



# **Managing Storage Nodes**

StorageGRID 11.5

NetApp  
January 04, 2024

This PDF was generated from <https://docs.netapp.com/us-en/storagegrid-115/admin/what-storage-node-is.html> on January 04, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

- Managing Storage Nodes. . . . . 1
  - What a Storage Node is . . . . . 1
  - Managing Storage Options . . . . . 5
  - Managing object metadata storage . . . . . 9
  - Configuring global settings for stored objects . . . . . 16
  - Storage Node configuration settings . . . . . 19
  - Managing full Storage Nodes . . . . . 23

# Managing Storage Nodes

Storage Nodes provide disk storage capacity and services. Managing Storage Nodes entails monitoring the amount of usable space on each node, using watermark settings, and applying Storage Node configuration settings.

- [What a Storage Node is](#)
- [Managing Storage Options](#)
- [Managing object metadata storage](#)
- [Configuring global settings for stored objects](#)
- [Storage Node configuration settings](#)
- [Managing full Storage Nodes](#)

## What a Storage Node is

Storage Nodes manage and store object data and metadata. Each StorageGRID system must have at least three Storage Nodes. If you have multiple sites, each site within your StorageGRID system must also have three Storage Nodes.

A Storage Node includes the services and processes required to store, move, verify, and retrieve object data and metadata on disk. You can view detailed information about the Storage Nodes on the **Nodes** page.

## What the ADC service is

The Administrative Domain Controller (ADC) service authenticates grid nodes and their connections with each other. The ADC service is hosted on each of the first three Storage Nodes at a site.

The ADC service maintains topology information including the location and availability of services. When a grid node requires information from another grid node or an action to be performed by another grid node, it contacts an ADC service to find the best grid node to process its request. In addition, the ADC service retains a copy of the StorageGRID deployment's configuration bundles, allowing any grid node to retrieve current configuration information. You can view ADC information for a Storage Node on the Grid Topology page (**Support > Grid Topology**).

To facilitate distributed and islanded operations, each ADC service synchronizes certificates, configuration bundles, and information about services and topology with the other ADC services in the StorageGRID system.

In general, all grid nodes maintain a connection to at least one ADC service. This ensures that grid nodes are always accessing the latest information. When grid nodes connect, they cache other grid nodes' certificates, enabling systems to continue functioning with known grid nodes even when an ADC service is unavailable. New grid nodes can only establish connections by using an ADC service.

The connection of each grid node lets the ADC service gather topology information. This grid node information includes the CPU load, available disk space (if it has storage), supported services, and the grid node's site ID. Other services ask the ADC service for topology information through topology queries. The ADC service responds to each query with the latest information received from the StorageGRID system.

## What the DDS service is

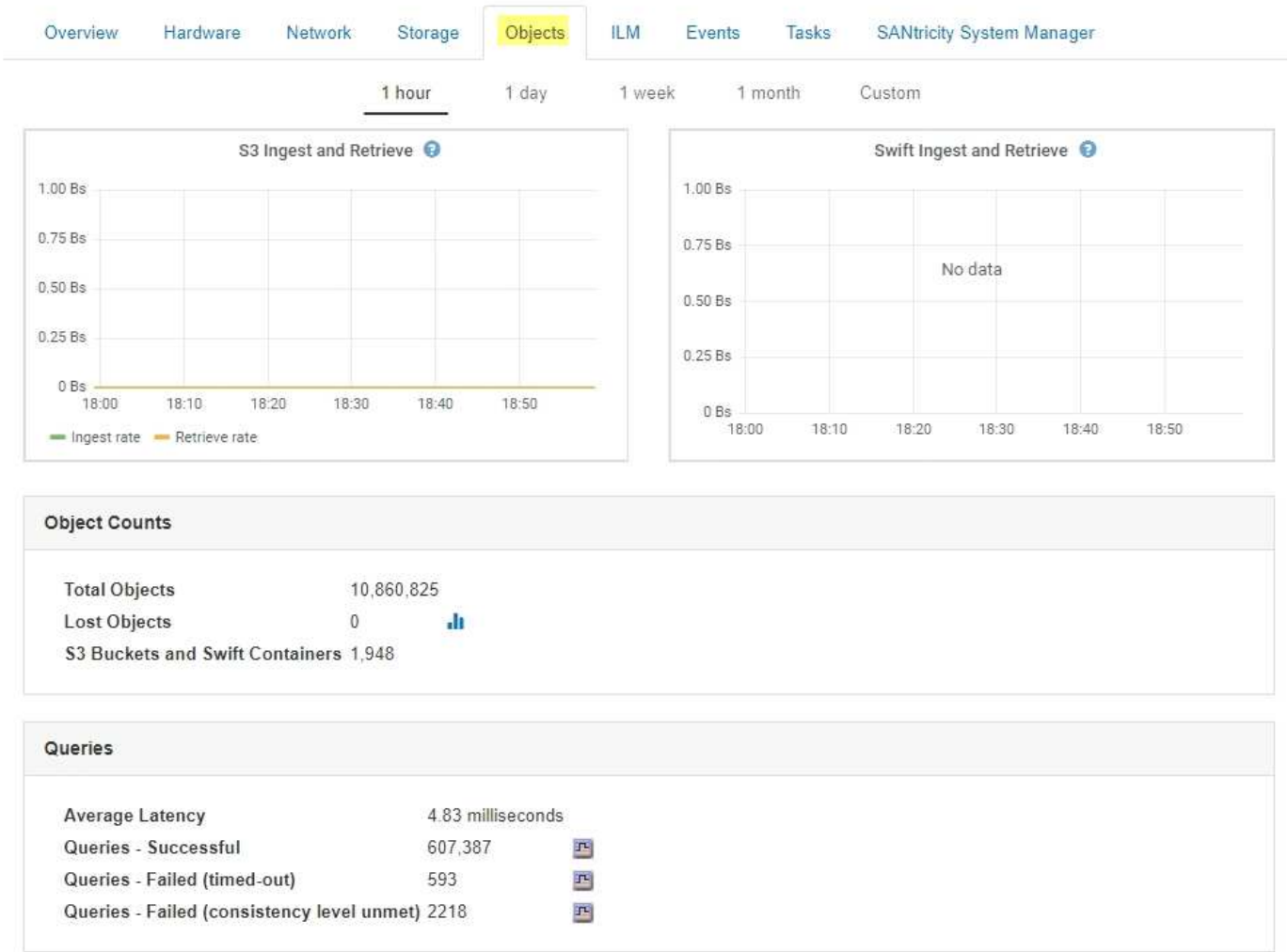
Hosted by a Storage Node, the Distributed Data Store (DDS) service interfaces with the Cassandra database to perform background tasks on the object metadata stored in the StorageGRID system.

