NetApp

Manage tenants

StorageGRID

NetApp
May 03, 2022

Table of Contents

Manage tenants

Manage tenants

As a grid administrator, you create and manage the tenant accounts that S3 and Swift clients use to store and retrieve objects, monitor storage usage, and manage the actions that clients are able to perform using your StorageGRID system.

What are tenant accounts?

Tenant accounts allow client applications that use the Simple Storage Service (S3) REST API or the Swift REST API to store and retrieve objects on StorageGRID.

Each tenant account supports the use of a single protocol, which you specify when you create the account. To store and retrieve objects to a StorageGRID system with both protocols, you must create two tenant accounts: one for S3 buckets and objects, and one for Swift containers and objects. Each tenant account has its own account ID, authorized groups and users, buckets or containers, and objects.

Optionally, you can create additional tenant accounts if you want to segregate the objects stored on your system by different entities. For example, you might set up multiple tenant accounts in either of these use cases:

- **Enterprise use case:** If you are administering a StorageGRID system in an enterprise application, you might want to segregate the grid's object storage by the different departments in your organization. In this case, you could create tenant accounts for the Marketing department, the Customer Support department, the Human Resources department, and so on.

  > (i) If you use the S3 client protocol, you can simply use S3 buckets and bucket policies to segregate objects between the departments in an enterprise. You do not need to use tenant accounts. See the instructions for implementing S3 client applications for more information.

- **Service provider use case:** If you are administering a StorageGRID system as a service provider, you can segregate the grid's object storage by the different entities that will lease the storage on your grid. In this case, you would create tenant accounts for Company A, Company B, Company C, and so on.

Create and configure tenant accounts

When you create a tenant account, you specify the following information:

- Display name for the tenant account.
- Which client protocol will be used by the tenant account (S3 or Swift).
- For S3 tenant accounts: Whether the tenant account has permission to use platform services with S3 buckets. If you permit tenant accounts to use platform services, you must ensure that the grid is configured to support their use. See "Managing platform services."
- Optionally, a storage quota for the tenant account—the maximum number of gigabytes, terabytes, or petabytes available for the tenant's objects. If the quota is exceeded, the tenant cannot create new objects.

  > (i) A tenant's storage quota represents a logical amount (object size), not a physical amount (size on disk).

- If identity federation is enabled for the StorageGRID system, which federated group has Root access permission to configure the tenant account.

- If single sign-on (SSO) is not in use for the StorageGRID system, whether the tenant account will use its own identity source or share the grid's identity source, and the initial password for the tenant's local root user.

After a tenant account is created, you can perform the following tasks:

- **Manage platform services for the grid**: If you enable platform services for tenant accounts, ensure that you understand how platform services messages are delivered and the networking requirements that the use of platform services place on your StorageGRID deployment.

- **Monitor a tenant account's storage usage**: After tenants begin using their accounts, you can use Grid Manager to monitor how much storage each tenant consumes.

> ⓘ A tenant's storage usage values might become out of date if nodes are isolated from other nodes in the grid. The totals will be updated when network connectivity is restored.

  If you have set quotas for tenants, you can enable the **Tenant quota usage high** alert to determine if tenants are consuming their quotas. If enabled, this alert is triggered when a tenant has used 90% of its quota. For more information, see the alerts reference in the instructions for monitoring and troubleshooting StorageGRID.

- **Configure client operations**: You can configure if some types of client operations are forbidden.

Configure S3 tenants

After an S3 tenant account is created, tenant users can access the Tenant Manager to perform tasks such as the following:

- Setting up identity federation (unless the identity source is shared with the grid) and creating local groups and users

- Managing S3 access keys

- Creating and managing S3 buckets

- Monitoring storage usage

- Using platform services (if enabled)

> ⓘ S3 tenant users can create and manage S3 access key and buckets with the Tenant Manager, but they must use an S3 client application to ingest and manage objects.

Configure Swift tenants

After a Swift tenant account is created, the tenant's root user can access the Tenant Manager to perform tasks such as the following:

- Setting up identity federation (unless the identity source is shared with the grid), and creating local groups and users

- Monitoring storage usage

Swift users must have the Root access permission to access the Tenant Manager. However, the Root access permission does not allow users to authenticate into the Swift REST API to create containers and ingest objects. Users must have the Swift Administrator permission to authenticate into the Swift REST API.

Related information

Use a tenant account

Create tenant account

You must create at least one tenant account to control access to the storage in your StorageGRID system.

