# Manage S3 platform services

StorageGRID 11.8

NetApp
March 19, 2024

This PDF was generated from https://docs.netapp.com/us-en/storagegrid-118/tenant/understanding-cloudmirror-replication-service.html on March 19, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

# Manage S3 platform services

## Manage platform services: Overview

StorageGRID platform services can help you implement a hybrid cloud strategy by allowing you to send event notifications and copies of S3 objects and object metadata to external destinations.

If the use of platform services is allowed for your tenant account, you can configure the following services for any S3 bucket:

**CloudMirror replication**

Use StorageGRID CloudMirror replication service 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**

Use per-bucket event notifications to send notifications about specific actions performed on objects to a specified external Amazon Simple Notification Service (Amazon 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.

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**

Use the search integration service 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.

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.

Because the target location for platform services is typically external to your StorageGRID deployment, platform services give you the power and flexibility that comes from using external storage resources, notification services, and search or analysis services for your data.

Any combination of platform services can be configured for a single S3 bucket. For example, you could configure both the CloudMirror service and notifications on a StorageGRID S3 bucket so that you can mirror specific objects to the Amazon Simple Storage Service, while sending a notification about each such object to a third party monitoring application to help you track your AWS expenses.

The use of platform services must be enabled for each tenant account by a StorageGRID administrator using the Grid Manager or the Grid Management API.

## How platform services are configured

Platform services communicate with external endpoints that you configure using the Tenant Manager or the Tenant Management API. Each endpoint represents an external destination, such as a StorageGRID S3 bucket, an Amazon Web Services bucket, an Amazon SNS topic, or an Elasticsearch cluster hosted locally, on AWS, or elsewhere.

After you create an external endpoint, you can enable a platform service for a bucket by adding XML configuration to the bucket. The XML configuration identifies the objects that the bucket should act on, the action that the bucket should take, and the endpoint that the bucket should use for the service.

You must add separate XML configurations for each platform service that you want to configure. For example:

- If you want all objects whose keys start with `/images` to be replicated to an Amazon S3 bucket, you must add a replication configuration to the source bucket.
- If you also want to send notifications when these objects are stored to the bucket, you must add a notifications configuration.
- Finally, if you want to index the metadata for these objects, you must add the metadata notification configuration that is used to implement search integration.

The format for the configuration XML is governed by the S3 REST APIs used to implement StorageGRID platform services:

| Platform service | S3 REST API | Refer to |
|---|---|---|
| CloudMirror replication | • GetBucketReplication<br>• PutBucketReplication | • CloudMirror replication<br>• Operations on buckets |
| Notifications | • GetBucketNotificationConfiguration<br>• PutBucketNotificationConfiguration | • Notifications<br>• Operations on buckets |
| Search integration | • GET Bucket metadata notification configuration<br>• PUT Bucket metadata notification configuration | • Search integration<br>• StorageGRID custom operations |

**Related information**

Considerations for platform services

## CloudMirror replication service

You can enable CloudMirror replication for an S3 bucket if you want StorageGRID to replicate specified objects added to the bucket to one or more destination buckets.

CloudMirror replication operates independently of the grid's active ILM policies. The CloudMirror service replicates objects as they are stored to the source bucket and delivers them to the destination bucket as soon as possible. Delivery of replicated objects is triggered when object ingest succeeds.

> CloudMirror replication has important similarities and differences with the cross-grid replication feature. To learn more, see Compare cross-grid replication and CloudMirror replication.

If you enable CloudMirror replication for an existing bucket, only the new objects added to that bucket are replicated. Any existing objects in the bucket aren't replicated. To force the replication of existing objects, you can update the existing object's metadata by performing an object copy.

> If you are using CloudMirror replication to copy objects to an Amazon S3 destination, be aware that Amazon S3 limits the size of user-defined metadata within each PUT request header to 2 KB. If an object has user-defined metadata greater than 2 KB, that object will not be replicated.

In StorageGRID, you can replicate the objects in a single bucket to multiple destination buckets. To do so, specify the destination for each rule in the replication configuration XML. You can't replicate an object to more than one bucket at the same time.

Additionally, you can configure CloudMirror replication on versioned or unversioned buckets, and you can specify a versioned or unversioned bucket as the destination. You can use any combination of versioned and unversioned buckets. For example, you could specify a versioned bucket as the destination for an unversioned source bucket, or vice versa. You can also replicate between unversioned buckets.

Deletion behavior for the CloudMirror replication service is the same as the deletion behavior of the Cross Region Replication (CRR) service provided by Amazon S3 — deleting an object in a source bucket never deletes a replicated object in the destination. If both source and destination buckets are versioned, the delete marker is replicated. If the destination bucket is not versioned, deleting an object in the source bucket does not replicate the delete marker to the destination bucket or delete the destination object.

As objects are replicated to the destination bucket, StorageGRID marks them as "replicas." A destination StorageGRID bucket will not replicate objects marked as replicas again, protecting you from accidental replication loops. This replica marking is internal to StorageGRID and does not prevent you from leveraging AWS CRR when using an Amazon S3 bucket as the destination.

> The custom header used to mark a replica is `x-ntap-sg-replica`. This marking prevents a cascading mirror. StorageGRID does support a bidirectional CloudMirror between two grids.

The uniqueness and ordering of events in the destination bucket aren't guaranteed. More than one identical copy of a source object might be delivered to the destination as a result of operations taken to guarantee delivery success. In rare cases, when the same object is updated simultaneously from two or more different StorageGRID sites, the ordering of operations on the destination bucket might not match the ordering of events on the source bucket.

CloudMirror replication is typically configured to use an external S3 bucket as a destination. However, you can also configure replication to use another StorageGRID deployment or any S3-compatible service.

## Understand notifications for buckets

You can enable event notification for an S3 bucket if you want StorageGRID to send notifications about specified events to a destination Kafka cluster or Amazon Simple Notification Service.

You can configure event notifications by associating notification configuration XML with a source bucket. The notification configuration XML follows S3 conventions for configuring bucket notifications, with the destination Kafka or Amazon SNS topic specified as the URN of an endpoint.

Event notifications are created at the source bucket as specified in the notification configuration and are delivered to the destination. If an event associated with an object succeeds, a notification about that event is created and queued for delivery.

The uniqueness and ordering of notifications aren't guaranteed. More than one notification of an event might be delivered to the destination as a result of operations taken to guarantee delivery success. And because delivery is asynchronous, the time ordering of notifications at the destination is not guaranteed to match the ordering of events on the source bucket, particularly for operations that originate from different StorageGRID sites. You can use the `sequencer` key in the event message to determine the order of events for a particular object, as described in Amazon S3 documentation.

**Supported notifications and messages**

StorageGRID event notifications follow the Amazon S3 API with some limitations:

- The following event types are supported:
  - s3:ObjectCreated:*
  - s3:ObjectCreated:Put
  - s3:ObjectCreated:Post
  - s3:ObjectCreated:Copy
  - s3:ObjectCreated:CompleteMultipartUpload
  - s3:ObjectRemoved:*
  - s3:ObjectRemoved:Delete
  - s3:ObjectRemoved:DeleteMarkerCreated
  - s3:ObjectRestore:Post
- Event notifications sent from StorageGRID use the standard JSON format but don't include some keys and use specific values for others, as shown in the table:

| Key name | StorageGRID value |
|---|---|
| eventSource | `sgws:s3` |
| awsRegion | not included |
| x-amz-id-2 | not included |
| arn | `urn:sgws:s3:::bucket_name` |

## Understand search integration service

You can enable search integration for an S3 bucket if you want to use an external search and data analysis service for your object metadata.

The search integration service is a custom StorageGRID service that automatically and asynchronously sends S3 object metadata to a destination endpoint whenever an object or its metadata is updated. You can then use sophisticated search, data analysis, visualization, or machine learning tools provided by the destination service to search, analyze, and gain insights from your object data.

You can enable the search integration service for any versioned or unversioned bucket. Search integration is configured by associating metadata notification configuration XML with the bucket that specifies which objects to act on and the destination for the object metadata.

Notifications are generated in the form of a JSON document named with the bucket name, object name, and version ID, if any. Each metadata notification contains a standard set of system metadata for the object in addition to all of the object's tags and user metadata.

> For tags and user metadata, StorageGRID passes dates and numbers to Elasticsearch as strings or as S3 event notifications. To configure Elasticsearch to interpret these strings as dates or numbers, follow the Elasticsearch instructions for dynamic field mapping and for mapping date formats. You must enable the dynamic field mappings on the index before you configure the search integration service. After a document is indexed, you can't edit the document's field types in the index.

Notifications are generated and queued for delivery whenever:

- An object is created.
- An object is deleted, including when objects are deleted as a result of the operation of the grid's ILM policy.
- Object metadata or tags are added, updated, or deleted. The complete set of metadata and tags is always sent on update — not just the changed values.

After you add metadata notification configuration XML to a bucket, notifications are sent for any new objects that you create and for any objects that you modify by updating its data, user metadata, or tags. However, notifications aren't sent for any objects that were already in the bucket. To ensure that object metadata for all objects in the bucket is sent to the destination, you should do either of the following:

- Configure the search integration service immediately after creating the bucket and before adding any objects.
- Perform an action on all objects already in the bucket that will trigger a metadata notification message to be sent to the destination.

The StorageGRID search integration service supports an Elasticsearch cluster as a destination. As with the other platform services, the destination is specified in the endpoint whose URN is used in the configuration XML for the service. Use the NetApp Interoperability Matrix Tool to determine the supported versions of Elasticsearch.

**Related information**

Configuration XML for search integration

Object metadata included in metadata notifications

JSON generated by search integration service

Configure search integration service

# Considerations for platform services

Before implementing platform services, review the recommendations and considerations for using these services.

For information about S3, see Use S3 REST API.