### Object counts

The DDS service tracks the total number of objects ingested into the StorageGRID system as well as the total number of objects ingested through each of the system’s supported interfaces (S3 or Swift).

You can see the Total Objects count on the Nodes page > Objects tab for any Storage Node.

ST-DC2-SG-5712-1 (Storage Node)



### Queries

You can identify the average time that it takes to run a query against the metadata store through the specific DDS service, the total number of successful queries, and the total number of queries that failed because of a timeout issue.

You might want to review query information to monitor the health of the metadata store, Cassandra, which impacts the system’s ingest and retrieval performance. For example, if the latency for an average query is slow and the number of failed queries due to timeouts is high, the metadata store might be encountering a higher load or performing another operation.

You can also view the total number of queries that failed because of consistency failures. Consistency level failures result from an insufficient number of available metadata stores at the time a query is performed through the specific DDS service.

You can use the Diagnostics page to obtain additional information on the current state of your grid. See [Running diagnostics](#).

## Consistency guarantees and controls

StorageGRID guarantees read-after-write consistency for newly created objects. Any GET operation following a successfully completed PUT operation will be able to read the newly written data. Overwrites of existing objects, metadata updates, and deletes remain eventually consistent.

## What the LDR service is

Hosted by each Storage Node, the Local Distribution Router (LDR) service handles content transport for the StorageGRID system. Content transport encompasses many tasks including data storage, routing, and request handling. The LDR service does the majority of the StorageGRID system's hard work by handling data transfer loads and data traffic functions.

The LDR service handles the following tasks:

- Queries
- Information lifecycle management (ILM) activity
- Object deletion
- Object data storage
- Object data transfers from another LDR service (Storage Node)
- Data storage management
- Protocol interfaces (S3 and Swift)

The LDR service also manages the mapping of S3 and Swift objects to the unique "content handles" (UUIDs) that the StorageGRID system assigns to each ingested object.

## Queries

LDR queries include queries for object location during retrieve and archive operations. You can identify the average time that it takes to run a query, the total number of successful queries, and the total number of queries that failed because of a timeout issue.

You can review query information to monitor the health of the metadata store, which impacts the system's ingest and retrieval performance. For example, if the latency for an average query is slow and the number of failed queries due to timeouts is high, the metadata store might be encountering a higher load or performing another operation.

You can also view the total number of queries that failed because of consistency failures. Consistency level failures result from an insufficient number of available metadata stores at the time a query is performed through the specific LDR service.

You can use the Diagnostics page to obtain additional information on the current state of your grid. See [Running diagnostics](#).

















































## ILM activity

Information lifecycle management (ILM) metrics allow you to monitor the rate at which objects are evaluated for ILM implementation. You can view these metrics on the Dashboard or on the Nodes page > ILM tab for each Storage Node.

## Object stores

The underlying data storage of an LDR service is divided into a fixed number of object stores (also known as storage volumes). Each object store is a separate mount point.

You can see the object stores for a Storage Node on the Nodes page > Storage tab.

Object Stores							
ID	Size	Available		Replicated Data	EC Data	Object Data (%)	Health
0000	4.40 TB	1.35 TB		43.99 GB	 0 bytes	 1.00%	No Errors
0001	1.97 TB	1.57 TB		44.76 GB	 351.14 GB	 20.09%	No Errors
0002	1.97 TB	1.46 TB		43.29 GB	 465.20 GB	 25.81%	No Errors
0003	1.97 TB	1.70 TB		43.51 GB	 223.98 GB	 13.58%	No Errors
0004	1.97 TB	1.92 TB		44.03 GB	 0 bytes	 2.23%	No Errors
0005	1.97 TB	1.46 TB		43.67 GB	 463.36 GB	 25.73%	No Errors
0006	1.97 TB	1.92 TB		43.10 GB	 1.61 GB	 2.27%	No Errors
0007	1.97 TB	1.35 TB		46.05 GB	 575.24 GB	 31.53%	No Errors
0008	1.97 TB	1.81 TB		46.00 GB	 112.84 GB	 8.06%	No Errors
0009	1.97 TB	1.57 TB		43.91 GB	 352.72 GB	 20.13%	No Errors
000A	1.97 TB	1.70 TB		44.31 GB	 226.81 GB	 13.76%	No Errors
000B	1.97 TB	1.92 TB		43.17 GB	 780.07 MB	 2.23%	No Errors
000C	1.97 TB	1.58 TB		44.32 GB	 339.56 GB	 19.48%	No Errors
000D	1.97 TB	1.82 TB		44.47 GB	 107.34 GB	 7.70%	No Errors
000E	1.97 TB	1.68 TB		43.07 GB	 241.70 GB	 14.45%	No Errors
000F	2.03 TB	1.50 TB		44.57 GB	 475.47 GB	 25.67%	No Errors

The object stores in a Storage Node are identified by a hexadecimal number from 0000 to 002F, which is known as the volume ID. Space is reserved in the first object store (volume 0) for object metadata in a Cassandra database; any remaining space on that volume is used for object data. All other object stores are used exclusively for object data, which includes replicated copies and erasure-coded fragments.

To ensure even space usage for replicated copies, object data for a given object is stored to one object store based on available storage space. When one or more object stores fill to capacity, the remaining object stores continue to store objects until there is no more room on the Storage Node.

## Metadata protection

Object metadata is information related to or a description of an object; for example, object modification time, or storage location. StorageGRID stores object metadata in a Cassandra database, which interfaces with the LDR service.

To ensure redundancy and thus protection against loss, three copies of object metadata are maintained at each site. The copies are evenly distributed across all Storage Nodes at each site. This replication is non-configurable and performed automatically.

## Managing Storage Options


You can view and configure Storage Options using the Configuration menu in the Grid Manager. Storage Options include the object segmentation settings and the current values for storage watermarks. You can also view the S3 and Swift ports used by the deprecated CLB service on Gateway Nodes and by the LDR service on Storage Nodes.

For information on port assignments, see [Summary: IP addresses and ports for client connections](#).

