設定と導入
ONTAP 9

NetApp
February 12, 2026

目次

設定と導入

ONTAPでのOAuth 2.0の導入準備

ONTAP環境でOAuth 2.0を設定する前に、導入の準備をする必要があります。ここでは、主なタスクと決定が必要な事項の概要を説明します。セクションは、一般に望ましいと考えられる順序で並んでいます。大半の環境にはこれで対応できますが、必要があれば環境に応じて調整してご利用ください。このほか、正式な導入計画の作成も検討してください。

環境に応じて、ONTAPに定義された認可サーバーの設定を選択できます。これには、導入タイプごとに指定する必要があるパラメータ値が含まれます。詳細については、"OAuth 2.0の導入シナリオ"を参照してください。

保護されたリソースとクライアント アプリケーション

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許可フレームワークです。そこで、導入に際してまず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が、重要な最初の手順になります。

クライアント アプリケーションの特定

REST API呼び出しを発行する際にOAuth 2.0を使用するクライアントと、それらのクライアントのアクセス先になる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制御できます。

OAuth 2.0へのグローバルな移行

OAuth 2.0許可は段階的に導入することもできますが、各許可サーバにグローバル フラグを設定することで、すべてのREST APIクライアントを一気にOAuth 2.0に移行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しなくても、ONTAPの既存の設定に基づいてアクセスを制御できます。

許可サーバ

許可サーバは、OAuth 2.0環境において、アクセス トークンを発行し、管理ポリシーを適用するという重要な役割を果たします。

許可サーバの選択とインストール

1つ以上の許可サーバを選択し、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しておくことが重要です。Microsoft Entra IDなど、一部の許可サーバは、名前ではなく、UUIDを使用してグループを表します。

許可ルート**CA**証明書をインストールする必要性の判断

ONTAPは、許可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。そのためにONTAPに必要なのが、ルートCA証明書と中間証明書です。これらの証明書は、事前にONTAPにインストールされている可能性があります。インストールされていない場合には、インストール

する必要があります。

ネットワークの位置の評価と設定

許可サーバがファイアウォールの内側にある場合は、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。

クライアント認証と許可

クライアントの認証と許可には、考慮すべき側面がいくつかあります。

自己完結型スコープかローカル**ONTAP ID**定義か

大きく分けて、許可サーバで自己完結型スコープを定義する方法と、ロールやユーザを含む既存のローカルONTAP ID定義を使用する方法があります

ローカル**ONTAP**処理に関するオプション

ONTAP ID定義を使用する場合は、次のどれを適用するのかを決定する必要があります。

- 指定RESTロール
- ローカル ユーザの照合
- Active DirectoryグループまたはLDAPグループ

ローカル検証とリモート 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許可サーバ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についても検討する必要があります。

送信者限定アクセス トークン

高度なセキュリティが必要な環境には、mTLSベースの送信者限定アクセス トークンを使用できます。この場合、クライアントごとに証明書が必要です。

UUIDとしてのグループおよび**ID**マッピング

UUIDを使用してグループを表す許可サーバを使用している場合は、これらをグループ名に、場合によっては関連付けられているロールにもマッピングする方法を計画する必要があります。

管理インターフェイス

OAuth 2.0は、次のいずれかのONTAPインターフェイスを通じて管理できます。

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

クライアントによるアクセス トークン要求の方法

クライアント アプリケーションは、許可サーバに直接アクセス トークンを要求しなければなりません。グラント タイプを含めて、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で、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 ユーザの定義

許可の設定に基づいて、ローカルのONTAP識別処理を使用できます。その場合は、RESTロールとユーザ定義を確認および定義する必要があります。また、許可サーバによっては、UUID値に基づいたグループの管理も含まれる場合があります。

コア設定

ONTAPのコア設定を行うには、主に次の3つの手順が必要です。

- 必要に応じて、許可サーバの証明書に署名したCAのルート証明書を（ある場合は中間証明書も）インストールします。
- 許可サーバを定義します。
- クラスタのOAuth 2.0処理を有効にします。