## Considerations for using platform services

| Consideration | Details |
| --- | --- |
| Destination endpoint monitoring | You must monitor the availability of each destination endpoint. If connectivity to the destination endpoint is lost for an extended period of time and a large backlog of requests exists, additional client requests (such as PUT requests) to StorageGRID will fail. You must retry these failed requests when the endpoint becomes reachable. |
| Destination endpoint throttling | 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.<br><br>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.<br><br>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. |
| Ordering guarantees | StorageGRID guarantees ordering of operations on an object within a site. As long as all operations against an object are within the same site, the final object state (for replication) will always equal the state in StorageGRID.<br><br>StorageGRID makes a best effort attempt to order requests when operations are made across StorageGRID sites. For example, if you write an object initially to site A and then later overwrite the same object at site B, the final object replicated by CloudMirror to the destination bucket is not guaranteed to be the newer object. |
| ILM-driven object deletions | To match the deletion behavior of the AWS CRR and Amazon Simple Notification Service, CloudMirror and event notification requests aren’t sent when an object in the source bucket is deleted because of StorageGRID ILM rules. For example, no CloudMirror or event notifications requests are sent if an ILM rule deletes an object after 14 days.<br><br>In contrast, search integration requests are sent when objects are deleted because of ILM. |

| Consideration | Details |
| --- | --- |
| Using Kafka endpoints | For Kafka endpoints, Mutual TLS is not supported. As a result, if you have `ssl.client.auth` set to `required` in your Kafka broker configuration, it might cause Kafka endpoint configuration issues.<br><br>The authentication of Kafka endpoints uses the following authentication types. These types are different from those used for the authentication of other endpoints, such as Amazon SNS, and require username and password credentials.<br><br>• SASL/PLAIN<br>• SASL/SCRAM-SHA-256<br>• SASL/SCRAM-SHA-512<br><br>**Note:** Configured storage proxy settings do not apply to Kafka platform services endpoints. |

## Considerations for using CloudMirror replication service

| Consideration | Details |
| --- | --- |
| Replication status | StorageGRID does not support the `x-amz-replication-status` header. |
| Object size | The maximum size for objects that can be replicated to a destination bucket by the CloudMirror replication service is 5 TiB, which is the same as the maximum *supported* object size.<br><br>**Note**: The maximum *recommended* size for a single PutObject operation is 5 GiB (5,368,709,120 bytes). If you have objects that are larger than 5 GiB, use multipart upload instead. |
| Bucket versioning and version IDs | If the source S3 bucket in StorageGRID has versioning enabled, you should also enable versioning for the destination bucket.<br><br>When using versioning, note that the ordering of object versions in the destination bucket is best effort and not guaranteed by the CloudMirror service, due to limitations in the S3 protocol.<br><br>**Note**: Version IDs for the source bucket in StorageGRID aren’t related to the version IDs for the destination bucket. |

| Consideration | Details |
| --- | --- |
| Tagging for object versions | The CloudMirror service does not replicate any PutObjectTagging or DeleteObjectTagging requests that supply a version ID, due to limitations in the S3 protocol. Because version IDs for the source and destination aren't related, there is no way to ensure that a tag update to a specific version ID will be replicated.<br><br>In contrast, the CloudMirror service does replicate PutObjectTagging requests or DeleteObjectTagging requests that don't specify a version ID. These requests update the tags for the latest key (or the latest version if the bucket is versioned). Normal ingests with tags (not tagging updates) are also replicated. |
| Multipart uploads and `ETag` values | When mirroring objects that were uploaded using a multipart upload, the CloudMirror service does not preserve the parts. As a result, the `ETag` value for the mirrored object will be different than the `ETag` value of the original object. |
| Objects encrypted with SSE-C (server-side encryption with customer-provided keys) | The CloudMirror service does not support objects that are encrypted with SSE-C. If you attempt to ingest an object into the source bucket for CloudMirror replication and the request includes the SSE-C request headers, the operation fails. |
| Bucket with S3 Object Lock enabled | If the destination S3 bucket for CloudMirror replication has S3 Object Lock enabled, the attempt to configure bucket replication (PutBucketReplication) will fail with an AccessDenied error. |

# Configure platform services endpoints

Before you can configure a platform service for a bucket, you must configure at least one endpoint to be the destination for the platform service.

Access to platform services is enabled on a per-tenant basis by a StorageGRID administrator. To create or use a platform services endpoint, you must be a tenant user with Manage endpoints or Root access permission, in a grid whose networking has been configured to allow Storage Nodes to access external endpoint resources. For a single tenant, you can configure a maximum of 500 platform services endpoints. Contact your StorageGRID administrator for more information.

## What is a platform services endpoint?

When you create a platform services endpoint, you specify the information that StorageGRID needs to access the external destination.

For example, if you want to replicate objects from a StorageGRID bucket to an Amazon S3 bucket, you create a platform services endpoint that includes the information and credentials StorageGRID needs to access the destination bucket on Amazon.

Each type of platform service requires its own endpoint, so you must configure at least one endpoint for each platform service you plan to use. After defining a platform services endpoint, you use the endpoint's URN as the destination in the configuration XML used to enable the service.

You can use the same endpoint as the destination for more than one source bucket. For example, you could

configure several source buckets to send object metadata to the same search integration endpoint so that you can perform searches across multiple buckets. You can also configure a source bucket to use more than one endpoint as a target, which enables you to do things like send notifications about object creation to one Amazon Simple Notification Service (Amazon SNS) topic and notifications about object deletion to a second Amazon SNS topic.

## Endpoints for CloudMirror replication

StorageGRID supports replication endpoints that represent S3 buckets. These buckets might be hosted on Amazon Web Services, the same or a remote StorageGRID deployment, or another service.

## Endpoints for notifications

StorageGRID supports Amazon SNS and Kafka endpoints. Simple Queue Service (SQS) or AWS Lambda endpoints aren't supported.

For Kafka endpoints, Mutual TLS is not supported. As a result, if you have `ssl.client.auth` set to `required` in your Kafka broker configuration, it might cause Kafka endpoint configuration issues.

## Endpoints for the search integration service

StorageGRID supports search integration endpoints that represent Elasticsearch clusters. These Elasticsearch clusters can be in a local data center or hosted in an AWS cloud or elsewhere.

The search integration endpoint refers to a specific Elasticsearch index and type. You must create the index in Elasticsearch before creating the endpoint in StorageGRID, or endpoint creation will fail. You don't need to create the type before creating the endpoint. StorageGRID will create the type if required when it sends object metadata to the endpoint.

**Related information**

Administer StorageGRID

## Specify URN for platform services endpoint

When you create a platform services endpoint, you must specify a Unique Resource Name (URN). You will use the URN to reference the endpoint when you create a configuration XML for the platform service. The URN for each endpoint must be unique.

StorageGRID validates platform services endpoints as you create them. Before you create a platform services endpoint, confirm that the resource specified in the endpoint exists and that it can be reached.

### URN elements

The URN for a platform services endpoint must start with either `arn:aws` or `urn:mysite`, as follows:

- If the service is hosted on Amazon Web Services (AWS), use `arn:aws`
- If the service is hosted on Google Cloud Platform (GCP), use `arn:aws`
- If the service is hosted locally, use `urn:mysite`

For example, if you are specifying the URN for a CloudMirror endpoint hosted on StorageGRID, the URN might begin with `urn:sgws`.

The next element of the URN specifies the type of platform service, as follows:

| Service | Type |
|---|---|
| CloudMirror replication | `s3` |
| Notifications | `sns` or `kafka` |
| Search integration | `es` |

For example, to continue specifying the URN for a CloudMirror endpoint hosted on StorageGRID, you would add `s3` to get `urn:sgws:s3`.

The final element of the URN identifies the specific target resource at the destination URI.

| Service | Specific resource |
|---|---|
| CloudMirror replication | `bucket-name` |
| Notifications | `sns-topic-name` or `kafka-topic-name` |
| Search integration | `domain-name/index-name/type-name`<br><br>**Note:** If the Elasticsearch cluster is **not** configured to create indexes automatically, you must create the index manually before you create the endpoint. |

**URNs for services hosted on AWS and GCP**

For AWS and GCP entities, the complete URN is a valid AWS ARN. For example:

- CloudMirror replication:

```
arn:aws:s3:::bucket-name
```

- Notifications:

```
arn:aws:sns:region:account-id:topic-name
```

- Search integration:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

For an AWS search integration endpoint, the `domain-name` must include the literal string `domain/`, as shown here.

**URNs for locally-hosted services**

When using locally-hosted services instead of cloud services, you can specify the URN in any way that creates a valid and unique URN, as long as the URN includes the required elements in the third and final positions. You can leave the elements indicated by optional blank, or you can specify them in any way that helps you identify the resource and make the URN unique. For example:

- CloudMirror replication:

  ```
  urn:mysite:s3:optional:optional:bucket-name
  ```

  For a CloudMirror endpoint hosted on StorageGRID, you can specify a valid URN that begins with `urn:sgws`:

  ```
  urn:sgws:s3:optional:optional:bucket-name
  ```

- Notifications:

  Specify an Amazon Simple Notification Service endpoint:

  ```
  urn:mysite:sns:optional:optional:sns-topic-name
  ```

  Specify a Kafka endpoint:

  ```
  urn:mysite:kafka:optional:optional:kafka-topic-name
  ```

- Search integration:

  ```
  urn:mysite:es:optional:optional:domain-name/index-name/type-name
  ```

For locally-hosted search integration endpoints, the `domain-name` element can be any string as long as the URN of the endpoint is unique.

## Create platform services endpoint

You must create at least one endpoint of the correct type before you can enable a platform service.

**Before you begin**

- You are signed in to the Tenant Manager using a supported web browser.
- Platform services were enabled for your tenant account by a StorageGRID administrator.
- You belong to a user group that has the Manage endpoints or Root access permission.
- The resource referenced by the platform services endpoint have been created:
  - CloudMirror replication: S3 bucket
  - Event notification: Amazon Simple Notification Service (Amazon SNS) or Kafka topic
  - Search notification: Elasticsearch index, if the destination cluster is not configured to automatically create indexes.
- You have the information about the destination resource:
  - Host and port for the Uniform Resource Identifier (URI)

    > If you plan to use a bucket hosted on a StorageGRID system as an endpoint for CloudMirror replication, contact the grid administrator to determine the values you need to enter.

  - Unique Resource Name (URN)

    Specify URN for platform services endpoint

  - Authentication credentials (if required):

    **AWS search integration endpoints**

    For AWS search integration endpoints, you can use the following credentials:

    - Access Key: Access key ID and secret access key
    - Basic HTTP: Username and password
    - CAP (C2S Access Portal): Temporary credentials URL, server and client certificates, client keys, and an optional client private key passphrase.