When you create a tenant account, you specify a name, a client protocol, and optionally a storage quota. If single sign-on (SSO) is enabled for StorageGRID, you also specify which federated group has Root access permission to configure the tenant account. If StorageGRID is not using single sign-on, you must also specify whether the tenant account will use its own identity source and configure the initial password for the tenant's local root user.

The Grid Manager provides a wizard that takes you through the steps for creating a tenant account. The steps vary based on whether identity federation and single sign-on are configured and whether the Grid Manager account you use to create the tenant account belongs to an admin group with the Root access permission.

What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have specific access permissions.
- If the tenant account will use the identity source that was configured for the Grid Manager, and you want to grant Root access permission for the tenant account to a federated group, you have imported that federated group into the Grid Manager. You do not need to assign any Grid Manager permissions to this admin group. See the instructions for managing admin groups.

Steps

1. Select **TENANTS**.

2. Select **Create** and enter the following information for the tenant:

   a. **Name**: Enter a name for the tenant account. Tenant names do not have to be unique. When the tenant account is created, it receives a unique, numeric account ID.

   b. **Description** (optional): Enter a description that helps you identify the tenant.

   c. **Client type**: Select the client type of either **S3** or **Swift**.

   d. **Storage quota** (optional): If you want this tenant to have a storage quota, enter a numerical value for the quota and select the correct units (GB, TB, or PB).

3. Select **Continue** and configure the S3 or Swift tenant.

S3 tenant

Select the appropriate permissions for the tenant. Some of these permissions have additional requirements. For details, see the online help for each permission.

- Allow platform services
- Use own identity source (selectable only if SSO is not being used)
- Allow S3 select (see Manage S3 Select for tenant accounts)

Swift tenant

If the tenant will use its own identity source, select **Use own identity source** (selectable only if SSO is not being used).

4. Select **Continue** and define root access for the tenant account.

Identity federation not configured

  a. Enter a password for the local root user.

  b. Select **Create tenant**.

SSO enabled

When SSO is enabled for StorageGRID, the tenant must use the identity source that was configured for the Grid Manager. No local users can sign in. You specify which federated group has Root access permission to configure the tenant account.

  a. Select an existing federated group from the Grid Manager to have the initial Root access permission for the tenant.

> ⓘ If you have adequate permissions, the existing federated groups from the Grid Manager are listed when you select the field. Otherwise, enter the group's unique name.

  b. Select **Create tenant**.

SSO not enabled

  a. Complete the steps described in the table depending on whether the tenant will manage its own groups and users or use the identity source that was configured for the Grid Manager.

If the tenant will…	Do this…
Manage its own groups and users	i. Select **Use own identity source**. **Note**: If this check box is selected and you want to use identity federation for tenant groups and users, the tenant must configure its own identity source. See the instructions for using tenant accounts. ii. Specify a password for the tenant's local root user, then select **Create tenant**. iii. Select **Sign in as root** to configure the tenant, or select **Finish** to configure the tenant later.
Use the groups and users configured for the Grid Manager	i. Do either or both of the following: ◦ Select an existing federated group from the Grid Manager that should have the initial Root access permission for the tenant. **Note**: If you have adequate permissions, the existing federated groups from the Grid Manager are listed when you select the field. Otherwise, enter the group's unique name. ◦ Specify a password for the tenant's local root user. ii. Select **Create tenant**.

5. To sign in to the tenant now:

- If you are accessing the Grid Manager on a restricted port, select **Restricted** in the Tenant table to learn more about accessing this tenant account.

  The URL for the Tenant Manager has this format:

  ```
  https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/
  ```

  - *FQDN_or_Admin_Node_IP* is a fully qualified domain name or the IP address of an Admin Node
  - *port* is the tenant-only port
  - *20-digit-account-id* is the tenant's unique account ID

- If you are accessing the Grid Manager on port 443 but you did not set a password for the local root user, in the Tenants table of the Grid Manager, select **Sign in**, and enter the credentials for a user in the Root access federated group.
- If you are accessing the Grid Manager on port 443 and you set a password for the local root user:

  a. Select **Sign in as root** to configure the tenant now.

  When you sign in, links appear for configuring buckets or containers, identity federation, groups, and users.

Create a tenant

✓ Enter details ——— ✓ Select permissions ——— ✓ Define root access

The tenant Tenant02 was created.

If you're ready to configure the tenant, select **Sign in as root.**

[Sign in as root]   ✓ Signed in

You can now access the Tenant Manager to configure these settings:

- Buckets ☑ : Create and manage buckets.
- Identity federation ☑ : Configure an external identity source to use federated groups.
- Groups ☑ : Manage groups and assign permissions.
- Users ☑ : Manage local users and assign users to groups.

