Create or modify access policy statements

ONTAP 9

NetApp
June 04, 2024

Table of Contents

Create or modify access policy statements . . . 1
About bucket and object store server policies . . . 1
Modify a bucket policy . . . 1
Create or modify an object store server policy . . . 4
Configure S3 access for external directory services . . . 6
Enable LDAP or domain users to generate their own S3 access keys . . . 8

Create or modify access policy statements

About bucket and object store server policies

User and group access to S3 resources is controlled by bucket and object store server policies. If you have a small number of users or groups, controlling access at the bucket level is probably sufficient, but if you have many users and groups, it is easier to control access at the object store server level.

Modify a bucket policy

You can add access rules to the default bucket policy. The scope of its access control is the containing bucket, so it is most appropriate when there is a single bucket.

Before you begin

An S3-enabled storage VM containing an S3 server and a bucket must already exist.

You must have already created users or groups before granting permissions.

About this task

You can add new statements for new users and groups, or you can modify the attributes of existing statements. For more options, see the `vserver object-store-server bucket policy` man pages.

User and group permissions can be granted when the bucket is created or as needed later. You can also modify the bucket capacity and QoS policy group assignment.

Beginning with ONTAP 9.9.1, if you plan to support AWS client object tagging functionality with the ONTAP S3 server, the actions `GetObjectTagging`, `PutObjectTagging`, and `DeleteObjectTagging` need to be allowed using the bucket or group policies.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Steps

1. Edit the bucket: click **Storage > Buckets**, click the desired bucket, and then click **Edit**. When adding or modifying permissions, you can specify the following parameters:
   - **Principal**: the user or group to whom access is granted.
   - **Effect**: allows or denies access to a user or group.
   - **Actions**: permissible actions in the bucket for a given user or group.
   - **Resources**: paths and names of objects within the bucket for which access is granted or denied.

     The defaults ***bucketname*** and ***bucketname/**** grant access to all objects in the bucket. You can also grant access to single objects; for example, ***bucketname/*_readme.txt**.
   - **Conditions** (optional): expressions that are evaluated when access is attempted. For example, you can specify a list of IP addresses for which access will be allowed or denied.

> Beginning with ONTAP 9.14.1, you can specify variables for the bucket policy in the **Resources** field. These variables are placeholders that are replaced with contextual values when the policy is evaluated. For example, If `${aws:username}` is specified as a variable for a policy, then this variable is replaced with the request context username, and the policy action can be performed as configured for that user.

CLI

Steps

1. Add a statement to a bucket policy:

```
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]
```

The following parameters define access permissions:

`-effect`	The statement may allow or deny access
`-action`	You can specify `*` to mean all actions, or a list of one or more of the following: `GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl,GetObjectAcl, ListBucketMultipartUploads,` and `ListMultipartUploadParts`.

`-principal`	A list of one or more S3 users or groups. • A maximum of 10 users or groups can be specified. • If an S3 group is specified, it must be in the form `group/group_name`. • `*` can be specified to mean public access; that is, access without an access-key and secret-key. • If no principal is specified, all S3 users in the storage VM are granted access.
`-resource`	The bucket and any object it contains. The wildcard characters `*` and `?` can be used to form a regular expression for specifying a resource. For a resource, you can specify variables in a policy. These are policy variables are placeholders that are replaced with the contextual values when the policy is evaluated.

You can optionally specify a text string as comment with the `-sid` option.

Examples

The following example creates an object store server bucket policy statement for the storage VM svm1.example.com and bucket1 which specifies allowed access to a readme folder for object store server user user1.

```
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"
```

The following example creates an object store server bucket policy statement for the storage VM svm1.example.com and bucket1 which specifies allowed access to all objects for object store server group group1.

```
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"
```

Beginning with ONTAP 9.14.1, you can specify variables for a bucket policy. The following example creates a server bucket policy statement for the storage VM `svm1` and `bucket1`, and specifies `${aws:username}` as a variable for a policy resource. When the policy is evaluated, the policy variable is replaced with the request context username, and the policy action can be performed as configured for that user. For example, when the following policy statement is evaluated, `${aws:username}` is replaced with the user performing the S3 operation. If a user `user1` performs the operation, that user is granted access to `bucket1` as `bucket1/user1/*`.

