클라이언트 인증
ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/ontap/authentication/oauth2-authorization.html on February 12, 2026. Always check docs.netapp.com for the latest.

목차

클라이언트 인증

ONTAP 클라이언트 인증에 대한 개요 및 옵션

ONTAP OAuth 2.0 구현은 유연하고 강력하도록 설계되어 ONTAP 환경을 보호하는 데 필요한 기능을 제공합니다. 상호 배타적인 구성 옵션은 여러 가지가 있습니다. 권한 부여 결정은 궁극적으로 OAuth 2.0 액세스 토큰에 포함되어 있거나 OAuth 2.0 액세스 토큰에서 파생된 ONTAP REST 역할을 기반으로 합니다.

만 사용할 수 있습니다 "ONTAP REST 역할" OAuth 2.0에 대한 권한 부여를 구성하는 경우. 이전 ONTAP의 기존 역할은 지원되지 않습니다.

ONTAP는 사용자의 구성에 따라 가장 적합한 하나의 인증 옵션을 적용합니다. ONTAP에서 클라이언트 액세스 결정을 내리는 방법에 대한 자세한 내용은 을 "ONTAP에서 액세스를 결정하는 방법"참조하십시오.

OAuth 2.0 독립형 범위

이러한 범위에는 액세스 토큰의 단일 문자열 내에 캡슐화된 하나 이상의 사용자 지정 REST 역할이 포함됩니다. ONTAP 역할 정의와는 독립적입니다. 권한 부여 서버에서 범위 문자열을 구성해야 합니다. 자세한 내용은 을 "자체 포함된 OAuth 2.0 범위" 참조하십시오.

로컬 **ONTAP REST** 역할

builtin 또는 custom 중 하나의 명명된 REST 역할을 사용할 수 있습니다. 명명된 역할의 범위 구문은 * ontap-role - * <URL-encoded-ONTAP-role-name>입니다. 예를 들어, ONTAP 역할이 인 경우 `admin` 범위 문자열은 입니다 `ontap-role-admin`.

사용자

"http" 응용 프로그램에 대한 액세스 권한으로 정의된 액세스 토큰의 사용자 이름을 사용할 수 있습니다. 사용자는 정의된 인증 방법인 암호, 도메인(Active Directory), nsswitch(LDAP)에 따라 다음 순서로 테스트됩니다.

그룹

권한 부여 서버는 인증에 ONTAP 그룹을 사용하도록 구성할 수 있습니다. 로컬 ONTAP 정의를 검사했지만 액세스를 결정할 수 없는 경우 Active Directory("도메인") 또는 LDAP("nsswitch") 그룹이 사용됩니다. 그룹 정보는 다음 두 가지 방법 중 하나로 지정할 수 있습니다.

- OAuth 2.0 범위 문자열

  그룹 멤버십을 가진 사용자가 없는 경우 클라이언트 자격 증명 흐름을 사용하여 기밀 응용 프로그램을 지원합니다. 범위의 이름은 * ontap-group - * <URL-encoded-ONTAP-group-name>여야 합니다. 예를 들어 그룹이 "development"인 경우 범위 문자열은 "ontap-group-development"가 됩니다.

- "그룹" 요구 사항

  리소스 소유자(암호 부여) 흐름을 사용하여 ADFS에서 발급한 액세스 토큰에 사용됩니다.

보다 "ONTAP 에서 OAuth 2.0 또는 SAML IdP 그룹 작업" 자세한 내용은.

ONTAP 의 독립형 OAuth 2.0 범위

자체 포함 범위는 액세스 토큰으로 전달되는 문자열입니다. 각각은 완전한 사용자 지정 역할 정의이며 ONTAP에서 액세스 결정을 내리는 데 필요한 모든 것을 포함합니다. 범위는 ONTAP 자체 내에 정의된 모든 REST 역할과 별개입니다.

범위 문자열의 형식입니다

기본 수준에서 범위는 연속된 문자열로 표시되며 콜론으로 구분된 6개의 값으로 구성됩니다. 범위 문자열에 사용되는 매개 변수는 아래에 설명되어 있습니다.

ONTAP 리터럴

범위는 리터럴 값으로 시작해야 합니다 `ontap` 소문자로 입력합니다. ONTAP에만 해당하는 범위를 식별합니다.

클러스터

범위가 적용되는 ONTAP 클러스터를 정의합니다. 값은 다음과 같습니다.

- 클러스터 UUID

  단일 클러스터를 식별합니다.