[Finish]

  b. Select the links to configure the tenant account.

  Each link opens the corresponding page in the Tenant Manager. To complete the page, see the instructions for using tenant accounts.

     c. Otherwise, select **Finish** to access the tenant later.

6. To access the tenant later:

If you are using…	Do one of these…

Port 443	• From the Grid Manager, select **TENANTS**, and select **Sign in** to the right of the tenant name.
	
	• Enter the tenant's URL in a web browser:
	
	`https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/`
	
	    ◦ `FQDN_or_Admin_Node_IP` is a fully qualified domain name or the IP address of an Admin Node
	
	    ◦ `20-digit-account-id` is the tenant's unique account ID

A restricted port	• From the Grid Manager, select **TENANTS**, and select **Restricted**.
	
	• Enter the tenant's URL in a web browser:
	
	`https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id`
	
	    ◦ `FQDN_or_Admin_Node_IP` is a fully qualified domain name or the IP address of an Admin Node
	
	    ◦ `port` is the tenant-only restricted port
	
	    ◦ `20-digit-account-id` is the tenant's unique account ID

Related information

- Control access through firewalls
- Manage platform services for S3 tenant accounts

Change password for tenant's local root user

You might need to change the password for a tenant's local root user if the root user is locked out of the account.

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

If single sign-on (SSO) is enabled for your StorageGRID system, the local root user cannot sign in to the tenant account. To perform root user tasks, users must belong to a federated group that has the Root access permission for the tenant.

Steps

1. Select **TENANTS**.

2. Select the tenant account you want to edit.

   The Actions button becomes enabled.

3. From the **Actions** drop-down, select **Change root password**.

4. Enter the new password for the tenant account.

5. Select **Save**.

Edit tenant account

You can edit a tenant account to change the display name, change the identity source setting, allow or disallow platform services, or enter a storage quota.

What you'll need

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

Steps

1. Select **TENANTS**.

2. Select the tenant account you want to edit.

   Use the search box to search for a tenant account by name or tenant ID.

3. From the Actions drop-down, select **Edit**.

   This example is for a grid that does not use single sign-on (SSO). This tenant account has not configured its own identity source.

4. Change the values for these fields as required:

   ◦ **Name**

   ◦ **Description**

   ◦ **Client type**

   ◦ **Storage quota**

5. Select **Continue**.

6. Select or unselect the permissions for the tenant account.

   ◦ If you disable **Platform services** for a tenant who is already using them, the services that they have configured for their S3 buckets will stop working. No error message is sent to the tenant. For example, if the tenant has configured CloudMirror replication for an S3 bucket, they can still store objects in the bucket, but copies of those objects will no longer be made in the external S3 bucket that they have configured as an endpoint.

   ◦ Change the setting of the **Uses own identity source** check box to determine whether the tenant account will use its own identity source or the identity source that was configured for the Grid Manager.

     If the **Uses own identity source** check box is:

     ▪ Disabled and checked, the tenant has already enabled its own identity source. A tenant must disable its identity source before it can use the identity source that was configured for the Grid Manager.

     ▪ Disabled and unchecked, SSO is enabled for the StorageGRID system. The tenant must use the

10

identity source that was configured for the Grid Manager.

- ◦ Enable or disable **S3 Select** as needed. See Manage S3 Select for tenant accounts.

7. Select **Save**.

Related information

- Manage platform services for S3 tenant accounts
- Use a tenant account

Delete tenant account

You can delete a tenant account if you want to permanently remove the tenant's access to the system.

What you'll need

- You must be signed in to the Grid Manager using a supported web browser.
- You must have specific access permissions.
- You must have removed all buckets (S3), containers (Swift), and objects associated with the tenant account.

Steps

1. Select **TENANTS**.

2. Select the tenant account you want to delete.

   Use the search box to search for a tenant account by name or tenant ID.

3. From the **Actions** drop-down, select **Delete**.

4. Select **OK**.

Manage platform services

Manage platform services for S3 tenant accounts

If you enable platform services for S3 tenant accounts, you must configure your grid so that tenants can access the external resources necessary to use these services.

What are platform services?

Platform services include CloudMirror replication, event notifications, and the search integration service.

These services allow tenants to use the following functionality with their S3 buckets:

- **CloudMirror replication**: The StorageGRID CloudMirror replication service is used to mirror specific objects from a StorageGRID bucket to a specified external destination.

