StorageGRID® Webscale 10.4

Administrator Guide

April 2017 | 215-11695_A0
doccomments@netapp.com
# Contents

**Understanding the StorageGRID Webscale system** ................................. 8  
What the StorageGRID Webscale system is ...................................................... 8  
Working with the StorageGRID Webscale system ........................................ 9  
  Web browser requirements ............................................................................ 11  
Signing in to the Grid Management Interface ................................................ 12  
Signing out of the Grid Management Interface .............................................. 13  
Changing your password ............................................................................... 13  
Changing the browser session timeout period .............................................. 14  
Viewing StorageGRID Webscale license information .................................. 15  
Updating StorageGRID Webscale license information .................................. 15  
Understanding the StorageGRID Webscale management API ....................... 15  

**Managing storage tenant accounts** ............................................................. 19  
Creating a tenant account .............................................................................. 19  
Editing a tenant account ................................................................................. 22  
Changing the password for a tenant account's root user ................................ 24  
Deleting tenant accounts ................................................................................. 25  

**Monitoring the StorageGRID Webscale system** ........................................ 26  
About alarms and email notifications ............................................................. 26  
  Alarm notification types .................................................................................. 26  
  Notification status and queues ..................................................................... 27  
  Configuring notifications ............................................................................. 27  
  Suppressing email notifications for a mailing list ........................................ 32  
  Suppressing email notifications system wide ............................................. 33  
  Selecting a preferred sender ....................................................................... 33  
Alarms management ........................................................................................... 34  
  Alarm class types ......................................................................................... 35  
  Alarm triggering logic ................................................................................. 37  
  Creating custom service or component alarms .......................................... 40  
  Creating Global Custom alarms ................................................................ 42  
Disabling alarms .............................................................................................. 44  
  Alarms and tables ......................................................................................... 45  
  Disabling default alarms for services ......................................................... 45  
  Disabling a default alarm system wide ...................................................... 46  
  Disabling Global Custom alarms for services ......................................... 47  
  Disabling Global Custom alarms system wide ......................................... 48  
  Clearing triggered alarms ...................................................................... 49  
What AutoSupport is ....................................................................................... 49  
  Triggering AutoSupport messages ............................................................. 50  
  Disabling weekly AutoSupport messages ............................................... 51  
  Troubleshooting AutoSupport .................................................................. 51  
Monitoring servers and grid nodes ............................................................... 52
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the SSM service</td>
<td>52</td>
</tr>
<tr>
<td>Monitoring StorageGRID Webscale Appliance Storage Nodes</td>
<td>54</td>
</tr>
<tr>
<td><strong>Managing objects through information lifecycle management</strong></td>
<td>61</td>
</tr>
<tr>
<td>What an information lifecycle management policy is</td>
<td>61</td>
</tr>
<tr>
<td>What an information lifecycle management rule is</td>
<td>62</td>
</tr>
<tr>
<td>How object storage locations are determined</td>
<td>62</td>
</tr>
<tr>
<td>How object data is protected from loss</td>
<td>62</td>
</tr>
<tr>
<td>How ILM rules filter objects</td>
<td>64</td>
</tr>
<tr>
<td>What Dual Commit is</td>
<td>66</td>
</tr>
<tr>
<td>Configuring information lifecycle management rules and policy</td>
<td>67</td>
</tr>
<tr>
<td>Creating and assigning storage grades</td>
<td>67</td>
</tr>
<tr>
<td>Configuring storage pools</td>
<td>69</td>
</tr>
<tr>
<td>Configuring Erasure Coding profiles</td>
<td>72</td>
</tr>
<tr>
<td>Specifying time values for time based metadata</td>
<td>74</td>
</tr>
<tr>
<td>Creating an ILM rule</td>
<td>74</td>
</tr>
<tr>
<td>Configuring, simulating, and activating an ILM policy</td>
<td>78</td>
</tr>
<tr>
<td>Working with ILM rules and ILM policies</td>
<td>91</td>
</tr>
<tr>
<td>Example ILM rules and policies</td>
<td>94</td>
</tr>
<tr>
<td>Example 1: ILM rules and policy for object storage</td>
<td>94</td>
</tr>
<tr>
<td>Example 2: ILM rules and policy for EC object size filtering</td>
<td>98</td>
</tr>
<tr>
<td>Example 3: ILM rules and policy for better protection for image files</td>
<td>101</td>
</tr>
<tr>
<td><strong>Managing disk storage</strong></td>
<td>105</td>
</tr>
<tr>
<td>What a Storage Node is</td>
<td>105</td>
</tr>
<tr>
<td>What the LDR service is</td>
<td>105</td>
</tr>
<tr>
<td>Monitoring ILM activity</td>
<td>107</td>
</tr>
<tr>
<td>What the DDS service is</td>
<td>109</td>
</tr>
<tr>
<td>CMS service</td>
<td>110</td>
</tr>
<tr>
<td>ADC service</td>
<td>111</td>
</tr>
<tr>
<td>Managing Storage Nodes</td>
<td>111</td>
</tr>
<tr>