    **CloudMirror replication and Amazon SNS endpoints**

    For CloudMirror replication and Amazon SNS endpoints, you can use the following credentials:

    - Access Key: Access key ID and secret access key
    - CAP (C2S Access Portal): Temporary credentials URL, server and client certificates, client keys, and an optional client private key passphrase.

    **Kafka endpoints**

    For Kafka endpoints, you can use the following credentials:

    - SASL/PLAIN: Username and password
    - SASL/SCRAM-SHA-256: Username and password
    - SASL/SCRAM-SHA-512: Username and password

  - Security certificate (if using a custom CA certificate)
- If the Elasticsearch security features are enabled, you have the monitor cluster privilege for connectivity

testing, and either the write index privilege or both the index and delete index privileges for document updates.

**Steps**

1. Select **STORAGE (S3)** > **Platform services endpoints**. The Platform services endpoints page appears.
2. Select **Create endpoint**.
3. Enter a display name to briefly describe the endpoint and its purpose.

   The type of platform service that the endpoint supports is shown beside the endpoint name when it is listed on the Endpoints page, so you don't need to include that information in the name.

4. In the **URI** field, specify the Unique Resource Identifier (URI) of the endpoint.

   Use one of the following formats:

   ```
   https://host:port
   http://host:port
   ```

   If you don't specify a port, the following default ports are used:

   - Port 443 for HTTPS URIs and port 80 for HTTP URIs (most endpoints)
   - Port 9092 for HTTPS and HTTP URIs (Kafka endpoints only)

   For example, the URI for a bucket hosted on StorageGRID might be:

   ```
   https://s3.example.com:10443
   ```

   In this example, `s3.example.com` represents the DNS entry for the virtual IP (VIP) of the StorageGRID high availability (HA) group, and `10443` represents the port defined in the load balancer endpoint.

   > Whenever possible, you should connect to an HA group of load-balancing nodes to avoid a single point of failure.

   Similarly, the URI for a bucket hosted on AWS might be:

   ```
   https://s3-aws-region.amazonaws.com
   ```

   > If the endpoint is used for the CloudMirror replication service, don't include the bucket name in the URI. You include the bucket name in the **URN** field.

5. Enter the Unique Resource Name (URN) for the endpoint.

   > You can't change an endpoint's URN after the endpoint has been created.

6. Select **Continue**.

7. Select a value for **Authentication type**.

**AWS search integration endpoints**

Enter or upload the credentials for an AWS search integration endpoint.

The credentials that you supply must have write permissions for the destination resource.

| Authentication type | Description | Credentials |
|---|---|---|
| Anonymous | Provides anonymous access to the destination. Only works for endpoints that have security disabled. | No authentication. |
| Access Key | Uses AWS-style credentials to authenticate connections with the destination. | • Access key ID<br>• Secret access key |
| Basic HTTP | Uses a username and password to authenticate connections to the destination. | • Username<br>• Password |
| CAP (C2S Access Portal) | Uses certificates and keys to authenticate connections to the destination. | • Temporary credentials URL<br>• Server CA certificate (PEM file upload)<br>• Client certificate (PEM file upload)<br>• Client private key (PEM file upload, OpenSSL encrypted format or unencrypted private key format)<br>• Client private key passphrase (optional) |

**CloudMirror replication or Amazon SNS endpoints**

Enter or upload the credentials for a CloudMirror replication or Amazon SNS endpoint.

The credentials that you supply must have write permissions for the destination resource.

| Authentication type | Description | Credentials |
|---|---|---|
| Anonymous | Provides anonymous access to the destination. Only works for endpoints that have security disabled. | No authentication. |
| Access Key | Uses AWS-style credentials to authenticate connections with the destination. | • Access key ID<br>• Secret access key |

| Authentication type | Description | Credentials |
| --- | --- | --- |
| CAP (C2S Access Portal) | Uses certificates and keys to authenticate connections to the destination. | • Temporary credentials URL<br>• Server CA certificate (PEM file upload)<br>• Client certificate (PEM file upload)<br>• Client private key (PEM file upload, OpenSSL encrypted format or unencrypted private key format)<br>• Client private key passphrase (optional) |

**Kafka endpoints**

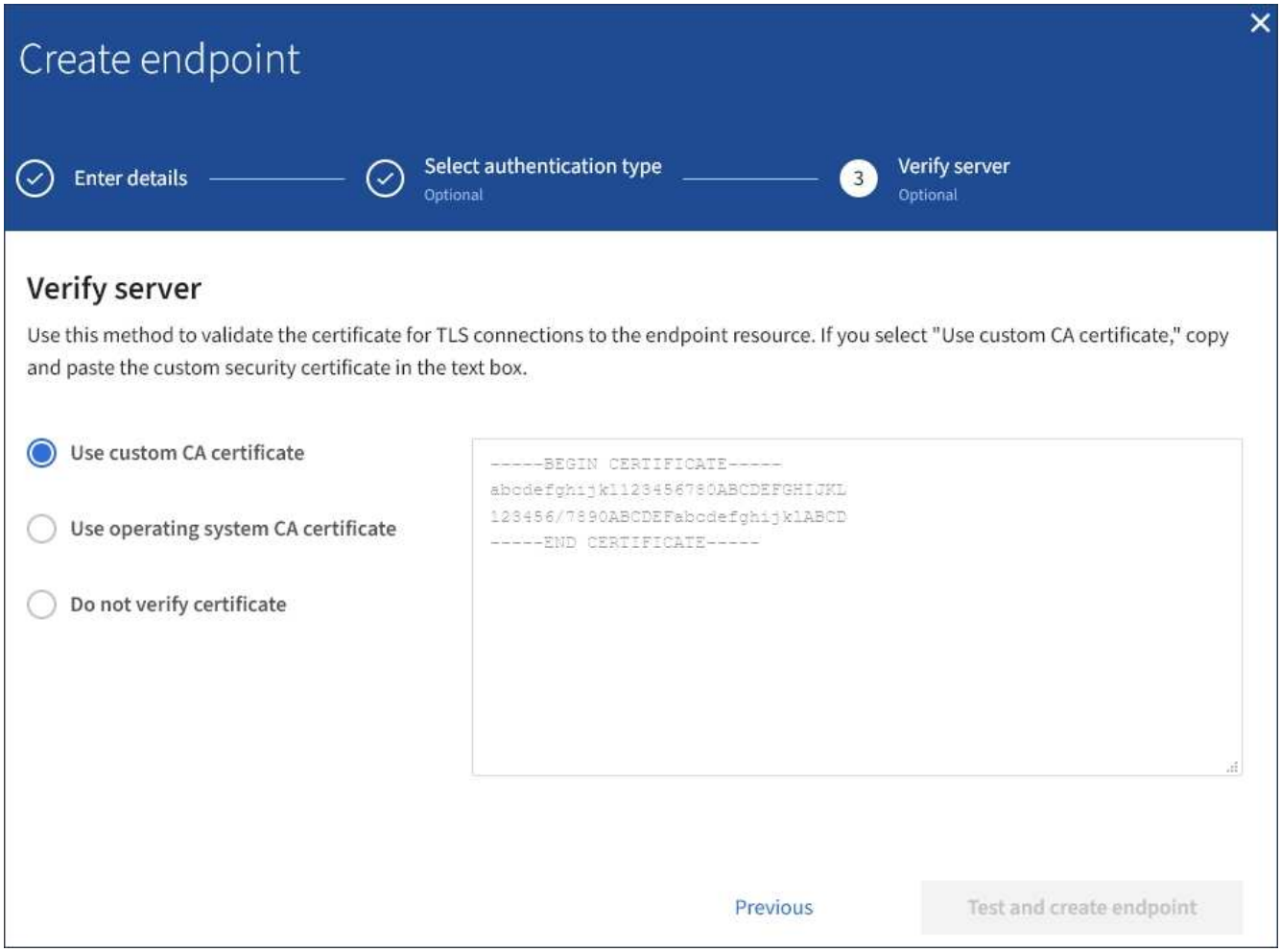
Enter or upload the credentials for a Kafka endpoint.

The credentials that you supply must have write permissions for the destination resource.

| Authentication type | Description | Credentials |
| --- | --- | --- |
| Anonymous | Provides anonymous access to the destination. Only works for endpoints that have security disabled. | No authentication. |
| SASL/PLAIN | Uses a username and password with plain text to authenticate connections to the destination. | • Username<br>• Password |
| SASL/SCRAM-SHA-256 | Uses a username and password using a challenge-response protocol and SHA-256 hashing to authenticate connections to the destination. | • Username<br>• Password |
| SASL/SCRAM-SHA-512 | Uses a username and password using a challenge-response protocol and SHA-512 hashing to authenticate connections to the destination. | • Username<br>• Password |

Select **Use delegation taken authentication** if the username and password are derived from a delegation token that was obtained from a Kafka cluster.

8. Select **Continue**.
9. Select a radio button for **Verify server** to choose how TLS connection to the endpoint is verified.




| Type of certificate verification | Description |
|---|---|
| Use custom CA certificate | Use a custom security certificate. If you select this setting, copy and paste the custom security certificate in the **CA Certificate** text box. |
| Use operating system CA certificate | Use the default Grid CA certificate installed on the operating system to secure connections. |
| Do not verify certificate | The certificate used for the TLS connection is not verified. This option is not secure. |

10. Select **Test and create endpoint**.
    - A success message appears if the endpoint can be reached using the specified credentials. The connection to the endpoint is validated from one node at each site.
    - An error message appears if endpoint validation fails. If you need to modify the endpoint to correct the error, select **Return to endpoint details** and update the information. Then, select **Test and create endpoint**.

> Endpoint creation fails if platform services aren't enabled for your tenant account. Contact your StorageGRID administrator.

After you have configured an endpoint, you can use its URN to configure a platform service.

**Related information**

Specify URN for platform services endpoint

Configure CloudMirror replication

Configure event notifications

Configure search integration service

## Test connection for platform services endpoint

If the connection to a platform service has changed, you can test the connection for the endpoint to validate that the destination resource exists and that it can be reached using the credentials you specified.