Storage Options

Overview

Configuration



### Storage Options Overview

Updated: 2019-03-22 12:49:16 MDT

---

#### Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

#### Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

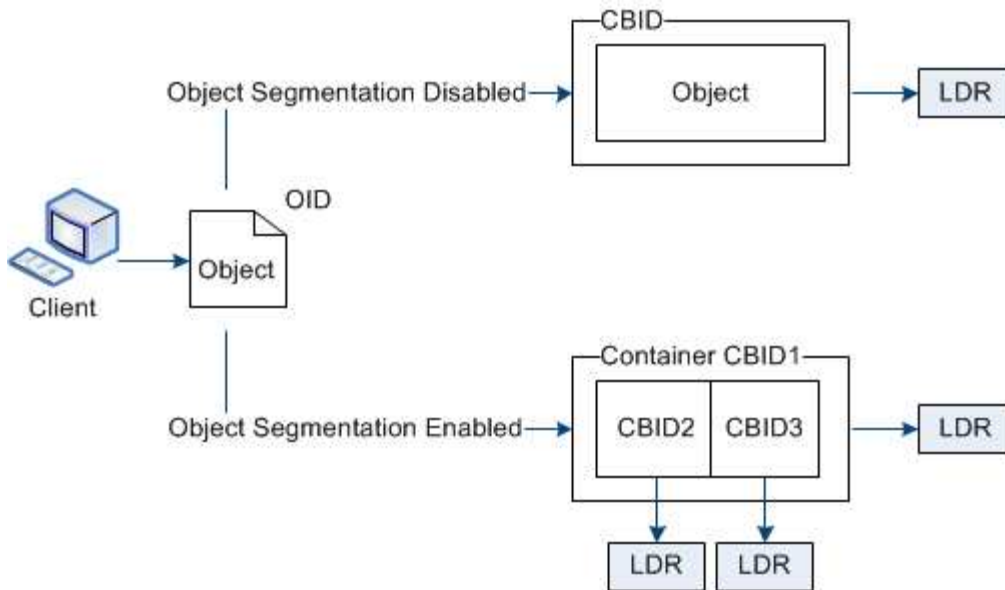
#### Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

### What object segmentation is

Object segmentation is the process of splitting up an object into a collection of smaller fixed-size objects in order to optimize storage and resources usage for large objects. S3 multi-part upload also creates segmented objects, with an object representing each part.

When an object is ingested into the StorageGRID system, the LDR service splits the object into segments, and creates a segment container that lists the header information of all segments as content.



If your StorageGRID system includes an Archive Node whose Target Type is Cloud Tiering — Simple Storage Service and the targeted archival storage system is Amazon Web Services (AWS), the Maximum Segment Size must be less than or equal to 4.5 GiB (4,831,838,208 bytes). This upper limit ensures that the AWS PUT limitation of five GBs is not exceeded. Requests to AWS that exceed this value fail.

On retrieval of a segment container, the LDR service assembles the original object from its segments and returns the object to the client.

The container and segments are not necessarily stored on the same Storage Node. Container and segments can be stored on any Storage Node.

Each segment is treated by the StorageGRID system independently and contributes to the count of attributes such as Managed Objects and Stored Objects. For example, if an object stored to the StorageGRID system is split into two segments, the value of Managed Objects increases by three after the ingest is complete, as follows:

segment container + segment 1 + segment 2 = three stored objects

You can improve performance when handling large objects by ensuring that:

- Each Gateway and Storage Node has sufficient network bandwidth for the throughput required. For example, configure separate Grid and Client Networks on 10 Gbps Ethernet interfaces.
- Enough Gateway and Storage Nodes are deployed for the throughput required.
- Each Storage Node has sufficient disk IO performance for the throughput required.

## What Storage Volume watermarks are

StorageGRID uses Storage Volume watermarks to allow you to monitor the amount of usable space available on Storage Nodes. If the amount of space available on a node is less than a configured watermark setting, the Storage Status (SSTS) alarm is triggered so that you can determine if you need to add Storage Nodes.

To view the current settings for the Storage Volume watermarks, select **Configuration > Storage Options > Overview**.





## Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

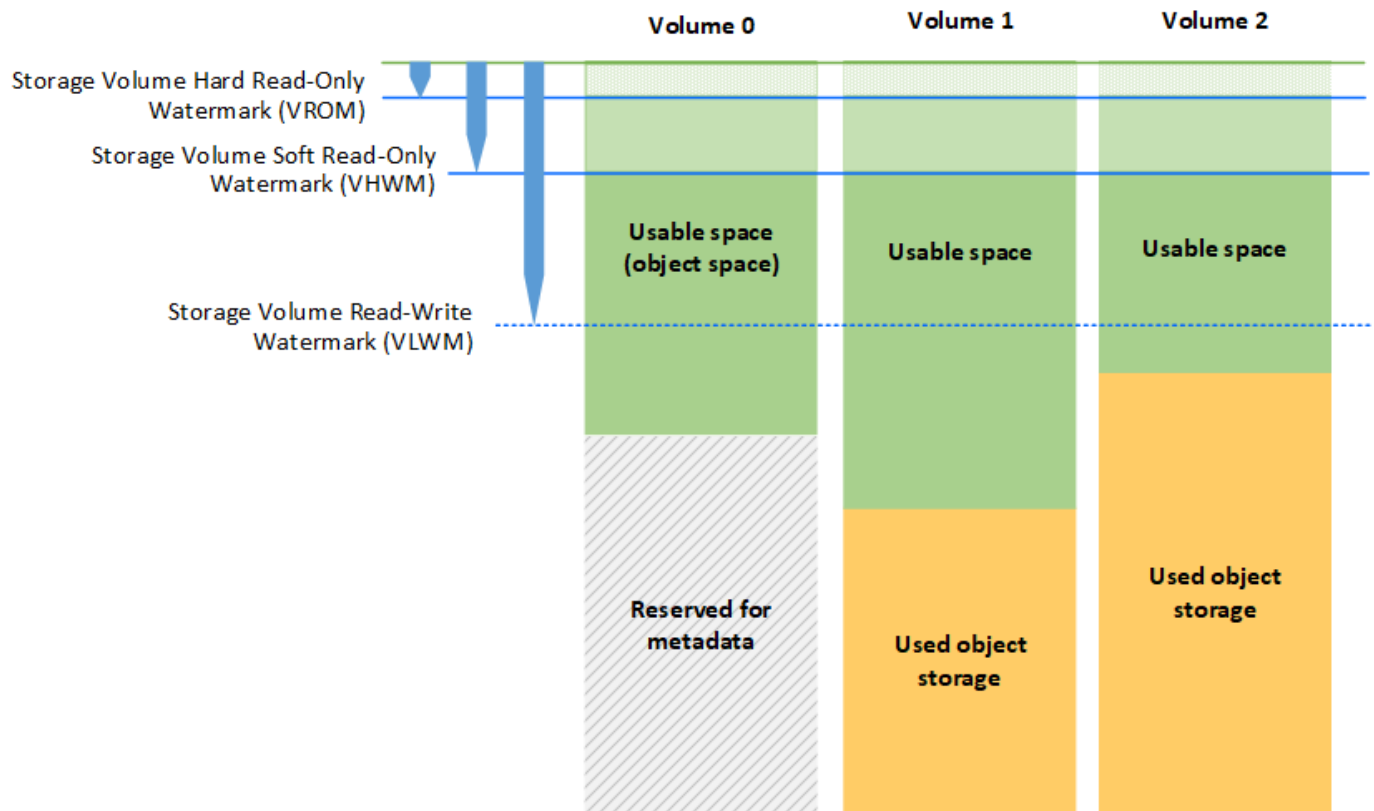
### Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

### Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

The following figure represents a Storage Node that has three volumes and shows the relative position of the three Storage Volume watermarks. Within each Storage Node, StorageGRID reserves space on volume 0 for object metadata; any remaining space on that volume is used for object data. All other volumes are used exclusively for object data, which includes replicated copies and erasure-coded fragments.



