Add storage capacity to an S3-enabled SVM

ONTAP 9

NetApp
May 13, 2022

Table of Contents

Add storage capacity to an S3-enabled SVM

Create a bucket

S3 objects are kept in *buckets*--they are not nested as files inside a directory inside other directories.

Before you begin

An SVM containing an S3 server must already exist.

About this task

When you create a bucket, you have two provisioning options:

- Let ONTAP select the underlying aggregates and FlexGroup components (default)
  - ONTAP creates and configures a FlexGroup volume for the first bucket by automatically selecting the aggregates. It will automatically select the highest service level available for your platform, or you can specify the storage service level. Any additional buckets you add later in the SVM will have the same underlying FlexGroup volume.
  - Alternatively, you can specify whether the bucket will be used for tiering, in which case ONTAP tries to select low-cost media with optimal performance for the tiered data.
- You select the underlying aggregates and FlexGroup components (requires advanced privilege command options)
  - You have the option to manually select the aggregates on which the bucket and containing FlexGroup volume must be created, and then specifying the number of constituents on each aggregate. When adding additional buckets:
    - If you specify aggregates and constituents for a new bucket, a new FlexGroup will be created for the new bucket.
    - If you do not specify aggregates and constituents for a new bucket, the new bucket will be added to an existing FlexGroup. See the FlexGroup documentation for more information.

    FlexGroup volumes management

  When you specify aggregates and constituents when creating a bucket, no QoS policy groups, default or custom, are applied. You can do so later with the `vserver object-store-server bucket modify` command.

Note: If you are serving buckets from Cloud Volumes ONTAP, it is strongly recommended that you manually select the underlying aggregates to ensure that they are using one node only. Using aggregates from both nodes can impact performance, because the nodes will be in geographically separated availability zones and hence susceptible to latency issues.

Storage service levels are predefined adaptive Quality of Service (QoS) policy groups, with *value*, *performance*, and *extreme* default levels. Instead of one of the default storage service levels, you can also define a custom QoS policy group and apply it to a bucket.

Storage service definitions

If you are configuring local capacity tiering, you create buckets and users in a data SVM, not in the system SVM where the S3 server is located.

See the `vserver object-store-server bucket` man pages for additional configuration and display options.

Steps

1. If you plan to select aggregates and FlexGroup components yourself, set the privilege level to advanced (otherwise, admin privilege level is sufficient): `set -privilege advanced`
2. Create a bucket:

   `vserver object-store-server bucket create -vserver` *`svm_name`* `-bucket` *`bucket_name`* `[-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

   The SVM name can be either a data SVM or `Cluster` (the system SVM name) if you are configuring local tiering.

   If you specify no options, ONTAP creates a 5GB bucket with the service level set to the highest level available for your system.

   If you want ONTAP to create a bucket based on performance or usage, use one of the following options:

   - service level

     Include the `-storage-service-level` option with one of the following values: `value`, `performance`, or `extreme`.

   - tiering

     Include the `-used-as-capacity-tier true` option.

   If you want to specify the aggregates on which to create the underlying FlexGroup volume, use the following options:

   - The `-aggr-list` parameter specifies the list of aggregates to be used for FlexGroup volume constituents.

     Each entry in the list creates a constituent on the specified aggregate. You can specify an aggregate multiple times to have multiple constituents created on the aggregate.

     For consistent performance across the FlexGroup volume, all of the aggregates must use the same disk type and RAID group configurations.

   - The `-aggr-list-multiplier` parameter specifies the number of times to iterate over the aggregates that are listed with the `-aggr-list` parameter when creating a FlexGroup volume.

     The default value of the `-aggr-list-multiplier` parameter is 4.

3. Add a QoS policy group if needed:

   `vserver object-store-server bucket modify -bucket` *`bucket_name`* `-qos-policy -group` *`qos_policy_group`*

4. Verify bucket creation:

```
vserver object-store-server bucket show [-instance]
```

Example

The following example creates a bucket for SVM vs1 of size 1TB and specifying the aggregate:

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

Create an S3 user

User authorization is required on all ONTAP object stores in order to restrict connectivity to authorized clients.

What you'll need

An S3-enabled SVM must already exist.

About this task

An S3 user can be granted access to any bucket in an SVM but not in multiple SVMs.

When you create an S3 user, an access-key and a secret-key will be generated. They must be shared with the user along with the object store's FQDN and bucket name. S3 users' keys can be displayed with the `vserver object-store-server user show` command.

You can grant specific access permissions to S3 users in a bucket policy or an object server policy.

> When an object store server is created, a root user (UID 0) is created, a privileged user with access all buckets. Rather than administering ONTAP S3 as root user, it is a best practice to create an admin user role with specific privileges.

Step

1. Create an S3 user:

```
vserver object-store-server user create -vserver svm_name -user user_name [-
comment text]
```

Create or modify S3 groups

You can simplify bucket access by creating groups of users with appropriate access authorizations.

What you'll need

S3 users in an S3-enabled SVM must already exist.

About this task

Users in an S3 group can be granted access to any bucket in an SVM but not in multiple SVMs. Group access

permissions can be configured in two ways:

- At the bucket level

  After creating a group of S3 users, you specify group permissions in bucket policy statements and they apply only to that bucket.

- At the SVM level

  After creating a group of S3 users, you specify object server policy names in the group definition. Those policies determine the buckets and access for the group members.