**Before you begin**

- You are signed in to the Tenant Manager using a supported web browser.
- You belong to a user group that has the Manage endpoints or Root access permission.

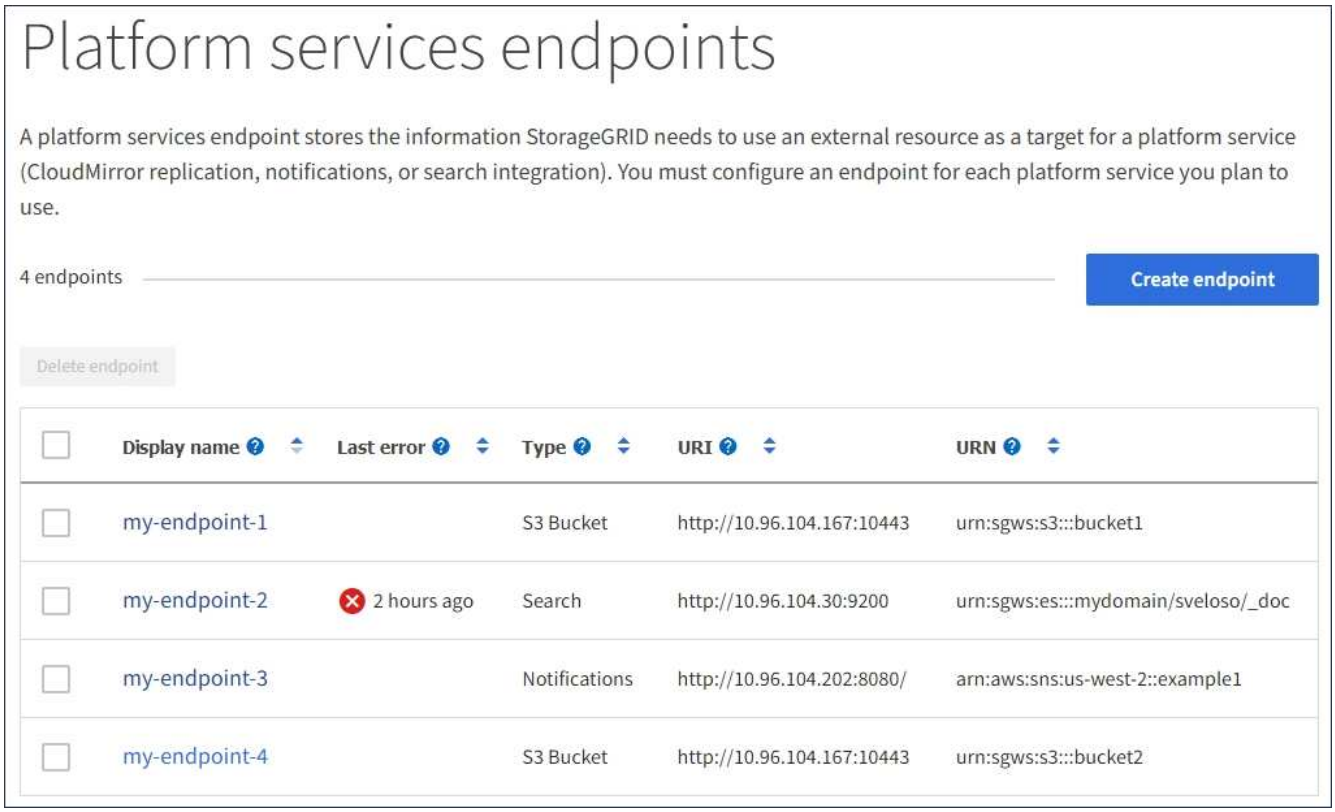
**About this task**

StorageGRID does not validate that the credentials have the correct permissions.

**Steps**

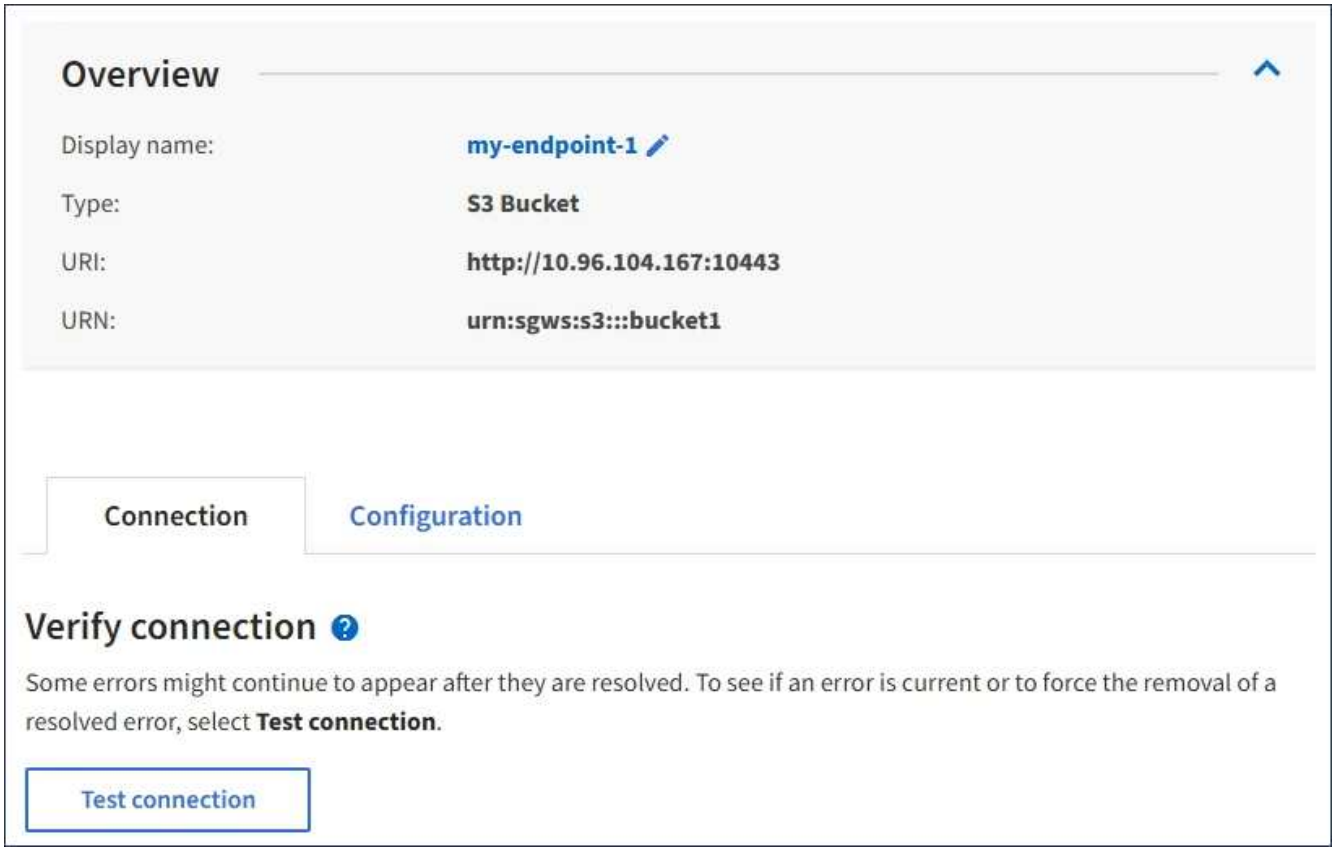
1. Select **STORAGE (S3)** > **Platform services endpoints**.

   The Platform services endpoints page appears and shows the list of platform services endpoints that have already been configured.




2. Select the endpoint whose connection you want to test.

   The endpoint details page appears.




3. Select **Test connection**.

- A success message appears if the endpoint can be reached using the specified credentials. The connection to the endpoint is validated from one node at each site.
- An error message appears if endpoint validation fails. If you need to modify the endpoint to correct the error, select **Configuration** and update the information. Then, select **Test and save changes**.

## Edit platform services endpoint

You can edit the configuration for a platform services endpoint to change its name, URI, or other details. For example, you might need to update expired credentials or change the URI to point to a backup Elasticsearch index for failover. You can't change the URN for a platform services endpoint.

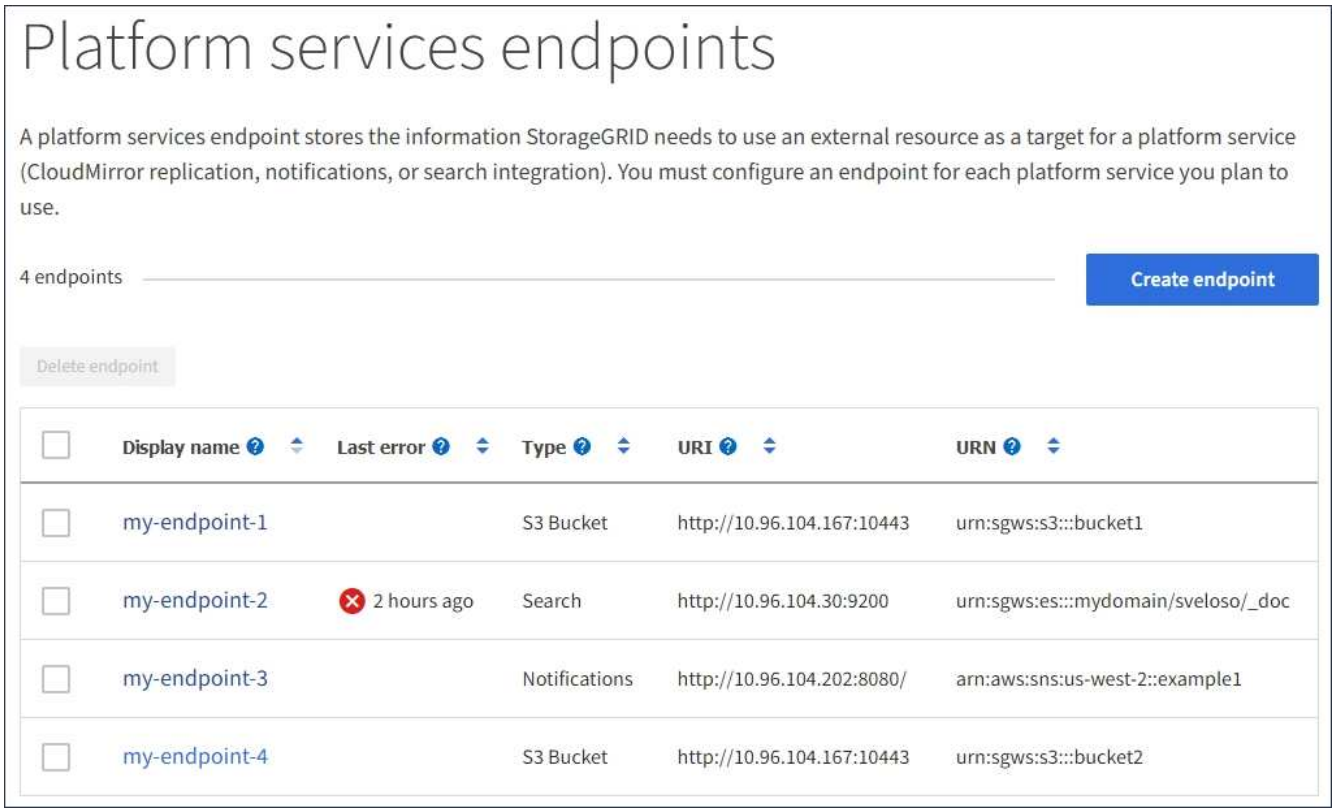
### Before you begin

- You are signed in to the Tenant Manager using a supported web browser.
- You belong to a user group that has the Manage endpoints or Root access permission.

