Attach StorageGRID as a cloud tier

StorageGRID

NetApp
March 02, 2022

Table of Contents

Attach StorageGRID as a cloud tier

Information needed to attach StorageGRID as a cloud tier

Before you can attach StorageGRID as a cloud tier for FabricPool, you must perform some configuration steps in StorageGRID and obtain certain values.

About this task

The following table lists the information you must provide to ONTAP when you attach StorageGRID as a cloud tier for FabricPool. The topics in this section explain how to use the StorageGRID Grid Manager and Tenant Manager to obtain the information you need.

> The exact field names listed and the process you use to enter the required values in ONTAP depend on whether you are using the ONTAP CLI (storage aggregate object-store config create) or ONTAP System Manager (**Storage** > **Aggregates & Disks** > **Cloud Tier**).

For more information, refer to the following:

- TR-4598: FabricPool Best Practices in ONTAP 9.9.1
- ONTAP 9 Documentation

ONTAP field	Description
Object store name	Any unique and descriptive name. For example, `StorageGRID_Cloud_Tier`.
Provider type	StorageGRID (ONTAP System Manager) or `SGWS` (ONTAP CLI).
Port	The port that FabricPool will use when it connects to StorageGRID. You determine which port number to use when you define the StorageGRID load balancer endpoint. Create a load balancer endpoint for FabricPool
Server name	The fully qualified domain name (FQDN) for the StorageGRID load balancer endpoint. For example, `s3.storagegrid.company.com`. Note the following: • The domain name that you specify here must match the domain name on the CA certificate you upload for the StorageGRID load balancer endpoint. • The DNS record for this domain name must map to each IP address you will use to connect to StorageGRID. Configure the DNS server for StorageGRID IP addresses

ONTAP field	Description
Container name	The name of the StorageGRID bucket you will use with this ONTAP cluster. For example, `fabricpool-bucket`. You can create this bucket in the Tenant Manager or, starting with ONTAP 9.10 System Manager, you can create the bucket with the FabricPool setup wizard. Note the following: • The bucket name cannot be changed once the configuration is created. • The bucket cannot have versioning enabled. • You must use a different bucket for each ONTAP cluster that will tier data to StorageGRID. Create an S3 bucket and obtain an access key
Access key and secret password	The access key and secret access key for the StorageGRID tenant account. You generate these values in the Tenant Manager. Create an S3 bucket and obtain an access key
SSL	Must be enabled.
Object store certificate	The CA certificate you uploaded when you created the StorageGRID load balancer endpoint. **Note:** If an intermediate CA issued the StorageGRID certificate, you must provide the intermediate CA certificate. If the StorageGRID certificate was issued directly by the Root CA, you must provide the Root CA certificate. Create a load balancer endpoint for FabricPool

After you finish

After you have obtained the required StorageGRID information, you can go to ONTAP to add StorageGRID as a cloud tier, add the cloud tier as an aggregate, and set volume tiering policies.

Best practices for load balancing

Before attaching StorageGRID as a FabricPool cloud tier, you must use the StorageGRID Grid Manager to configure at least one load balancer endpoint.

What is load balancing?

When data is tiered from FabricPool to a StorageGRID system, StorageGRID uses a load balancer to manage the ingest and retrieval workload. Load balancing maximizes speed and connection capacity by distributing the FabricPool workload across multiple Storage Nodes.

The StorageGRID Load Balancer service is installed on all Admin Nodes and all Gateway Nodes and provides Layer 7 load balancing. It performs Transport Layer Security (TLS) termination of client requests, inspects the requests, and establishes new secure connections to the Storage Nodes.

The Load Balancer service on each node operates independently when forwarding client traffic to the Storage Nodes. Through a weighting process, the Load Balancer service routes more requests to Storage Nodes with higher CPU availability.

Although the StorageGRID Load Balancer service is the recommended load balancing mechanism, you might want to integrate a third-party load balancer instead. For information, contact your NetApp account representative or refer to TR-4626: StorageGRID third-party and global load balancers.

