구성 및 배포

ONTAP 9

NetApp
April 24, 2024

목차

구성 및 배포

ONTAP와 함께 OAuth 2.0을 배포할 준비를 하십시오

ONTAP 환경에서 OAuth 2.0을 구성하기 전에 배포를 준비해야 합니다. 주요 작업과 결정에 대한 요약이 아래에 나와 있습니다. 섹션의 정렬은 일반적으로 따라야 할 순서에 맞춰집니다. 그러나 대부분의 배포에는 적용되지만 필요에 따라 환경에 맞게 조정해야 합니다. 공식 배포 계획을 작성하는 것도 고려해야 합니다.

> 사용자 환경에 따라 ONTAP에 정의된 인증 서버에 대한 구성을 선택할 수 있습니다. 여기에는 각 배포 유형에 대해 구체화해야 하는 매개 변수 값이 포함됩니다. 을 참조하십시오 "OAuth 2.0 배포 시나리오" 를 참조하십시오.

보호된 리소스 및 클라이언트 응용 프로그램

OAuth 2.0은 보호된 리소스에 대한 액세스를 제어하기 위한 권한 부여 프레임워크입니다. 이 점을 감안하면 모든 배포에서 중요한 첫 단계는 사용 가능한 리소스가 무엇이고 어떤 클라이언트가 액세스할 필요가 있는지 확인하는 것입니다.

클라이언트 애플리케이션을 식별합니다

REST API 호출을 실행할 때 OAuth 2.0을 사용할 클라이언트와 이들이 액세스해야 하는 API 엔드포인트를 결정해야 합니다.

기존 **ONTAP REST** 역할 및 로컬 사용자를 검토합니다

REST 역할 및 로컬 사용자를 포함하여 기존 ONTAP ID 정의를 검토해야 합니다. OAuth 2.0을 구성하는 방법에 따라 이러한 정의를 액세스 결정에 사용할 수 있습니다.

OAuth 2.0으로의 글로벌 전환

OAuth 2.0 인증을 점진적으로 구현할 수도 있지만 각 인증 서버에 대한 글로벌 플래그를 설정하여 모든 REST API 클라이언트를 OAuth 2.0으로 즉시 이동할 수도 있습니다. 따라서 자체 포함된 범위를 만들 필요 없이 기존 ONTAP 구성을 기반으로 액세스 결정을 내릴 수 있습니다.

인증 서버

권한 부여 서버는 액세스 토큰을 발행하고 관리 정책을 시행함으로써 OAuth 2.0 배포에서 중요한 역할을 수행합니다.

인증 서버를 선택하여 설치합니다

하나 이상의 인증 서버를 선택하여 설치해야 합니다. 범위를 정의하는 방법을 비롯하여 ID 공급자의 구성 옵션 및 절차를 숙지하는 것이 중요합니다.

인증 루트 **CA** 인증서를 설치해야 하는지 확인합니다

ONTAP는 인증 서버의 인증서를 사용하여 클라이언트가 제공하는 서명된 액세스 토큰의 유효성을 검사합니다. 이렇게 하려면 ONTAP에서 루트 CA 인증서와 모든 중간 인증서가 필요합니다. ONTAP와 함께 사전 설치되어 있을 수 있습니다. 그렇지 않은 경우 설치해야 합니다.

네트워크 위치 및 구성을 평가합니다

인증 서버가 방화벽 뒤에 있는 경우 프록시 서버를 사용하도록 ONTAP를 구성해야 합니다.

클라이언트 인증 및 권한 부여

클라이언트 인증 및 권한 부여에는 몇 가지 측면을 고려해야 합니다.

자체 포함된 범위 또는 로컬 **ONTAP ID** 정의

상위 수준에서는 권한 부여 서버에서 정의된 자체 포함 범위를 정의하거나 역할 및 사용자를 비롯한 기존 로컬 ONTAP ID 정의를 사용할 수 있습니다.

로컬 **ONTAP** 처리 옵션

ONTAP ID 정의를 사용하는 경우 다음을 포함하여 적용할 항목을 결정해야 합니다.

- 이름이 지정된 REST 역할입니다
- 로컬 사용자와 일치합니다
- Active Directory 또는 LDAP 그룹

로컬 검증 또는 원격 검사

액세스 토큰의 유효성을 ONTAP에서 로컬로 검사할지, 아니면 자체 검사를 통해 인증 서버에서 검사할지 결정해야 합니다. 또한 새로 고침 간격과 같이 고려해야 할 여러 관련 값도 있습니다.

