NetApp

S3 configuration with System Manager

ONTAP 9

NetApp
December 01, 2021

Table of Contents

S3 configuration with System Manager

ONTAP S3 configuration overview with System Manager

The topics in this section show you how to configure and manage S3 object storage services with ONTAP System Manager in ONTAP 9.8 and later releases.

Beginning with ONTAP 9.8, you can enable an ONTAP Simple Storage Service (S3) object storage server in an ONTAP cluster. For more information, see S3 support in ONTAP 9.

System Manager supports two on-premises use case scenarios for serving S3 object storage:

- FabricPool tier to a bucket on local cluster (tier to a local bucket) or remote cluster (cloud tier).
- S3 client app access to a bucket on the local cluster or a remote cluster.

For more information about FabricPool tiering, see FabricPool tier management overview with System Manager.

> (i) ONTAP S3 is appropriate if you want S3 capabilities on existing clusters without additional hardware and management. For deployments larger than 300TB, NetApp StorageGRID software continues to be the NetApp flagship solution for object storage. For more information, see the StorageGRID documentation.

When you create an S3 bucket using System Manager, ONTAP configures a default performance service level that is the highest available on your system. For example, on an AFF system, the default setting would be **Extreme**. Performance service levels are predefined adaptive Quality of Service (QoS) policy groups. Instead of one of the default service levels, you can specify a custom QoS policy group or no policy group.

Predefined adaptive QoS policy groups are:

- **Extreme**: Used for applications that expect the lowest latency and highest performance.
- **Performance**: Used for applications with modest performance needs and latency.
- **Value**: Used for applications for which throughput and capacity are more important than latency.
- **Custom**: Specify a custom QoS policy or no QoS policy.

If you select **Use for tiering**, no performance service levels are selected, and the system tries to select low-cost media with optimal performance for the tiered data.

See also: Use adaptive QoS policy groups.

ONTAP tries to provision this bucket on local tiers that have the most appropriate disks, satisfying the chosen service level. However, if you need to specify which disks to include in the bucket, consider configuring S3 object storage from the CLI by specifying the local tiers (aggregate). If you configure the S3 server from the CLI, you can still manage it with System Manager if desired. For more information, see the documentation for S3 configuration with the CLI.

Enable an S3 server on a storage

Add an S3 server to a new or existing storage VM for serving content to S3 clients.

An S3 server can coexist in a storage VM with other protocol servers, or you can create a new storage VM to isolate the namespace and workload.

Before you begin

You should be prepared to enter an S3 server name (FQDN) and IP addresses for interface role Data.

If you are using an external-CA signed certificate, you will be prompted to enter it during this procedure; you also have the option to use a system-generated certificate.

Steps

1. Enable S3 on a storage VM.

   a. Add a new storage VM: click **Storage > Storage VMs**, then click **Add**.

      If this is a new system with no existing storage VMs: click **Dashboard > Configure Protocols**.

      If you are adding an S3 server to an existing storage VM: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click ⚙ under **S3**.

   b. Click **Enable S3**, then enter the S3 Server Name.

      This will be the Fully Qualified Domain Name (FQDN) that clients will use.

   c. Select the certificate type.

      Whether you select system-generated certificate or one of your own, it will be required for client access.

   d. Enter the network interfaces.

2. If you selected the system-generated certificate, you see the certificate information when the new storage VM creation is confirmed. Click **Download** and save it for client access.

   ◦ The secret key will not be displayed again.

   ◦ If you need the certificate information again: click **Storage > Storage VMs**, select the storage VM, and click **Settings**.

Provision buckets

Add an S3 bucket for the new S3 object store or add additional buckets to an existing object store.

For remote client access, you must configure buckets in an S3-enabled storage VM. If you create a bucket in a storage VM that is not S3-enabled, it will only be available for local tiering.

> ⓘ Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

Steps

1. Add a new bucket on an S3-enabled storage VM.

   a. Click **Storage > Buckets**, then click **Add**.

   b. Enter a name, select the storage VM, and enter a size.

- If you click **Save** at this point, a bucket is created with these default settings:
  - No users are granted access to the bucket unless any group policies are already in effect.

    > You should not use the S3 root user to manage ONTAP object storage and share its permissions, because it has unlimited access to the object store. Instead, create a user or group with administrative privileges that you assign.

  - A Quality of Service (performance) level that is the highest available for your system.
- You can click **More Options** to configure user permissions and performance level when you configure the bucket, or you can modify these settings later.
  - You must have already created user and groups before using **More Options** to configure their permissions.
  - If you intend to use the S3 object store for FabricPool tiering, consider selecting **Use for tiering** (use low-cost media with optimal performance for the tiered data) rather than a performance service level.

2. On S3 client apps – another ONTAP system or an external 3rd-party app – verify access to the new bucket by entering the following:
   - The S3 server CA certificate.
   - The user's access key and secret key.
   - The S3 server FQDN name and bucket name.

Add S3 users and groups

Edit the storage VM to add users, and to add users to groups.

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 **Users**, then click **Add**.

   a. Enter a name and click **Save**.

   b. Be sure to save the access key and secret key, they will be required for access from S3 clients.

3. If desired, add a group: click **Groups**, then click **Add**.

   a. Enter a group name and select from a list of users.

   b. You can select an existing group policy or add one now, or you can add a policy later.

Manage user access to buckets

Edit the bucket to modify the list users with access to the bucket and specify their permissions.

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.

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

In ONTAP 9.9.1 and later releases, 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.

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.

Manage user access to S3-enabled storage VMs

Edit the storage VM to add a policy that controls user and group access permissions to multiple buckets.

You can add a group policy to manage access to one or more buckets in an S3-enabled storage VM, rather than managing access permissions for individual buckets. Doing so simplifies management when buckets are added or when access needs change.

You must have already created users and at least one group before granting permissions in a policy.

In ONTAP 9.9.1 and later releases, 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.

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.