構成と導入
ONTAP 9

NetApp
April 24, 2024

目次

構成と導入

ONTAPを使用したOAuth 2.0の導入準備

ONTAP環境でOAuth 2.0を構成する前に、展開の準備をする必要があります。主なタスクと決定事項の概要を以下に示します。セクションの配置は、通常、従うべき順序に沿って配置されます。ただし、ほとんどの環境に適用できますが、必要に応じて環境に適応する必要があります。また、正式な導入計画の作成も検討する必要があります。

> 環境に応じて、ONTAPに定義されている認証サーバの設定を選択できます。これには、導入のタイプごとに指定する必要があるパラメータ値も含まれます。を参照してください "OAuth 2.0の導入シナリオ" を参照してください。

リソースとクライアントアプリケーションを保護

OAuth 2.0は、保護されたリソースへのアクセスを制御するための承認フレームワークです。このため、導入の最初の重要なステップは、使用可能なリソースと、それらにアクセスする必要があるクライアントを特定することです。

クライアントアプリケーションを特定する

REST API呼び出しを発行するときにOAuth 2.0を使用するクライアントと、アクセスが必要なAPIエンドポイントを決定する必要があります。

既存の**ONTAP REST**ロールとローカルユーザの確認

RESTロールやローカルユーザなど、既存のONTAP IDの定義を確認する必要があります。OAuth 2.0の設定方法によっては、これらの定義を使用してアクセスを決定できます。

OAuth 2.0へのグローバルな移行

OAuth 2.0認証を段階的に実装することもできますが、各認証サーバーにグローバルフラグを設定することで、すべてのREST APIクライアントをOAuth 2.0にすぐに移動することもできます。これにより、自己完結型スコープを作成することなく、既存のONTAP構成に基づいてアクセスを決定できます。

認証サーバ

認証サーバーは、アクセストークンを発行し、管理ポリシーを適用することで、OAuth 2.0の展開において重要な役割を果たします。

認可サーバーを選択してインストールします。

1つ以上の認可サーバーを選択してインストールする必要があります。スコープの定義方法など、アイデンティティプロバイダの設定オプションと手順を理解することが重要です。

認証ルート**CA**証明書をインストールする必要があるかどうかを判断する

ONTAPでは、認証サーバの証明書を使用して、クライアントから提示された署名済みアクセストークンを検証します。これを行うには、ONTAPにルートCA証明書と中間証明書が必要です。ONTAPがプリインストールされている場合があります。そうでない場合は、インストールする必要があります。

ネットワークの場所と構成の評価

認証サーバがファイアウォールの背後にある場合は、プロキシサーバを使用するようにONTAPを設定する必要があります。

クライアントの認証と許可

クライアントの認証と許可には、いくつかの側面を考慮する必要があります。

自己完結型スコープまたはローカル**ONTAP ID**定義

大まかに言えば、認可サーバーで定義された自己完結型スコープを定義することも、役割やユーザーを含む既存のローカルONTAP ID定義に依存することもできます。

ローカル**ONTAP**処理を使用するオプション

ONTAP ID定義を使用する場合は、適用するものを次のように決定する必要があります。

- ネームドRESTロール
- ローカルユーザの一致
- Active DirectoryまたはLDAPグループ

ローカル検証またはリモートイントロスペクション

アクセストークンがONTAPによってローカルで検証されるか、イントロスペクションによって認可サーバーで検証されるかを決定する必要があります。また、更新間隔など、いくつかの関連する値も考慮する必要があります。

送信者に制約されたアクセストークン

高度なセキュリティが必要な環境では、MTLSに基づいて送信制限付きアクセストークンを使用できます。これには、クライアントごとに証明書が必要です。

管理インターフェイス

OAuth 2.0の管理は、次のいずれかのONTAPインターフェイスを使用して実行できます。

- コマンドラインインターフェイス
- System Manager の略
- REST API

クライアントニヨルアクセストークンノヨウキュウホウホウ

クライアントアプリケーションは、許可サーバからアクセストークンを直接要求する必要があります。許可の種類を含め、これをどのように行うかを決定する必要があります。

ONTAPの設定

ONTAPのいくつかの設定タスクを実行する必要があります。

RESTロールとローカルユーザを定義する

認証設定に基づいて、ローカルのONTAP識別処理を使用できます。この場合は、RESTロールとユーザ定義を確認して定義する必要があります。

コア構成

コアONTAP構成の実行には、主に次の3つの手順が必要です。

- 必要に応じて、認証サーバの証明書に署名したCAのルート証明書（および中間証明書）をインストールします。
- 認可サーバを定義します。
- クラスタに対してOAuth 2.0の処理を有効にします。

ONTAPでのOAuth 2.0の導入

OAuth 2.0のコア機能の展開には、主に3つのステップがあります。

作業を開始する前に

ONTAPを設定する前に、OAuth 2.0の展開を準備する必要があります。たとえば、証明書がどのように署名されたか、ファイアウォールの内側にあるかなど、承認サーバーを評価する必要があります。を参照してください "ONTAPを使用したOAuth 2.0の導入準備" を参照してください。