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

Create or modify an object store server policy

You can create policies that can apply to one or more buckets in an object store. Object store server policies can be attached to groups of users, thereby simplifying the management of resource access across multiple buckets.

Before you begin

An S3-enabled SVM containing an S3 server and a bucket must already exist.

About this task

You can enable access policies at the SVM level by specifying a default or custom policy in an object storage server group. The policies do not take effect until they are specified in the group definition.

> When you use object storage server policies, you specify principals (that is, users and groups) in the group definition, not in the policy itself.

There are three read-only default policies for access to ONTAP S3 resources:

- FullAccess
- NoS3Access
- ReadOnlyAccess

You can also create new custom policies, then add new statements for new users and groups, or you can modify the attributes of existing statements. For more options, see the `vserver object-store-server policy` command reference.

Beginning with ONTAP 9.9.1, if you plan to support AWS client object tagging functionality with the ONTAP S3 server, the actions `GetObjectTagging`, `PutObjectTagging`, and `DeleteObjectTagging` need to be allowed using the bucket or group policies.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Use System Manager to create or modify an object store server policy

Steps

1. Edit the storage VM: click **Storage > storage VMs**, click the storage VM, click **Settings** and then click ✎ under S3.
2. Add a user: click **Policies**, then click **Add**.
   a. Enter a policy name and select from a list of groups.
   b. Select an existing default policy or add a new one.

      When adding or modifying a group policy, you can specify the following parameters:

      - Group: the groups to whom access is granted.
      - Effect: allows or denies access to one or more groups.
      - Actions: permissible actions in one or more buckets for a given group.
      - Resources: paths and names of objects within one or more buckets for which access is granted or denied. For example:
        - ***** grants access to all buckets in the storage VM.
        - **bucketname** and **bucketname/*** grant access to all objects in a specific bucket.
        - **bucketname/readme.txt** grants access to an object in a specific bucket.

   c. If desired, add statements to existing policies.

CLI

Use the CLI to create or modify an object store server policy

Steps

1. Create an object storage server policy:

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

2. Create a statement for the policy:

   ```
   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]
   ```

   The following parameters define access permissions:

`-effect`	The statement may allow or deny access

`-action`	You can specify `*` to mean all actions, or a list of one or more of the following: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`,`GetBucketAcl`, `GetObjectAcl`, `ListAllMyBuckets`, `ListBucketMultipartUploads`, and `ListMultipartUploadParts`.
`-resource`	The bucket and any object it contains. The wildcard characters `*` and `?` can be used to form a regular expression for specifying a resource.

You can optionally specify a text string as comment with the `-sid` option.

By default, new statements are added to the end of the list of statements, which are processed in order. When you add or modify statements later, you have the option to modify the statement's `-index` setting to change the processing order.

Configure S3 access for external directory services

Beginning with ONTAP 9.14.1, services for external directories have been integrated with ONTAP S3 object storage. This integration simplifies user and access management through external directory services.

You can provide user groups belonging to an external directory service with access to your ONTAP object storage environment. Lightweight Directory Access Protocol (LDAP) is an interface for communicating with directory services, such as Active Directory, that provide a database and services for identity and access management (IAM). To provide access, you need to configure LDAP groups in your ONTAP S3 environment. After you have configured access, the group members have permissions to ONTAP S3 buckets. For information about LDAP, see Overview of using LDAP.

You can also configure Active Directory user groups for fast bind mode, so that user credentials can be validated and third-party and open-source S3 applications can be authenticated over LDAP connections.

Before you begin

Ensure the following before configuring LDAP groups and enabling the fast bind mode for group access:

1. An S3-enabled storage VM containing an S3 server has been created. See Create an SVM for S3.
2. A bucket has been created in that storage VM. See Create a bucket.
3. DNS is configured on the storage VM. See Configure DNS services.
4. A self-signed root certification authority (CA) certificate of the LDAP server is installed on the storage VM. See Install the self-signed root CA certificate on the SVM.
5. An LDAP client is configured with TLS enabled on the SVM. See Create an LDAP client configuration and Associate the LDAP client configuration with SVMs for information.