  For example, you might use CloudMirror replication to mirror specific customer records into Amazon S3 and then leverage AWS services to perform analytics on your data.

  > ⓘ   CloudMirror replication is not supported if the source bucket has S3 Object Lock enabled.

- **Notifications**: Per-bucket event notifications are used to send notifications about specific actions performed on objects to a specified external Amazon Simple Notification Service™ (SNS).

  For example, you could configure alerts to be sent to administrators about each object added to a bucket, where the objects represent log files associated with a critical system event.

  > ℹ️ Although event notification can be configured on a bucket with S3 Object Lock enabled, the S3 Object Lock metadata (including Retain Until Date and Legal Hold status) of the objects will not be included in the notification messages.

- **Search integration service**: The search integration service is used to send S3 object metadata to a specified Elasticsearch index where the metadata can be searched or analyzed using the external service.

  For example, you could configure your buckets to send S3 object metadata to a remote Elasticsearch service. You could then use Elasticsearch to perform searches across buckets, and perform sophisticated analyses of patterns present in your object metadata.

  > ℹ️ Although Elasticsearch integration can be configured on a bucket with S3 Object Lock enabled, the S3 Object Lock metadata (including Retain Until Date and Legal Hold status) of the objects will not be included in the notification messages.

Platform services give tenants the ability to use external storage resources, notification services, and search or analysis services with their data. Because the target location for platform services is typically external to your StorageGRID deployment, you must decide if you want to permit tenants to use these services. If you do, you must enable the use of platform services when you create or edit tenant accounts. You must also configure your network such that the platform services messages that tenants generate can reach their destinations.

Recommendations for using platform services

Before using platform services, be aware of the following recommendations:

- If an S3 bucket in the StorageGRID system has both versioning and CloudMirror replication enabled, you should also enable S3 bucket versioning for the destination endpoint. This allows CloudMirror replication to generate similar object versions on the endpoint.

- You should not use more than 100 active tenants with S3 requests requiring CloudMirror replication, notifications, and search integration. Having more than 100 active tenants can result in slower S3 client performance.

- Requests to an endpoint that cannot be completed will be queued to a maximum of 500,000 requests. This limit is equally shared among active tenants. New tenants are allowed to temporarily exceed this 500,000 limit so that newly created tenants are not unfairly penalized.

Related information

- Use a tenant account
- Configure Storage proxy settings
- Monitor and troubleshoot

Network and ports for platform services

If you allow an S3 tenant to use platform services, you must configure networking for the grid to ensure that platform services messages can be delivered to their destinations.

You can enable platform services for an S3 tenant account when you create or update the tenant account. If platform services are enabled, the tenant can create endpoints that serve as a destination for CloudMirror replication, event notifications, or search integration messages from its S3 buckets. These platform services messages are sent from Storage Nodes that run the ADC service to the destination endpoints.

For example, tenants might configure the following types of destination endpoints:

- A locally-hosted Elasticsearch cluster
- A local application that supports receiving Simple Notification Service (SNS) messages
- A locally-hosted S3 bucket on the same or another instance of StorageGRID
- An external endpoint, such as an endpoint on Amazon Web Services.

To ensure that platform services messages can be delivered, you must configure the network or networks containing the ADC Storage Nodes. You must ensure that the following ports can be used to send platform services messages to the destination endpoints.

By default, platform services messages are sent on the following ports:

- **80**: For endpoint URIs that begin with http
- **443**: For endpoint URIs that begin with https

Tenants can specify a different port when they create or edit an endpoint.

> (i) If a StorageGRID deployment is used as the destination for CloudMirror replication, replication messages might be received on a port other than 80 or 443. Ensure that the port being used for S3 by the destination StorageGRID deployment is specified in the endpoint.

If you use a non-transparent proxy server, you must also configure Storage proxy settings to allow messages to be sent to external endpoints, such as an endpoint on the internet.

Related information

- Use a tenant account

Per-site delivery of platform services messages

All platform services operations are performed on a per-site basis.