手順1：認証サーバ証明書をインストールする

ONTAPには、多数のルートCA証明書が事前にインストールされています。そのため、多くの場合、認証サーバの証明書は追加の設定なしでONTAPによってすぐに認識されます。ただし、許可サーバ証明書の署名方法によっては、ルートCA証明書と中間証明書のインストールが必要になる場合があります。

必要に応じて、次の手順に従って証明書をインストールします。必要な証明書はすべてクラスタレベルでインストールする必要があります。

ONTAPへのアクセス方法に基づいて、正しい手順を選択します。

例 **1.** 手順

System Manager の略

1. System Managerで、**[**クラスタ**]>***[設定]*を選択します。
2. [セキュリティ]*セクションまで下にスクロールします。
3. の横にある→*をクリックします。
4. タブで[追加]*をクリックします。
5. [インポート]*をクリックし、証明書ファイルを選択します。
6. 環境に合わせて設定パラメータを設定します。
7. [追加（ Add ）] をクリックします。

CLI の使用

1. インストールを開始します。

   ```
   security certificate install -type server-ca
   ```

2. 次のコンソールメッセージを確認します。

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

3. 証明書ファイルをテキストエディタで開きます。
4. 次の行を含む証明書全体をコピーします。

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

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

5. コマンドプロンプトの後に証明書を端末に貼り付けます。
6. Enter*キーを押してインストールを完了します。
7. 次のいずれかを使用して証明書がインストールされていることを確認します。

   ```
   security certificate show-user-installed

   security certificate show
   ```

手順**2**：認証サーバを設定する

ONTAPに対する認可サーバーを少なくとも1つ定義する必要があります。設定と導入計画に基づいてパラメータ値を選択する必要があります。レビュー "OAuth2導入シナリオ" をクリックして、構成に必要な正確なパラメータを決定します。

> 認可サーバー定義を変更するには、既存の定義を削除して新しい定義を作成します。

次の例は、最初のシンプルな導入シナリオに基づいています。 "ローカル検証"。自己完結型スコープはプロキシなしで使用されます。

ONTAPへのアクセス方法に基づいて、正しい手順を選択します。CLI手順では、コマンドを実行する前に置き換える必要があるシンボリック変数を使用します。

例 **2.** 手順

System Manager の略

1. System Managerで、**[**クラスタ**]>***[設定]*を選択します。
2. [セキュリティ]*セクションまで下にスクロールします。
3. * OAuth 2.0 authorization の横にある+*をクリックします。
4. [その他のオプション]*を選択します。
5. 導入に必要な値を次のように指定します。
   - 名前
   - アプリケーション（http）
   - プロバイダJWKS URI
   - 発行者URI
6. [追加（ Add ）] をクリックします。

CLI の使用

1. 定義を再作成します。

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

例：

```
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
```

手順**3**：**OAuth 2.0**を有効にする

最後のステップは、OAuth 2.0を有効にすることです。これはONTAPクラスタのグローバル設定です。

> ONTAP、認可サーバー、およびサポートサービスがすべて正しく設定されていることを確認するまで、OAuth 2.0の処理を有効にしないでください。

ONTAPへのアクセス方法に基づいて、正しい手順を選択します。

例 **3.** 手順

System Manager の略

1. System Managerで、**[**クラスタ**]>***[設定]*を選択します。
2. [セキュリティ]セクション*まで下にスクロールします。
3. * OAuth 2.0 authorization の横にある→*をクリックします。
4. * OAuth 2.0認証*を有効にします。

CLI の使用

1. OAuth 2.0を有効にします。

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

2. OAuth 2.0が有効になっていることを確認します。

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

OAuth 2.0を使用したREST API呼び出しの問題

ONTAPのOAuth 2.0実装では、REST APIクライアントアプリケーションがサポートされています。curlを使用して簡単なREST API呼び出しを問題し、OAuth 2.0の使用を開始できます。次の例は、ONTAPクラスタのバージョンを取得します。

作業を開始する前に

ONTAPクラスタに対してOAuth 2.0機能を設定して有効にする必要があります。これには、認可サーバーの定義が含まれます。

ステップ**1**：アクセストークンを取得する

REST API呼び出しで使用するアクセストークンを取得する必要があります。トークン要求はONTAPの外部で実行され、正確な手順は認可サーバとその設定によって異なります。Webブラウザ、curlコマンド、またはプログラミング言語を使用してトークンを要求できます。

説明のために、curlを使用してKeycloakからアクセストークンを要求する方法の例を以下に示します。

キークロークの例

```
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'
```

返されたトークンをコピーして保存する必要があります。

手順2：REST API呼び出しを問題する

有効なアクセストークンを取得したら、curlコマンドとアクセストークンを使用してREST API呼び出しを問題できます。

パラメータと変数

curlの例の2つの変数について、次の表で説明します。

変数（**Variable**）	説明
$FQDN_IP	ONTAP管理LIFの完全修飾ドメイン名またはIPアドレス。
$access_token	認可サーバーによって発行されたOAuth 2.0アクセストークン。

curlの例を発行する前に、まずBashシェル環境でこれらの変数を設定する必要があります。たとえば、Linux CLIで次のコマンドを入力して、FQDN変数を設定および表示します。

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

両方の変数をローカルのBashシェルで定義したら、curlコマンドをコピーしてCLIに貼り付けることができます。Enter *を押して変数を置き換え、コマンドを問題します。

カールの例

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