ONTAPでのOAuth 2.0の導入

OAuth 2.0のコア機能の導入には、主に3つの手順があります。

開始する前に

ONTAPを設定する前に、OAuth 2.0の導入準備を行う必要があります。例えば、証明書の署名方法やファイアウォールの背後にあるかどうかなど、認可サーバを評価する必要があります。詳細については、"ONTAPでのOAuth 2.0の導入準備"をご覧ください。

ステップ1：認証サーバーのルートCA証明書をインストールする

ONTAPには、豊富なルート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、許可サーバの証明書は、追加の設定をしなくても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。

必要な場合は、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対応した手順に従ってください。

例 **1.** 手順

System Manager

1. System Managerで、クラスター > *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. 証明書*の横にある→*をクリックします。
4. *信頼された証明機関*タブで*追加*をクリックします。
5. *Import*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、パラメータの設定を完了します。
7. *[追加]*をクリックします。

CLI

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 メッセージを探します。

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

3. テキスト エディタで証明書ファイルを開きます。
4. 次の行を含めて、証明書全体をコピーします。

   ```
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

5. コマンド プロンプトの末尾に証明書を貼り付けます。
6. **Enter** 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たことを確認します。

   ```
   security certificate show-user-installed
   ```

   ```
   security certificate show
   ```

ステップ**2**：認可サーバーを構成する

ONTAPに少なくとも1つの認証サーバーを定義する必要があります。パラメータ値は、設定と導入計画に基づいて選択してください。"OAuth2の導入シナリオ"を確認して、設定に必要な正確なパラメータを決定してください。

許可サーバの定義を変更するために、既存の定義を削除して新しい定義を作成することもできます。

以下に示す例は、"ローカル検証"の最初の単純なデプロイメントシナリオに基づいています。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対応した手順に従ってください。CLIの手順では記号変数が使われているので、コマンドを実行する前に置き換える必要があります。

例 **2.** 手順

System Manager

1. System Managerで、クラスター > *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. 環境に必要な値を指定します。例は次のとおりです。
   - Name
   - Application（http）
   - Provider JWKS URI
   - Issuer URI
6. *[追加]*をクリックします。

CLI

1. 改めて定義を作成します。

```
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
```

```
`security oauth2 client create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-
cli/security-oauth2-client-create.html["ONTAPコマンド リファレンス
"^]をご覧ください。
```

ステップ3：OAuth 2.0を有効にする

最後に、OAuth 2.0を有効にします。これはONTAPクラスタのグローバル設定です。

> ONTAP、許可サーバ、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できるまで、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対応した手順に従ってください。

例 3. 手順

System Manager

1. System Managerで、クラスター > *設定*を選択します。
2. *Security 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

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
   ```

関連情報

- "security certificate install"
- "セキュリティ証明書の表示"
- "セキュリティ oauth2 修正"
- "security oauth2 show"

OAuth 2.0を使用してONTAP REST API呼び出しを発行する

ONTAPに導入したOAuth 2.0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ます。curlを使用して簡単なREST API呼び出しを発行し、OAuth 2.0の使用を開始できます。ここでは、ONTAPクラスタのバージョンを取得する例を紹介します。

開始する前に

ONTAPクラスタにOAuth 2.0の機能を設定して有効にする必要があります。これには、許可サーバ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。トークンの要求はONTAPの外部で実行され、正確な手順は許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通じてトークンを要求できます。

参考までに、curlを使用してKeycloakからアクセス トークンを要求する方法を掲載します。

Keycloak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'
```

返されたトークンは、コピーして保存する必要があります。

ステップ2：REST API呼び出しを発行する

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呼び出しを発行できます。

パラメータと変数

次の表は、curlの例にある2つの変数についての解説です。

変数	概要
$FQDN_IP	ONTAP管理LIFの完全修飾ドメイン名またはIPアドレスです。
$ACCESS_TOKEN	許可サーバによって発行されたOAuth 2.0アクセス トークンです。

curlの例を実行する前に、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
```

ローカルのBashシェルで両方の変数を定義したら、curlコマンドをコピーしてCLIに貼り付けます。*Enter*キーを押して変数を置き換え、コマンドを実行します。

Curlの例

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

著作権に関する情報

商標に関する情報