That is, if a tenant uses a client to perform an S3 API Create operation on an object by connecting to a Gateway Node at Data Center Site 1, the notification about that action is triggered and sent from Data Center Site 1.
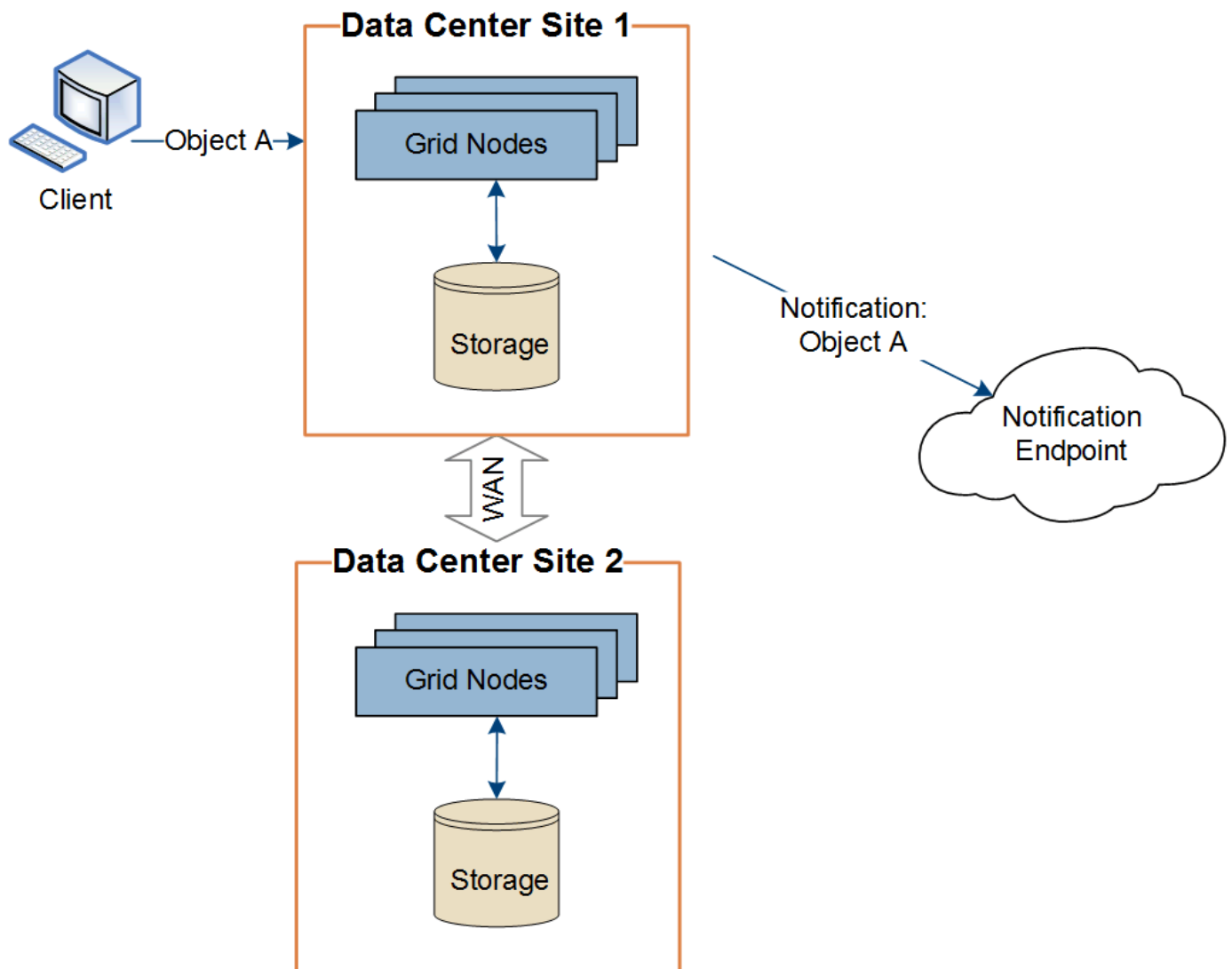
If the client subsequently performs an S3 API Delete operation on that same object from Data Center Site 2, the notification about the delete action is triggered and sent from Data Center Site 2.
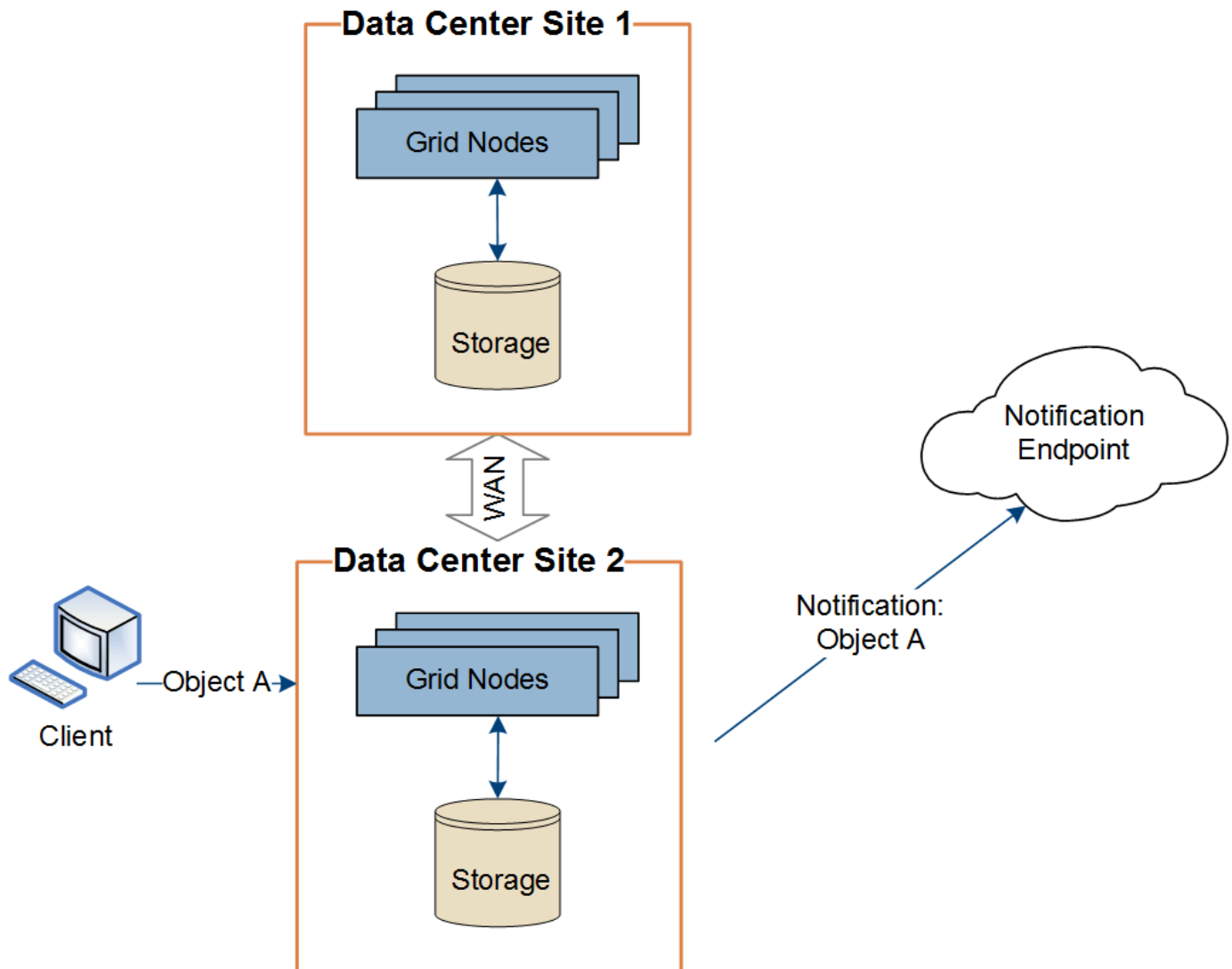
Make sure that the networking at each site is configured such that platform services messages can be delivered to their destinations.