<td>Monitoring Storage Node capacity</td>
<td>111</td>
</tr>
<tr>
<td>Watermarks</td>
<td>113</td>
</tr>
<tr>
<td>Storage Node configuration settings</td>
<td>114</td>
</tr>
<tr>
<td>Managing full Storage Nodes</td>
<td>117</td>
</tr>
<tr>
<td>Monitoring storage</td>
<td>118</td>
</tr>
<tr>
<td>Monitoring storage capacity system-wide</td>
<td>118</td>
</tr>
<tr>
<td>Monitoring storage capacity per Storage Node</td>
<td>118</td>
</tr>
<tr>
<td>Configuring settings for stored objects</td>
<td>119</td>
</tr>
<tr>
<td>Configuring stored object encryption</td>
<td>119</td>
</tr>
<tr>
<td>Configuring stored object hashing</td>
<td>120</td>
</tr>
<tr>
<td>Configuring stored object compression</td>
<td>121</td>
</tr>
<tr>
<td>Enabling Prevent Client Modify</td>
<td>122</td>
</tr>
<tr>
<td>Mounted storage devices</td>
<td>123</td>
</tr>
<tr>
<td>What security partitions are</td>
<td>124</td>
</tr>
<tr>
<td>What object segmentation is</td>
<td>125</td>
</tr>
<tr>
<td>Verifying object integrity</td>
<td>126</td>
</tr>
</tbody>
</table>
What background verification is ................................................................. 126
Configuring the background verification rate ............................................. 126
What foreground verification is ................................................................. 128
Running foreground verification ................................................................. 128
How load balancing works ........................................................................ 130
Managing archival storage ........................................................................ 131
What an Archive Node is .......................................................................... 131
What the ARC service is .......................................................................... 131
About supported archive targets ................................................................. 132
Managing connections to archival storage .................................................... 132
Configuring connection settings for S3 API ................................................ 133
Modifying connection settings for S3 API ................................................... 135
Configuring connections to Tivoli Storage Manager middleware ................ 136
Managing Archive Nodes .......................................................................... 138
Optimizing Archive Node's TSM middleware sessions ................................ 138
Managing an Archive Node when TSM server reaches capacity .................. 139
Configuring Archive Node replication ........................................................ 141
Configuring retrieve settings .................................................................... 142
Configuring the archive store .................................................................... 143
Setting custom alarms for the Archive Node ............................................. 144
What an Admin Node is ........................................................................... 146
Admin Node redundancy .......................................................................... 147
Alarm acknowledgments .......................................................................... 147
Email notifications and AutoSupport messages ......................................... 148
Changing the name of an Admin Node ....................................................... 149
NMS entities ............................................................................................ 149
Managing networking ............................................................................... 150
Viewing IP addresses ............................................................................... 151
Configuring SNMP monitoring .................................................................. 152
Management Information Base file ......................................................... 152
Detailed registry ....................................................................................... 152
Link costs .................................................................................................. 153
Updating link costs .................................................................................. 153
Changing network transfer encryption ....................................................... 154
Configuring passwordless SSH access ...................................................... 155
Configuring certificates ............................................................................ 156
Configuring custom server certificates for the Grid Management Interface .......................................................... 156
Restoring the default server certificates for the Grid Management Interface .......................................................... 157
Configuring custom server certificates for storage API endpoints ............... 157
Restoring the default server certificates for storage API endpoints ............. 158
Copying the StorageGRID Webscale system's CA certificate .................... 158
Configuring audit client access ................................................................ 160
Configuring audit clients for CIFS ............................................................ 160
Configuring audit clients for Workgroup .................................................... 160
Configuring audit clients for Active Directory ........................................... 162
Adding a user or group to a CIFS audit share ............................................. 165
Removing a user or group from a CIFS audit share .................................... 167
Changing a CIFS audit share user or group name ....................................... 168
Verifying CIFS audit integration ....................................................................... 168
Configuring the audit client for NFS ............................................................ 169
Adding an NFS audit client to an audit share .............................................. 170
Verifying NFS audit integration ..................................................................... 172
Removing an NFS audit client from the audit share ................................... 172
Changing the IP address of an NFS audit client .......................................... 173