The Storage Volume watermarks are system-wide defaults that indicate the minimum amount of free space required on each volume in the Storage Node to prevent StorageGRID from changing the node's read-write behavior or triggering an alarm. Note that all volumes must reach the watermark before StorageGRID takes action. If some volumes have more than the minimum required amount of free space, the alarm is not triggered and the node's read-write behavior does not change.

### Storage Volume Soft Read-Only Watermark (VHWM)

The Storage Volume Soft Read-Only Watermark is the first watermark to indicate that a node's usable space for object data is becoming full. This watermark represents how much free space must exist on every volume in a Storage Node to prevent the node from going into "soft read-only mode." Soft read-only mode means that the Storage Node advertises read-only services to the rest of the StorageGRID system, but fulfills all pending write requests.

If the amount of free space on each volume is less than the setting of this watermark, the Storage Status (SSTS) alarm is triggered at the Notice level, and the Storage Node transitions to soft read-only mode.

For example, suppose the Storage Volume Soft Read-Only Watermark is set to 10 GB, which is its default value. If less than 10 GB of free space remains on each volume in the Storage Node, the SSTS alarm is triggered at the Notice level, and the Storage Node transitions to soft read-only mode.

### Storage Volume Hard Read-Only Watermark (VROM)

The Storage Volume Hard Read-Only Watermark is the next watermark to indicate that a node's usable space

for object data is becoming full. This watermark represents how much free space must exist on every volume in a Storage Node to prevent the node from going in to “hard read-only mode.” Hard read-only mode means that the Storage Node is read-only and no longer accepts write requests.

If the amount of free space on every volume in a Storage Node is less than the setting of this watermark, the Storage Status (SSTS) alarm is triggered at the Major level, and the Storage Node transitions to hard read-only mode.

For example, suppose the Storage Volume Hard Read-Only Watermark is set to 5 GB, which is its default value. If less than 5 GB of free space remains on each storage volume in the Storage Node, the SSTS alarm is triggered at the Major level, and the Storage Node transitions to hard read-only mode.

The value of the Storage Volume Hard Read-Only Watermark must be less than the value of the Storage Volume Soft Read-Only Watermark.

### **Storage Volume Read-Write Watermark (VLWM)**

The Storage Volume Read-Write Watermark only applies to Storage Nodes that have transitioned to read-only mode. This watermark determines when the Storage Node is allowed to become read-write again.

For example, suppose a Storage Node has transitioned to hard read-only mode. If the Storage Volume Read-Write Watermark is set to 30 GB (default), the free space on every storage volume in the Storage Node must increase from 5 GB to 30 GB before the node can become read-write again.

The value of the Storage Volume Read-Write Watermark must be greater than the value of the Storage Volume Soft Read-Only Watermark.

### **Related information**

[Managing full Storage Nodes](#)

## **Managing object metadata storage**

The object metadata capacity of a StorageGRID system controls the maximum number of objects that can be stored on that system. To ensure that your StorageGRID system has adequate space to store new objects, you must understand where and how StorageGRID stores object metadata.

### **What is object metadata?**

Object metadata is any information that describes an object. StorageGRID uses object metadata to track the locations of all objects across the grid and to manage each object’s lifecycle over time.

For an object in StorageGRID, object metadata includes the following types of information:

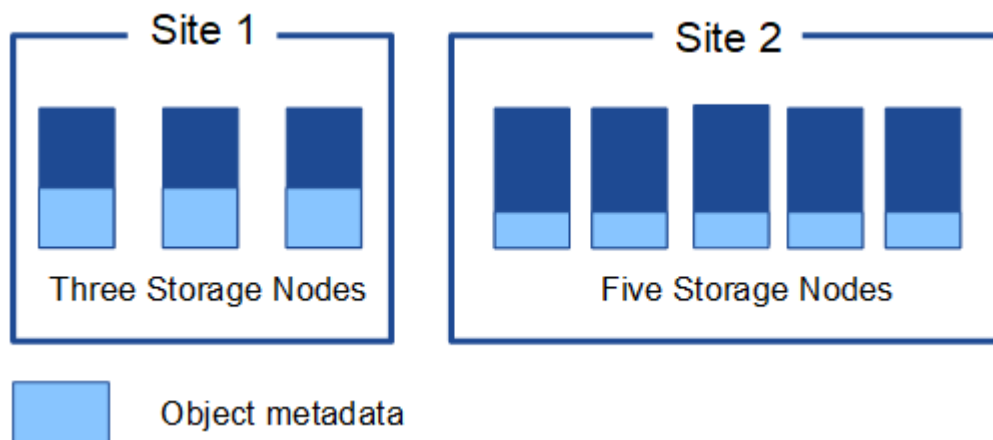
- System metadata, including a unique ID for each object (UUID), the object name, the name of the S3 bucket or Swift container, the tenant account name or ID, the logical size of the object, the date and time the object was first created, and the date and time the object was last modified.
- Any custom user metadata key-value pairs associated with the object.
- For S3 objects, any object tag key-value pairs associated with the object.
- For replicated object copies, the current storage location of each copy.
- For erasure-coded object copies, the current storage location of each fragment.

- For object copies in a Cloud Storage Pool, the location of the object, including the name of the external bucket and the object's unique identifier.
- For segmented objects and multipart objects, segment identifiers and data sizes.

