アクセスポリシーステートメントを作成または変更します

ONTAP 9

NetApp
April 24, 2024

目次

アクセスポリシーステートメントを作成または変更します

バケットとオブジェクトストアのサーバポリシーについて

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のサーバポリシーによって制御されます。ユーザまたは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あると考えられますが、ユーザやグループが多数ある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する方が簡単です。

バケットポリシーを変更する

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。アクセス制御の範囲はコンテナバケットなので、バケットが 1 つしかない場合は最も適しています。

作業を開始する前に

S3サーバとバケットを含むS3対応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。

このタスクについて

新しいユーザと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。その他のオプションについては、を参照してください `vserver object-store-server bucket policy` マニュアルページ

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できます。バケットの容量と QoS ポリシーグループの割り当てを変更することもできます。

ONTAP 9.9.1以降では、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場合の処理 `GetObjectTagging`、 `PutObjectTagging`および `DeleteObjectTagging` バケットまたはグループポリシーを使用して許可されている必要があります。

実行する手順 は、System ManagerまたはCLIを使用するインターフェイスによって異なります。

System Manager の略

手順

1. バケットを編集します。 * Storage > Bucket* をクリックし、目的のバケットをクリックして * Edit * をクリックします。 権限を追加または変更するときに、次のパラメータを指定できます。
   - * Principal *：アクセス権を付与するユーザまたはグループ。
   - 影響：ユーザまたはグループへのアクセスを許可または拒否します。
   - * Actions *：特定のユーザまたはグループに対してバケットで許可されているアクション。
   - * Resources *：アクセスが許可または拒否されてい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** および * *bketname* / * _ * 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、 **_bketname/*_readme.txt * と指定します。

   - * Conditions *（オプション）：アクセス試行時に評価される式。たとえば、アクセスを許可または拒否する IP アドレスを指定できます。

> 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、この変数は要求コンテキストのユーザ名に置き換えられ、そのユーザに対して設定されたとおりにポリシーアクションを実行できます。

CLI の使用

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`	この文では ' アクセスを許可または拒否できます
`-action`	を指定できます `*` すべてのアクション、または次の1つ以上のリストを意味します。 `GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl,GetObjectAcl, ListBucketMultipartUploads,` および `ListMultipartUploadParts`。

`-principal`	1 つ以上の S3 ユーザまたはグループのリスト。 • 最大 10 のユーザまたはグループを指定できます。 • S3グループを指定する場合は、の形式で指定する必要があります `group/group_name`. • `*` には、パブリックアクセス（アクセスキーとシークレットキーを使用しないアクセス）を指定できます。 • プリンシパルを指定しない場合、Storage VM内のすべてのS3ユーザにアクセスが許可されます。
`-resource`	バケットとバケットに含まれるすべてのオブジェクト。ワイルドカード文字 `*` および `?` リソースを指定するための正規表現を作成するために使用できます。リソースについては、ポリシーで変数を指定できます。これらのポリシー変数は、ポリシーが評価されるときにコンテキスト値に置き換えられるプレースホルダです。

オプションで、テキスト文字列をコメントとして指定できます `-sid` オプション

例

次の例では、Storage VM svm1.example.comと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と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、バケットポリシーの変数を指定できます。次の例は、Storage VM用のサーババケットポリシーステートメントを作成します。 `svm1` および `bucket1`、およびを指定します。 `${aws:username}` ポリシーリソースの変数として指定します。ポリシーが評価されると、ポリシー変数は要求コンテキストのユーザ名に置き換えられ、そのユーザに対して設定されたとおりにポリシーアクションを実行できます。たとえば、次のポリシーステートメントが評価されると、 `${aws:username}` は、S3処理を実行するユーザに置き換えられます。ユーザーが `user1` 操作を実行し、そのユーザーにアクセスを許可します。 `bucket1` として `bucket1/user1/*`。

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

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 1 つ以上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のポリシーをユーザのグループに関連付けることで、複数のバケット間のリソースアクセスの管理を簡易化することができます。