Controlling system access with administration user accounts and groups ............................................................... 175

Configuring identity federation .................................................................................. 175
Guidelines for configuring an OpenLDAP server ................................................... 178
Forcing synchronization with the identity source ................................................. 178
Disabling identity federation ................................................................................ 179
About admin group permissions ............................................................................. 179
Deactivating features from the StorageGRID Webscale management API ................................................................. 181
About admin user accounts ................................................................................. 182
Creating admin groups ......................................................................................... 183
Modifying an admin group .................................................................................... 184
Deleting an admin group ......................................................................................... 184
Creating an admin users account .......................................................................... 185
Modifying an admin users account ........................................................................ 185
Deleting an admin users account .......................................................................... 186
Changing local users’ passwords .......................................................................... 186

Monitoring and managing grid tasks ......................................................... 188

Monitoring grid tasks ......................................................................................... 188
Running a grid task ............................................................................................... 190
Pausing an active grid task ..................................................................................... 191
Resuming a paused grid task .................................................................................. 192
Cancelling a grid task .............................................................................................. 192
Aborting a grid task ............................................................................................... 193
Submitting a Task Signed Text Block ...................................................................... 194
Removing grid tasks from the Historical table ..................................................... 195
Troubleshooting grid tasks .................................................................................... 196
Grid task fails to complete and moves to Historical table .................................... 196
Grid task retries multiple times ............................................................................... 196
Grid task has Error status ...................................................................................... 197

What data migration is ......................................................................................... 198