### Steps

1. Select **STORAGE (S3)** > **Platform services endpoints**.

   The Platform services endpoints page appears and shows the list of platform services endpoints that have already been configured.




2. Select the endpoint you want to edit.

   The endpoint details page appears.

3. Select **Configuration**.

4. As needed, change the configuration of the endpoint.

   > You can't change an endpoint's URN after the endpoint has been created.

   a. To change the display name for the endpoint, select the edit icon .
   b. As needed, change the URI.
   c. As needed, change the authentication type.
      - For Access Key authentication, change the key as necessary by selecting **Edit S3 key** and pasting a new access key ID and secret access key. If you need to cancel your changes, select **Revert S3 key edit**.
      - For CAP (C2S Access Portal) authentication, change the temporary credentials URL or optional client private key passphrase and upload new certificate and key files as needed.

        > The Client private key must be in OpenSSL encrypted format or unencrypted private key format.

   d. As needed, change the method for verifying the server.
5. Select **Test and save changes**.
   - A success message appears if the endpoint can be reached using the specified credentials. The connection to the endpoint is verified from one node at each site.
   - An error message appears if endpoint validation fails. Modify the endpoint to correct the error, and then select **Test and save changes**.

## Delete platform services endpoint

You can delete an endpoint if you no longer want to use the associated platform service.

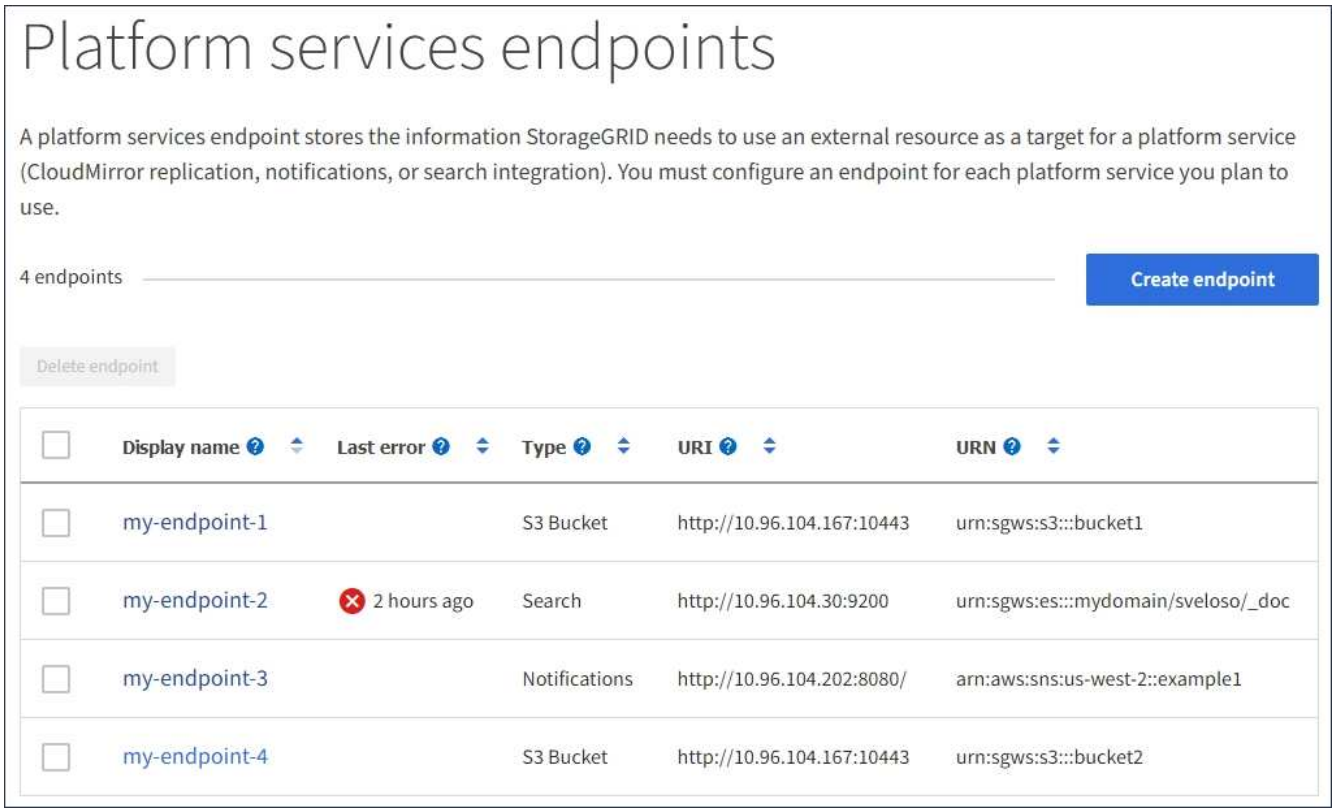
**Before you begin**

- You are signed in to the Tenant Manager using a supported web browser.
- You belong to a user group that has the Manage endpoints or Root access permission.

**Steps**

1. Select **STORAGE (S3)** > **Platform services endpoints**.

   The Platform services endpoints page appears and shows the list of platform services endpoints that have already been configured.

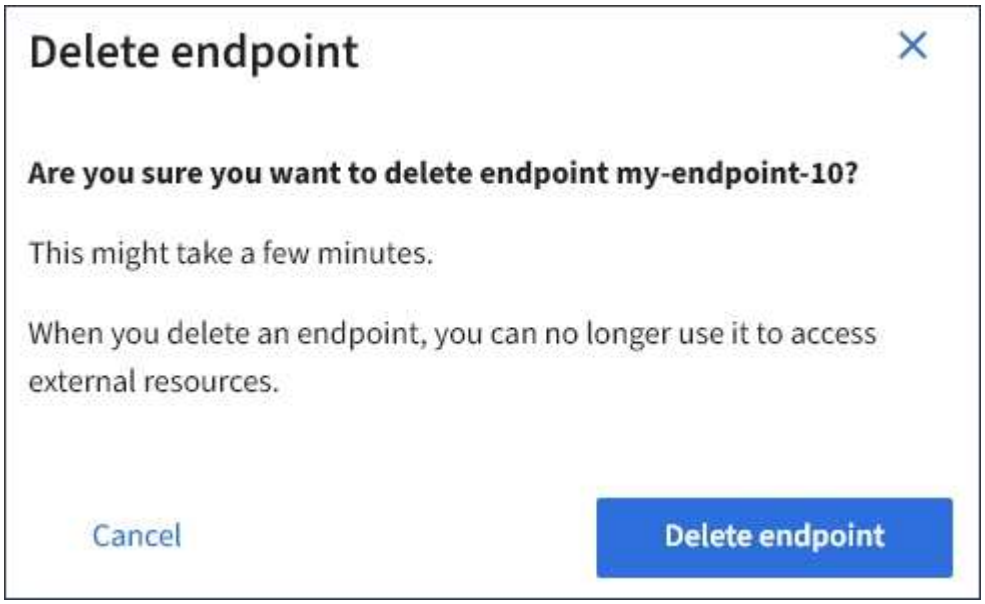



2. Select the checkbox for each endpoint you want to delete.

> If you delete a platform services endpoint that is in use, the associated platform service will be disabled for any buckets that use the endpoint. Any requests that have not yet been completed will be dropped. Any new requests will continue to be generated until you change your bucket configuration to no longer reference the deleted URN. StorageGRID will report these requests as unrecoverable errors.

3. Select **Actions** > **Delete endpoint**.

   A confirmation message appears.



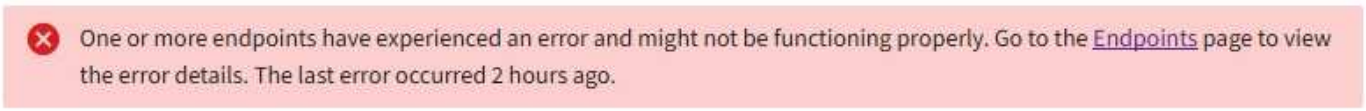
4. Select **Delete endpoint**.

## Troubleshoot platform services endpoint errors

If an error occurs when StorageGRID attempts to communicate with a platform services endpoint, a message is displayed on the dashboard. On the Platform services endpoints page, the Last error column indicates how long ago the error occurred. No error is displayed if the permissions associated with an endpoint's credentials are incorrect.

