# StorageGRID custom operations

StorageGRID 11.8

NetApp
May 17, 2024

# Table of Contents

# StorageGRID custom operations

## StorageGRID custom operations: Overview

The StorageGRID system supports custom operations that are added on to the S3 REST API.

The following table lists the custom operations supported by StorageGRID.

| Operation | Description |
|---|---|
| GET Bucket consistency | Returns the consistency being applied to a particular bucket. |
| PUT Bucket consistency | Sets the consistency applied to a particular bucket. |
| GET Bucket last access time | Returns whether last access time updates are enabled or disabled for a particular bucket. |
| PUT Bucket last access time | Allows you to enable or disable last access time updates for a particular bucket. |
| DELETE Bucket metadata notification configuration | Deletes the metadata notification configuration XML associated with a particular bucket. |
| GET Bucket metadata notification configuration | Returns the metadata notification configuration XML associated with a particular bucket. |
| PUT Bucket metadata notification configuration | Configures the metadata notification service for a bucket. |
| GET Storage Usage | Tells you the total amount of storage in use by an account and for each bucket associated with the account. |
| Deprecated: CreateBucket with compliance settings | Deprecated and not supported: You can no longer create new buckets with Compliance enabled. |
| Deprecated: GET Bucket compliance | Deprecated but supported: Returns the compliance settings currently in effect for an existing legacy Compliant bucket. |
| Deprecated: PUT Bucket compliance | Deprecated but supported: Allows you to modify the compliance settings for an existing legacy Compliant bucket. |

## GET Bucket consistency

The GET Bucket consistency request allows you to determine the consistency being applied to a particular bucket.

The default consistency is set to guarantee read-after-write for newly created objects.

You must have the s3:GetBucketConsistency permission, or be account root, to complete this operation.

## Request example

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

## Response

In the response XML, `<Consistency>` will return one of the following values:

| Consistency | Description |
|---|---|
| all | All nodes receive the data immediately, or the request will fail. |
| strong-global | Guarantees read-after-write consistency for all client requests across all sites. |
| strong-site | Guarantees read-after-write consistency for all client requests within a site. |
| read-after-new-write | (Default) Provides read-after-write consistency for new objects and eventual consistency for object updates. Offers high availability and data protection guarantees. Recommended for most cases. |
| available | Provides eventual consistency for both new objects and object updates. For S3 buckets, use only as required (for example, for a bucket that contains log values that are rarely read, or for HEAD or GET operations on keys that don’t exist). Not supported for S3 FabricPool buckets. |

## Response example

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

**Related information**

Consistency values

# PUT Bucket consistency

The PUT Bucket consistency request allows you to specify the consistency to apply to operations performed on a bucket.

The default consistency is set to guarantee read-after-write for newly created objects.

**Before you begin**

You must have the s3:PutBucketConsistency permission, or be account root, to complete this operation.

## Request

The `x-ntap-sg-consistency` parameter must contain one of the following values:

| Consistency | Description |
|---|---|
| all | All nodes receive the data immediately, or the request will fail. |
| strong-global | Guarantees read-after-write consistency for all client requests across all sites. |
| strong-site | Guarantees read-after-write consistency for all client requests within a site. |
| read-after-new-write | (Default) Provides read-after-write consistency for new objects and eventual consistency for object updates. Offers high availability and data protection guarantees. Recommended for most cases. |

| Consistency | Description |
| --- | --- |
| available | Provides eventual consistency for both new objects and object updates. For S3 buckets, use only as required (for example, for a bucket that contains log values that are rarely read, or for HEAD or GET operations on keys that don’t exist). Not supported for S3 FabricPool buckets. |

**Note:** In general, you should use the "Read-after-new-write" consistency. If requests aren’t working correctly, change the application client behavior if possible. Or, configure the client to specify the consistency for each API request. Set the consistency at the bucket level only as a last resort.

### Request example

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

**Related information**

Consistency values

# GET Bucket last access time

The GET Bucket last access time request allows you to determine if last access time updates are enabled or disabled for individual buckets.

You must have the s3:GetBucketLastAccessTime permission, or be account root, to complete this operation.

### Request example

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

### Response example

This example shows that last access time updates are enabled for the bucket.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

# PUT Bucket last access time

The PUT Bucket last access time request allows you to enable or disable last access time updates for individual buckets. Disabling last access time updates improves performance, and is the default setting for all buckets created with version 10.3.0, or later.

