アクセス ポリシー ステートメントの作成と変更

ONTAP 9

NetApp
February 12, 2026

目次

アクセス ポリシー ステートメントの作成と変更 . . . 1
- ONTAP S3バケットとオブジェクトストアサーバのポリシーについて学ぶ . . . 1
- デフォルトのONTAP S3バケットポリシーにアクセスルールを追加する . . . 1
- ONTAP S3オブジェクトストアサーバポリシーを作成または変更する . . . 4
- ONTAP S3アクセス用の外部ディレクトリサービスを設定する . . . 6
  - LDAPのS3アクセスを設定する . . . 7
  - 認証でのLDAP高速バインド モードの使用 . . . 8
  - Active DirectoryまたはSMBサーバのS3アクセスを設定する . . . 9
- LDAPまたはドメインユーザーが独自のONTAP S3アクセスキーを生成できるようにする . . . 10
  - アクセス キー生成のためのユーザの設定 . . . 10
  - S3ユーザまたはLDAPユーザによる独自のアクセス キーの生成 . . . 13

アクセス ポリシー ステートメントの作成と変更

ONTAP S3バケットとオブジェクトストアサーバのポリシーについて学ぶ

S3リソースへのユーザとグループのアクセスは、バケットとオブジェクト ストア サーバのポリシーで制御されます。ユーザやグループの数が少ない場合はバケット レベルでアクセスを制御すれば十分ですが、ユーザやグループが多数の場合はオブジェクト ストア サーバ レベルでアクセスを制御した方が簡単です。

デフォルトのONTAP S3バケットポリシーにアクセスルールを追加する

デフォルトのバケット ポリシーにアクセス ルールを追加できます。デフォルト ポリシーのアクセス制御対象は対応するバケットであるため、バケットが1つだけの場合はデフォルト ポリシーが最も適しています。

開始する前に

S3サーバとバケットを含むS3対応のStorage VMがすでに存在している必要があります。

権限を付与するには、事前にユーザまたはグループを作成しておく必要があります。

タスク概要

新しいユーザーやグループに新しいステートメントを追加したり、既存のステートメントの属性を変更したりできます。 `vserver object-store-server bucket policy`の詳細については、"ONTAPコマンド リファレンス"をご覧ください。

ユーザとグループの権限は、バケットの作成時、または必要に応じてあとから付与することができます。バケットの容量やQoSポリシー グループの割り当ても変更できます。

ONTAP 9.9.1 以降、ONTAP S3 サーバで AWS クライアントオブジェクトのタグ付け機能をサポートする予定の場合は、 `GetObjectTagging`、 `PutObjectTagging`、および `DeleteObjectTagging`のアクションをバケットまたはグループポリシーを使用して許可する必要があります。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

手順

1. バケットを編集するには、「ストレージ > バケット」をクリックし、対象のバケットをクリックして「編集」をクリックします。権限を追加または変更する際には、以下のパラメータを指定できます：
   - プリンシパル：アクセスが許可されるユーザーまたはグループ。
   - 効果：ユーザーまたはグループへのアクセスを許可または拒否します。
   - アクション：特定のユーザーまたはグループに対してバケット内で許可されるアクション。
   - リソース：アクセスが許可または拒否されるバケット内のオブジェクトのパスと名前。

     デフォルトの ***bucketname*** と ***bucketname/**** は、バケット内のすべてのオブジェクトへのアクセスを許可します。また、単一のオブジェクトへのアクセスを許可することもできます。たとえば、***bucketname/*_readme.txt*** などです。

   - 条件（オプション）：アクセス試行時に評価される条件式。例えば、アクセスを許可または拒否するIPアドレスのリストを指定できます。

> ONTAP 9.14.1以降では、*Resources*フィールドでバケットポリシーの変数を指定できます。これらの変数はプレースホルダであり、ポリシーの評価時にコンテキスト値に置き換えられます。例えば、 `${aws:username}`がポリシーの変数として指定されている場合、この変数はリクエストコンテキストのユーザー名に置き換えられ、そのユーザーに対して設定されたポリシーアクションを実行できます。