### Determine if error has occurred

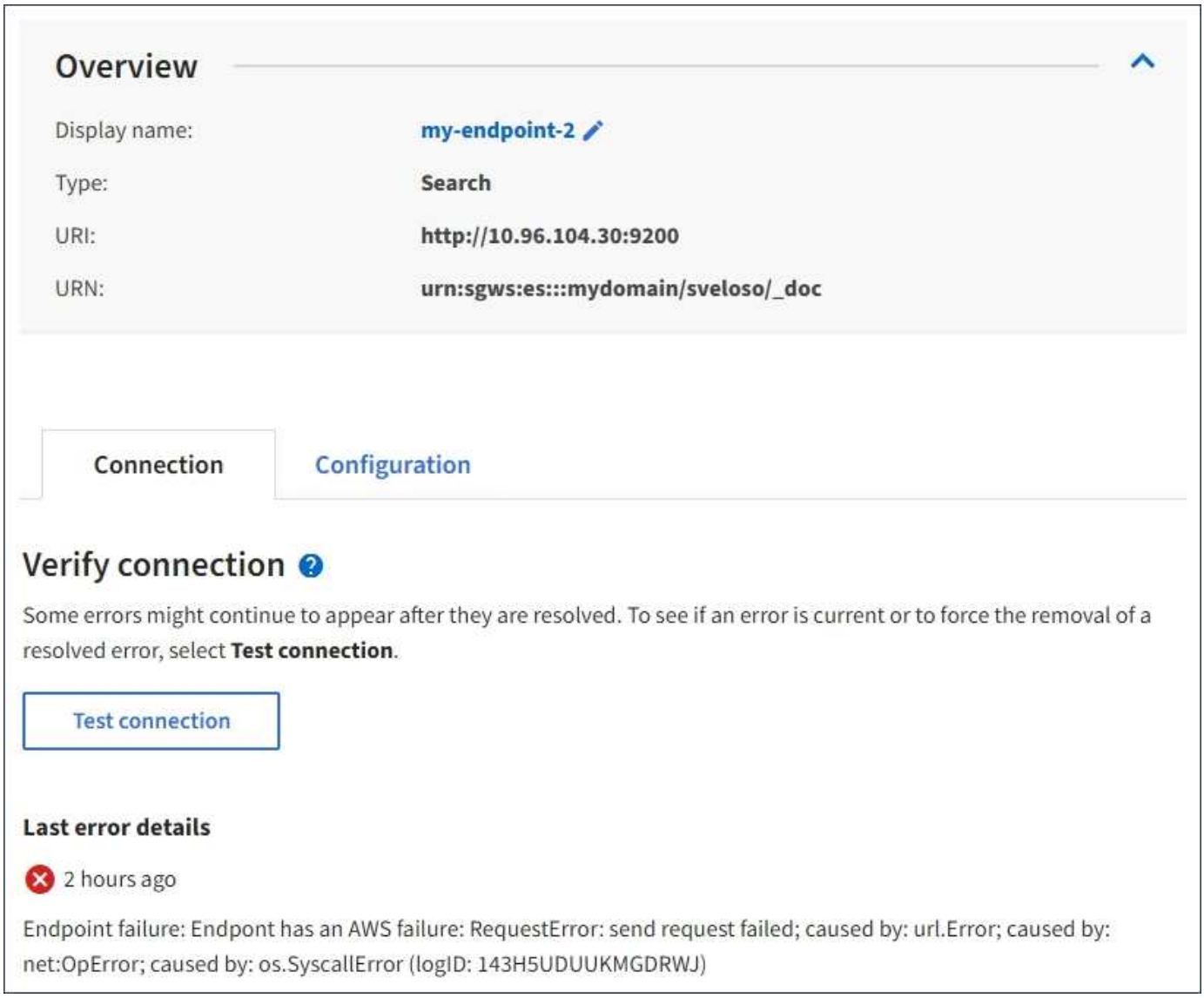
If any platform services endpoint errors have occurred within the past 7 days, the Tenant Manager dashboard displays an alert message. You can go the Platform services endpoints page to see more details about the error.




The same error that appears on the dashboard also appears at the top of the Platform services endpoints page. To view a more detailed error message:

#### Steps

1. From the list of endpoints, select the endpoint that has the error.
2. On the endpoint details page, select **Connection**. This tab displays only the most recent error for an endpoint and indicates how long ago the error occurred. Errors that include the red X icon occurred within the past 7 days.




### Check if error is still current

Some errors might continue to be shown in the **Last error** column even after they are resolved. To see if an error is current or to force the removal of a resolved error from the table:

**Steps**

1. Select the endpoint.

   The endpoint details page appears.

2. Select **Connection** > **Test connection**.

Selecting **Test connection** causes StorageGRID to validate that the platform services endpoint exists and that it can be reached with the current credentials. The connection to the endpoint is validated from one node at each site.

### Resolve endpoint errors

You can use the **Last error** message on the endpoint details page to help determine what is causing the error. Some errors might require you to edit the endpoint to resolve the issue. For example, a CloudMirroring error

can occur if StorageGRID is unable to access the destination S3 bucket because it does not have the correct access permissions or the access key has expired. The message is "Either the endpoint credentials or the destination access needs to be updated," and the details are "AccessDenied" or "InvalidAccessKeyId."

If you need to edit the endpoint to resolve an error, selecting **Test and save changes** causes StorageGRID to validate the updated endpoint and confirm that it can be reached with the current credentials. The connection to the endpoint is validated from one node at each site.

**Steps**

1. Select the endpoint.
2. On the endpoint details page, select **Configuration**.
3. Edit the endpoint configuration as needed.
4. Select **Connection** > **Test connection**.

**Endpoint credentials with insufficient permissions**

When StorageGRID validates a platform services endpoint, it confirms that the endpoint's credentials can be used to contact the destination resource and it does a basic permissions check. However, StorageGRID does not validate all of the permissions required for certain platform services operations. For this reason, if you receive an error when attempting to use a platform service (such as "403 Forbidden"), check the permissions associated with the endpoint's credentials.

**Related information**

- Administer StorageGRID > Troubleshoot platform services
- Create platform services endpoint
- Test connection for platform services endpoint
- Edit platform services endpoint

# Configure CloudMirror replication

The CloudMirror replication service is one of the three StorageGRID platform services. You can use CloudMirror replication to automatically replicate objects to an external S3 bucket.

**Before you begin**

- Platform services were enabled for your tenant account by a StorageGRID administrator.
- You have already created a bucket to act as the replication source.
- The endpoint that you intend to use as a destination for CloudMirror replication already exists, and you have its URN.
- You belong to a user group that has the Manage all buckets or Root access permission. These permissions override the permission settings in group or bucket policies when configuring the bucket using the Tenant Manager.

**About this task**

CloudMirror replication copies objects from a source bucket to a destination bucket that is specified in an endpoint.

CloudMirror replication has important similarities and differences with the cross-grid replication feature. To learn more, see Compare cross-grid replication and CloudMirror replication.

To enable CloudMirror replication for a bucket, you must create and apply a valid bucket replication configuration XML. The replication configuration XML must use the URN of an S3 bucket endpoint for each destination.

Replication is not supported for source or destination buckets with S3 Object Lock enabled.

For general information about bucket replication and how to configure it, see Amazon Simple Storage Service (S3) documentation: Replicating objects. For information about how StorageGRID implements GetBucketReplication, DeleteBucketReplication, and PutBucketReplication, see the Operations on buckets.

If you enable CloudMirror replication on a bucket that contains objects, new objects added to the bucket are replicated, but the existing objects in the bucket aren't replicated. You must update existing objects to trigger replication.

If you specify a storage class in the replication configuration XML, StorageGRID uses that class when performing operations against the destination S3 endpoint. The destination endpoint must also support the specified storage class. Be sure to follow any recommendations provided by the destination system vendor.

**Steps**

1. Enable replication for your source bucket:

   Use a text editor to create the replication configuration XML required to enable replication, as specified in the S3 replication API. When configuring the XML:

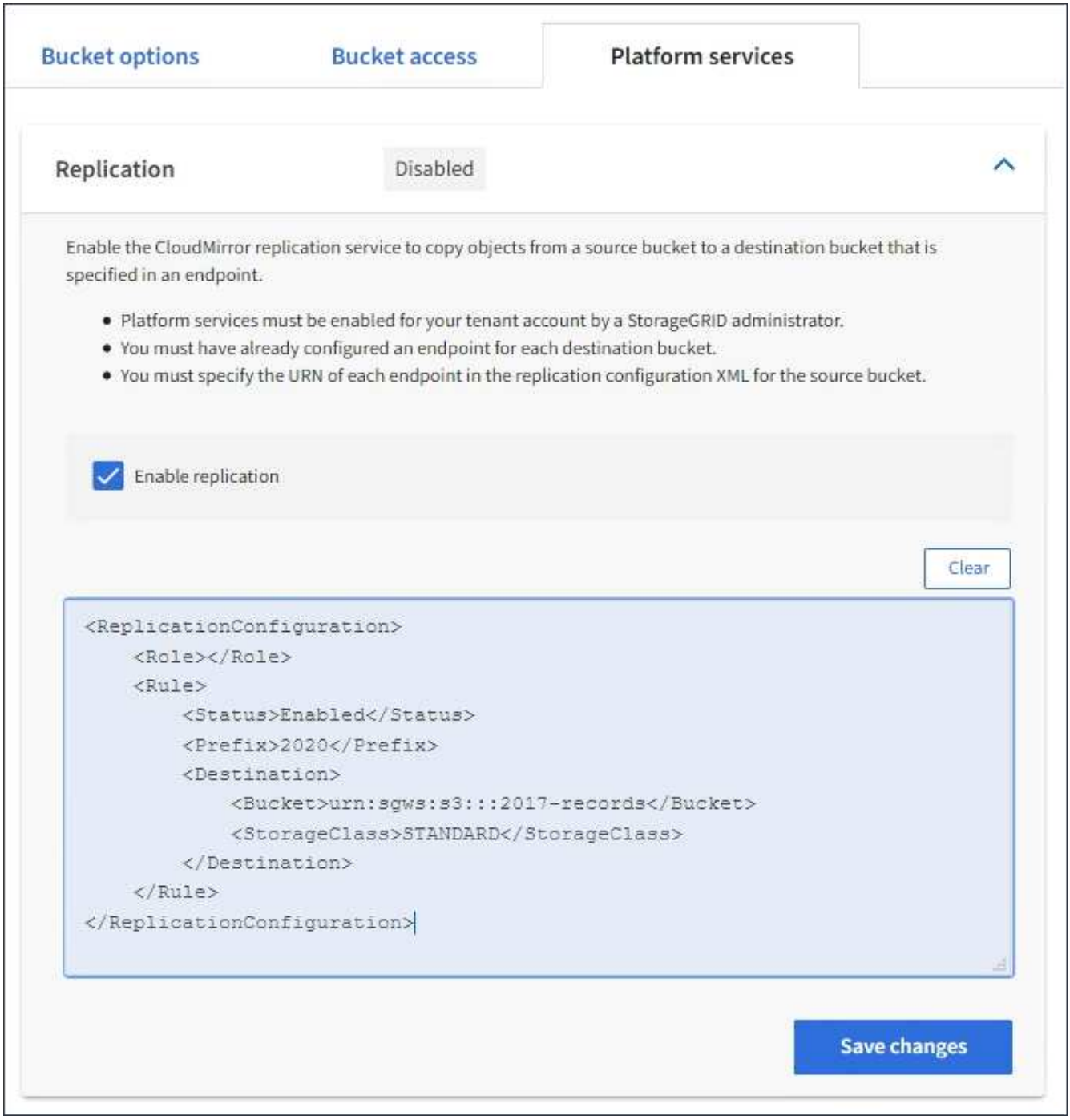
   - Note that StorageGRID only supports V1 of the replication configuration. This means that StorageGRID does not support the use of the `Filter` element for rules, and follows V1 conventions for deletion of object versions. See the Amazon documentation on replication configuration for details.
   - Use the URN of an S3 bucket endpoint as the destination.
   - Optionally add the `<StorageClass>` element, and specify one of the following:
     - `STANDARD`: The default storage class. If you don't specify a storage class when you upload an object, the `STANDARD` storage class is used.
     - `STANDARD_IA`: (Standard - infrequent access.) Use this storage class for data that is accessed less frequently, but that still requires rapid access when needed.
     - `REDUCED_REDUNDANCY`: Use this storage class for noncritical, reproducible data that can be stored with less redundancy than the `STANDARD` storage class.
   - If you specify a `Role` in the configuration XML it will be ignored. This value is not used by StorageGRID.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. Select **View buckets** from the dashboard, or select **STORAGE (S3)** > **Buckets**.
3. Select the name of the source bucket.

