クライアント許可
ONTAP 9

NetApp
February 12, 2026

目次

クライアント許可

ONTAPクライアント許可の概要とオプション

ONTAP OAuth 2.0の実装は、柔軟性と堅牢性を考慮した設計になっていて、ONTAP環境の保護に必要な機能を提供します。これには、同時に指定できない設定オプションがいくつかあります。許可の決定は、最終的にはOAuth 2.0のアクセス トークンに含まれている、またはアクセス トークンから導き出されたONTAP RESTロールに基づいて行われます。

OAuth 2.0の認証を設定する場合にのみ"ONTAP RESTロール"を使用できます。以前のONTAPの従来のロールはサポートされていません。

ONTAPは、設定に基づいて最も適切な単一の認証オプションを適用します。ONTAPがクライアントアクセスを決定する方法の詳細については、"ONTAPによるアクセスの制御方法"を参照してください。

OAuth 2.0の自己完結型スコープ

これらのスコープには、1つ以上のカスタムRESTロールが含まれており、それぞれがアクセストークン内の単一の文字列にカプセル化されています。これらはONTAPロール定義とは独立しています。スコープ文字列は認可サーバで設定する必要があります。詳細については、"自己完結型OAuth 2.0スコープ"を参照してください。

ローカル**ONTAP REST**ロール

組み込みまたはカスタムの単一の名前付きRESTロールを使用できます。名前付きロールのスコープ構文は**ontap-role-**<URL-encoded-ONTAP-role-name>です。例えば、ONTAPロールが `admin`の場合、スコープ文字列は `ontap-role-admin`になります。

ユーザ

アプリケーション「http」へのアクセスが定義されたアクセス トークン内のユーザ名を使用できます。ユーザは、定義された認証方法に基づいて、password、domain（Active Directory）、nsswitch（LDAP）の順にテストされます。

グループ

許可にONTAPグループを使用するように許可サーバを設定できます。ローカルONTAPの定義を調べてもアクセスの可否を判定できない場合は、Active Directory（「domain」）グループかLDAP（「nsswitch」）グループが使用されます。グループ情報は、次の2つの方法のいずれかで指定できます。

- OAuth 2.0のスコープ文字列

  グループメンバーシップを持つユーザーが存在しないクライアント資格情報フローを使用した機密アプリケーションをサポートします。スコープ名は **ontap-group-**<URL-encoded-ONTAP-group-name> とする必要があります。例えば、グループが「development」の場合、スコープ文字列は「ontap-group-development」になります。

- 「グループ」のクレーム

  これは、リソース オーナー（パスワード グラント）フローを使用してADFSによって発行されるアクセストークンが対象です。

詳細については、"ONTAP で OAuth 2.0 または SAML IdP グループを使用する"を参照してください。

ONTAPの自己完結型OAuth 2.0スコープ

自己完結型スコープは、アクセス トークンで伝送される文字列です。それぞれが完結したカスタム ロール定義であり、ONTAPがアクセスの可否を判定するために必要なものがすべて含まれています。スコープは、ONTAP内で定義されているRESTロールとは別の、独立したものです。

スコープ文字列のフォーマット

基本的に、スコープは連続した文字列で表され、コロンで区切られた6つの値で構成されます。ここでは、スコープ文字列で使用されるパラメータについて説明します。

ONTAPリテラル

スコープは、小文字のリテラル値 `ontap`で始まる必要があります。これにより、スコープがONTAPに固有であることが識別されます。

クラスタ

スコープが適用されるONTAPクラスタを定義します。指定できる値は、次のとおりです。

- クラスタUUID

  単一のクラスタを特定します。

- アスタリスク（*）

  スコープをすべてのクラスタに適用することを意味します。

ONTAP CLIコマンド `cluster identity show`を使用して、クラスタのUUIDを表示できます。指定しない場合は、スコープがすべてのクラスタに適用されます。"ONTAPコマンド リファレンス"の `cluster identity show`の詳細をご覧ください。

ロール

自己完結型スコープに含まれるRESTロールの名前です。この値は、ONTAPで確認されたり、ONTAPに定義されている既存のRESTロールと照合されたりすることはありません。この名前は、ロギングに使用されます。

アクセス レベル

この値は、スコープ内でAPIエンドポイントを使用する場合にクライアント アプリケーションに適用されるアクセス レベルを表します。次の表に、設定できる6つの値をまとめておきます。

アクセス レベル	概要
なし	指定したエンドポイントへのアクセスをすべて拒否します。

アクセス レベル	概要
readonly	GETを使用した読み取りアクセスのみを許可します。
read_create	読み取りアクセスと、POSTを使用した新しいリソース インスタンスの作成を許可します。
read_modify	読み取りアクセスと、PATCHを使用した既存のリソースの更新を許可します。
read_create_modify	削除以外のアクセスをすべて許可します。許可される処理は、GET（読み取り）、POST（作成）、PATCH（更新）です。
all	フル アクセスを許可します。

