クライアント許可
ONTAP 9

NetApp
December 20, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/authentication/oauth2-authorization.html on December 20, 2024. Always check docs.netapp.com for the latest.

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て設計されており、ONTAP環境を保護するために必要な機能を提供します。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。承認の決定は、最終的には、OAuth 2.0アクセストークンに含まれるか、OAuth 2.0アクセストークンから派生したONTAP RESTロールに基づいて行われます。

OAuth 2.0の認可を設定する場合にのみ使用でき"ONTAP RESTロール"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1つの許可オプションを適用します。ONTAPによるクライアントアクセスの決定方法の詳細については、を参照してください"ONTAPニヨルアクセスノケツテイホウホウ"。

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1つの文字列内にカプセル化されています。ONTAPロールの定義には依存しません。認可サーバでスコープ文字列を設定する必要があります。詳細については、を参照してください "自己完結型OAuth 2.0スコープ" 。

ローカル**ONTAP REST**ロール

組み込みまたはカスタムの名前付きRESTロールを1つ使用できます。指定したロールのscope構文は、* ontap-role-*<URL-encoded-ONTAP-role-name>です。たとえば、ONTAPロールがスコープ文字列の場合、`admin`はになります `ontap-role-admin`。

ユーザ

アプリケーション「http」へのアクセスで定義されたアクセストークン内のユーザー名を使用できます。ユーザは、定義された認証方式に基づいて、パスワード、ドメイン（Active Directory）、nsswitch（LDAP）の順にテストされます。

グループ

認可サーバは、認可にONTAPグループを使用するように設定できます。ローカルONTAPの定義を調べても、アクセスを決定できない場合は、Active Directory（「domain」）または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スコープ文字列

  グループメンバーシップを持つユーザがいない場合、クライアントのクレデンシャルフローを使用して機密アプリケーションをサポートします。スコープには* ontap-group-*<URL-encoded-ONTAP-group-name>という名前を付けます。たとえば、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」の主張

  これは、リソース所有者(パスワード付与)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を対象としています。

詳細については、を参照してください "グループの操作" 。

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。各ロールは完全なカスタムロール定義であり、アクセスを決定するためにONTAPが必要とするすべての機能が含まれています。スコープは、ONTAP内で定義されているRESTロールとは別のものです。

スコープ文字列の形式

基本レベルでは、スコープは連続した文字列として表され、コロンで区切られた6つの値で構成されます。スコープ文字列で使用されるパラメータについては、以下で説明します。

ONTAPリテラル

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

クラスタ

スコープを適用するONTAPクラスタを定義します。次の値を指定できます。

- クラスタUUID

  単一のクラスタを識別します。

- アスタリスク(*)

  スコープがすべてのクラスタに適用されることを示します。

クラスタのUUIDは、ONTAP CLIのコマンドを使用して表示できます `cluster identity show`。指定しない場合、範囲はすべてのクラスタに適用されます。

ロール

自己完結型スコープに含まれるRESTロールの名前。この値は、ONTAPで検証されたり、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とき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示します。次の表に示す6つの値があります。

アクセスレベル	説明
なし	指定したエンドポイントへのすべてのアクセスを拒否します。
読み取り専用	GETを使用した読み取りアクセスのみを許可します。

アクセスレベル	説明
read_create	POSTを使用して、読み取りアクセスと新しいリソースインスタンスの作成を許可します。
read_modify	読み取りアクセスを許可し、PATCHを使用して既存のリソースを更新する機能を許可します。
read_create_modify	削除以外のすべてのアクセスを許可します。許可される処理は、GET（読み取り）、POST（作成）、およびPATCH（更新）です。
すべて	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内のSVMの名前。すべてのSVMを示すために、*（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のパラメータは無視して、プレースホルダにアスタリスクを使用できます。で "ONTAPリリースノート"今後のSVMのサポートを確認します。

REST API URI

リソースまたは関連リソースのセットへの完全パスまたは部分パス。文字列はで始まる必要があります `/api`。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。

範囲の例

自己完結型スコープの例を以下に示します。

ONTAP：：joes-role：read_create_modify：：/api/cluster

このロールを割り当てられたユーザに、エンドポイントへの読み取り、作成、および変更アクセスを許可します `/cluster`。

CLI管理ツール

自己完結型スコープの管理を容易にし、エラーが発生しにくくするために、ONTAPには、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コマンドが用意されて `security oauth2 scope`います。