- 별표(*)

  범위가 모든 클러스터에 적용됨을 나타냅니다.

ONTAP CLI 명령을 사용하여 클러스터의 UUID를 표시할 수 있습니다 `cluster identity show`. 지정하지 않으면 범위가 모든 클러스터에 적용됩니다. 에 대한 자세한 내용은 `cluster identity show` "ONTAP 명령 참조입니다 "을 참조하십시오.

역할

자체 포함된 범위에 포함된 REST 역할의 이름입니다. 이 값은 ONTAP에서 검사하거나 ONTAP에 정의된 기존 REST 역할과 일치하지 않습니다. 이 이름은 로깅에 사용됩니다.

액세스 수준

이 값은 범위에서 API 끝점을 사용할 때 클라이언트 응용 프로그램에 적용되는 액세스 수준을 나타냅니다. 아래 표에 설명된 대로 6개의 값이 있습니다.

액세스 수준	설명
없음	지정된 끝점에 대한 모든 액세스를 거부합니다.
읽기 전용	GET를 사용하여 읽기 액세스만 허용합니다.
read_create 를 참조하십시오	POST를 사용하여 새 리소스 인스턴스를 만들고 읽기 액세스를 허용합니다.
read_modify 를 참조하십시오	패치를 사용하여 기존 리소스를 업데이트할 수 있을 뿐 아니라 읽기 액세스를 허용합니다.

액세스 수준	설명
READ_CREATE_MODIFY을 참조하십시오	삭제를 제외한 모든 액세스를 허용합니다. 허용되는 작업에는 GET(읽기), POST(작성) 및 패치(업데이트)가 포함됩니다.
모두	전체 액세스를 허용합니다.

SVM

클러스터 내 SVM의 이름이 범위에 적용됩니다. * 값(별표)을 사용하여 모든 SVM을 나타냅니다.

> 이 기능은 ONTAP 9.14.1에서 완벽하게 지원되지 않습니다. SVM 매개 변수를 무시하고 별표를 자리 표시자로 사용할 수 있습니다. 를 검토합니다 "ONTAP 릴리즈 노트" 향후 SVM 지원 확인

REST API URI입니다

리소스 또는 관련 리소스 집합에 대한 전체 또는 부분 경로입니다. 문자열은 로 시작해야 합니다 `/api`. 값을 지정하지 않으면 범위가 ONTAP 클러스터의 모든 API 끝점에 적용됩니다.

범위 예

다음은 자급식 범위의 몇 가지 예입니다.

ONTAP: *:joes-역할**: read_create_modify: *:/api/cluster**

이 역할에 할당된 사용자에게 에 대한 읽기, 생성 및 수정 액세스 권한을 제공합니다 `/cluster` 엔드포인트.

CLI 관리 도구

ONTAP는 자체 포함된 범위를 보다 쉽게 관리할 수 있도록 CLI 명령을 제공합니다 `security oauth2 scope` 입력 매개 변수를 기반으로 범위 문자열을 생성합니다.

명령을 입력합니다 `security oauth2 scope` 은 고객 입력에 따라 두 가지 사용 사례를 가지고 있습니다.

- 문자열 범위를 지정하는 CLI 매개 변수입니다

  이 버전의 명령을 사용하여 입력 매개 변수를 기반으로 범위 문자열을 생성할 수 있습니다.

- 문자열을 CLI 매개 변수로 지정합니다

  이 버전의 명령을 사용하여 입력 범위 문자열을 기반으로 명령 매개 변수를 생성할 수 있습니다.

예

다음 예제에서는 아래 명령 예제 다음에 포함된 출력으로 범위 문자열을 생성합니다. 이 정의는 모든 클러스터에 적용됩니다.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

에 대한 자세한 내용은 `security oauth2 scope` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 의 OAuth 2.0 외부 역할 매핑

외부 역할은 ONTAP에서 사용하도록 구성된 식별 공급자에서 정의됩니다. ONTAP CLI를 사용하여 이러한 외부 역할과 ONTAP 역할 간의 매핑 관계를 만들고 관리할 수 있습니다.

ONTAP REST API를 사용하여 외부 역할 매핑 기능을 구성할 수도 있습니다. 자세한 내용은 을 "ONTAP 자동화 설명서"참조하십시오.

액세스 토큰의 외부 역할

다음은 두 개의 외부 역할이 포함된 JSON 액세스 토큰의 일부입니다.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

구성

ONTAP 명령줄 인터페이스를 사용하여 외부 역할 매핑 기능을 관리할 수 있습니다.