CLI

手順

1. バケット ポリシーにステートメントを追加します。

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

次のパラメータでアクセス権限を定義します。

`-effect`	アクセスを許可するか拒否するかを指定します。
`-action`	`*`すべてのアクションを意味するように指定することも、次の 1 つ以上のリストを指定することもできます： `GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl,GetObjectAcl, ListBucketMultipartUploads,`および `ListMultipartUploadParts`。

`-principal`	S3ユーザまたはグループのリストを指定します。 • 指定できるユーザまたはグループの数は最大10個までです。 • S3グループを指定する場合は、次の形式にする必要があります `group/group_name`. • `*`を指定すると、パブリックアクセス（アクセスキーとシークレットキーなしでのアクセス）を意味します。 • プリンシパルが指定されていない場合は、ストレージVM内のすべてのS3ユーザーにアクセスが許可されます。
`-resource`	バケットとそれに含まれるオブジェクト。ワイルドカード文字 `*`と `?`を使用して、リソースを指定するための正規表現を作成できます。リソースに対して、ポリシー内で変数を指定できます。これらのポリシー変数はプレースホルダであり、ポリシーが評価される際にコンテキスト値に置き換えられます。

`-sid`オプションを使用して、コメントとしてテキスト文字列をオプションで指定できます。

例

次の例では、Storage VM svm1.example.comのbucket1に対するオブジェクト ストア サーバ バケット ポリシーのステートメントを作成し、オブジェクト ストア サーバ ユーザuser1にreadmeフォルダへのアクセスを許可するように指定しています。

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

次の例では、Storage VM svm1.example.comのbucket1に対するオブジェクト ストア サーバ バケット ポリシーのステートメントを作成し、オブジェクト ストア サーバ グループgroup1にすべてのオブジェクトへのアクセスを許可するように指定しています。

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

ONTAP 9.14.1以降では、バケットポリシーに変数を指定できます。次の例では、ストレージVM `svm1`と `bucket1`のサーババケットポリシーステートメントを作成し、 `${aws:username}`をポリシーリソースの変数として指定します。ポリシーが評価されると、ポリシー変数はリクエストコンテキストのユーザー名に置き換えられ、そのユーザーに対して設定されたポリシーアクションを実行できます。たとえ

ば、次のポリシーステートメントが評価されると、 `${aws:username}`はS3操作を実行するユーザーに置き換えられます。ユーザー `user1`が操作を実行すると、そのユーザーには `bucket1`として `bucket1/user1/*`へのアクセスが許可されます。

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

ONTAP S3オブジェクトストアサーバポリシーを作成または変更する

オブジェクト ストア内のバケットに適用できるポリシーを作成できます。オブジェクトストア サーバ ポリシーはユーザのグループに関連付けることができるため、複数のバケットへのリソース アクセスの管理が簡単になります。

開始する前に

S3サーバとバケットを含むS3対応のSVMがすでに存在している必要があります。

タスク概要

オブジェクト ストレージ サーバ グループにデフォルトまたはカスタムのポリシーを指定することで、SVMレベルでアクセス ポリシーを有効にすることができます。ポリシーは、グループ定義で指定するまで有効になりません。

> オブジェクト ストレージ サーバ ポリシーを使用する場合、プリンシパル（ユーザとグループ）はポリシーではなくグループ定義に指定します。

ONTAP S3リソースへのアクセスに使用するデフォルトの読み取り専用ポリシーは3つあります。

- FullAccess
- NoS3Access
- ReadOnlyAccess

新しいカスタムポリシーを作成し、新しいユーザーやグループに新しいステートメントを追加したり、既存のステートメントの属性を変更したりすることもできます。"ONTAPコマンド リファレンス"の `vserver object-store-server policy`の詳細をご覧ください。

ONTAP 9.9.1 以降、ONTAP S3 サーバで AWS クライアントオブジェクトのタグ付け機能をサポートする予定の場合は、 `GetObjectTagging`、 `PutObjectTagging`、および `DeleteObjectTagging`のアクションをバケットまたはグループポリシーを使用して許可する必要があります。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