Confirming capacity of the StorageGRID Webscale system ........................................ 198
Determining the ILM policy for migrated data ...................................................... 198
Impact of migration on operations ........................................................................ 199
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling data migration</td>
<td>199</td>
</tr>
<tr>
<td>Monitoring data migration</td>
<td>199</td>
</tr>
<tr>
<td>Creating custom notifications for migration alarms</td>
<td>200</td>
</tr>
<tr>
<td>What Server Manager is</td>
<td>202</td>
</tr>
<tr>
<td>Server Manager command shell procedures</td>
<td>202</td>
</tr>
<tr>
<td>Viewing Server Manager status and version</td>
<td>202</td>
</tr>
<tr>
<td>Viewing current status of all services</td>
<td>203</td>
</tr>
<tr>
<td>Starting Server Manager and all services</td>
<td>204</td>
</tr>
<tr>
<td>Restarting Server Manager and all services</td>
<td>205</td>
</tr>
<tr>
<td>Stopping Server Manager and all services</td>
<td>205</td>
</tr>
<tr>
<td>Viewing current status of a service</td>
<td>206</td>
</tr>
<tr>
<td>Stopping a service</td>
<td>206</td>
</tr>
<tr>
<td>Forcing a service to terminate</td>
<td>207</td>
</tr>
<tr>
<td>Restarting a service</td>
<td>208</td>
</tr>
<tr>
<td>Rebooting a grid node</td>
<td>208</td>
</tr>
<tr>
<td>Powering down servers</td>
<td>209</td>
</tr>
<tr>
<td>Using a DoNotStart file</td>
<td>209</td>
</tr>
<tr>
<td>Adding a DoNotStart file for a service</td>
<td>209</td>
</tr>
<tr>
<td>Troubleshooting Server Manager</td>
<td>211</td>
</tr>
<tr>
<td>Accessing the Server Manager log file</td>
<td>211</td>
</tr>
<tr>
<td>Service fails to start</td>
<td>211</td>
</tr>
<tr>
<td>Service with an error state</td>
<td>212</td>
</tr>
<tr>
<td>Integrating Tivoli Storage Manager</td>
<td>213</td>
</tr>
<tr>
<td>Archive Node configuration and operation</td>
<td>213</td>
</tr>
<tr>
<td>Configuration best practices</td>
<td>213</td>
</tr>
<tr>
<td>Completing the Archive Node setup</td>
<td>214</td>
</tr>
<tr>
<td>Installing a new TSM server</td>
<td>214</td>
</tr>
<tr>
<td>Configuring the TSM server</td>
<td>214</td>
</tr>
<tr>
<td>Glossary</td>
<td>219</td>
</tr>
<tr>
<td>Copyright information</td>
<td>226</td>
</tr>
<tr>
<td>Trademark information</td>
<td>227</td>
</tr>
<tr>
<td>How to send comments about documentation and receive update notifications</td>
<td>228</td>
</tr>
<tr>
<td>Index</td>
<td>229</td>
</tr>
</tbody>
</table>
Understanding the StorageGRID Webscale system

The Administrator Guide contains system administration information and procedures required to manage and monitor the StorageGRID Webscale system on a day-to-day basis. This guide also includes information on how to configure the StorageGRID Webscale system to meet a deployment’s unique operational requirements.

This guide is not intended as an introduction to the StorageGRID Webscale system and its functional areas. For a general introduction to the StorageGRID Webscale system, see the Grid Primer.

This guide is intended for technical personnel trained to configure and support the StorageGRID Webscale system.

This guide assumes a general understanding of the StorageGRID Webscale system. A fairly high level of computer literacy is assumed, including knowledge of Linux/UNIX command shells, networking, and server hardware setup and configuration.

Related information

StorageGRID Webscale 10.4 Grid Primer

What the StorageGRID Webscale system is

The StorageGRID Webscale system is a distributed object storage system that stores, protects, and preserves fixed-content data over long periods of time. By employing a grid architecture that distributes copies of object data throughout the system, a highly reliable system is created where data is continuously available. If one part of the system goes down, another immediately takes over, resulting in objects always being available for retrieval.

To implement this architecture, the StorageGRID Webscale system employs a system of network-connected servers hosting grid nodes. These grid nodes host a collection of one or more services, each providing a set of capabilities to the StorageGRID Webscale system.

To manage objects ingested into the system, the StorageGRID Webscale system employs metadata-based information lifecycle management (ILM) rules. These ILM rules determine what happens to an object’s data once it is ingested — where it is stored, how it is protected from loss, and for how long it is stored.

The StorageGRID Webscale system operates over wide area network (WAN) links, providing the system with the capability of off-site loss protection. Copies are made and distributed throughout the system so that objects are continuously available. In systems with multiple sites, this distribution of
copies means that if a site is lost, data is not lost, and clients are able to seamlessly retrieve from other sites. For a general introduction to the StorageGRID Webscale system, see the Grid Primer.

Related information

StorageGRID Webscale 10.4 Grid Primer

Working with the StorageGRID Webscale system

Most day-to-day activities are performed through a supported web browser. The Grid Management Interface provides access to the various levels of system functionality.

