



RBAC

ONTAP Automation

NetApp
July 11, 2024

목차

RBAC	1
RBAC를 사용하도록 준비합니다.....	1
역할을 생성합니다	1
역할이 있는 사용자를 생성합니다	5

RBAC

RBAC를 사용하도록 준비합니다

ONTAP RBAC 기능은 환경에 따라 여러 가지 방법으로 사용할 수 있습니다. 이 섹션에서는 몇 가지 일반적인 시나리오를 워크플로로 설명합니다. 각각의 경우 특정 보안 및 관리 목표에 중점을 둡니다.

역할을 생성하고 ONTAP 사용자 계정에 역할을 할당하기 전에 아래에 제시된 주요 보안 요구 사항 및 옵션을 검토하여 준비해야 합니다. 또한 [이 문서](#)에서 일반적인 워크플로 개념을 검토해야 합니다 "[워크플로우 사용을 준비하십시오](#)".

어떤 **ONTAP** 릴리스를 사용하고 있습니까?

ONTAP 릴리스는 사용 가능한 REST 엔드포인트 및 RBAC 기능을 결정합니다.

보호된 리소스 및 범위를 식별합니다

보호할 리소스 또는 명령과 범위(클러스터 또는 SVM)를 식별해야 합니다.

사용자는 어떤 액세스 권한을 가져야 합니까?

리소스 및 범위를 파악한 후에는 부여할 액세스 수준을 결정해야 합니다.

사용자는 **ONTAP**에 어떻게 액세스합니까?

사용자는 REST API 또는 CLI 또는 둘 다를 통해 ONTAP에 액세스할 수 있습니다.

기본 제공 역할 중 하나가 충분합니까, 아니면 사용자 지정 역할이 필요합니까?

기존 기본 제공 역할을 사용하는 것이 더 편리하지만 필요한 경우 새 사용자 지정 역할을 만들 수 있습니다.

어떤 유형의 역할이 필요합니까?

보안 요구 사항 및 ONTAP 액세스를 기반으로 REST 또는 기존 역할을 생성할지 여부를 선택해야 합니다.

역할을 생성합니다

SVM 볼륨 작업으로 액세스 제한

SVM 내에서 스토리지 볼륨 관리를 제한하는 역할을 정의할 수 있습니다.

이 워크플로 정보

먼저 복제를 제외한 모든 주요 볼륨 관리 기능에 액세스할 수 있도록 기존 역할이 생성됩니다. 역할은 다음과 같은 특성으로 정의됩니다.

- 가져오기, 생성, 수정 및 삭제를 포함한 모든 CRUD 볼륨 작업을 수행할 수 있습니다
- 볼륨 클론을 생성할 수 없습니다

그런 다음 필요에 따라 역할을 업데이트할 수 있습니다. 이 워크플로우에서는 두 번째 단계에서 사용자가 볼륨 클론을 생성할 수 있도록 역할이 변경됩니다.

1단계: 역할을 만듭니다

API 호출을 실행하여 RBAC 역할을 생성할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/API/보안/역할

컬의 예

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON 입력 예

```
{  
  "name": "role1",  
  "owner": {  
    "name": "cluster-1",  
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"  
  },  
  "privileges": [  
    { "path": "volume create", "access": "all" },  
    { "path": "volume delete", "access": "all" }  
  ]  
}
```

2단계: 역할을 업데이트합니다

API 호출을 실행하여 기존 역할을 업데이트할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/API/보안/역할

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
\$SVM_ID입니다	경로	예	역할 정의가 포함된 SVM의 UUID입니다.
\$ROLE_NAME입니다	경로	예	업데이트할 SVM 내에서 역할의 이름입니다.

컬의 예

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/priveleges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON 입력 예

```
{
  "path": "volume clone",
  "access": "all"
}
```

데이터 보호 관리 활성화

사용자에게 제한된 데이터 보호 기능을 제공할 수 있습니다.

이 워크플로 정보

생성된 전통적인 역할은 다음과 같은 특성을 가지고 정의됩니다.

- SnapMirror 관계를 업데이트할 뿐만 아니라 스냅샷을 생성 및 삭제할 수 있습니다
- 볼륨 또는 SVM과 같은 상위 레벨의 객체를 생성하거나 수정할 수 없습니다

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/API/보안/역할

컬의 예

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON 입력 예

```
{  
  "name": "role1",  
  "owner": {  
    "name": "cluster-1",  
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"  
  },  
  "privileges": [  
    {"path": "volume snapshot create", "access": "all"},  
    {"path": "volume snapshot delete", "access": "all"},  
    {"path": "volume show", "access": "readonly"},  
    {"path": "vserver show", "access": "readonly"},  
    {"path": "snapmirror show", "access": "readonly"},  
    {"path": "snapmirror update", "access": "all"}  
  ]  
}
```

ONTAP 보고서 생성을 허용합니다

REST 역할을 생성하여 사용자에게 ONTAP 보고서를 생성할 수 있는 기능을 제공할 수 있습니다.

이 워크플로 정보

생성된 역할은 다음과 같은 특성으로 정의됩니다.