보낸 사람 제한 액세스 토큰

높은 수준의 보안이 필요한 환경에서는 MTL을 기반으로 보내기 제한 액세스 토큰을 사용할 수 있습니다. 이렇게 하려면 각 클라이언트에 대한 인증서가 필요합니다.

관리 인터페이스

다음을 비롯한 모든 ONTAP 인터페이스를 통해 OAuth 2.0을 관리할 수 있습니다.

- 명령줄 인터페이스입니다
- 시스템 관리자
- REST API

클라이언트가 액세스 토큰을 요청하는 방법

클라이언트 응용 프로그램은 권한 부여 서버에서 직접 액세스 토큰을 요청해야 합니다. 허가 유형을 포함하여 이 작업을 수행하는 방법을 결정해야 합니다.

ONTAP를 구성합니다

몇 가지 ONTAP 구성 작업을 수행해야 합니다.

REST 역할 및 로컬 사용자를 정의합니다

인증 구성에 따라 로컬 ONTAP 식별 처리를 사용할 수 있습니다. 이 경우 REST 역할 및 사용자 정의를 검토하고 정의해야 합니다.

코어 구성

핵심 ONTAP 구성을 수행하는 데 필요한 주요 단계는 다음과 같습니다.

- 선택적으로 인증 서버의 인증서를 서명한 CA에 대한 루트 인증서(및 모든 중간 인증서)를 설치합니다.
- 인증 서버를 정의합니다.

- 클러스터에 대해 OAuth 2.0 처리를 활성화합니다.

ONTAP에 OAuth 2.0 배포

핵심 OAuth 2.0 기능을 배포하려면 세 가지 기본 단계가 필요합니다.

시작하기 전에

ONTAP를 구성하기 전에 OAuth 2.0 배포를 준비해야 합니다. 예를 들어 인증서의 서명 방법 및 방화벽 뒤에 있는지 등 인증 서버를 평가해야 합니다. 을 참조하십시오 "ONTAP와 함께 OAuth 2.0을 배포할 준비를 하십시오" 를 참조하십시오.

1단계: 인증 서버 인증서를 설치합니다

ONTAP에는 미리 설치된 루트 CA 인증서가 다수 포함되어 있습니다. 따라서 대부분의 경우 추가 구성 없이 ONTAP에서 인증 서버의 인증서를 즉시 인식합니다. 그러나 인증 서버 인증서 서명 방법에 따라 루트 CA 인증서와 중간 인증서를 설치해야 할 수도 있습니다.

필요한 경우 아래 제공된 지침에 따라 인증서를 설치합니다. 필요한 모든 인증서를 클러스터 수준에서 설치해야 합니다.

ONTAP 액세스 방법에 따라 올바른 절차를 선택합니다.

예 **1.** 단계

시스템 관리자

1. System Manager에서 * 클러스터 * > * 설정 * 을 선택합니다.
2. 아래로 스크롤하여 * 보안 * 섹션으로 이동합니다.
3. Certificates * 옆에 있는 * → * 를 클릭합니다.
4. 신뢰할 수 있는 인증 기관 * 탭에서 * 추가 * 를 클릭합니다.
5. 가져오기 * 를 클릭하고 인증서 파일을 선택합니다.
6. 사용자 환경에 대한 구성 매개 변수를 입력합니다.
7. 추가 * 를 클릭합니다.

CLI를 참조하십시오

1. 설치를 시작합니다.

   보안 인증서설치형 server-ca

2. 다음 콘솔 메시지를 찾습니다.

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. 텍스트 편집기로 인증서 파일을 엽니다.
4. 다음 행을 포함하여 전체 인증서를 복사합니다.

   ```
   -----BEGIN CERTIFICATE-----

   -----END CERTIFICATE-----
   ```

5. 명령 프롬프트 후 터미널에 인증서를 붙여 넣습니다.
6. Enter * 키를 눌러 설치를 완료합니다.
7. 다음 중 하나를 사용하여 인증서가 설치되었는지 확인합니다.

   ```
   security certificate show-user-installed

   security certificate show
   ```

2단계: 인증 서버를 구성합니다

ONTAP에 하나 이상의 인증 서버를 정의해야 합니다. 구성 및 배포 계획에 따라 매개 변수 값을 선택해야 합니다. 검토 "OAuth2 배포 시나리오" 구성에 필요한 정확한 매개 변수를 결정합니다.

> 권한 부여 서버 정의를 수정하려면 기존 정의를 삭제하고 새 정의를 만듭니다.