System Manager を使用してオブジェクト ストア サーバー ポリシーを作成または変更する

手順

1. ストレージ VM を編集します。ストレージ **>** ストレージ **VM** をクリックし、ストレージ VM をクリックして、設定 をクリックし、S3 の下の をクリックします。
2. ユーザーを追加するには：*ポリシー*をクリックし、*追加*をクリックします。
   a. ポリシー名を入力し、リストからグループを選択します。
   b. 既存のデフォルト ポリシーを選択するか、新しいポリシーを追加します。

      グループ ポリシーを追加または変更する際には次のパラメータを指定できます。

      - Group：アクセスを付与するグループ。
      - Effect：1つ以上のグループにアクセスを許可するか拒否するか。
      - Actions：特定のグループに許可する1つ以上のバケット内での処理。
      - リソース：アクセスが許可または拒否される1つ以上のバケット内のオブジェクトのパスと名前。例：
        - * はストレージ VM 内のすべてのバケットへのアクセスを許可します。
        - **bucketname** と **bucketname/*** は、特定のバケット内のすべてのオブジェクトへのアクセスを許可します。
        - **bucketname/readme.txt** は、特定のバケット内のオブジェクトへのアクセスを許可します。
   c. 必要に応じて、既存のポリシーにステートメントを追加します。

CLI

CLI を使用してオブジェクト ストア サーバー ポリシーを作成または変更する

手順

1. オブジェクト ストレージ サーバ ポリシーを作成します。

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. ポリシーのステートメントを作成します。

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   次のパラメータでアクセス権限を定義します。

`-effect`	アクセスを許可するか拒否するかを指定します。

`-action`	`*`すべてのアクションを意味するように指定することも、次の 1 つ以上のリストを指定することもできます： `GetObject, PutObject, DeleteObject, ListBucket,GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads,`および `ListMultipartUploadParts`。
`-resource`	バケットとそれに含まれるオブジェクト。ワイルドカード文字 `*`と `?`を使用して、リソースを指定するための正規表現を作成できます。

`-sid`オプションを使用して、コメントとしてテキスト文字列をオプションで指定できます。

デフォルトでは、新しいステートメントはステートメントリストの末尾に追加され、順番に処理されます。後からステートメントを追加または変更する場合は、ステートメントの `-index`設定を変更して処理順序を変更できます。

この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

ONTAP S3アクセス用の外部ディレクトリサービスを設定する

ONTAP 9.14.1以降では、外部ディレクトリのサービスがONTAP S3オブジェクト ストレージに統合されています。この統合により、外部ディレクトリ サービスによるユーザとアクセスの管理が簡単になります。

外部ディレクトリサービスに属するユーザーグループに、ONTAPオブジェクトストレージ環境へのアクセス権限を付与できます。Lightweight Directory Access Protocol（LDAP）は、Active Directoryなどのディレクトリサービスと通信するためのインターフェースであり、IDおよびアクセス管理（IAM）用のデータベースとサービスを提供します。アクセス権限を付与するには、ONTAP S3環境でLDAPグループを設定する必要があります。アクセス権限を設定すると、グループメンバーにONTAP S3バケットへの権限が付与されます。LDAPの詳細については、"ONTAP NFS SVMでのLDAPネームサービスの使用について学習します"を参照してください。

また、Active Directoryユーザ グループを高速バインド モードに設定することで、ユーザ クレデンシャルを検証し、サードパーティおよびオープンソースのS3アプリケーションをLDAP接続を介して認証するようにもできます。

開始する前に

LDAPグループを設定し、グループ アクセスの高速バインド モードを有効にする場合は、事前に以下を確認してください。

1. S3サーバを含むS3対応Storage VMが作成されました。"S3用SVMの作成"を参照してください。
2. ストレージVMにバケットが作成されました。"バケットの作成"を参照してください。
3. ストレージVMにDNSが設定されています。"DNSサービスを設定する"を参照してください。
4. LDAPサーバの自己署名ルート認証局（CA）証明書がストレージVMにインストールされています。"SVMに自己署名ルートCA証明書をインストールする"を参照してください。
5. LDAPクライアントは、SVM上でTLSを有効にして設定されています。"ONTAP NFSアクセス用のLDAPクライアント構成を作成する"および"LDAPクライアント設定をONTAP NFS SVMに関連付けて情報を取得する"を参照してください。

