당 CLI 작업은 일반적으로 REST 작업(생성, 표시, 수정, 삭제)에 매핑됩니다.

액세스 수준	Rest 프리미티브	추가되었습니다	REST 역할만 해당
없음	해당 없음	9.6	아니요
읽기 전용	가져오기	9.6	아니요
모두	다운로드, POST, 패치, 삭제	9.6	아니요
read_create 를 참조하십시오	POST를 완료합니다	9.11.1	예
read_modify 를 참조하십시오	패치	9.11.1	예

액세스 수준	Rest 프리미티브	추가되었습니다	REST 역할만 해당
READ_CREATE_MODIFY를 참조하십시오	GET, POST, 패치	9.11.1	예

선택적 쿼리입니다

기존 역할을 만들 때 * query * 값을 선택적으로 포함하여 명령 또는 명령 디렉터리에 적용할 수 있는 개체의 하위 집합을 식별할 수 있습니다.

기본 제공 역할 요약

ONTAP에는 클러스터 또는 SVM 레벨에서 사용할 수 있는 사전 정의된 여러 역할이 포함되어 있습니다.

클러스터 범위 역할

클러스터 범위에는 몇 가지 기본 제공 역할이 있습니다.

을 참조하십시오 ["클러스터 관리자를 위한 사전 정의된 역할"](#) 를 참조하십시오.

역할	설명
관리자	이 역할을 가진 관리자는 제한되지 않은 권한을 가지고 있으며 ONTAP 시스템에서 모든 작업을 수행할 수 있습니다. 모든 클러스터 레벨 및 SVM 레벨 리소스를 구성할 수 있습니다.
AutoSupport	이는 AutoSupport 계정에 맞게 조정된 특수 역할입니다.
백업	시스템을 백업해야 하는 백업 소프트웨어에 대한 특수 역할입니다.
SnapLock	이는 SnapLock 계정에 맞게 조정된 특수 역할입니다.
읽기 전용	이 역할을 가진 관리자는 클러스터 수준에서 모든 항목을 볼 수 있지만 변경할 수는 없습니다.
없음	관리 기능은 제공되지 않습니다.

SVM 범위 역할

SVM 범위에는 여러 가지 기본 제공 역할이 있습니다. vsadmin * 은 가장 일반적이고 강력한 기능에 대한 액세스를 제공합니다. 다음과 같은 특정 관리 작업에 맞게 조정된 추가 역할이 몇 가지 있습니다.

- vsadmin - 볼륨
- vsadmin - 프로토콜
- vsadmin - 백업
- vsadmin - SnapLock
- vsadmin - 읽기 전용입니다

을 참조하십시오 ["SVM 관리자를 위한 사전 정의된 역할"](#) 를 참조하십시오.

역할 유형 비교

REST * 역할 또는 * 기존 * 역할을 선택하기 전에 차이점을 알고 있어야 합니다. 두 역할 유형을 비교할 수 있는 몇 가지

방법은 아래에 설명되어 있습니다.



고급 또는 복잡한 RBAC 사용 사례의 경우 일반적으로 기존 역할을 사용해야 합니다.

사용자가 **ONTAP**에 액세스하는 방법

역할을 생성하기 전에 사용자가 ONTAP 시스템에 액세스하는 방법을 알아야 합니다. 이를 바탕으로 역할 유형을 결정할 수 있습니다.

액세스	추천 유형입니다
REST API만 해당	REST 역할은 REST API와 함께 사용하도록 설계되었습니다.
REST API 및 CLI	REST 역할을 정의하여 이에 상응하는 기존 역할을 생성할 수도 있습니다.
CLI만 해당됩니다	기존 역할을 생성할 수 있습니다.

액세스 경로의 정밀도

REST 역할에 대해 정의된 액세스 경로는 REST 엔드포인트를 기반으로 합니다. 기존 역할의 액세스 경로는 CLI 명령 또는 명령 디렉토리를 기반으로 합니다. 또한 선택적 쿼리 매개 변수를 기존 역할과 함께 포함하여 명령 매개 변수 값에 따라 액세스를 추가로 제한할 수 있습니다.

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.