## How is object metadata stored?

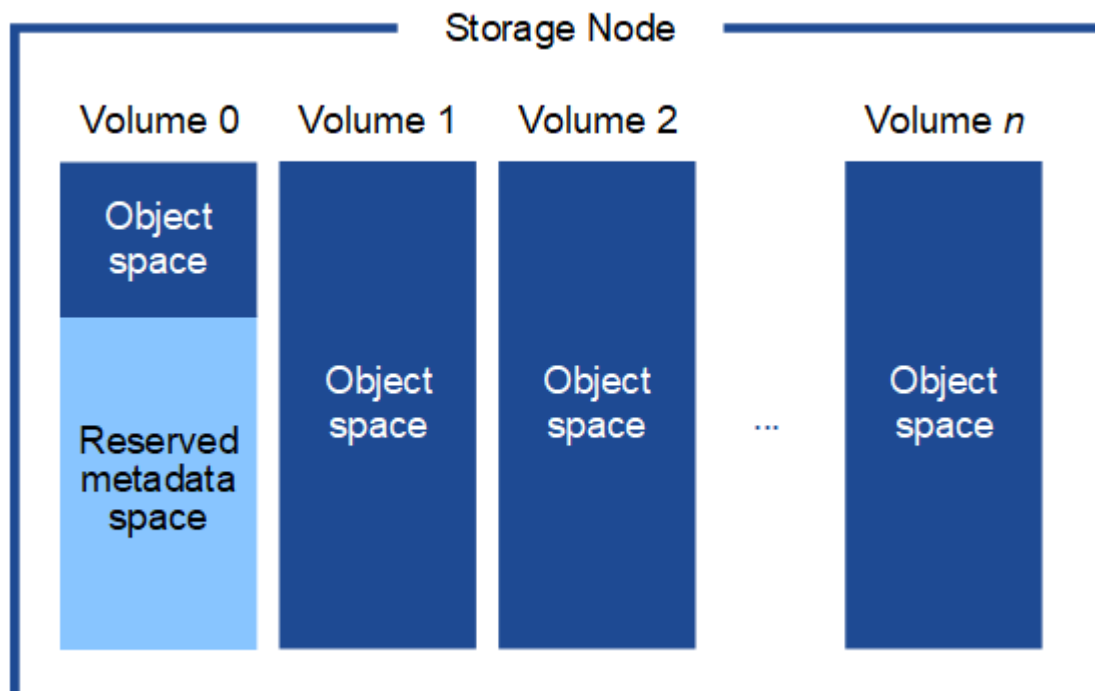
StorageGRID maintains object metadata in a Cassandra database, which is stored independently of object data. To provide redundancy and to protect object metadata from loss, StorageGRID stores three copies of the metadata for all objects in the system at each site. The three copies of object metadata are evenly distributed across all Storage Nodes at each site.

This figure represents the Storage Nodes at two sites. Each site has the same amount of object metadata, which is equally distributed across the Storage Nodes at that site.



## Where is object metadata stored?

This figure represents the storage volumes for a single Storage Node.



As shown in the figure, StorageGRID reserves space for object metadata on storage volume 0 of each Storage Node. It uses the reserved space to store object metadata and to perform essential database operations. Any remaining space on storage volume 0 and all other storage volumes in the Storage Node are used exclusively for object data (replicated copies and erasure-coded fragments).

The amount of space that is reserved for object metadata on a particular Storage Node depends on a number of factors, which are described below.

## Metadata Reserved Space setting

The *Metadata Reserved Space* is a system-wide setting that represents the amount of space that will be reserved for metadata on volume 0 of every Storage Node. As shown in the table, the default value of this setting for StorageGRID 11.5 is based the following:

- The software version you were using when you initially installed StorageGRID.
- The amount of RAM on each Storage Node.

Version used for initial StorageGRID installation	Amount of RAM on Storage Nodes	Default Metadata Reserved Space setting for StorageGRID 11.5
11.5	128 GB or more on each Storage Node in the grid	8 TB (8,000 GB)
	Less than 128 GB on any Storage Node in the grid	3 TB (3,000 GB)
11.1 to 11.4	128 GB or more on each Storage Node at any one site	4 TB (4,000 GB)
	Less than 128 GB on any Storage Node at each site	3 TB (3,000 GB)
11.0 or earlier	Any amount	2 TB (2,000 GB)

To view the Metadata Reserved Space setting for your StorageGRID system:

1. Select **Configuration > System Settings > Storage Options**.
2. In the Storage Watermarks table, locate **Metadata Reserved Space**.



## Storage Options Overview

Updated: 2021-02-23 11:58:33 MST

### Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

### Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	8,000 GB

In the screenshot, the **Metadata Reserved Space** value is 8,000 GB (8 TB). This is the default setting for a new StorageGRID 11.5 installation in which each Storage Node has 128 GB or more of RAM.

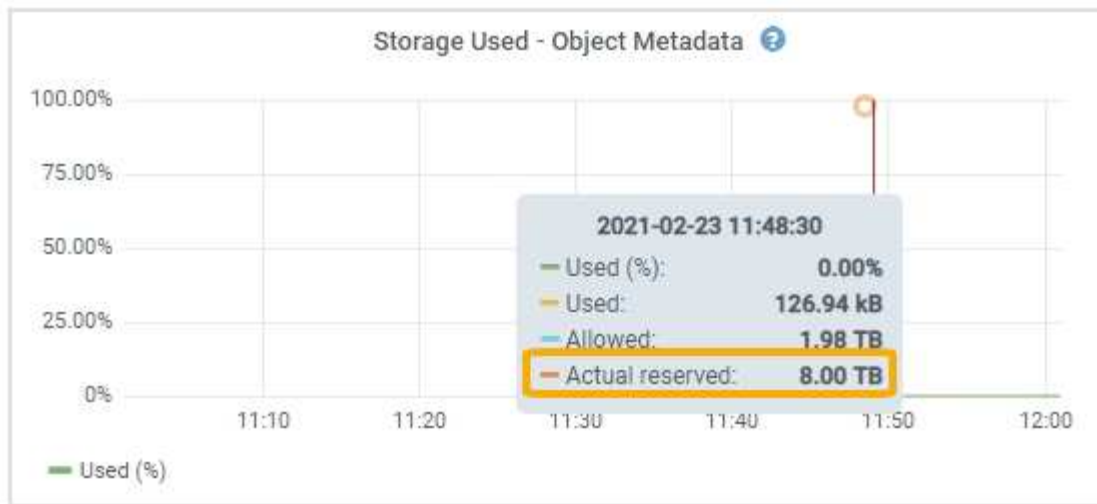
### Actual reserved space for metadata

In contrast to the system-wide Metadata Reserved Space setting, the *actual reserved space* for object metadata is determined for each Storage Node. For any given Storage Node, the actual reserved space for metadata depends on the size of volume 0 for the node and the system-wide **Metadata Reserved Space** setting.

Size of volume 0 for the node	Actual reserved space for metadata
Less than 500 GB (non production use)	10% of volume 0
500 GB or more	The smaller of these values: <ul style="list-style-type: none"><li>• Volume 0</li><li>• Metadata Reserved Space setting</li></ul>

To view the actual reserved space for metadata on a particular Storage Node:

1. From the Grid Manager, select **Nodes > Storage Node**.
2. Select the **Storage** tab.
3. Hover your cursor over the Storage Used — Object Metadata chart and locate the **Actual reserved** value.



In the screenshot, the **Actual reserved** value is 8 TB. This screenshot is for a large Storage Node in a new StorageGRID 11.5 installation. Because the system-wide Metadata Reserved Space setting is smaller than volume 0 for this Storage Node, the actual reserved space for this node equals the Metadata Reserved Space setting.