> The separate Connection Load Balancer (CLB) service on Gateway Nodes is deprecated and no longer recommended for use with FabricPool.

Best practices for StorageGRID load balancing

As a general best practice, each site in your StorageGRID system should include two or more nodes with the Load Balancer service. For example, a site might include two Gateway Nodes or both an Admin Node and a Gateway Node. Make sure that there is adequate networking, hardware, or virtualization infrastructure for each load-balancing node, whether you are using SG100 or SG1000 services appliances, bare metal nodes, or virtual machine (VM) based nodes.

You must configure a StorageGRID load balancer endpoint to define the port that Gateway Nodes and Admin Nodes will use for incoming and outgoing FabricPool requests.

Best practices for the load balancer endpoint certificate

When creating a load balancer endpoint for use with FabricPool, you should use HTTPS as the protocol. Communicating with StorageGRID without TLS encryption is supported but not recommended

You can then either upload a certificate that is signed by either a publicly trusted or a private certificate authority (CA), or you can generate a self-signed certificate. The certificate allows ONTAP to authenticate with StorageGRID.

As a best practice, you should use a CA server certificate to secure the connection. Certificates signed by a CA can be rotated nondisruptively.

When requesting a CA certificate for use with the load balancer endpoint, ensure that the domain name on the certificate matches the server name you enter in ONTAP for that load balancer endpoint. If possible, use a wildcard (*) to allow for virtual-host-style URLs. For example:

```
*.s3.storagegrid.company.com
```

When you add StorageGRID as a FabricPool cloud tier, you must install the same certificate to the ONTAP cluster, as well as the root and any subordinate certificate authority (CA) certificates.

> StorageGRID uses server certificates for a number of purposes. If you are connecting to the Load Balancer service, you can optionally use the S3 and Swift API certificate.

To learn more about the server certificate for a load balancing endpoint:

- Configure load balancer endpoints
- Hardening guidelines for server certificates

Best practices for high availability groups

Before attaching StorageGRID as a FabricPool cloud tier, you should use the StorageGRID Grid Manager to configure a high availability (HA) group.

What is a high availability (HA) group?

To ensure that the Load Balancer service is always available to manage FabricPool data, you can group the network interfaces of multiple Admin and Gateway Nodes into a single entity, known as a high availability (HA) group. If the active node in the HA group fails, another node in the group can continue to manage the workload.

Each HA group provides highly available access to the shared services on the associated nodes. For example, an HA group that consists of interfaces only on Gateway Nodes or on both Admin Nodes and Gateway Nodes provides highly available access to the shared Load Balancer service.

To create an HA group, you perform these general steps:

1. Select network interfaces for one or more Admin Nodes or Gateway Nodes. You can select the Grid Network interface (eth0), Client Network interface (eth2), or a VLAN interface.

   > If you plan to use a VLAN interface to segregate FabricPool traffic, a network administrator must first configure a trunk interface and the corresponding VLAN. Each VLAN is identified by a numeric ID or tag. For example, your network might use VLAN 100 for FabricPool traffic.

2. Assign one or more virtual IP (VIP) addresses to the group. Clients applications, such as FabricPool, can use any of these VIP addresses to connect to StorageGRID.
3. Specify one interface to be the Primary interface and determine the priority order for any Backup interfaces. The Primary interface is the active interface unless a failure occurs.

If the HA group includes more than one interface and the Primary interface fails, the VIP addresses move to the first backup interface in the priority order. If that interface fails, the VIP addresses move to the next backup interface, and so on. This failover process generally takes only a few seconds and is fast enough that client applications should experience little impact and can rely on normal retry behaviors to continue operation.

When the failure is resolved and a higher priority interface becomes available again, the VIP addresses are automatically moved to the highest priority interface that is available.