コマンド `security oauth2 scope`には、入力内容に基づいて次の2つのユースケースがあります。

- 文字列をスコープするCLIパラメータ

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

- scope string to CLIパラメータ

  このバージョンのコマンドを使用すると、入力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

次の例では、次のコマンド例のあとに出力が含まれたスコープ文字列を生成します。この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
```

グループの操作

ONTAPには、認可サーバに基づいてグループを設定するためのいくつかのオプションが用意されています。グループをロールにマッピングして、ONTAPでアクセスの決定に使用されるようにします。

グループの識別方法

承認サーバーでグループを構成すると、名前またはUUIDのいずれかを使用して、OAuth 2.0アクセストークンでグループが識別されて伝送されます。ONTAPを設定する前に、認可サーバがグループをどのように処理するかを理解しておく必要があります。

アクセストークンに複数のグループが含まれている場合、ONTAPは一致するまで各グループを使用しようとします。

グループ名

多くの認可サーバーは、名前を使用してグループを識別し、表現します。これは、複数のグループを含むActive Directoryフェデレーションサービス(ADFS)によって生成されたJSONアクセストークンの断片です。詳細については、を参照してください [名前付きのグループを管理します。] 。

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

グループ**UUID**

一部の認証サーバは、UUIDを使用してグループを識別し、表現します。これは、複数のグループを含むMicrosoft Entra IDによって生成されたJSONアクセストークンの断片です。詳細については、を参照してください UUIDを使用したグループの管理 。

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

名前付きのグループを管理します。

認可サーバーが名前を使用してグループを識別する場合は、各グループがONTAPに定義されていることを確認する必要があります。セキュリティ環境によっては、グループがすでに定義されている場合があります。

ここでは、ONTAPに対してグループを定義するCLIコマンドの例を示します。サンプルアクセストークンの名前付きグループを使用していることに注目してください。このコマンドを実行するには、ONTAP * admin *権限レベルである必要があります。

例

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

この機能は、ONTAP REST APIを使用して設定することもできます。詳細については、を"ONTAP自動化に関するドキュメント"参照してください。

UUIDを使用したグループの管理

認証サーバがUUID値を使用するグループを表している場合は、グループを使用する前に2段階の設定を行う必要があります。ONTAP 9 .16.1以降では、2つのマッピング機能を使用でき、MicrosoftエントラIDでテストされています。CLIコマンドを実行するには、ONTAP * admin *権限レベルである必要があります。

これらの機能は、ONTAP REST APIを使用して設定することもできます。詳細については、を"ONTAP自動化に関するドキュメント"参照してください。

関連情報

- "ONTAP CLIコマンド"

グループ**UUID**をグループ名にマッピングする

UUID値を使用するグループを表す認証サーバーを使用している場合は、グループUUIDをグループ名にマッピングする必要があります。ONTAP CLIの主な操作について次に説明します。

作成

新しいグループマッピング設定は、コマンドを使用して定義できます `security login group create`。グループのUUIDと名前は、許可サーバの設定と一致する必要があります。

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次に示します。

パラメータ	説明
`vserver`	必要に応じて、グループを関連付けるSVM（SVM）の名前を指定します。省略すると、グループはONTAPクラスタに関連付けられます。
`name`	ONTAPが使用するグループの一意の名前。
`type`	この値は、グループの発信元のアイデンティティプロバイダを示します。
`uuid`	認可サーバによって提供されるグループのUniversally Unique Identifierを指定します。

ここでは、ONTAPに対してグループを定義するCLIコマンドの例を示します。サンプルアクセストークンのUUIDグループを使用していることに注目してください。

例

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

グループを作成すると、グループに対して一意の読み取り専用整数識別子が生成されます。

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

オプションを使用すると、グループに対して生成された一意のグループIDを取得できます `show`。詳細については、ONTAPコマンドのリファレンスドキュメントを参照してください。

グループ**UUID**をロールにマッピングする

UUID値を使用するグループを表す認証サーバーを使用している場合は、そのグループをロールにマッピングできます。ONTAP CLIの主な操作について次に説明します。また、コマンドを実行するには、ONTAP * admin *権限レベルにある必要があります。

最初に、グループに対して生成された一意の整数IDを取得する必要がありグループUUIDをグループ名にマッピングするます。グループをロールにマッピングするには、IDが必要です。

作成

新しいロールマッピングは、コマンドを使用して定義できます `security login group role-mapping create`。

パラメータ

グループをロールにマッピングするために使用されるパラメータを次に示します。

パラメータ	説明
`group-id`	コマンドを使用して、グループに対して生成される一意のIDを指定します `security login group create`。
`role`	グループのマッピング先のONTAPロールの名前。

例

```
security login group role-mapping create -group-id 1 -role admin
```

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

詳細については、ONTAPコマンドのリファレンスドキュメントを参照してください。

外部ロールのマッピング

外部ロールは、ONTAPで使用するように設定されたIdentify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、を "ONTAP自動化に関するドキュメント"参照してください。

関連情報

- "ONTAP CLIコマンド"です。

アクセストークンの外部ロール

これは、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

ロールマッピング設定は、コマンドを使用して定義できます `security login external-role-mapping create`。このコマンドおよび関連するオプションを実行するには、ONTAP * admin *権限レベルである必要があります。

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次に示します。

パラメータ	説明
`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
```