Configure S3 access for external directory services

1. Specify LDAP as the *name service database* of the SVM for the group and password to LDAP:

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

   For more information about this command, see the vserver services name-service ns-switch modify command.

2. Create an object store bucket policy statement with the `principal` set to the LDAP group to which you want to grant access:

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

   Example: The following example creates a bucket policy statement for `buck1`. The policy allows access for the LDAP group `group1` to the resource (bucket and its objects) `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. Verify that a user from the LDAP group `group1` is able to the perform S3 operations from the S3 client.

Use LDAP fast bind mode for authentication

1. Specify LDAP as the *name service database* of the SVM for the group and password to LDAP:

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

   For more information about this command, see the vserver services name-service ns-switch modify command.

2. Ensure that an LDAP user accessing the S3 bucket has permissions defined in the bucket-policies. For more information, see Modify a bucket policy.
3. Verify that a user from the LDAP group can perform the following operations:
   a. Configure the access key on the S3 client in this format:
   `"NTAPFASTBIND" + base64-encode(user-name:password)`
   Example: `"NTAPFASTBIND"` + base64-encode(ldapuser:password), which results in `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

      The S3 client might prompt for a secret key. In the absence of a secret key, any password of at least 16 characters can be entered.

   b. Perform basic S3 operations from the S3 client for which the user has permissions.

Enable LDAP or domain users to generate their own S3 access keys

Beginning with ONTAP 9.14.1, as an ONTAP administrator, you can create custom roles and grant them to local or domain groups or Lightweight Directory Access Protocol (LDAP) groups, so that the users belonging to those groups can generate their own access and secret keys for S3 client access.

You have to perform a few configuration steps on your storage VM, so that the custom role can be created and assigned to the user that invokes the API for access key generation.

Before you begin

Ensure the following:

1. An S3-enabled storage VM containing an S3 server has been created. See Create an SVM for S3.
2. A bucket has been created in that storage VM. See Create a bucket.
3. DNS is configured on the storage VM. See Configure DNS services.
4. A self-signed root certification authority (CA) certificate of the LDAP server is installed on the storage VM. See Install the self-signed root CA certificate on the SVM.
5. An LDAP client is configured with TLS enabled on the storage VM. See Create an LDAP client configuration and .
6. Associate the client configuration with the Vserver. See Associate the LDAP client configuration with SVMs and vserver services name-service ldap create.
7. If you are using a data storage VM, create a management network interface (LIF) and on the VM, and also a service policy for the LIF. See the network interface create and network interface service-policy create commands.

Configure users for access key generation

1. Specify LDAP as the *name service database* of the storage VM for the group and password to LDAP:

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

For more information about this command, see the vserver services name-service ns-switch modify command.

2. Create a custom role with access to S3 user REST API endpoint:
`security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`
In this example, the `s3-role` role is generated for users on the storage VM `svm-1`, to which all access rights, read, create, and update are granted.

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

For more information about this command, see the security login rest-role create command.

3. Create an LDAP user group with the security login command and add the new custom role for accessing the S3 user REST API endpoint. For more information about this command, see the security login create command.

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

In this example, the LDAP group `ldap-group-1` is created in `svm-1`, and the custom role `s3role` is added to it for accessing the API endpoint, along with enabling LDAP access in the fast bind mode.

```
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
```

For more information, see Use LDAP fast bind for nsswitch authentication.

Adding the custom role to the domain or LDAP group allows users in that group a limited access to the ONTAP `/api/protocols/s3/services/{svm.uuid}/users` endpoint. By invoking the API, the domain or LDAP group users can generate their own access and secret keys to access the S3 client. They can generate the keys for only themselves and not for other users.

As an S3 or LDAP user, generate your own access keys

Beginning with ONTAP 9.14.1, you can generate your own access and secret keys for accessing S3 clients, if your administrator has granted you the role to generate your own keys. You can generate keys for only yourself

by using the following ONTAP REST API endpoint.

HTTP method and endpoint

This REST API call uses the following method and endpoint. For information about the other methods of this endpoint, see the reference API documentation.

HTTP method	Path
POST	/api/protocols/s3/services/{svm.uuid}/users

Curl example

```
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 output example

```
{
  "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"
}
```

Copyright information

Trademark information