Best practices for high availability (HA) groups

The best practices for creating a StorageGRID HA group for FabricPool depend on the workload, as follows:

- If you plan to use FabricPool with primary workload data, you must create a HA group that includes at least two load-balancing nodes to prevent data retrieval interruption.
- If you plan to use the FabricPool snapshot-only volume tiering policy or non-primary local performance tiers (for example, disaster recovery locations or NetApp SnapMirror® destinations), you can configure an HA group with only one node.

These instructions describe setting up an HA group for Active-Backup HA (one node is active and one node is backup). However, you might prefer to use DNS Round Robin or Active-Active HA. To learn the benefits of these other HA configurations, see Configuration options for HA groups.

Configure the DNS server for StorageGRID IP addresses

After configuring high availability groups and load balancer endpoints, you must ensure that the domain name system (DNS) for the ONTAP system includes a record to associate the StorageGRID server name (fully qualified domain name) to the IP address that FabricPool will use to make connections.

The IP address you enter in the DNS record depends on whether you are using an HA group of load-balancing nodes:

- If you have configured a HA group, FabricPool will connect to the virtual IP addresses of that HA group.
- If you are not using a HA group, FabricPool can connect to the StorageGRID Load Balancer service using the IP address of any Gateway Node or Admin Node.

You must also ensure that the DNS record references all required endpoint domain names, including any wildcard names.

Create a high availability (HA) group for FabricPool

When configuring StorageGRID for use with FabricPool, you can optionally create one or more high availability (HA) groups. An HA group consists of one or more network interfaces on Admin Nodes, Gateway Nodes, or both.

What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have the Root Access permission.
- If you plan to use a VLAN, you have created the VLAN interface. See Configure VLAN interfaces.

About this task

Each HA group uses virtual IP addresses (VIPs) to provide highly available access to the shared services on the associated nodes.

For details about this task, see Manage high availability groups.

Steps

1. Select **CONFIGURATION** > **Network** > **High availability groups**.
2. Select **Create**.
3. Enter a unique name and optionally a description.
4. Select one or more interfaces to add to this HA group.

   Use the column headers to sort the rows, or enter a search term to locate interfaces more quickly.

5. Determine the Primary interface and any backup interfaces for this HA group.

   Drag and drop rows to change the values in the **Priority order** column.

The first interface in the list is the Primary interface. The Primary interface is the active interface unless a failure occurs.

If the HA group includes more than one interface and the active interface fails, the VIP addresses move to the first backup interface in the priority order. If that interface fails, the VIP addresses move to the next backup interface, and so on. When failures are resolved, the VIP addresses move back to highest priority interface available.

6. Specify the VIP subnet in CIDR notation—an IPv4 address followed by a slash and the subnet length (0-32).

   The network address must not have any host bits set. For example, `192.16.0.0/22`.

7. Optionally, if the ONTAP IP addresses used to access StorageGRID are not on the same subnet as the StorageGRID VIP addresses, enter the StorageGRID VIP local gateway IP address. The local gateway IP address must be within the VIP subnet.
8. Enter one or more virtual IP addresses for the HA group. You can add up to 10 IP addresses. All VIPs must be within the VIP subnet.

   You must provide at least one IPv4 address. Optionally, you can specify additional IPv4 and IPv6 addresses.

9. Select **Create HA group** and then select **Finish**.

Create a load balancer endpoint for FabricPool

When configuring StorageGRID for use with FabricPool, you must configure a load balancer endpoint and upload the load balancer endpoint certificate, which is used to secure the connection between ONTAP and StorageGRID.