생성

명령을 사용하여 역할 매핑 구성을 정의할 수 `security login external-role-mapping create` 있습니다. 이 명령과 관련 옵션을 실행하려면 ONTAP * admin * 권한 수준이어야 합니다.

매개 변수

그룹 매핑을 생성하는 데 사용되는 매개 변수는 아래에 설명되어 있습니다.

매개 변수	설명
`external-role`	외부 ID 공급자에 정의된 역할의 이름입니다.
`provider`	ID 공급자의 이름입니다. 시스템의 식별자여야 합니다.
`ontap-role`	외부 역할이 매핑되는 기존 ONTAP 역할을 나타냅니다.

예

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

에 대한 자세한 내용은 `security login external-role-mapping create` "ONTAP 명령 참조입니다"을 참조하십시오.

추가 **CLI** 작업

이 명령을 실행하면 다음과 같은 몇 가지 추가 작업이 지원됩니다.

- 표시
- 수정
- 삭제

관련 정보

- "ONTAP 명령 참조입니다"

ONTAP가 클라이언트 액세스를 결정하는 방법

OAuth 2.0을 올바르게 설계하고 구현하려면 ONTAP에서 클라이언트의 액세스 결정을 내리기 위해 인증 구성이 사용되는 방법을 이해해야 합니다. 액세스를 결정하는 데 사용되는 주요 단계는 ONTAP 릴리스에 따라 아래에 나와 있습니다.

ONTAP 9.15.1에서 중요한 OAuth 2.0 업데이트가 없었습니다. 9.15.1 릴리스를 사용하는 경우 ONTAP 9.14.1에 대한 설명을 참조하십시오.

관련 정보

- "OAuth 2.0 기능은 ONTAP에서 지원됩니다"

ONTAP 9.16.1

ONTAP 9.16.1은 표준 OAuth 2.0 지원을 확장하여 기본 Entra ID 그룹에 대한 Microsoft Entra ID별 확장 및 외부 역할 매핑을 포함합니다.

ONTAP 9.16.1에 대한 클라이언트 액세스를 확인합니다

1단계**:** 자체 포함 범위

액세스 토큰에 자체 포함된 범위가 포함되어 있는 경우 ONTAP는 먼저 이러한 범위를 검사합니다. 자체 포함된 범위가 없는 경우 2단계로 이동합니다.

하나 이상의 자체 포함 범위가 있는 경우 ONTAP는 명시적 * allow * 또는 * deny * 결정을 내릴 수 있을 때까지 각 범위를 적용합니다. 명시적인 결정이 내려지면 처리가 종료됩니다.

ONTAP에서 명시적인 액세스 결정을 내릴 수 없는 경우 2단계를 계속 진행합니다.

2단계**:** 로컬 역할 플래그를 확인합니다

ONTAP는 부울 매개 변수를 `use-local-roles-if-present`검사합니다. 이 플래그의 값은 ONTAP로 정의된 각 인증 서버에 대해 별도로 설정됩니다.

- 값이 이면 `true` 3단계를 계속 진행합니다.
- 값이 이면 `false` 처리가 종료되고 액세스가 거부됩니다.

3단계**:** 이름이 지정된 **ONTAP REST** 역할입니다

액세스 토큰에 OR `scp` 필드에 이름이 지정된 REST 역할이 포함되어 있거나 클레임으로 포함되어 있는 경우 `scope` ONTAP는 해당 역할을 사용하여 액세스 결정을 내립니다. 이렇게 하면 항상 * allow * 또는 * deny * 결정이 되고 처리가 종료됩니다.

이름이 지정된 REST 역할이 없거나 역할을 찾을 수 없는 경우 4단계를 계속 진행하십시오.

4단계**:** 사용자

액세스 토큰에서 사용자 이름을 추출하고 "http" 응용 프로그램에 액세스할 수 있는 사용자와 일치시키려고 시도합니다. 사용자는 다음과 같은 순서로 인증 방법에 따라 검사됩니다.

- 암호
- 도메인(Active Directory)
- Nsswitch(LDAP)

일치하는 사용자가 발견되면 ONTAP는 사용자에게 정의된 역할을 사용하여 액세스 결정을 내립니다. 이로 인해 항상 * allow * 또는 * deny * 결정이 내려지고 처리가 종료됩니다.

사용자가 일치하지 않거나 액세스 토큰에 사용자 이름이 없는 경우 5단계를 계속 진행합니다.