You must have the s3:PutBucketLastAccessTime permission for a bucket, or be account root, to complete this operation.

> Starting with StorageGRID version 10.3, updates to last access time are disabled by default for all new buckets. If you have buckets that were created using an earlier version of StorageGRID and you want to match the new default behavior, you must explicitly disable last access time updates for each of those earlier buckets. You can enable or disable updates to last access time using the PUT Bucket last access time request or from the details page for a bucket in the Tenant Manager. See Enable or disable last access time updates.

If last access time updates are disabled for a bucket, the following behavior is applied to operations on the bucket:

- GetObject, GetObjectAcl, GetObjectTagging, and HeadObject requests don't update last access time. The object is not added to queues for information lifecycle management (ILM) evaluation.
- CopyObject and PutObjectTagging requests that update only the metadata also update last access time. The object is added to queues for ILM evaluation.
- If updates to last access time are disabled for the source bucket, CopyObject requests don't update last access time for the source bucket. The object that was copied is not added to queues for ILM evaluation for the source bucket. However, for the destination, CopyObject requests always update last access time. The copy of the object is added to queues for ILM evaluation.
- CompleteMultipartUpload requests update last access time. The completed object is added to queues for ILM evaluation.

## Request examples

This example enables last access time for a bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

This example disables last access time for a bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

# DELETE Bucket metadata notification configuration

The DELETE Bucket metadata notification configuration request allows you to disable the search integration service for individual buckets by deleting the configuration XML.

You must have the s3:DeleteBucketMetadataNotification permission for a bucket, or be account root, to complete this operation.

## Request example

This example shows disabling the search integration service for a bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

# GET Bucket metadata notification configuration

The GET Bucket metadata notification configuration request allows you to retrieve the configuration XML used to configure search integration for individual buckets.

You must have the s3:GetBucketMetadataNotification permission, or be account root, to complete this operation.

## Request example

This request retrieves the metadata notification configuration for the bucket named `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

## Response

The response body includes the metadata notification configuration for the bucket. The metadata notification configuration lets you determine how the bucket is configured for search integration. That is, it allows you to determine which objects are indexed, and which endpoints their object metadata is being sent to.

```
<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>
```

Each metadata notification configuration includes one or more rules. Each rule specifies the objects that it applies to and the destination where StorageGRID should send object metadata. Destinations must be specified using the URN of a StorageGRID endpoint.

| 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 |

| Name | Description | Required |
| --- | --- | --- |
| 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 |
| 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 |

| Name | Description | Required |
| --- | --- | --- |
| 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 |

## Response example

The XML included between the `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tags shows how integration with a search integration endpoint is configured for the bucket. In this example, object metadata is being sent to an Elasticsearch index named `current` and type named `2017` that is hosted in an AWS domain named `records`.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

**Related information**

Use a tenant account

# PUT Bucket metadata notification configuration

The PUT Bucket metadata notification configuration request allows you to enable the search integration service for individual buckets. The metadata notification configuration XML that you supply in the request body specifies the objects whose metadata is sent to the destination search index.

You must have the s3:PutBucketMetadataNotification permission for a bucket, or be account root, to complete this operation.

## Request

The request must include the metadata notification configuration in the request body. Each metadata notification configuration includes one or more rules. Each rule specifies the objects that it applies to, and the destination where StorageGRID should send object 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 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 included one rule for for objects with the prefix `test` and a second rule for objects with the prefix `test2` would not be allowed.

Destinations must be specified using the URN of a StorageGRID endpoint. The endpoint must exist when the

metadata notification configuration is submitted, or the request fails as a `400 Bad Request`. The error message states: `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN`.

```
<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 |

## Request examples

This example shows enabling search integration for a bucket. In this example, object metadata for all objects is sent to the same destination.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

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

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.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<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>
```

## JSON generated by the 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 | Description |
|---|---|---|
| Bucket and object information | bucket | Name of the bucket |
| Bucket and object information | key | Object key name |
| Bucket and object information | versionID | Object version, for objects in versioned buckets |
| Bucket and object information | region | Bucket region, for example `us-east-1` |
| System metadata | size | Object size (in bytes) as visible to an HTTP client |

| Type | Item name | Description |
|---|---|---|
| System metadata | md5 | Object hash |
| User metadata | metadata *key:value* | All user metadata for the object, as key-value pairs |
| Tags | tags *key:value* | All object tags defined for the object, as key-value pairs |

> 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.