What you'll need

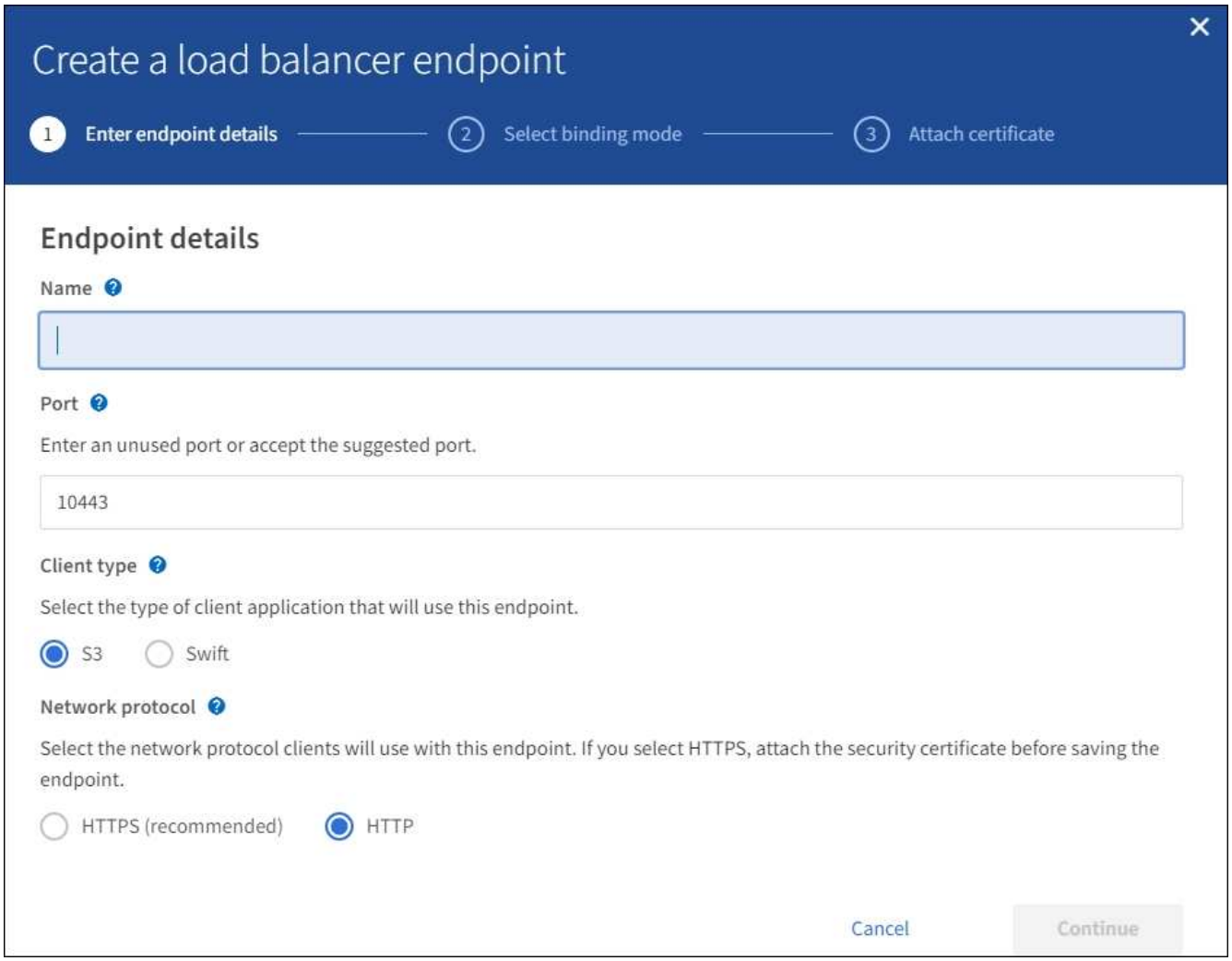
- You are signed in to the Grid Manager using a supported web browser.
- You have the Root access permission.
- You have the following files:
  - Server Certificate: The custom server certificate file.
  - Server Certificate Private Key: The custom server certificate private key file.
  - CA Bundle: A single optional file containing the certificates from each intermediate issuing certificate authority (CA). The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.

About this task

For details about this task, see Configure load balancer endpoints.