作業を開始する前に

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。

このタスクについて

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され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のポリシーを使用する場合は、ポリシー自体ではなく、グループ定義でプリンシパル（ユーザとグループ）を指定します。

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

- フルアクセス
- NoS3アクセス
- ReadOnlyAccess の略

また、新しいカスタムポリシーを作成し、新しいユーザと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。その他のオプションについては、を参照してください `vserver object-store-server policy` "コマンドリファレンス"。

ONTAP 9.9.1以降では、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場合の処理 `GetObjectTagging`、 `PutObjectTagging`および `DeleteObjectTagging` バケットまたはグループポリシーを使用して許可されている必要があります。

実行する手順 は、System ManagerまたはCLIを使用するインターフェイスによって異なります。

System Manager の略

- System Managerを使用して、オブジェクトストアサーバポリシー*を作成または変更します

手順

1. Storage VM を編集します。 * Storage > Storage VM* をクリックし、 Storage VM をクリックして * Settings * をクリックし、をクリックします S3 の下。
2. ユーザーの追加： [* 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、グループのリストから選択します。
   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。

      - グループ：アクセス権が付与されるグループ。
      - Effect ： 1 つ以上の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：特定のグループの 1 つ以上のバケット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。 例：
        - * は、 Storage VM 内のすべてのバケットへのアクセスを許可します。
        - * bucketname * および * 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 * を指定すると、特定のバケット内のオブジェクトへのアクセスが許可されます。
   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 の使用

- CLIを使用して、オブジェクトストアサーバポリシー*を作成または変更します

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`	この文では ' アクセスを許可または拒否できます

-action	を指定できます * すべてのアクション、または次の1つ以上のリストを意味します。 GetObject, PutObject, DeleteObject, ListBucket,GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads, および ListMultipartUploadParts。
-resource	バケットとバケットに含まれるすべてのオブジェクト。ワイルドカード文字 * および ? リソースを指定するための正規表現を作成するために使用できます。

オプションで、テキスト文字列をコメントとして指定できます -sid オプション

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のリストの末尾に追加され、順番に処理されます。後でステートメントを追加または変更する場合は、ステートメントのを変更するオプションがあります -index 処理順序を変更するための設定。

外部ディレクトリサービス用の**S3**アクセスの設定

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ました。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素化されます。

外部ディレクトリサービスに属するユーザグループに、ONTAPオブジェクトストレージ環境へのアクセスを提供できます。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イスで、IDおよびアクセス管理（IAM）のデータベースとサービスを提供します。アクセスを提供するには、ONTAP S3環境でLDAPグループを設定する必要があります。アクセスの設定が完了すると、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、を参照してください。 "LDAP の使用方法の概要"。

また、Active Directoryユーザグループを高速バインドモードに設定して、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接続を介して認証できるようにすることもできます。

作業を開始する前に

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前に、次のことを確認してください。

1. S3サーバを含むS3対応Storage VMが作成されている。を参照してください "S3 用の SVM を作成します"。
2. そのStorage VMにバケットが作成されている。を参照してください "バケットを作成する"。
3. Storage VMにDNSが設定されています。を参照してください "DNS サービスを設定する"。
4. LDAPサーバの自己署名ルート認証局（CA）証明書がStorage VMにインストールされている。を参照してください "自己署名ルート CA 証明書を SVM にインストールします"。

5. SVMでTLSを有効にしてLDAPクライアントが設定されている。を参照してください "LDAP クライアント設定を作成します" および "情報を取得するためのLDAPクライアント設定とSVMの関連付け"。

外部ディレクトリサービス用の**S3**アクセスの設定

1. グループのSVMの_name service database_ofとしてldapを指定し、ldapのパスワードを指定します。

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

このコマンドの詳細については、を参照してください "vserver services name-service ns-switch modify" コマンドを実行します