The **Actual reserved** value corresponds to this Prometheus metric:

```
storagegrid_storage_utilization_metadata_reserved_bytes
```

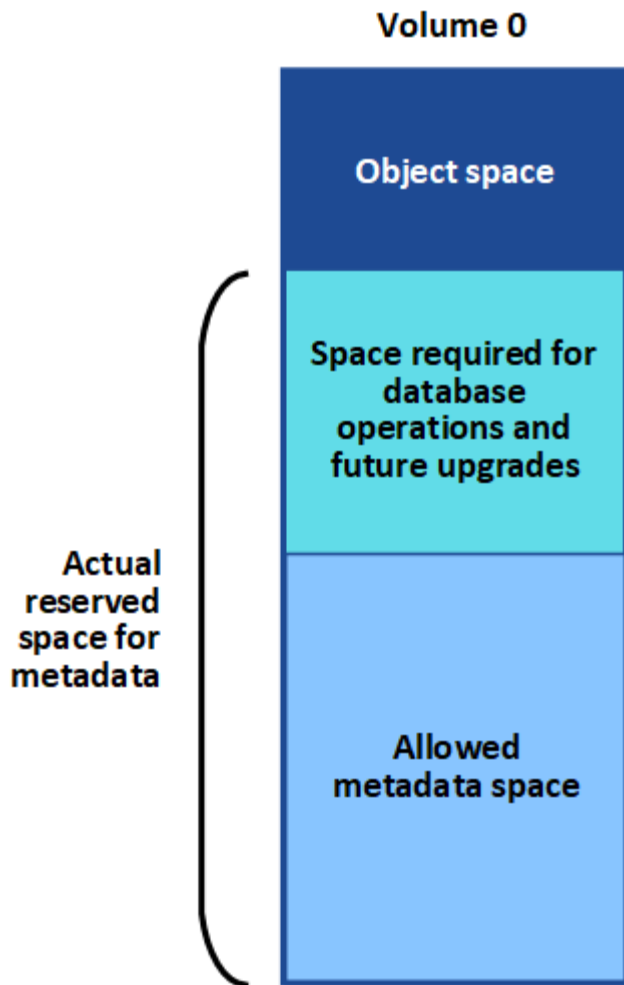
## Example for actual reserved metadata space

Suppose you install a new StorageGRID system using version 11.5. For this example, assume that each Storage Node has more than 128 GB of RAM and that volume 0 of Storage Node 1 (SN1) is 6 TB. Based on these values:

- The system-wide **Metadata Reserved Space** is set to 8 TB. (This is the default value for a new StorageGRID 11.5 installation if each Storage Node has more than 128 GB RAM.)
- The actual reserved space for metadata for SN1 is 6 TB. (The entire volume is reserved because volume 0 is smaller than the **Metadata Reserved Space** setting.)

## Allowed metadata space

Each Storage Node's actual reserved space for metadata is subdivided into the space available for object metadata (the *allowed metadata space*) and the space required for essential database operations (such as compaction and repair) and future hardware and software upgrades. The allowed metadata space governs overall object capacity.



The following table summarizes how StorageGRID determines the allowed metadata space value for a Storage Node.

Actual reserved space for metadata	Allowed metadata space
4 TB or less	60% of actual reserved space for metadata, up to a maximum of 1.98 TB
More than 4 TB	$(\text{Actual reserved space for metadata} - 1 \text{ TB}) \times 60\%$ , up to a maximum of 2.64 TB



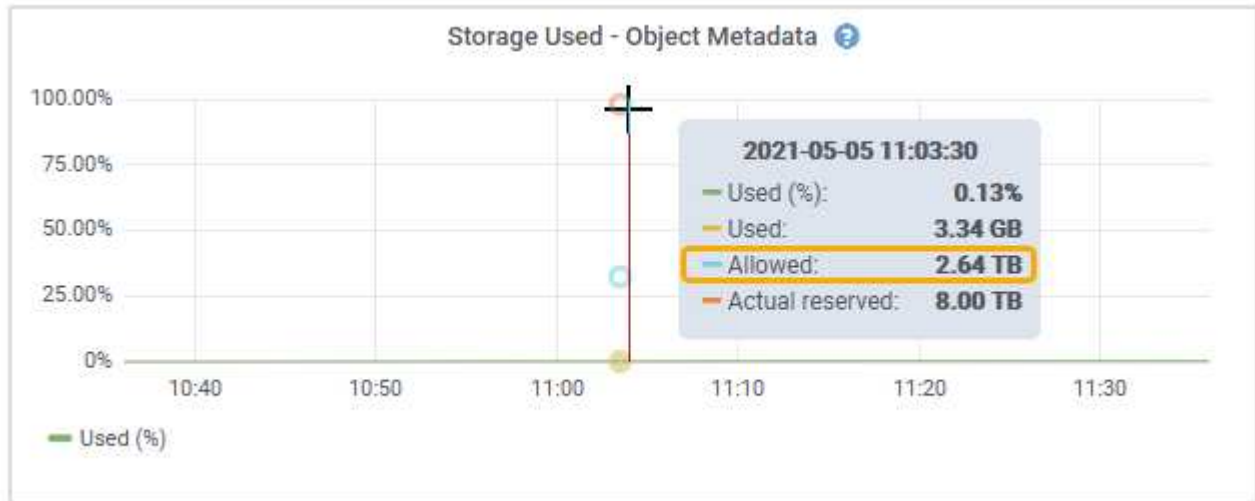
If your StorageGRID system stores (or is expected to store) more than 2.64 TB of metadata on any Storage Node, the allowed metadata space can be increased in some cases. If your Storage Nodes each have more than 128 GB of RAM and available free space on storage volume 0, contact your NetApp account representative. NetApp will review your requirements and increase the allowed metadata space for each Storage Node, if possible.

To view the allowed metadata space for a Storage Node:

1. From the Grid Manager, select **Node > Storage Node**.
2. Select the **Storage** tab.



3. Hover your cursor over the Storage Used — Object Metadata chart and locate the **Allowed** value.



In the screenshot, the **Allowed** value is 2.64 TB, which is the maximum value for a Storage Node whose actual reserved space for metadata is more than 4 TB.

The **Allowed** value corresponds to this Prometheus metric:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

## Example for allowed metadata space

Suppose you install a StorageGRID system using version 11.5. For this example, assume that each Storage Node has more than 128 GB of RAM and that volume 0 of Storage Node 1 (SN1) is 6 TB. Based on these values:

- The system-wide **Metadata Reserved Space** is set to 8 TB. (This is the default value for StorageGRID 11.5 when each Storage Node has more than 128 GB RAM.)
- The actual reserved space for metadata for SN1 is 6 TB. (The entire volume is reserved because volume 0 is smaller than the **Metadata Reserved Space** setting.)
- The allowed space for metadata on SN1 is 2.64 TB. (This is the maximum value for actual reserved space.)

## How Storage Nodes of different sizes affect object capacity

As described above, StorageGRID evenly distributes object metadata across the Storage Nodes at each site. For this reason, if a site contains Storage Nodes of different sizes, the smallest node at the site determines the site's metadata capacity.