LDAPのS3アクセスを設定する

1. SVMのグループとパスワードの_ネームサービスデータベース_としてLDAPを指定します：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

ONTAPコマンドリファレンスのhttps://docs.netapp.com/us-en/ontap-cli/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify`^]コマンドの詳細を参照してください。

2. アクセスを許可するLDAPグループに `principal`を設定したオブジェクトストアバケットポリシーステートメントを作成します：

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

例：次の例では、 `buck1`のバケットポリシーステートメントを作成します。このポリシーは、LDAPグループ `group1`にリソース（バケットとそのオブジェクト） `buck1`へのアクセスを許可します。

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. LDAPグループのユーザー `group1`がS3クライアントからS3操作を実行できることを確認します。

認証でのLDAP高速バインド モードの使用

1. SVMのグループとパスワードの_ネームサービスデータベース_としてLDAPを指定します：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

   ONTAPコマンドリファレンスのhttps://docs.netapp.com/us-en/ontap-cli/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify`^]コマンドの詳細を参照してください。

2. S3バケットにアクセスするLDAPユーザーに、バケットポリシーで定義された権限が付与されていることを確認してください。詳細については、"バケット ポリシーの変更"をご覧ください。

3. LDAPグループのユーザが次の処理を実行できることを確認します。

   a. S3クライアントのアクセスキーを次の形式で設定します（ `"NTAPFASTBIND" + base64-encode(user-name:password)`例（ `"NTAPFASTBIND"+ base64-encode(ldapuser:password)、結果は次のようになります `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

   > S3クライアントからシークレット キーの入力を求められることがあります。シークレット キーがない場合は、16文字以上のパスワードを入力できます。

   b. ユーザが権限を持っているS3クライアントから基本的なS3処理を実行します。

Base64認証情報

ONTAP S3のデフォルト設定では、HTTPは使用されず、HTTPSとトランスポート層セキュリティ（TLS）接続のみが使用されます。ONTAPは自己署名証明書を生成できますが、サードパーティの認証局（CA）が発行した証明書を使用することを推奨します。CA証明書を使用すると、クライアントアプリケーションとONTAPオブジェクトストアサーバの間に信頼関係が確立されます。

Base64を使用してエンコードされた認証情報は簡単にデコードされることに注意してください。HTTPSを使用すると、中間者攻撃によるパケットスニファーによるエンコードされた認証情報の傍受を防ぐことができます。

事前署名済みURLを作成する際は、認証にLDAPファストバインドモードを使用しないでください。認証は、事前署名済みURLに含まれるBase64アクセスキーのみに基づいて行われます。ユーザ名とパスワードは、Base64アクセスキーをデコードしたすべてのユーザに公開されます。

認証方法は**nsswitch**で**LDAP**が有効になっている例

```
$curl -siku <user>:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>", "name":<user>,"key_time_to_live":"PT6H3M"}
```

APIをSVMのデータLIFではなく、クラスタ管理LIFに転送します。ユーザが独自のキーを生成できるようにする場合は、curlを使用するためのHTTP権限をユーザのロールに追加する必要があります。この権限は、S3 API権限に追加されます。

Active DirectoryまたはSMBサーバのS3アクセスを設定する

バケットポリシーステートメントで指定されたNASグループ、またはNASグループに属するユーザーにUIDとGIDが設定されていない場合、これらの属性が見つからないため検索は失敗します。Active DirectoryはUIDではなくSIDを使用します。SIDエントリをUIDにマッピングできない場合は、必要なデータをONTAPに取り込む必要があります。

これを行うには、"vserver active-directory create"を使用して、SVMがActive Directoryで認証し、必要なユーザおよびグループ情報を取得できるようにします。

または、"vserver cifs create"を使用して、Active Directoryドメインに SMB サーバを作成します。

ネームサーバーとオブジェクトストアで異なるドメイン名を使用している場合、検索エラーが発生する可能性があります。検索エラーを回避するには、NetAppではUPN形式のリソース認証に信頼できるドメインを使用することをお勧めします： `nasgroup/group@trusted_domain.com`信頼できるドメインとは、SMBサーバーの信頼済みドメインリストに追加されているドメインです。SMBサーバーリストで"優先する信頼済みドメインの追加、削除、変更"追加する方法については、こちらをご覧ください。