**Related information**

Use a tenant account

# GET Storage Usage request

The GET Storage Usage request tells you the total amount of storage in use by an account, and for each bucket associated with the account.

The amount of storage used by an account and its buckets can be obtained by a modified ListBuckets request with the `x-ntap-sg-usage` query parameter. Bucket storage usage is tracked separately from the PUT and DELETE requests processed by the system. There might be some delay before the usage values match the expected values based on the processing of requests, particularly if the system is under heavy load.

By default, StorageGRID attempts to retrieve usage information using strong-global consistency. If strong-global consistency can't be achieved, StorageGRID attempts to retrieve the usage information at a strong-site consistency.

You must have the s3:ListAllMyBuckets permission, or be account root, to complete this operation.

## Request example

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

## Response example

This example shows an account that has four objects and 12 bytes of data in two buckets. Each bucket contains two objects and six bytes of data.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

### Versioning

Every object version stored will contribute to the `ObjectCount` and `DataBytes` values in the response. Delete markers aren't added to the `ObjectCount` total.

#### Related information

Consistency values

# Deprecated bucket requests for legacy Compliance

## Deprecated bucket requests for legacy Compliance

You might need to use the StorageGRID S3 REST API to manage buckets that were created using the legacy Compliance feature.

#### Compliance feature deprecated

The StorageGRID Compliance feature that was available in previous StorageGRID versions is deprecated and has been replaced by S3 Object Lock.

If you previously enabled the global Compliance setting, the global S3 Object Lock setting is enabled in StorageGRID 11.6. You can no longer create new buckets with Compliance enabled; however, as required, you can use the StorageGRID S3 REST API to manage any existing legacy Compliant buckets.

- Use S3 REST API to configure S3 Object Lock
- Manage objects with ILM
- NetApp Knowledge Base: How to manage legacy Compliant buckets in StorageGRID 11.5

Deprecated compliance requests:

- Deprecated - PUT Bucket request modifications for compliance

  The SGCompliance XML element is deprecated. Previously, you could include this StorageGRID custom element in the optional XML request body of PUT Bucket requests to create a Compliant bucket.

- Deprecated - GET Bucket compliance

  The GET Bucket compliance request is deprecated. However, you can continue to use this request to determine the compliance settings currently in effect for an existing legacy Compliant bucket.

- Deprecated - PUT Bucket compliance

  The PUT Bucket compliance request is deprecated. However, you can continue to use this request to modify the compliance settings for an existing legacy Compliant bucket. For example, you can place an existing bucket on legal hold or increase its retention period.

## Deprecated: CreateBucket request modifications for compliance

The SGCompliance XML element is deprecated. Previously, you could include this StorageGRID custom element in the optional XML request body of CreateBucket requests to create a Compliant bucket.

> The StorageGRID Compliance feature that was available in previous StorageGRID versions is deprecated and has been replaced by S3 Object Lock. See the following for more details:
>
> - Use S3 REST API to configure S3 Object Lock
> - NetApp Knowledge Base: How to manage legacy Compliant buckets in StorageGRID 11.5

You can no longer create new buckets with Compliance enabled. The following error message is returned if you attempt to use the CreateBucket request modifications for compliance to create a new Compliant bucket:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

## Deprecated: GET Bucket compliance request

The GET Bucket compliance request is deprecated. However, you can continue to use this request to determine the compliance settings currently in effect for an existing legacy

Compliant bucket.

> The StorageGRID Compliance feature that was available in previous StorageGRID versions is deprecated and has been replaced by S3 Object Lock. See the following for more details:
>
> - Use S3 REST API to configure S3 Object Lock
> - NetApp Knowledge Base: How to manage legacy Compliant buckets in StorageGRID 11.5

You must have the s3:GetBucketCompliance permission, or be account root, to complete this operation.

**Request example**

This example request allows you to determine the compliance settings for the bucket named `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

**Response example**

In the response XML, `<SGCompliance>` lists the compliance settings in effect for the bucket. This example response shows the compliance settings for a bucket in which each object will be retained for one year (525,600 minutes), starting from when the object is ingested into the grid. There is currently no legal hold on this bucket. Each object will be automatically deleted after one year.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

| Name | Description |
|---|---|
| RetentionPeriodMinutes | The length of the retention period for objects added to this bucket, in minutes. The retention period starts when the object is ingested into the grid. |

| Name | Description |
| --- | --- |
| LegalHold | • True: This bucket is currently under a legal hold. Objects in this bucket can't be deleted until the legal hold is lifted, even if their retention period has expired.<br>• False: This bucket is not currently under a legal hold. Objects in this bucket can be deleted when their retention period expires. |
| AutoDelete | • True: The objects in this bucket will be deleted automatically when their retention period expires, unless the bucket is under a legal hold.<br>• False: The objects in this bucket will not be deleted automatically when the retention period expires. You must delete these objects manually if you need to delete them. |

#### Error responses

If the bucket was not created to be compliant, the HTTP status code for the response is `404 Not Found`, with an S3 error code of `XNoSuchBucketCompliance`.