- 용량 및 성능(예: 볼륨, qtree, LUN, 애그리게이트, 노드, SnapMirror 관계 포함)
- 더 높은 수준의 오브젝트(예: 볼륨 또는 SVM)를 생성하거나 수정할 수 없음

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/API/보안/역할

컬의 예

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON 입력 예

```
{  
  "name": "rest_role1",  
  "owner": {  
    "name": "cluster-1",  
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"  
  },  
  "privileges": [  
    {"path": "/api/storage/volumes", "access": "readonly"},  
    {"path": "/api/storage/qtrees", "access": "readonly"},  
    {"path": "/api/storage/luns", "access": "readonly"},  
    {"path": "/api/storage/aggregates", "access": "readonly"},  
    {"path": "/api/cluster/nodes", "access": "readonly"},  
    {"path": "/api/snapmirror/relationships", "access": "readonly"},  
    {"path": "/api/svm/svms", "access": "readonly"}  
  ]  
}
```

역할이 있는 사용자를 생성합니다

이 워크플로를 사용하여 연결된 REST 역할을 가진 사용자를 만들 수 있습니다.

이 워크플로 정보

이 워크플로에는 사용자 지정 REST 역할을 만들고 새 사용자 계정과 연결하는 데 필요한 일반적인 단계가 포함되어 있습니다. 사용자와 역할 모두 SVM 범위를 가지고 있으며 특정 데이터 SVM과 연관됩니다. 일부 단계는 선택 사항이거나 환경에 따라 변경해야 할 수 있습니다.

1단계: 클러스터의 데이터 SVM을 나열합니다

다음 REST API 호출을 수행하여 클러스터에 SVM을 표시합니다. 각 SVM의 UUID 및 이름은 출력에 제공됩니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메서드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/svm/sSVM

컬의 예

```
curl --request GET \
--location "https://$FQDN_IP/api/svm/svms?order_by=name" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

작업을 마친 후

새 사용자 및 역할을 생성할 목록에서 원하는 SVM을 선택합니다.

2단계: SVM에 정의된 사용자를 나열합니다

다음 REST API 호출을 수행하여 선택한 SVM에 정의된 사용자를 나열할 수 있습니다. 소유자 매개 변수를 통해 SVM을 식별할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/security/accounts

컬의 예

```
curl --request GET \
--location "https://$FQDN_IP/api/security/accounts?owner.name=dmp" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

작업을 마친 후

SVM에 이미 정의된 사용자를 기준으로 새 사용자의 이름을 선택합니다.

3단계: SVM에 정의된 REST 역할 나열

선택한 SVM에 정의된 역할을 나열하려면 다음 REST API 호출을 수행합니다. 소유자 매개 변수를 통해 SVM을 식별할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/API/보안/역할

컬의 예

```
curl --request GET \
--location "https://$FQDN_IP/api/security/roles?owner.name=dmp" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

작업을 마친 후

SVM에 이미 정의된 역할에 따라 새 역할에 맞는 고유한 이름을 선택하십시오.

4단계: 사용자 지정 **REST** 역할을 만듭니다

SVM에서 맞춤형 REST API를 생성하여 다음 REST API 호출을 수행합니다. 이 역할에는 처음에 모든 액세스가 거부되도록 기본 액세스 권한을 *없음*으로 설정하는 하나의 권한만 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/API/보안/역할

컬의 예

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON 입력 예

```
{
  "name": "dprole1",
  "owner": {
    "name": "dmp",
    "uuid": "752d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
    {"path": "/api", "access": "none"},
  ]
}
```

작업을 마친 후

필요에 따라 3단계를 다시 수행하여 새 역할을 표시합니다. ONTAP CLI에서 역할을 표시할 수도 있습니다.

5단계: 권한을 추가하여 역할을 업데이트합니다

필요에 따라 권한을 추가하여 역할을 수정하려면 다음 REST API 호출을 수행합니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/api/security/roles/{owner.uuid}/{name}/권한

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
\$SVM_ID입니다	경로	예	역할 정의가 포함된 SVM의 UUID입니다.
\$ROLE_NAME입니다	경로	예	업데이트할 SVM 내의 역할 이름입니다.

컬의 예

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/privileges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON 입력 예

```
{
  "path": "/api/storage/volumes",
  "access": "readonly"
}
```

작업을 마친 후

필요에 따라 3단계를 다시 수행하여 새 역할을 표시합니다. ONTAP CLI에서 역할을 표시할 수도 있습니다.

6단계: 사용자 생성

사용자 계정 생성을 위해 다음 REST API 호출을 수행합니다. 위에서 생성한 * dprole1 * 역할은 새 사용자와 연결됩니다.



역할 없이 사용자를 만들 수 있습니다. 이 경우 사용자에게 기본 역할(둘 중 하나)이 할당됩니다 admin 또는 vsadmin) 사용자가 클러스터 또는 SVM 범위로 정의되었는지 여부에 따라 결정됩니다. 다른 역할을 할당하도록 사용자를 수정해야 합니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/api/security/accounts

컬의 예

```
curl --request POST \
--location "https://$FQDN_IP/api/security/accounts" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON 입력 예

```
{
  "owner": {"uuid": "daf84055-248f-11ed-a23d-005056ac4fe6"},
  "name": "david",
  "applications": [
    {"application": "ssh",
     "authentication_methods": ["password"],
     "second_authentication_method": "none"}
  ],
  "role": "dprole1",
  "password": "netapp123"
}
```

작업을 마친 후

새 사용자의 자격 증명을 사용하여 SVM 관리 인터페이스에 로그인할 수 있습니다.

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.