Troubleshoot platform services

The endpoints used in platform services are created and maintained by tenant users in the Tenant Manager; however, if a tenant has issues configuring or using platform services, you might be able to use the Grid Manager to help resolve the issue.

Issues with new endpoints

Before a tenant can use platform services, they must create one or more endpoints using the Tenant Manager. Each endpoint represents an external destination for one platform service, such as a StorageGRID S3 bucket, an Amazon Web Services bucket, a Simple Notification Service topic, or an Elasticsearch cluster hosted locally or on AWS. Each endpoint includes both the location of the external resource and the credentials needed to access that resource.

When a tenant creates an endpoint, the StorageGRID system validates that the endpoint exists and that it can be reached using the credentials that were specified. The connection to the endpoint is validated from one node at each site.

If endpoint validation fails, an error message explains why endpoint validation failed. The tenant user should resolve the issue, then try creating the endpoint again.

> ⓘ   Endpoint creation will fail if platform services are not enabled for the tenant account.

Issues with existing endpoints

If an error occurs when StorageGRID tries to reach an existing endpoint, a message is displayed on the Dashboard in the Tenant Manager.

> ❌ One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

Tenant users can go to the Endpoints page to review the most recent error message for each endpoint and to determine how long ago the error occurred. The **Last error** column displays the most recent error message for each endpoint and indicates how long ago the error occurred. Errors that include the ❌ icon occurred within the past 7 days.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

> ❌ One or more endpoints have experienced an error. Select the endpoint for more details about the error. Meanwhile, the platform service request will be retried automatically.