## Deprecated: PUT Bucket compliance request

The PUT Bucket compliance request is deprecated. However, you can continue to use this request to modify the compliance settings for an existing legacy Compliant bucket. For example, you can place an existing bucket on legal hold or increase its retention period.

> The StorageGRID Compliance feature that was available in previous StorageGRID versions is deprecated and has been replaced by S3 Object Lock. See the following for more details:
>
> • Use S3 REST API to configure S3 Object Lock
> • NetApp Knowledge Base: How to manage legacy Compliant buckets in StorageGRID 11.5

You must have the s3:PutBucketCompliance permission, or be account root, to complete this operation.

You must specify a value for every field of the compliance settings when issuing a PUT Bucket compliance request.

#### Request example

This example request modifies the compliance settings for the bucket named `mybucket`. In this example, objects in `mybucket` will now be retained for two years (1,051,200 minutes) instead of one year, starting from when the object is ingested into the grid. There is no legal hold on this bucket. Each object will be automatically deleted after two years.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

| Name | Description |
|---|---|
| RetentionPeriodMinutes | The length of the retention period for objects added to this bucket, in minutes. The retention period starts when the object is ingested into the grid.<br><br>**Important** When specifying a new value for RetentionPeriodMinutes, you must specify a value that is equal to or greater than the bucket's current retention period. After the bucket's retention period is set, you can't decrease that value; you can only increase it. |
| LegalHold | • True: This bucket is currently under a legal hold. Objects in this bucket can't be deleted until the legal hold is lifted, even if their retention period has expired.<br>• False: This bucket is not currently under a legal hold. Objects in this bucket can be deleted when their retention period expires. |
| AutoDelete | • True: The objects in this bucket will be deleted automatically when their retention period expires, unless the bucket is under a legal hold.<br>• False: The objects in this bucket will not be deleted automatically when the retention period expires. You must delete these objects manually if you need to delete them. |

**Consistency for compliance settings**

When you update the compliance settings for an S3 bucket with a PUT Bucket compliance request, StorageGRID attempts to update the bucket's metadata across the grid. By default, StorageGRID uses the **Strong-global** consistency to guarantee that all data center sites and all Storage Nodes that contain bucket metadata have read-after-write consistency for the changed compliance settings.

If StorageGRID can't achieve the **Strong-global** consistency because a data center site or multiple Storage Nodes at a site are unavailable, the HTTP status code for the response is `503 Service Unavailable`.

If you receive this response, you must contact the grid administrator to ensure that the required storage services are made available as soon as possible. If the grid administrator is unable to make enough of the

Storage Nodes at each site available, technical support might direct you to retry the failed request by forcing the **Strong-site** consistency.

> Never force the **Strong-site** consistency for PUT bucket compliance unless you have been directed to do so by technical support and unless you understand the potential consequences of using this level.

When the consistency is reduced to **Strong-site**, StorageGRID guarantees that updated compliance settings will have read-after-write consistency only for client requests within a site. This means that the StorageGRID system might temporarily have multiple, inconsistent settings for this bucket until all sites and Storage Nodes are available. The inconsistent settings can result in unexpected and undesired behavior. For example, if you are placing a bucket under a legal hold and you force a lower consistency, the bucket's previous compliance settings (that is, legal hold off) might continue to be in effect at some data center sites. As a result, objects that you think are on legal hold might be deleted when their retention period expires, either by the user or by AutoDelete, if enabled.

To force the use of the **Strong-site** consistency, reissue the PUT Bucket compliance request and include the `Consistency-Control` HTTP request header, as follows:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

### Error responses

- If the bucket was not created to be compliant, the HTTP status code for the response is `404 Not Found`.
- If `RetentionPeriodMinutes` in the request is less than the bucket's current retention period, the HTTP status code is `400 Bad Request`.

### Related information

Deprecated: PUT Bucket request modifications for compliance

## Copyright information



## Trademark information