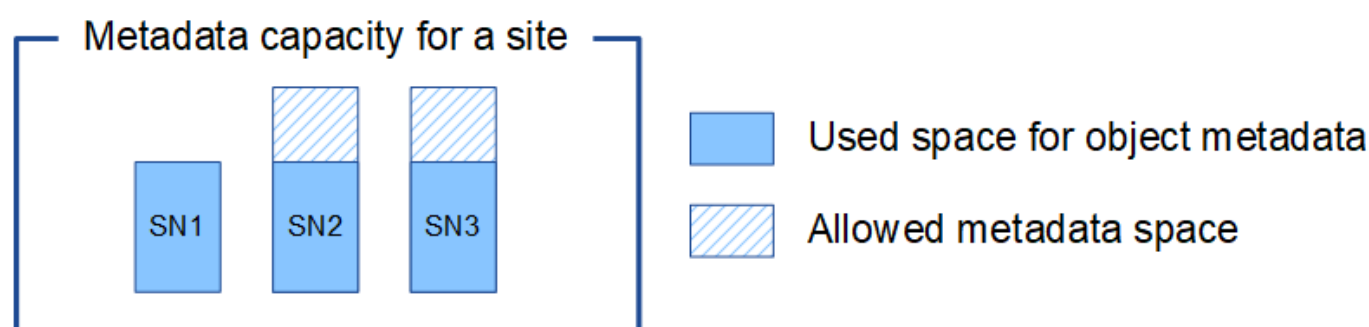
Consider the following example:

- You have a single-site grid containing three Storage Nodes of different sizes.
- The **Metadata Reserved Space** setting is 4 TB.
- The Storage Nodes have the following values for the actual reserved metadata space and the allowed

metadata space.

Storage Node	Size of volume 0	Actual reserved metadata space	Allowed metadata space
SN1	2.2 TB	2.2 TB	1.32 TB
SN2	5 TB	4 TB	1.98 TB
SN3	6 TB	4 TB	1.98 TB

Because object metadata is evenly distributed across the Storage Nodes at a site, each node in this example can only hold 1.32 TB of metadata. The additional 0.66 TB of allowed metadata space for SN2 and SN3 cannot be used.



Similarly, because StorageGRID maintains all object metadata for a StorageGRID system at each site, the overall metadata capacity of a StorageGRID system is determined by the object metadata capacity of the smallest site.

And because object metadata capacity controls the maximum object count, when one node runs out of metadata capacity, the grid is effectively full.

#### Related information

- To learn how to monitor the object metadata capacity for each Storage Node:

[Monitor & troubleshoot](#)

- To increase the object metadata capacity for your system, you must add new Storage Nodes:

[Expand your grid](#)

## Configuring global settings for stored objects

You can use Grid Options to configure the settings for all of the objects stored in your StorageGRID system, including stored object compression, stored object encryption, and stored object hashing.

- [Configuring stored object compression](#)
- [Configuring stored object encryption](#)

- [Configuring stored object hashing](#)

## Configuring stored object compression

You can use the Compress Stored Objects grid option to reduce the size of objects stored in StorageGRID, so that objects consume less storage.

### What you'll need

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

### About this task

The Compress Stored Objects grid option is disabled by default. If you enable this option, StorageGRID attempts to compress each object when saving it, using lossless compression.



If you change this setting, it will take about one minute for the new setting to be applied. The configured value is cached for performance and scaling.

Before enabling this option, be aware of the following:

- You should not enable compression unless you know that the data being stored is compressible.
- Applications that save objects to StorageGRID might compress objects before saving them. If a client application has already compressed an object before saving it to StorageGRID, enabling Compress Stored Objects will not further reduce an object's size.
- Do not enable compression if you are using NetApp FabricPool with StorageGRID.
- If the Compress Stored Objects grid option is enabled, S3 and Swift client applications should avoid performing GET Object operations that specify a range of bytes be returned. These “range read” operations are inefficient because StorageGRID must effectively uncompress the objects to access the requested bytes. GET Object operations that request a small range of bytes from a very large object are especially inefficient; for example, it is inefficient to read a 10 MB range from a 50 GB compressed object.

If ranges are read from compressed objects, client requests can time out.



If you need to compress objects and your client application must use range reads, increase the read timeout for the application.

### Steps

1. Select **Configuration > System Settings > Grid Options**.
2. In the Stored Object Options section, select the **Compress Stored Objects** check box.

## Stored Object Options



Compress Stored Objects ? 

Stored Object Encryption ? ☒ None ☐ AES-128 ☐ AES-256

Stored Object Hashing ? ☒ SHA-1 ☐ SHA-256

3. Click **Save**.

## Configuring stored object encryption

You can encrypt stored objects if you want to ensure that data cannot be retrieved in a readable form if an object store is compromised. By default, objects are not encrypted.

### What you'll need

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

### About this task

Stored object encryption enables the encryption of all object data as it is ingested through S3 or Swift. When you enable the setting, all newly ingested objects are encrypted but no change is made to existing stored objects. If you disable encryption, currently encrypted objects remain encrypted but newly ingested objects are not encrypted.



If you change this setting, it will take about one minute for the new setting to be applied. The configured value is cached for performance and scaling.



Stored objects can be encrypted using the AES-128 or AES-256 encryption algorithm.

The Stored Object Encryption setting applies only to S3 objects that have not been encrypted by bucket-level or object-level encryption.

### Steps

1. Select **Configuration > System Settings > Grid Options**.
2. In the Stored Object Options section, change Stored Object Encryption to **None** (default), **AES-128**, or **AES-256**.

## Stored Object Options

Compress Stored Objects  

Stored Object Encryption  ☒ None ☐ AES-128 ☐ AES-256

Stored Object Hashing  ☒ SHA-1 ☐ SHA-256

3. Click **Save**.

## Configuring stored object hashing

The Stored Object Hashing option specifies the hashing algorithm used to verify object integrity.

### What you'll need

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

### About this task

By default, object data is hashed using the SHA-1 algorithm. The SHA-256 algorithm requires additional CPU resources and is generally not recommended for integrity verification.





If you change this setting, it will take about one minute for the new setting to be applied. The configured value is cached for performance and scaling.

### Steps

1. Select **Configuration > System Settings > Grid Options**.
2. In the Stored Object Options section, change Stored Object Hashing to **SHA-1** (default) or **SHA-256**.

## Stored Object Options

Compress Stored Objects  

Stored Object Encryption  ☒ None ☐ AES-128 ☐ AES-256

Stored Object Hashing  ☒ SHA-1 ☐ SHA-256

3. Click **Save**.

## Storage Node configuration settings

Each Storage Node uses a number of configuration settings and counters. You might

need to view the current settings or reset counters to clear alarms (legacy system).