5 endpoints   **Create endpoint**

Delete endpoint

	Display name ❓ ⇕	Last error ❓ ⇕	Type ❓ ⇕	URI ❓ ⇕	URN ❓ ⇕
☐	my-endpoint-2	❌ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
☐	my-endpoint-3	❌ 3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
☐	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
☐	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
☐	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1

> ⓘ Some error messages in the **Last error** column might include a logID in parentheses. A grid administrator or technical support can use this ID to locate more detailed information about the error in the bycast.log.

Issues related to proxy servers

If you have configured a Storage proxy between Storage Nodes and platform service endpoints, errors might occur if your proxy service does not allow messages from StorageGRID. To resolve these issues, check the

settings of your proxy server to ensure that platform service-related messages are not blocked.

Determine if an error has occurred

If any endpoint errors have occurred within the past 7 days, the Dashboard in the Tenant Manager displays an alert message. You can go the Endpoints page to see more details about the error.

Client operations fail

Some platform services issues might cause client operations on the S3 bucket to fail. For example, S3 client operations will fail if the internal Replicated State Machine (RSM) service stops, or if there are too many platform services messages queued for delivery.

To check the status of services:

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Select *site* > *Storage Node* > **SSM** > **Services**.

Recoverable and unrecoverable endpoint errors

After endpoints have been created, platform service request errors can occur for various reasons. Some errors are recoverable with user intervention. For example, recoverable errors might occur for the following reasons:

- The user's credentials have been deleted or have expired.
- The destination bucket does not exist.
- The notification cannot be delivered.

If StorageGRID encounters a recoverable error, the platform service request will be retried until it succeeds.

Other errors are unrecoverable. For example, an unrecoverable error occurs if the endpoint is deleted.

If StorageGRID encounters an unrecoverable endpoint error, the Total Events (SMTT) legacy alarm is triggered in the Grid Manager. To view the Total Events legacy alarm:

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Select *site* > *node* > **SSM** > **Events**.
3. View Last Event at the top of the table.

   Event messages are also listed in `/var/local/log/bycast-err.log`.

4. Follow the guidance provided in the SMTT alarm contents to correct the issue.
5. Select the **Configuration** tab to reset event counts.
6. Notify the tenant of the objects whose platform services messages have not been delivered.
7. Instruct the tenant to re-trigger the failed replication or notification by updating the object's metadata or tags.

   The tenant can resubmit the existing values to avoid making unwanted changes.

Platform services messages cannot be delivered

If the destination encounters an issue that prevents it from accepting platform services messages, the client operation on the bucket succeeds, but the platform services message is not delivered. For example, this error might happen if credentials are updated on the destination such that StorageGRID can no longer authenticate to the destination service.

If platform services messages cannot be delivered because of an unrecoverable error, the Total Events (SMTT) legacy alarm is triggered in the Grid Manager.

Slower performance for platform service requests

StorageGRID software might throttle incoming S3 requests for a bucket if the rate at which the requests are being sent exceeds the rate at which the destination endpoint can receive the requests. Throttling only occurs when there is a backlog of requests waiting to be sent to the destination endpoint.

The only visible effect is that the incoming S3 requests will take longer to execute. If you start to detect significantly slower performance, you should reduce the ingest rate or use an endpoint with higher capacity. If the backlog of requests continues to grow, client S3 operations (such as PUT requests) will eventually fail.

CloudMirror requests are more likely to be affected by the performance of the destination endpoint because these requests typically involve more data transfer than search integration or event notification requests.

Platform service requests fail

To view the request failure rate for platform services:

1. Select **NODES**.
2. Select *site* > **Platform Services**.
3. View the Request error rate chart.
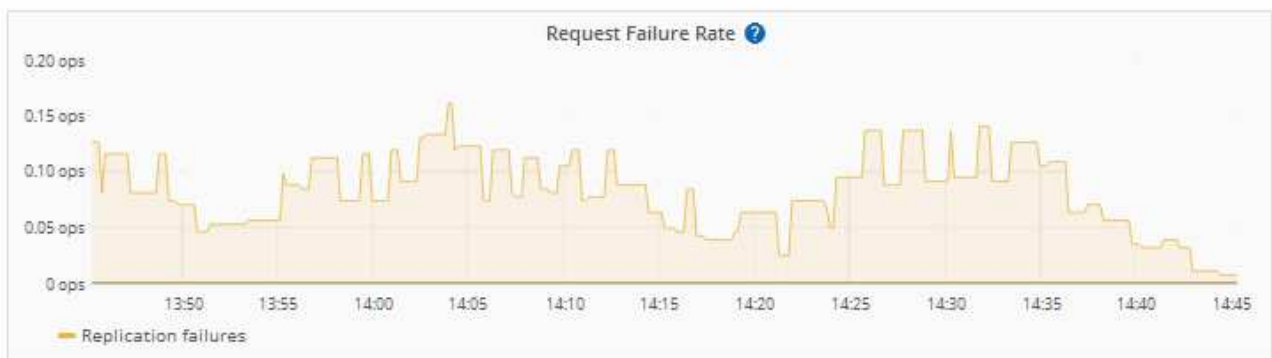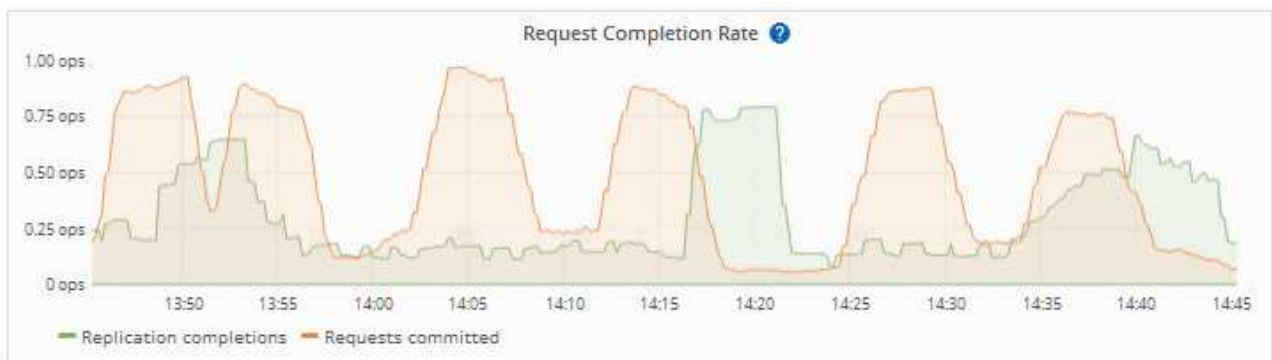
Platform services unavailable alert

The **Platform services unavailable** alert indicates that no platform service operations can be performed at a site because too few Storage Nodes with the RSM service are running or available.

The RSM service ensures platform service requests are sent to their respective endpoints.

To resolve this alert, determine which Storage Nodes at the site include the RSM service. (The RSM service is present on Storage Nodes that also include the ADC service.) Then, ensure that a simple majority of those Storage Nodes are running and available.

(i)	If more than one Storage Node that contains the RSM service fails at a site, you lose any pending platform service requests for that site.

Additional troubleshooting guidance for platform services endpoints

For additional information about troubleshooting platform services endpoints, see the instructions for using a tenant account.

Related information

- Monitor and troubleshoot
- Configure Storage proxy settings

Manage S3 Select for tenant accounts

You can allow certain S3 tenants to use S3 Select to issue SelectObjectContent requests on individual objects.

S3 Select provides an efficient way to search through large amounts of data without having to deploy a database and associated resources to enable searches. It also reduces the cost and latency of retrieving data.

What is S3 Select?

S3 Select allows S3 clients to use SelectObjectContent requests to filter and retrieve only the data needed from an object. The StorageGRID implementation of S3 Select includes a subset of S3 Select commands and features.

Considerations and requirements for using S3 Select

StorageGRID requires the following for S3 Select queries:

- The object you want to query is in CSV format, or is a GZIP or BZIP2 compressed file containing a CSV formatted file.
- Tenants must be granted S3 Select ability by the grid administrator. Select **Allow S3 Select** when creating a tenant or editing a tenant.
- The SelectObjectContent request must be sent to a StorageGRID load balancer endpoint. The Admin and Gateway Nodes used by the endpoint must be SG100 or SG1000 appliance nodes or VMware-based software nodes.

Note the following limitations:

- Bare-metal load balancer nodes are not supported.
- Queries cannot be sent directly to Storage Nodes.
- Queries sent through the deprecated CLB service are not supported.

(i)	SelectObjectContent requests can decrease load-balancer performance for all S3 clients and all tenants. Enable this feature only when required and only for trusted tenants.

See the instructions for using S3 Select.

To view Grafana charts for S3 Select operations over time, select **SUPPORT** > **Tools** > **Metrics** in the Grid Manager.