Step

1. Create an S3 group:

   ```
   vserver object-store-server group create -vserver svm_name -name group_name
   -users user_name\(s\) [-policies policy_names] [-comment text\]
   ```

   The `-policies` option can be omitted in configurations with only one bucket in an object store; the group name can be added to the bucket policy.

   The `-policies` option can be added later with the `vserver object-store-server group modify` command after object storage server policies are created.

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.

What you'll need

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

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.

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 SVM 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.

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 SVM 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 SVM 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"
```

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.

What you'll need

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` man pages.

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.

Enable client access to S3 object storage

Enable ONTAP S3 access for remote FabricPool tiering

For ONTAP S3 to be used as a remote FabricPool capacity (cloud) tier, the ONTAP S3 administrator must provide information about the S3 server configuration to the remote ONTAP cluster administrator.

About this task

The following S3 server information is required to configure FabricPool cloud tiers:

- server name (FQDN)
- bucket name
- CA certificate
- access key
- password (secret access key)

In addition, the following networking configuration is required:

- There must be an entry for the remote ONTAP S3 server's hostname in the DNS server configured for the admin SVM, including the S3 server's FQDN name and the IP addresses on its LIFs.
- Intercluster LIFs must be configured on both local and remote clusters, although cluster peering is not required.

See the FabricPool documentation about configuring ONTAP S3 as a cloud tier.

Managing Storage Tiers By Using FabricPool

Enable ONTAP S3 access for local FabricPool tiering

For ONTAP S3 to be used as a local FabricPool capacity tier, you must define an object store based on the bucket you created, and then attach the object store to a performance tier aggregate to create a FabricPool.

What you'll need

You must have the ONTAP S3 server name and a bucket name, and the S3 server must have been created using cluster LIFs (with the `-vserver Cluster` parameter).

About this task

The object-store configuration contains information about the local capacity tier, including the S3 server and bucket names and authentication requirements.

An object-store configuration once created must not be reassociated with a different object-store or bucket. You can create multiple buckets for local tiers, but you cannot create multiple object stores in a single bucket.

A FabricPool license is not required for a local capacity tier.

Steps

1. Create the object store for the local capacity tier:

   ```
   storage aggregate object-store config create -object-store-name store_name
   -ipspace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
   -name bucket_name -access-key access_key -secret-password password
   ```

   - The `-container-name` is the S3 bucket you created.
   - The `-access-key` parameter authorizes requests to the ONTAP S3 server.
   - The `-secret-password` parameter (secret access key) authenticates requests to the ONTAP S3 server.
   - You can set the `-is-certificate-validation-enabled` parameter to `false` to disable certificate checking for ONTAP S3.

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name MyLocalObjStore -ipspace Cluster -provider-type
   ONTAP_S3 -server s3.example.com
   -container-name bucket1 -access-key myS3key -secret-password myS3pass
   ```

2. Display and verify the object store configuration information:

   ```
   storage aggregate object-store config show
   ```

3. Optional: To see how much data in a volume is inactive, follow the steps in Determining how much data in a volume is inactive by using inactive data reporting.

   Seeing how much data in a volume is inactive can help you decide which aggregate to use for FabricPool local tiering.

4. Attach the object store to an aggregate:

`storage aggregate object-store attach -aggregate aggr_name -object-store-name store_name`

You can use the `allow-flexgroup` **`true`** option to attach aggregates that contain FlexGroup volume constituents.

```
cluster1::> storage aggregate object-store attach
-aggregate aggr1 -object-store-name MyLocalObjStore
```

5. Display the object store information and verify that the attached object store is available:

`storage aggregate object-store show`

```
cluster1::> storage aggregate object-store show

Aggregate    Object Store Name    Availability State
---------    -----------------    ------------------
aggr1        MyLocalObjStore      available
```

Enable client access from an S3 app

For S3 client apps to access the ONTAP S3 server, the ONTAP S3 administrator must provide configuration information to the S3 user.

What you'll need

The S3 client app must be capable of authenticating with the ONTAP S3 server using the following AWS signature versions:

- Signature Version 4, ONTAP 9.8 and later
- Signature Version 2, ONTAP 9.11.1 and later

Other signature versions are not supported by ONTAP S3.

The ONTAP S3 administrator must have created S3 users and granted them access permissions, as an individual users or as a group member, in the bucket policy or the object storage server policy.

The S3 client app must be capable of resolving the ONTAP S3 server name, which requires that ONTAP S3 administrator provide the S3 server name (FQDN) and IP addresses for the S3 server's LIFs.

About this task

To access an ONTAP S3 bucket, a user on the S3 client app enters information provided by the ONTAP S3 administrator.

Beginning with ONTAP 9.9.1, the ONTAP S3 server supports the following AWS client functionality:

- user-defined object metadata

  A set of key-value pairs can be assigned to objects as metadata when they are created using PUT (or

POST). When a GET/HEAD operation is performed on the object, the user-defined metadata is returned along with the system metadata.

- object tagging

  A separate set of key-value pairs can be assigned as tags for categorizing objects. Unlike metadata, tags are created and read with REST APIs independently of the object, and they implemented when objects are created or any time after.

> To enable clients to get and put tagging information, the actions `GetObjectTagging`, `PutObjectTagging`, and `DeleteObjectTagging` need to be allowed using the bucket or group policies.

For more information, see the AWS S3 documentation.

Steps

1. Authenticate the S3 client app with the ONTAP S3 server by entering the S3 server name and the CA certificate.
2. Authenticate a user on the S3 client app by entering the following information:
   - S3 server name (FQDN) and bucket name
   - the user's access key and secret key