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

```
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`。このポリシーは、LDAPグループへのアクセスを許可します。 `group1` リソース（バケットとそのオブジェクト）に `buck1`。

```
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グループのユーザが `group1` S3クライアントからS3処理を実行できます。

認証に**LDAP**高速バインドモードを使用する

1. グループのSVMの_name service database_ofとしてldapを指定し、ldapのパスワードを指定します。

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

このコマンドの詳細については、を参照してください "vserver services name-service ns-switch modify" コマンドを実行します

2. S3バケットにアクセスするLDAPユーザの権限がバケットポリシーで定義されていることを確認します。詳細については、を参照してください "バケットポリシーを変更する"。
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クライアントで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 -エンコード(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. ユーザに権限が割り当てられているS3クライアントから基本的なS3処理を実行します。

LDAPユーザまたはドメインユーザが自分の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てローカルグループ、ドメイングループ、またはLightweight Directory Access Protocol（LDAP）グループに付与し、それらのグループに属するユーザがS3クライアントアクセス用に独自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することができます。

カスタムロールを作成してアクセスキーを生成するAPIを呼び出すユーザに割り当てるには、Storage VMでいくつかの設定手順を実行する必要があります。

作業を開始する前に

次の点を確認します。

1. S3サーバを含むS3対応Storage VMが作成されている。を参照してください "S3 用の SVM を作成します"。
2. そのStorage VMにバケットが作成されている。を参照してください "バケットを作成する"。
3. Storage VMにDNSが設定されています。を参照してください "DNS サービスを設定する"。
4. LDAPサーバの自己署名ルート認証局（CA）証明書がStorage VMにインストールされている。を参照してください "自己署名ルート CA 証明書を SVM にインストールします"。
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。を参照してください "LDAP クライアント設定を作成します" および。
6. クライアント設定をSVMに関連付けます。を参照してください "LDAP クライアント設定を SVM に関連付けます" および "vserver services name-service ldap createを使用して"。
7. データStorage VMを使用している場合は、管理ネットワークインターフェイス（LIF）とVM上に、LIFのサービスポリシーを作成します。を参照してください "ネットワークインターフェイスの作成" および "network interface service-policy createを実行します" コマンド

アクセスキー生成のためのユーザの設定

1. グループのStorage VMの_name service database_としてldapを指定し、ldapのパスワードを指定します。

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

   このコマンドの詳細については、を参照してください "vserver services name-service ns-switch modify" コマンドを実行します

2. S3ユーザREST APIエンドポイントへのアクセスを含む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、を使用しています `s3-role` Storage VMのユーザ用にロールが生成されました `svm-1`をクリックします。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
   ```

   このコマンドの詳細については、を参照してください "security login rest -role create" コマンドを実行します

3. security loginコマンドを使用してLDAPユーザグループを作成し、S3ユーザ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。このコマンドの詳細については、を参照してください "security login create を実行します" コマンドを実行します

   ```
   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` が作成された場所 `svm-1`、およびカスタムロール `s3role` 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LDAPアクセスを有効にします。

   ```
   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、を参照してください "nsswitch認証にLDAP高速バインドを使用できます"。

ドメインまたはLDAPグループにカスタムロールを追加すると、そのグループのユーザにONTAPへの制限付きアクセスが許可されます。 `/api/protocols/s3/services/{svm.uuid}/users` エンドポイント。APIを

呼び出すことで、ドメインまたはLDAPグループのユーザは、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。キーを生成できるのは自分だけで、他のユーザーには生成できません。

S3ユーザまたはLDAPユーザとして、独自のアクセスキーを生成

ONTAP 9.14.1以降では、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（管理者が独自のキーを生成するロールをユーザに許可している場合）。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。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次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他のメソッドの詳細については、リファレンスを参照してください。 "APIドキュメント"。

HTTP メソッド	パス
投稿（ Post ）	/api/protocols/s3/services/｛svm.uuid｝/users

カールの例

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

JSON 出力例


```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```