認証方法がドメインで、信頼されたドメインが **Active Directory** に構成されている場合にキーを生成します

UPN形式で指定されたユーザーで `s3/services/<svm_uuid>/users`エンドポイントを使用します。例：

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user@fqdn>,"key_time_to_live":"PT6H3M"}
```

APIをSVMのデータLIFではなく、クラスタ管理LIFに転送します。ユーザが独自のキーを生成できるようにする場合は、curlを使用するためのHTTP権限をユーザのロールに追加する必要があります。この権限は、S3 API権限に追加されます。

認証方法がドメインで、信頼できるドメインがない場合にキーを生成する

このアクションは、LDAPが無効になっている場合、または非POSIXユーザがUIDとGIDを設定していない場合に可能です。例：

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn]>,"key_time_to_live":"PT6H3M"}
```

APIをSVMのデータLIFではなく、クラスタ管理LIFに誘導してください。ユーザーが独自のキーを生成できるようにするには、curlを使用するためのHTTP権限をロールに追加する必要があります。この権限は、S3 API権限に加えて付与されます。信頼できるドメインがない場合にのみ、ユーザー名にオプションのドメイン値（@fqdn）を追加する必要があります。

LDAPまたはドメインユーザーが独自のONTAP S3アクセスキーを生成できるようにする

ONTAP 9.14.1以降では、ONTAP管理者がカスタム ロールを作成し、それをローカル グループ、ドメイン グループ、またはLightweight Directory Access Protocol（LDAP）グループに割り当てることができます。このようにすると、各グループに所属するユーザがS3クライアント アクセス用に自身のアクセス キーとシークレット キーを生成できるようになります。

カスタムロールを作成し、アクセスキー生成用のAPIを呼び出すユーザーに割り当てることができるように、ストレージVMでいくつかの設定手順を実行する必要があります。

LDAPが無効になっている場合は、"ONTAP S3アクセス用の外部ディレクトリサービスを設定する"ユーザーがアクセスキーを生成できるようにすることができます。

開始する前に

以下を確認してください。

1. S3サーバを含むS3対応Storage VMが作成されました。"S3用SVMの作成"を参照してください。
2. ストレージVMにバケットが作成されました。"バケットの作成"を参照してください。
3. ストレージVMにDNSが設定されています。"DNSサービスを設定する"を参照してください。
4. LDAPサーバの自己署名ルート認証局（CA）証明書がストレージVMにインストールされています。"SVMに自己署名ルートCA証明書をインストールする"を参照してください。
5. Storage VMでTLSが有効になっているLDAPクライアントが設定されています。"ONTAP NFSアクセス用のLDAPクライアント構成を作成する"を参照してください。
6. クライアント構成をVserverに関連付けます。"LDAPクライアント設定をONTAP NFS SVMに関連付ける"を参照してください。 `vserver services name-service ldap create`の詳細については、"ONTAPコマンド リファレンス"を参照してください。
7. データストレージVMを使用している場合は、VM上に管理ネットワークインターフェース（LIF）と、LIFのサービスポリシーを作成します。 `network interface create`と `network interface service-policy create`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

アクセス キー生成のためのユーザの設定

例 **1.** 手順

LDAPユーザ

1. ストレージVMのグループとパスワードの_ネームサービスデータベース_としてLDAPを指定します：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

`vserver services name-service ns-switch modify`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-services-name-service-ns-switch-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

2. S3ユーザREST APIエンドポイントへのアクセス権を持つカスタムロールを作成します：
`security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`この例では、 `s3-role`ロールがストレージVM `svm-1`上のユーザーに対して生成され、読み取り、作成、更新のすべてのアクセス権が付与されます。

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

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

3. `security login`コマンドを使用してLDAPユーザーグループを作成し、S3ユーザーREST APIエンドポイントにアクセスするための新しいカスタムロールを追加します。"ONTAPコマンド リファレンス"の `security login create`の詳細をご覧ください。

```
security login create -user-or-group-name <ldap-group-name>
-application http -authentication-method nsswitch -role <custom-
role-name> -is-ns-switch-group yes
```