SVM

スコープが適用されるクラスター内のSVMの名前。すべてのSVMを指定するには、*（アスタリスク）を使用します。

> この機能はONTAP 9.14.1では完全にはサポートされていません。SVMパラメータは無視し、プレースホルダとしてアスタリスクを使用できます。 "ONTAPリリース ノート"を確認して、今後のSVMサポートについてチェックしてください。

REST API URI

リソースまたは関連リソースセットへの完全パスまたは部分パス。文字列は `/api`で始まる必要があります。値を指定しない場合、スコープはONTAPクラスタのすべてのAPIエンドポイントに適用されます。

スコープの例

自己完結型スコープの例を、いくつか紹介します。

ontap:*:joes-role:read_create_modify:*:/api/cluster

このロールを割り当てられたユーザーに `/cluster`エンドポイントへの読み取り、作成、および変更アクセス権を付与します。

CLI管理ツール

自己完結型スコープの管理を容易にし、エラーの発生を抑えるために、ONTAP は `security oauth2 scope`入力パラメータに基づいてスコープ文字列を生成する CLI コマンドを提供しています。

このコマンド `security oauth2 scope`には、入力内容に基づいて2つの使用例があります：

- CLIパラメータからスコープ文字列を生成

  このバージョンのコマンドを使用すると、入力したパラメータに基づいてスコープ文字列を生成できます。

- スコープ文字列からCLIパラメータを生成

  このバージョンのコマンドを使用すると、入力したスコープ文字列に基づいてコマンド パラメータを生成できます。

例

次の例は、スコープ文字列を生成するものです。コマンド例に続いて、出力結果も掲載しています。定義は、すべてのクラスタに適用されます。

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

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

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

ONTAP での OAuth 2.0 外部ロールマッピング

外部ロールは、ONTAPで使用するように設定されたアイデンティティ プロバイダで定義されます。ONTAP CLIを使用して、これらの外部ロールとONTAPロールのマッピング関係を作成および管理できます。

ONTAP REST APIを使用して外部ロールマッピング機能を設定することもできます。詳細については、 "ONTAP自動化ドキュメント"をご覧ください。

アクセス トークン内の外部ロール

以下は、2つの外部ロールを含むJSONアクセス トークンの一部です。

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

構成

外部ロール マッピング機能は、ONTAPコマンドライン インターフェイスを使用して管理できます。

作成

`security login external-role-mapping create`コマンドを使用して、ロールマッピング設定を定義できます。このコマンドおよび関連オプションを実行するには、ONTAPの*admin*権限レベルが必要です。

パラメータ

グループ マッピングの作成に使用するパラメータを以下に示します。

パラメータ	概要
external-role	外部のアイデンティティ プロバイダで定義されているロールの名前。
provider	アイデンティティ プロバイダの名前。これはシステムの識別子である必要があります。
ontap-role	外部ロールがマッピングされている既存のONTAPロールを示します。

例

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

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

その他のCLI処理

このコマンドでは、次のような追加の処理がサポートされます。

- 表示
- 変更
- 削除

関連情報

- "ONTAPコマンド リファレンス"

ONTAPによるクライアント アクセスの制御方法

OAuth 2.0を適切に設計、導入するには、ONTAPがどのように許可設定を使用してクライアントのアクセス可否を判定しているのかを理解しておく必要があります。ここでは、アクセスを制御するために使用する主な手順をONTAPリリース別に紹介します。

ONTAP 9.15.1では、OAuth 2.0の重要な更新はありませんでした。9.15.1リリースを使用している場合は、ONTAP 9.14.1の説明を参照してください。

関連情報

- "ONTAPでサポートされるOAuth 2.0の機能"

ONTAP 9.16.1

ONTAP 9.16.1では、OAuth 2.0の標準のサポートが拡張され、ネイティブのEntra IDグループ用のMicrosoft Entra ID固有の拡張機能と外部のロール マッピングが追加されています。

ONTAP 9.16.1のクライアント アクセスの制御

ステップ**1**：自己完結型スコープ

アクセス トークンに自己完結型のスコープが含まれている場合、ONTAPは最初にそれらのスコープを調べます。自己完結型スコープがない場合は、手順2に進みます。

1つ以上の自己完結型スコープが存在する場合、ONTAPは明示的な*ALLOW*または*DENY*の決定が下されるまで各スコープを適用します。明示的な決定が下されると、処理は終了します。

ONTAPが明示的にアクセスの可否を判定できない場合は、手順2に進みます。

ステップ**2**：ローカルロールフラグを確認する

ONTAPはブールパラメータ `use-local-roles-if-present`を調べます。このフラグの値は、ONTAPに定義された各認証サーバーに対して個別に設定されます。