   The bucket details page appears.

4. Select **Platform services** > **Replication**.
5. Select the **Enable replication** checkbox.
6. Paste the replication configuration XML into the text box, and select **Save changes**.




Platform services must be enabled for each tenant account by a StorageGRID administrator using the Grid Manager or Grid Management API. Contact your StorageGRID administrator if an error occurs when you save the configuration XML.

7. Verify that replication is configured correctly:
   a. Add an object to the source bucket that meets the requirements for replication as specified in the replication configuration.

      In the example shown earlier, objects that match the prefix "2020" are replicated.

   b. Confirm that the object has been replicated to the destination bucket.

For small objects, replication happens quickly.

**Related information**

Create platform services endpoint

# Configure event notifications

The notifications service is one of the three StorageGRID platform services. You can enable notifications for a bucket to send information about specified events to a destination Kafka cluster or service that supports the AWS Simple Notification Service (Amazon SNS).

**Before you begin**

- Platform services were enabled for your tenant account by a StorageGRID administrator.
- You have already created a bucket to act as the source of notifications.
- The endpoint that you intend to use as a destination for event notifications already exists, and you have its URN.
- You belong to a user group that has the Manage all buckets or Root access permission. These permissions override the permission settings in group or bucket policies when configuring the bucket using the Tenant Manager.

**About this task**

After you configure event notifications, whenever a specified event occurs for an object in the source bucket, a notification is generated and sent to the Amazon SNS or Kafka topic used as the destination endpoint. To enable notifications for a bucket, you must create and apply valid notification configuration XML. The notification configuration XML must use the URN of an event notifications endpoint for each destination.

For general information about event notifications and how to configure them, see Amazon documentation. For information about how StorageGRID implements the S3 bucket notification configuration API, see the instructions for implementing S3 client applications.

If you enable event notifications for a bucket that contains objects, notifications are sent only for actions that are performed after the notification configuration is saved.

**Steps**

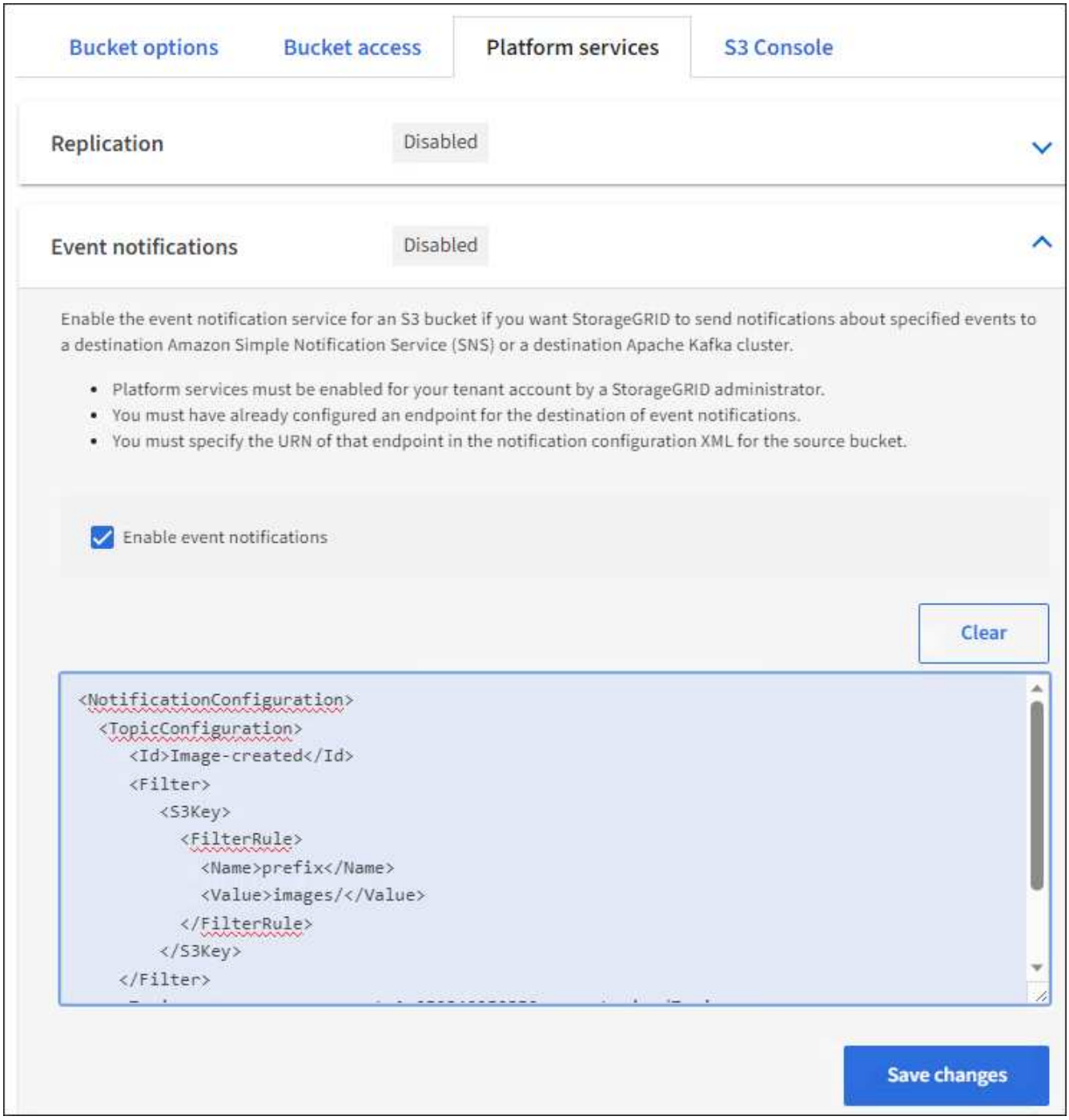
1. Enable notifications for your source bucket:
    - Use a text editor to create the notification configuration XML required to enable event notifications, as specified in the S3 notification API.
    - When configuring the XML, use the URN of an event notifications endpoint as the destination topic.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. In the Tenant Manager select **STORAGE (S3)** > **Buckets**.
3. Select the name of the source bucket.

   The bucket details page appears.

4. Select **Platform services** > **Event notifications**.
5. Select the **Enable event notifications** checkbox.
6. Paste the notification configuration XML into the text box, and select **Save changes**.




Platform services must be enabled for each tenant account by a StorageGRID administrator using the Grid Manager or Grid Management API. Contact your StorageGRID administrator if an error occurs when you save the configuration XML.

7. Verify that event notifications are configured correctly:
   a. Perform an action on an object in the source bucket that meets the requirements for triggering a notification as configured in the configuration XML.

      In the example, an event notification is sent whenever an object is created with the `images/` prefix.

   b. Confirm that a notification has been delivered to the destination Amazon SNS or Kafka topic.

For example, if your destination topic is hosted on the Amazon SNS, you could configure the service to send you an email when the notification is delivered.

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

If the notification is received at the destination topic, you have successfully configured your source bucket for StorageGRID notifications.

**Related information**

Understand notifications for buckets

Use S3 REST API

Create platform services endpoint

# Use search integration service

The search integration service is one of the three StorageGRID platform services. You can enable this service to send object metadata to a destination search index whenever an object is created, deleted, or its metadata or tags are updated.

You can configure search integration by using the Tenant Manager to apply custom StorageGRID configuration XML to a bucket.

> Because the search integration service causes object metadata to be sent to a destination, its configuration XML is referred to as *metadata notification configuration XML*. This configuration XML is different than the *notification configuration XML* used to enable event notifications.

See the instructions for implementing S3 client applications for details about the following custom StorageGRID S3 REST API operations:

- DELETE Bucket metadata notification configuration
- GET Bucket metadata notification configuration
- PUT Bucket metadata notification configuration

**Related information**

Configuration XML for search integration

Object metadata included in metadata notifications

JSON generated by search integration service

Configure search integration service

Use S3 REST API

## Configuration XML for search integration

The search integration service is configured using a set of rules contained within `<MetadataNotificationConfiguration>` and `</MetadataNotificationConfiguration>` tags. Each rule specifies the objects that the rule applies to, and the destination where StorageGRID should send those objects' metadata.