この例では、LDAPグループ `ldap-group-1`が `svm-1`に作成され、カスタムロール `s3role`がAPIエンドポイントにアクセスするために追加され、高速バインドモードでのLDAPアクセスが有効になります。

```
security login create -user-or-group-name ldap-group-1 -application
http -authentication-method nsswitch -role s3role -is-ns-switch
-group yes -second-authentication-method none -vserver svm-1 -is
-ldap-fastbind yes
```

詳細については、"ONTAP NFS SVMのnsswitch認証にLDAP高速バインドを使用する"を参照してください。

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

LDAPグループにカスタムロールを追加すると、そのグループ内のユーザーにONTAP `/api/protocols/s3/services/{svm.uuid}/users`エンドポイントへの限定的なアクセスが許可されます。APIを呼び出すことで、LDAPグループのユーザーはS3クライアントにアクセスするための独自のアクセスキーとシークレットキーを生成できます。キーは自分自身のみ生成でき、他のユーザー用には生成できません。

ドメイン ユーザ

1. S3ユーザREST APIエンドポイントへのアクセス権を持つカスタム ロールを作成します。

```
security login rest-role create -vserver <vserver-name> -role <custom-
role-name> -api "/api/protocols/s3/services/*/users" -access <access-
type>
```

この例では、 `s3-role`ロールがストレージVM `svm-1`上のユーザーに対して生成され、読み取り、作成、更新のすべてのアクセス権が付与されます。

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

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

1. `security login`コマンドを使用してドメインユーザーグループを作成し、S3ユーザーREST APIエンドポイントにアクセスするための新しいカスタムロールを追加します。"ONTAPコマンド リファレンス"の `security login create`の詳細をご覧ください。

```
security login create -vserver <vserver-name> -user-or-group-name
domain\<group-name> -application http -authentication-method domain
-role <custom-role-name>
```

この例では、ドメイングループ `domain\group1`が `svm-1`に作成され、カスタムロール `s3role`がAPIエンドポイントにアクセスするためにそのグループに追加されます。

```
security login create -user-or-group-name domain\group1 -application
http -authentication-method domain -role s3role -vserver svm-1
```

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

ドメイングループにカスタムロールを追加すると、そのグループ内のユーザーに ONTAP /api/protocols/s3/services/{svm.uuid}/users エンドポイントへの限定的なアクセスが許可されます。API を呼び出すことで、ドメイングループのユーザーは S3 クライアントにアクセスするための独自のアクセスキーとシークレットキーを生成できます。キーは自分自身のみ生成でき、他のユーザー用には生成できません。

S3ユーザまたはLDAPユーザによる独自のアクセス キーの生成

ONTAP 9.14.1以降では、独自のキーを生成できるロールが割り当てられているユーザは、S3クライアントにアクセスするための独自のアクセス キーとシークレット キーを生成できます。次のONTAP REST APIエンドポイントを使用すると、自分専用のキーを生成できます。

S3ユーザを作成してキーを生成

このREST API呼び出しでは、以下のメソッドとエンドポイントを使用します。このエンドポイントの詳細については、リファレンス "APIのドキュメント"をご覧ください。

HTTPメソッド	パス
POST	/api/protocols/s3/services/{svm.uuid}/users

ドメインユーザーの場合は、S3ユーザー名に次の形式を使用します： user@fqdn。ここで、 `fqdn`はドメインの完全修飾ドメイン名です。

Curlの例

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"user1@example.com"}'
```

JSON出力の例

```
{
  "records": [
    {
      "access_key": "4KX07KF7ML8YNWY01JWG",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

S3ユーザのキーを再生成

S3ユーザーが既に存在する場合は、アクセスキーとシークレットキーを再生成できます。このREST API呼び出しでは、以下のメソッドとエンドポイントを使用します。

HTTPメソッド	パス
PATCH	/api/protocols/s3/services/{svm.uuid}/users/{name}

Curlの例

```
curl
--request PATCH \
--location "https://$FQDN_IP
/api/protocols/s3/services/{svm.uuid}/users/{name} " \
--include \
--header "Authorization: Basic $BASIC_AUTH" \
--data '{"regenerate_keys":"True"}'
```

JSON出力の例

```
{
  "records": [
    {
      "access_key": "DX12U609DMRVD8U30Z1M",
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

著作権に関する情報

商標に関する情報