5단계**:** 그룹

하나 이상의 그룹이 포함된 경우 형식이 검사됩니다. 그룹이 UUID로 표현된 경우 내부 그룹 매핑 테이블이 검색됩니다. 그룹과 일치하는 역할이 있고 연관된 역할이 있는 경우, ONTAP 해당 그룹에 정의된 역할을 사용하여 액세스 결정을 내립니다. 이는 항상 **ALLOW** 또는 **DENY** 결정으로 이어지고 처리가 종료됩니다. 자세한 내용은 다음을 참조하십시오. "ONTAP 에서 OAuth 2.0 또는 SAML IdP 그룹 작업" .

그룹이 이름으로 표시되고 도메인 또는 nsswitch 인증을 사용하여 구성된 경우 ONTAP는 각 그룹을 Active Directory 또는 LDAP 그룹과 일치시키려고 시도합니다. 그룹 일치 항목이 있는 경우 ONTAP는 그룹에 대해 정의된 역할을 사용하여 액세스 결정을 내립니다. 이로 인해 항상 * allow * 또는 * deny * 결정이 내려지고 처리가 종료됩니다.

일치하는 그룹이 없거나 액세스 토큰에 그룹이 없으면 액세스가 거부되고 처리가 종료됩니다.

ONTAP 9.14.1

지원되는 초기 OAuth 2.0은 표준 OAuth 2.0 기능을 기반으로 하는 ONTAP 9.14.1에 도입되었습니다.

ONTAP 9.14.1에 대한 클라이언트 액세스를 확인합니다

1단계**:** 자체 포함 범위

액세스 토큰에 자체 포함된 범위가 포함되어 있는 경우 ONTAP는 먼저 이러한 범위를 검사합니다. 자체 포함된 범위가 없는 경우 2단계로 이동합니다.

하나 이상의 자체 포함 범위가 있는 경우 ONTAP는 명시적 * allow * 또는 * deny * 결정을 내릴 수 있을 때까지 각 범위를 적용합니다. 명시적인 결정이 내려지면 처리가 종료됩니다.

ONTAP에서 명시적인 액세스 결정을 내릴 수 없는 경우 2단계를 계속 진행합니다.

2단계**:** 로컬 역할 플래그를 확인합니다

ONTAP는 부울 매개 변수를 `use-local-roles-if-present`검사합니다. 이 플래그의 값은 ONTAP로 정의된 각 인증 서버에 대해 별도로 설정됩니다.

- 값이 이면 `true` 3단계를 계속 진행합니다.
- 값이 이면 `false` 처리가 종료되고 액세스가 거부됩니다.

3단계**:** 이름이 지정된 **ONTAP REST** 역할입니다

액세스 토큰에 OR `scp` 필드에 이름이 지정된 REST 역할이 포함된 경우 `scope` ONTAP는 해당 역할을 사용하여 액세스 결정을 내립니다. 이렇게 하면 항상 * allow * 또는 * deny * 결정이 되고 처리가 종료됩니다.

이름이 지정된 REST 역할이 없거나 역할을 찾을 수 없는 경우 4단계를 계속 진행하십시오.

4단계**:** 사용자

액세스 토큰에서 사용자 이름을 추출하고 "http" 응용 프로그램에 액세스할 수 있는 사용자와 일치시키려고 시도합니다. 사용자는 다음과 같은 순서로 인증 방법에 따라 검사됩니다.

- 암호
- 도메인(Active Directory)
- Nsswitch(LDAP)

일치하는 사용자가 발견되면 ONTAP는 사용자에게 정의된 역할을 사용하여 액세스 결정을 내립니다. 이로 인해 항상 * allow * 또는 * deny * 결정이 내려지고 처리가 종료됩니다.

사용자가 일치하지 않거나 액세스 토큰에 사용자 이름이 없는 경우 5단계를 계속 진행합니다.

5단계**:** 그룹

하나 이상의 그룹이 도메인 또는 nsswitch 인증을 사용하여 포함되어 구성된 경우 ONTAP는 이러한 그룹을 각각 Active Directory 또는 LDAP 그룹과 일치시키려고 시도합니다.

그룹 일치 항목이 있는 경우 ONTAP는 그룹에 대해 정의된 역할을 사용하여 액세스 결정을 내립니다. 이로 인해 항상 * allow * 또는 * deny * 결정이 내려지고 처리가 종료됩니다.

일치하는 그룹이 없거나 액세스 토큰에 그룹이 없으면 액세스가 거부되고 처리가 종료됩니다.

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.