아래에 제공된 예는 의 첫 번째 간단한 배포 시나리오를 기반으로 합니다 "로컬 검증". 독립 실행형 범위는 프록시 없이 사용됩니다.

ONTAP 액세스 방법에 따라 올바른 절차를 선택합니다. CLI 절차에서는 명령을 실행하기 전에 교체해야 하는 기호 변수를 사용합니다.

예 **2.** 단계

시스템 관리자

1. System Manager에서 * 클러스터 * > * 설정 * 을 선택합니다.
2. 아래로 스크롤하여 * 보안 * 섹션으로 이동합니다.
3. OAuth 2.0 권한 부여 * 옆에 있는 * + * 를 클릭합니다.
4. 추가 옵션 * 을 선택합니다.
5. 다음과 같이 배포에 필요한 값을 제공합니다.
   - 이름
   - 응용 프로그램(http)
   - 공급자 JWKS URI입니다
   - 발급자 URI입니다
6. 추가 * 를 클릭합니다.

CLI를 참조하십시오

1. 정의를 다시 만듭니다.

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

예를 들면 다음과 같습니다.

```
security oauth2 client create \
-config-name auth0 \
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
realm/protocol/openid-connect/certs \
-application http \
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

3단계: OAuth 2.0을 활성화합니다

마지막 단계는 OAuth 2.0을 활성화하는 것입니다. ONTAP 클러스터에 대한 전역 설정입니다.

> ONTAP, 인증 서버 및 지원 서비스가 모두 올바르게 구성되었는지 확인하기 전까지는 OAuth 2.0 처리를 활성화하지 마십시오.

ONTAP 액세스 방법에 따라 올바른 절차를 선택합니다.

예 **3.** 단계

시스템 관리자

1. System Manager에서 * 클러스터 * > * 설정 * 을 선택합니다.
2. 아래로 스크롤하여 * 보안 섹션 * 을 찾습니다.
3. OAuth 2.0 권한 부여 * 옆에 있는 * → * 를 클릭합니다.
4. OAuth 2.0 권한 부여 * 를 활성화합니다.

CLI를 참조하십시오

1. OAuth 2.0 활성화:

   ```
   security oauth2 modify -enabled true
   ```

2. OAuth 2.0이 활성화되어 있는지 확인합니다.

   ```
   security oauth2 show
   Is OAuth 2.0 Enabled: true
   ```

OAuth 2.0을 사용하여 REST API 호출을 실행합니다

ONTAP의 OAuth 2.0 구현은 REST API 클라이언트 애플리케이션을 지원합니다. curl을 사용하여 간단한 REST API 호출을 실행하여 OAuth 2.0을 사용할 수 있습니다. 아래 예에서는 ONTAP 클러스터 버전을 검색합니다.

시작하기 전에

ONTAP 클러스터에 대해 OAuth 2.0 기능을 구성하고 사용하도록 설정해야 합니다. 여기에는 인증 서버 정의가 포함됩니다.

1단계**:** 액세스 토큰을 획득합니다

REST API 호출에 사용할 액세스 토큰을 얻어야 합니다. 토큰 요청은 ONTAP 외부에서 수행되며 정확한 절차는 인증 서버 및 해당 구성에 따라 다릅니다. 웹 브라우저, curl 명령 또는 프로그래밍 언어를 사용하여 토큰을 요청할 수 있습니다.

설명 목적으로 curl을 사용하여 Keycloak에서 액세스 토큰을 요청하는 방법에 대한 예가 아래에 나와 있습니다.

Keycloak 예

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

반환된 토큰을 복사하여 저장해야 합니다.

2단계: REST API 호출을 실행합니다

유효한 액세스 토큰이 있으면 액세스 토큰과 함께 curl 명령을 사용하여 REST API 호출을 실행할 수 있습니다.

매개 변수 및 변수

컬링 예제의 두 변수는 아래 표에 설명되어 있습니다.

변수	설명
$FQDN_IP입니다	ONTAP 관리 LIF의 정규화된 도메인 이름 또는 IP 주소
$access_token입니다	인증 서버에서 발급한 OAuth 2.0 액세스 토큰

curl 예제를 실행하기 전에 먼저 Bash 셸 환경에서 이러한 변수를 설정해야 합니다. 예를 들어, Linux CLI에서 다음 명령을 입력하여 FQDN 변수를 설정하고 표시합니다.

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

두 변수가 모두 로컬 Bash 셸에 정의되면 curl 명령을 복사하여 CLI에 붙여 넣을 수 있습니다. Enter * 키를 눌러 변수를 대체하고 명령을 실행합니다.

컬의 예

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```