- 値が `true`の場合は、手順 3 に進みます。
- 値が `false`の場合、処理は終了し、アクセスは拒否されます。

ステップ**3**：名前付き**ONTAP REST**ロール

アクセストークンの `scope`または `scp`フィールド、あるいはクレームとして名前付きRESTロールが含まれている場合、ONTAPはそのロールを使用してアクセス決定を行います。その結果は常に*ALLOW*または*DENY*となり、処理は終了します。

指定RESTロールがない場合、またはロールが見つからない場合は、手順4に進みます。

ステップ**4**：ユーザー

アクセス トークンからユーザ名が抽出され、アプリケーション「http」にアクセスできるユーザとの照合が試みられます。ユーザは、認証方法に基づいて次の順序で検証されます。

- password
- domain（Active Directory）
- nsswitch（LDAP）

一致するユーザーが見つかった場合、ONTAPはそのユーザーに定義されたロールを使用してアクセスを決定します。その結果は常に*ALLOW*または*DENY*となり、処理は終了します。

一致するユーザがいない場合、またはアクセス トークンにユーザ名が含まれていない場合は、手順5に進みます。

ステップ**5**：グループ

1つ以上のグループが含まれている場合、フォーマットが検査されます。グループがUUIDで表現されている場合は、内部グループマッピングテーブルが検索されます。一致するグループと関連付けられたロールがある場合、ONTAPはグループに定義されているロールを使用してアクセスを決定します。その結果は常に*ALLOW*または*DENY*となり、処理は終了します。詳細については、"ONTAP で OAuth 2.0 または SAML IdP グループを使用する"をご覧ください。

グループが名前で表現され、ドメインまたはnsswitch認証が設定されている場合、ONTAPはそれぞれActive DirectoryまたはLDAPグループとの照合を試みます。グループが一致する場合、ONTAPはグループに定義されているロールを使用してアクセス判定を行います。その結果は常に*ALLOW*または*DENY*となり、処理は終了します。

一致するグループがない場合、またはアクセス トークンにグループが含まれていない場合、アクセスは拒否され、処理は終了します。

ONTAP 9.14.1

サポートされている初期のOAuth 2.0は、OAuth 2.0の標準機能に基づいて、ONTAP 9.14.1で導入されました。

ONTAP 9.14.1のクライアント アクセスの制御

ステップ**1**：自己完結型スコープ

アクセス トークンに自己完結型のスコープが含まれている場合、ONTAPは最初にそれらのスコープを調べます。自己完結型スコープがない場合は、手順2に進みます。

1つ以上の自己完結型スコープが存在する場合、ONTAPは明示的な*ALLOW*または*DENY*の決定が下されるまで各スコープを適用します。明示的な決定が下されると、処理は終了します。

ONTAPが明示的にアクセスの可否を判定できない場合は、手順2に進みます。

ステップ**2**：ローカルロールフラグを確認する

ONTAPはブールパラメータ `use-local-roles-if-present`を調べます。このフラグの値は、ONTAPに定義された各認証サーバーに対して個別に設定されます。

- 値が `true`の場合は、手順 3 に進みます。
- 値が `false`の場合、処理は終了し、アクセスは拒否されます。

ステップ**3**：名前付き**ONTAP REST**ロール

アクセストークンの `scope`または `scp`フィールドに名前付きREST roleが含まれている場合、ONTAPはそのロールを使用してアクセスを決定します。その結果は常に*ALLOW*または*DENY*となり、処理は終了します。

指定RESTロールがない場合、またはロールが見つからない場合は、手順4に進みます。

ステップ**4**：ユーザー

アクセス トークンからユーザ名が抽出され、アプリケーション「http」にアクセスできるユーザとの照合が試みられます。ユーザは、認証方法に基づいて次の順序で検証されます。

- password
- domain（Active Directory）
- nsswitch（LDAP）

一致するユーザーが見つかった場合、ONTAPはそのユーザーに定義されたロールを使用してアクセスを決定します。その結果は常に*ALLOW*または*DENY*となり、処理は終了します。

一致するユーザがいない場合、またはアクセス トークンにユーザ名が含まれていない場合は、手順5に進みます。

ステップ**5**：グループ

1つ以上のグループが含まれていて、domainまたはnsswitchの許可が設定されている場合、ONTAPはそれらのグループとそれぞれActive DirectoryまたはLDAPグループとの照合を試みます。

グループが一致する場合、ONTAPはグループに定義されたロールを使用してアクセスを決定します。その結果は常に*ALLOW*または*DENY*となり、処理は終了します。

一致するグループがない場合、またはアクセス トークンにグループが含まれていない場合、アクセスは拒否され、処理は終了します。