Steps

1. Select **CONFIGURATION** > **Network** > **Load balancer endpoints**.
2. Select **Create**.



3. Enter endpoint details.

Field	Description
Name	A descriptive name for the endpoint
Port	The StorageGRID port you want to use for load balancing. This field defaults to 10433, but you can enter any unused external port. If you enter 80 or 443, the endpoint is configured only on Gateway Nodes, since these ports are reserved on Admin Nodes. **Note:** Ports used by other grid services are not permitted. See the Network port reference. You must provide this same port number to ONTAP when you attach StorageGRID as a FabricPool cloud tier.
Client type	Select **S3**.
Network protocol	Select **HTTPS**. **Note**: Using **HTTP** is supported but not recommended.

4. Select **Continue**.
5. Specify the binding mode.

   Use the **Global** setting (recommended) or restrict the accessibility of this endpoint to one of the following:

   - Specific network interfaces of specific nodes.
   - Specific high availability (HA) virtual IP addresses (VIPs). Use this selection only if you require much higher levels of isolation of workloads.
6. Select **Continue**.
7. Select **Upload Certificate** (recommended) and then browse to your server certificate, certificate private key, and optional CA bundle.
8. Select **Create**.

Changes to an endpoint certificate can take up to 15 minutes to be applied to all nodes.

Create a tenant account for FabricPool

You must create a tenant account in the Grid Manager for FabricPool use.

What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have specific access permissions.

About this task

Tenant accounts allow client applications to store and retrieve objects on StorageGRID. Each tenant account has its own account ID, authorized groups and users, buckets, and objects.

You can use the same tenant account for multiple ONTAP clusters. Or, you can create a dedicated tenant account for each ONTAP cluster as required.

These instructions assume that you have configured single sign-on (SSO) for the Grid Manager. If SSO is not enabled, use these instructions to create a tenant account instead.

Steps

1. Select **TENANTS**.
2. Select **Create**.
3. Enter a display name and a description.
4. Select **S3**.
5. Leave the **Storage quota** field blank.
6. Select **Allow platform services** to enable the use of platform services.

   If platform services are enabled, a tenant can use features, such as CloudMirror replication, that access external services.
7. Do not select **Use own identity source**.
8. Do not select **Allow S3 Select**.

9. Select an existing federated group from the Grid Manager to have the initial Root Access permission for the tenant.
10. Select **Create tenant**.

Create an S3 bucket and obtain an access key

Before using StorageGRID with a FabricPool workload, you must create an S3 bucket for your FabricPool data. You also need to obtain an access key and secret access key for the tenant account you will use for FabricPool.

What you'll need

- You have created a tenant account for FabricPool use.

About this task

These instructions describe how to use the StorageGRID Tenant Manager to create a bucket and obtain access keys. You can also perform these tasks using the Tenant Management API or the StorageGRID S3 REST API. Or, if you are using ONTAP 9.10, you can create the bucket using the FabricPool setup wizard instead.

To learn more:

- Use a tenant account
- Use S3

Steps

1. Sign in to the Tenant Manager.

   You can do either of the following:

   - From the Tenant Accounts page in the Grid Manager, select the **Sign in** link for the tenant, and enter your credentials.
   - Enter the URL for the tenant account in a web browser, and enter your credentials.

2. Create an S3 bucket for FabricPool data.

   You must create a unique bucket for each ONTAP cluster you plan to use.

   a. Select **STORAGE (S3)** > **Buckets**.
   b. Select **Create bucket**.
   c. Enter the name of the StorageGRID bucket you will use with FabricPool. For example, `fabricpool-bucket`.

      > You cannot change the bucket name after creating the bucket.