Except when specifically instructed in documentation, you should consult with technical support before modifying any Storage Node configuration settings. As required, you can reset event counters to clear legacy alarms.

To access a Storage Node's configuration settings and counters:

1. Select **Support > Tools > Grid Topology**.
2. Select **site > Storage Node**.
3. Expand the Storage Node and select the service or component.
4. Select the **Configuration** tab.

The following tables summarize Storage Node configuration settings.

## LDR

Attribute Name	Code	Description
HTTP State	HSTE	<p>The current state of the HTTP protocol for S3, Swift, and other internal StorageGRID traffic:</p> <ul style="list-style-type: none"><li>• Offline: No operations are allowed, and any client application that attempts to open an HTTP session to the LDR service receives an error message. Active sessions are gracefully closed.</li><li>• Online: Operation continues normally</li></ul>
Auto-Start HTTP	HTAS	<ul style="list-style-type: none"><li>• If selected, the state of the system on restart depends on the state of the <b>LDR &gt; Storage</b> component. If the <b>LDR &gt; Storage</b> component is Read-only on restart, the HTTP interface is also Read-only. If the <b>LDR &gt; Storage</b> component is Online, then HTTP is also Online. Otherwise, the HTTP interface remains in the Offline state.</li><li>• If not selected, the HTTP interface remains Offline until explicitly enabled.</li></ul>

## LDR > Data Store

Attribute Name	Code	Description
Reset Lost Objects Count	RCOR	Reset the counter for the number of lost objects on this service.

## LDR > Storage

Attribute Name	Code	Description
Storage State — Desired	SSDS	<p>A user-configurable setting for the desired state of the storage component. The LDR service reads this value and attempts to match the status indicated by this attribute. The value is persistent across restarts.</p> <p>For example, you can use this setting to force storage to become read-only even when there is ample available storage space. This can be useful for troubleshooting.</p> <p>The attribute can take one of the following values:</p> <ul style="list-style-type: none"> <li>• Offline: When the desired state is Offline, the LDR service takes the <b>LDR &gt; Storage</b> component offline.</li> <li>• Read-only: When the desired state is Read-only, the LDR service moves the storage state to read-only and stops accepting new content. Note that content might continue to be saved to the Storage Node for a short time until open sessions are closed.</li> <li>• Online: Leave the value at Online during normal system operations. The Storage State — Current of the storage component will be dynamically set by the service based on the condition of the LDR service, such as the amount of available object storage space. If space is low, the component becomes Read-only.</li> </ul>
Health Check Timeout	SHCT	The time limit in seconds within which a health check test must complete in order for a storage volume to be considered healthy. Only change this value when directed to do so by Support.

## LDR > Verification

Attribute Name	Code	Description
Reset Missing Objects Count	VCMI	Resets the count of Missing Objects Detected (OMIS). Use only after foreground verification completes. Missing replicated object data is restored automatically by the StorageGRID system.
Verify	FVOV	Select object stores on which to perform foreground verification.

Attribute Name	Code	Description
Verification Rate	VPRI	Set the rate at which background verification takes place. See information on configuring the background verification rate.
Reset Corrupt Objects Count	VCCR	Reset the counter for corrupt replicated object data found during background verification. This option can be used to clear the Corrupt Objects Detected (OCOR) alarm condition. For details, see the instructions for monitoring and troubleshooting StorageGRID.
Delete Quarantined Objects	OQRT	<p>Delete corrupt objects from the quarantine directory, reset the count of quarantined objects to zero, and clear the Quarantined Objects Detected (OQRT) alarm. This option is used after corrupt objects have been automatically restored by the StorageGRID system.</p> <p>If a Lost Objects alarm is triggered, technical support might want to access the quarantined objects. In some cases, quarantined objects might be useful for data recovery or for debugging the underlying issues that caused the corrupt object copies.</p>

## LDR > Erasure Coding

Attribute Name	Code	Description
Reset Writes Failure Count	RSWF	Reset the counter for write failures of erasure-coded object data to the Storage Node.
Reset Reads Failure Count	RSRF	Reset the counter for read failures of erasure-coded object data from the Storage Node.
Reset Deletes Failure Count	RSDF	Reset the counter for delete failures of erasure-coded object data from the Storage Node.
Reset Corrupt Copies Detected Count	RSCC	Reset the counter for the number of corrupt copies of erasure-coded object data on the Storage Node.
Reset Corrupt Fragments Detected Count	RSCD	Reset the counter for corrupt fragments of erasure-coded object data on the Storage Node.
Reset Missing Fragments Detected Count	RSMD	Reset the counter for missing fragments of erasure-coded object data on the Storage Node. Use only after foreground verification completes.



## LDR > Replication

Attribute Name	Code	Description
Reset Inbound Replication Failure Count	RICR	Reset the counter for inbound replication failures. This can be used to clear the RIRF (Inbound Replication — Failed) alarm.
Reset Outbound Replication Failure Count	ROCR	Reset the counter for outbound replication failures. This can be used to clear the RORF (Outbound Replications — Failed) alarm.
Disable Inbound Replication	DSIR	<p>Select to disable inbound replication as part of a maintenance or testing procedure. Leave unchecked during normal operation.</p> <p>When inbound replication is disabled, objects can be retrieved from the Storage Node for copying to other locations in the StorageGRID system, but objects cannot be copied to this Storage Node from other locations: the LDR service is read-only.</p>
Disable Outbound Replication	DSOR	<p>Select to disable outbound replication (including content requests for HTTP retrievals) as part of a maintenance or testing procedure. Leave unchecked during normal operation.</p> <p>When outbound replication is disabled, objects can be copied to this Storage Node, but objects cannot be retrieved from the Storage Node to be copied to other locations in the StorageGRID system. The LDR service is write-only.</p>

### Related information

[Monitor & troubleshoot](#)

## Managing full Storage Nodes

As Storage Nodes reach capacity, you must expand the StorageGRID system through the addition of new storage. There are three options available: adding storage volumes, adding storage expansion shelves, and adding Storage Nodes.

### Adding storage volumes

Each Storage Node supports a maximum number of storage volumes. The defined maximum varies by platform. If a Storage Node contains fewer than the maximum number of storage volumes, you can add volumes to increase its capacity. See the instructions for expanding a StorageGRID system.

## Adding storage expansion shelves

Some StorageGRID appliance Storage Nodes, such as the SG6060, can support additional storage shelves. If you have StorageGRID appliances with expansion capabilities that have not already been expanded to maximum capacity, you can add storage shelves to increase capacity. See the instructions for expanding a StorageGRID system.

## Adding Storage Nodes

You can increase storage capacity by adding Storage Nodes. Careful consideration of currently active ILM rules and capacity requirements must be taken when adding storage. See the instructions for expanding a StorageGRID system.

### Related information

[Expand your grid](#)

## Copyright information

Copyright © 2023 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.