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

詳細については、ONTAPコマンドリファレンスドキュメントまたはONTAP CLIのマニュアルページを参照してください。

ONTAPニヨルクライアントアクセスノケツテイホウホウ

OAuth 2.0を適切に設計および実装するには、ONTAPが許可設定を使用してクライアントのアクセスを決定する方法を理解する必要があります。アクセスを確認するために使用する主な手順は、ONTAPリリースに基づいて次のとおりです。

ONTAP 9 .15.1では、OAuth 2.0の重要なアップデート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機能"

ONTAP 9 .16.1

ONTAP 9 .16.1では、標準のOAuth 2.0のサポートが拡張され、ネイティブのエントラIDグループ用のMicrosoftエントラID固有の拡張機能と外部の役割マッピングが含まれるようになりました。

ONTAP 9のクライアントアクセスを確認します。**16.1**

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は最初にこ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、ステップ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*決定が行われるまで、各スコープを適用します。明示的な決定が行われた場合、処理は終了します。

ONTAPが明示的にアクセスを決定できない場合は、手順2に進みます。

手順**2**：ローカルロールフラグを確認する

ONTAPでは、ブーリアンパラメータが検証され`use-local-roles-if-present`ます。このフラグの値は、ONTAPに定義された認可サーバーごとに個別に設定されます。

- 値がの場合は、 `true`手順3に進みます。
- 値がの場合は `false`、処理が終了し、アクセスが拒否されます。

手順**3**：名前付き**ONTAP REST**ロール

アクセストークンに名前付きRESTロールがOR `scp`フィールドに含まれている場合、または要求として含まれている場合 `scope`、ONTAPはそのロールを使用してアクセスの決定を行います。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

名前付き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。

手順**4**：ユーザ

アクセストークンからユーザ名を抽出し、アプリケーション「http」にアクセスできるユーザと照合します。ユーザは、認証方式に基づいて次の順序で検証されます。

- パスワード
- ドメイン（Active Directory）
- nsswitch（LDAP）

一致するユーザが見つかった場合、ONTAPはそのユーザに対して定義されたロールを使用してアクセスを決定します。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

ユーザが一致しない場合、またはアクセストークンにユーザ名がない場合は、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は、形式が検査されます。グループがUUIDとして表されている場合は、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ているロールがある場合、ONTAPはその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。これにより、常に* allow または deny *の決定が行われ、処理が終了します。詳細については、を参照してください "グループの操作"。

グループが名前で表され、ドメインまたはnsswitch許可が設定されている場合、ONTAPはそれらのグループをそれぞれActive DirectoryまたはLDAPグループと照合しようとします。一致するグループがある場合、ONTAPはその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。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

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、標準のOAuth 2.0機能に基づいて、ONTAP 9 .14.1で導入されました。

ONTAP 9のクライアントアクセスを確認します。**14.1**

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は最初にこ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、ステップ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*決定が行われるまで、各スコープを適用します。明示的な決定が行われた場合、処理は終了します。

ONTAPが明示的にアクセスを決定できない場合は、手順2に進みます。

手順**2**：ローカルロールフラグを確認する

ONTAPでは、ブーリアンパラメータが検証され `use-local-roles-if-present`ます。このフラグの値は、ONTAPに定義された認可サーバーごとに個別に設定されます。

- 値がの場合は、 `true`手順3に進みます。
- 値がの場合は `false`、処理が終了し、アクセスが拒否されます。

手順**3**：名前付き**ONTAP REST**ロール

アクセストークンのフィールドまたは `scp`フィールドに名前付き`REST`ロールが含まれている場合 `scope`、ONTAPはそのロールを使用してアクセスを決定します。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

名前付き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。

手順**4**：ユーザ

アクセストークンからユーザ名を抽出し、アプリケーション「http」にアクセスできるユーザと照合します。ユーザは、認証方式に基づいて次の順序で検証されます。

- パスワード
- ドメイン（Active Directory）
- nsswitch（LDAP）

一致するユーザが見つかった場合、ONTAPはそのユーザに対して定義されたロールを使用してアクセスを決定します。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

ユーザが一致しない場合、またはアクセストークンにユーザ名がない場合は、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、ドメインまたはnsswitch認証が設定されている場合、ONTAPはそれらのグループをそれぞれActive DirectoryまたはLDAPグループと照合しようとします。

一致するグループがある場合、ONTAPはその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。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

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ない場合、アクセスは拒否され、処理は終了します。

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。