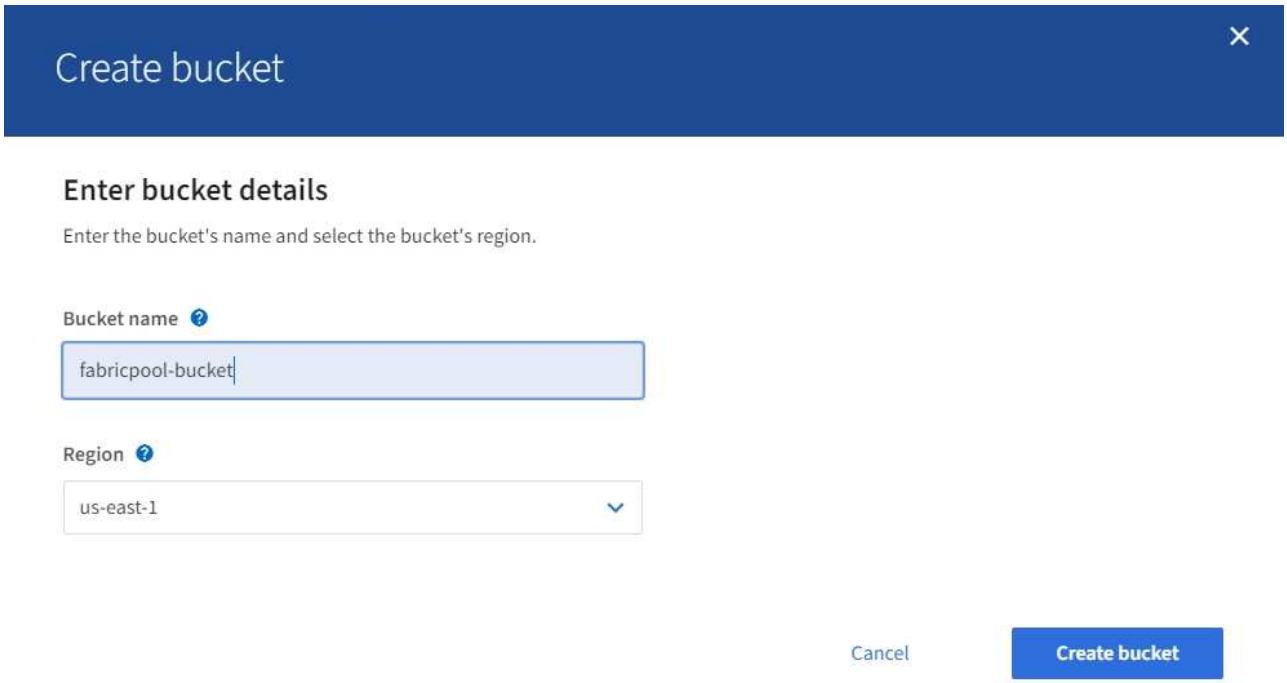
      Bucket names must comply with these rules:

      - Must be unique across each StorageGRID system (not just unique within the tenant account).
      - Must be DNS compliant.
      - Must contain at least 3 and no more than 63 characters.

- Can be a series of one or more labels, with adjacent labels separated by a period. Each label must start and end with a lowercase letter or a number and can only use lowercase letters, numbers, and hyphens.
- Must not look like a text-formatted IP address.
- Should not use periods in virtual hosted style requests. Periods will cause problems with server wildcard certificate verification.

d. Select the region for this bucket.

By default, all buckets are created in the `us-east-1` region.



e. Select **Create bucket**.

> For FabricPool buckets, the recommended bucket consistency level is “read-after-new-write.” The “available” consistency level is not recommended. See Change the consistency level.

3. Create an access key and a secret access key.
   a. Select **STORAGE (S3)** > **My access keys**.
   b. Select **Create key**.
   c. Select **Create access key**.
   d. Copy the access key ID and the secret access key to a safe location, or select **Download .csv** to save a spreadsheet file containing the access key ID and secret access key.

   You will enter these values in ONTAP when you configure StorageGRID as a FabricPool cloud tier.

> If you create a new access key and secret access key in the future, remember to update the corresponding values in ONTAP immediately to ensure that ONTAP can store and retrieve data in StorageGRID without interruption.