# RBAC

## ONTAP Automation

NetApp
July 11, 2024

# 목차

# 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 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.

**1**단계**:** 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" }
    ]
}
```

**2**단계**:** 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 메소드와 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



## 상표 정보