Objects can be filtered on the prefix of the object name. For example, you could send metadata for objects with the prefix `images` to one destination, and metadata for objects with the prefix `videos` to another. Configurations that have overlapping prefixes aren't valid, and are rejected when they are submitted. For example, a configuration that includes one rule for objects with the prefix `test` and a second rule for objects with the prefix `test2` is not allowed.

Destinations must be specified using the URN of a StorageGRID endpoint that has been created for the search integration service. These endpoints refer to an index and type defined on an Elasticsearch cluster.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

The table describes the elements in the metadata notification configuration XML.

| Name | Description | Required |
|---|---|---|
| MetadataNotificationConfiguration | Container tag for rules used to specify the objects and destination for metadata notifications.<br><br>Contains one or more Rule elements. | Yes |
| Rule | Container tag for a rule that identifies the objects whose metadata should be added to a specified index.<br><br>Rules with overlapping prefixes are rejected.<br><br>Included in the MetadataNotificationConfiguration element. | Yes |
| ID | Unique identifier for the rule.<br><br>Included in the Rule element. | No |
| Status | Status can be 'Enabled' or 'Disabled'. No action is taken for rules that are disabled.<br><br>Included in the Rule element. | Yes |

| Name | Description | Required |
| --- | --- | --- |
| Prefix | Objects that match the prefix are affected by the rule, and their metadata is sent to the specified destination.<br><br>To match all objects, specify an empty prefix.<br><br>Included in the Rule element. | Yes |
| Destination | Container tag for the destination of a rule.<br><br>Included in the Rule element. | Yes |
| Urn | URN of the destination where object metadata is sent. Must be the URN of a StorageGRID endpoint with the following properties:<br><br>• `es` must be the third element.<br>• The URN must end with the index and type where the metadata is stored, in the form `domain-name/myindex/mytype`.<br><br>Endpoints are configured using the Tenant Manager or Tenant Management API. They take the following form:<br><br>• `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype`<br>• `urn:mysite:es:::mydomain/myindex/mytype`<br><br>The endpoint must be configured before the configuration XML is submitted, or configuration will fail with a 404 error.<br><br>URN is included in the Destination element. | Yes |

Use the sample metadata notification configuration XML to learn how to construct your own XML.

**Metadata notification configuration that applies to all objects**

In this example, object metadata for all objects is sent to the same destination.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

**Metadata notification configuration with two rules**

In this example, object metadata for objects that match the prefix `/images` is sent to one destination, while object metadata for objects that match the prefix `/videos` is sent to a second destination.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

**Related information**

Use S3 REST API

Object metadata included in metadata notifications

JSON generated by search integration service

Configure search integration service

## Configure the search integration service

The search integration service sends object metadata to a destination search index whenever an object is created, deleted, or its metadata or tags are updated.

### Before you begin

- Platform services were enabled for your tenant account by a StorageGRID administrator.
- You have already created an S3 bucket whose contents you want to index.
- The endpoint that you intend to use as a destination for the search integration service already exists, and you have its URN.
- You belong to a user group that has the Manage all buckets or Root access permission. These permissions override the permission settings in group or bucket policies when configuring the bucket using the Tenant Manager.

### About this task

After you configure the search integration service for a source bucket, creating an object or updating an object's metadata or tags triggers object metadata to be sent to the destination endpoint. If you enable the search integration service for a bucket that already contains objects, metadata notifications aren't automatically sent for existing objects. You must update these existing objects to ensure that their metadata is added to the destination search index.

### Steps

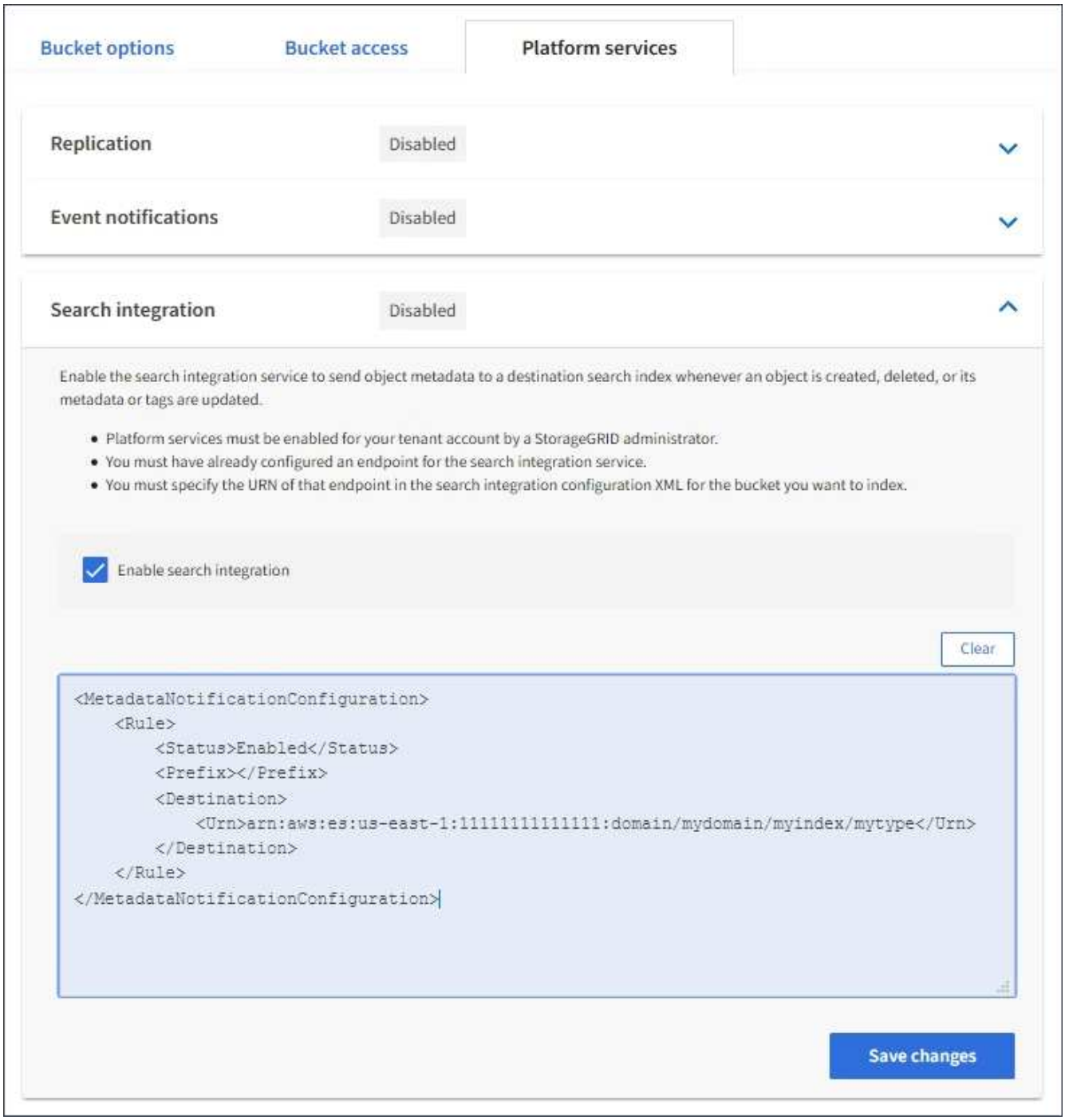
1. Use a text editor to create the metadata notification XML required to enable search integration.
   - See the information about configuration XML for search integration.
   - When configuring the XML, use the URN of a search integration endpoint as the destination.

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. In the Tenant Manager select **STORAGE (S3)** > **Buckets**.
3. Select the name of the source bucket.

   The bucket details page appears.

4. Select **Platform services** > **Search integration**
5. Select the **Enable search integration** checkbox.
6. Paste the metadata notification configuration into the text box, and select **Save changes**.




Platform services must be enabled for each tenant account by a StorageGRID administrator using the Grid Manager or Management API. Contact your StorageGRID administrator if an error occurs when you save the configuration XML.

7. Verify that the search integration service is configured correctly:
   a. Add an object to the source bucket that meets the requirements for triggering a metadata notification as specified in the configuration XML.

      In the example shown earlier, all objects added to the bucket trigger a metadata notification.

   b. Confirm that a JSON document that contains the object's metadata and tags was added to the search index specified in the endpoint.

**After you finish**

As necessary, you can disable search integration for a bucket using either of the following methods:

- Select **STORAGE (S3)** > **Buckets** and clear the **Enable search integration** checkbox.
- If you are using the S3 API directly, use a DELETE Bucket metadata notification request. See the instructions for implementing S3 client applications.

**Related information**

Understand search integration service

Configuration XML for search integration

Use S3 REST API

Create platform services endpoint

## JSON generated by search integration service

When you enable the search integration service for a bucket, a JSON document is generated and sent to the destination endpoint each time object metadata or tags are added, updated, or deleted.

This example shows an example of the JSON that could be generated when an object with the key `SGWS/Tagging.txt` is created in a bucket named `test`. The `test` bucket is not versioned, so the `versionId` tag is empty.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

## Object metadata included in metadata notifications

The table lists all the fields that are included in the JSON document that is sent to the destination endpoint when search integration is enabled.

The document name includes the bucket name, object name, and version ID if present.

| Type | Item name and description |
| --- | --- |
| Bucket and object information | `bucket`: Name of the bucket |
| | `key`: Object key name |
| | `versionID`: Object version, for objects in versioned buckets |
| | `region`: Bucket region, for example `us-east-1` |
| System metadata | `size`: Object size (in bytes) as visible to an HTTP client |
| | `md5`: Object hash |
| User metadata | `metadata`: All user metadata for the object, as key-value pairs<br><br>`key:value` |
| Tags | `tags`: All object tags defined for the object, as key-value pairs<br><br>`key:value` |

For tags and user metadata, StorageGRID passes dates and numbers to Elasticsearch as strings or as S3 event notifications. To configure Elasticsearch to interpret these strings as dates or numbers, follow the Elasticsearch instructions for dynamic field mapping and for mapping date formats. You must enable the dynamic field mappings on the index before you configure the search integration service. After a document is indexed, you can't edit the document's field types in the index.

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.