When you first sign in to the Grid Management Interface, the Dashboard lets you monitor system activities at a glance. The Dashboard includes information about health and alerts, usage metrics, and operational trends and graphs.

Grid Topology tree

The Grid Topology tree provides access to StorageGRID Webscale system elements: sites, grid nodes, services, and components.
To access the Grid Topology tree, select Grid from the menu bar above the Dashboard.

**Grid nodes**

The basic building block of a StorageGRID Webscale system is the grid node. A grid node consists of one or more services hosted by a virtual machine. For a detailed description of grid nodes, see the Grid Primer.
Services

A service is a software module that provides a set of capabilities to a grid node. The same service can be installed and used on more than one grid node. Changes made to settings for one service do not affect the settings of the same service type for a different grid node. Services are listed under each grid node. For a detailed description of services, see the Grid Primer.

Components

Each service includes a sub-group of components. Each component performs a particular function for that service.

Attributes

Attributes report values and statuses for all of the functions of the StorageGRID Webscale system. Attributes and the values they report form the basis for monitoring the StorageGRID Webscale system.

Related references

Web browser requirements on page 11

Related information

StorageGRID Webscale 10.4 Grid Primer

Web browser requirements

You must use a supported web browser.

<table>
<thead>
<tr>
<th>Web browser</th>
<th>Minimum supported version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>54</td>
</tr>
<tr>
<td>Microsoft Internet Explorer</td>
<td>11 (Native Mode)</td>
</tr>
</tbody>
</table>
### Signing in to the Grid Management Interface

You access the Sign In page for the Grid Management Interface by entering the web address or host name defined by your system administrator into the address bar of a supported web browser.

#### Before you begin

- You must have an authorized user name and password.
- You must have the IP address or fully qualified domain name of an Admin Node.
- You must have access to a supported web browser.
- Cookies must be enabled in your web browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

#### About this task

When you sign in to the Grid Management Interface, you are connecting to an Admin Node. Each StorageGRID Webscale system includes one primary Admin Node and any number of non-primary Admin Nodes. You can connect to any Admin Node, and each Admin Node displays a similar view of the StorageGRID Webscale system; however, alarm acknowledgments made through one Admin Node are not copied to other Admin Nodes. Therefore, the Grid Topology tree might not look the same for each Admin Node.

**Note:** The StorageGRID Webscale system uses a security certificate to secure access to the Grid Management Interface. You can use the default certificate created during installation, or you can replace the default certificate with your own custom certificate.

#### Steps

1. Launch a supported web browser.

2. In the browser’s address bar, enter the IP address or fully qualified domain name of the Admin Node.

   **Note:** If you are prompted with a security alert, view and install the certificate using the browser’s installation wizard. The alert will not appear the next time you access this URL.

The StorageGRID Webscale system’s Sign In page appears.
3. Enter your case-sensitive username and password, and click **Sign In**.

   The home page of the Grid Management Interface appears, which includes the Dashboard.

**Related concepts**

- *Configuring certificates* on page 156
- *Working with the StorageGRID Webscale system* on page 9

**Related references**

- *Web browser requirements* on page 11

---

### Signing out of the Grid Management Interface

When you have completed working with the Grid Management Interface, you must sign out to keep the system secure.

**About this task**

You must sign out of the Grid Management Interface to ensure that unauthorized users cannot access the StorageGRID Webscale system. Closing your browser does not sign you out of the system.

**Step**

1. Click **Sign Out** located at the top-right corner of the page.

   You are signed out, and the Sign In page appears.

---

### Changing your password

If you are a local user of the Grid Management Interface, you can change your own password.

**Before you begin**

You must be signed in to the Grid Management Interface using a supported browser.

**About this task**

Federated users cannot change their passwords directly in Grid Management Interface; they must change passwords in the external identity source, for example, Active Directory or OpenLDAP.

**Steps**

1. From the Grid Management Interface header, select **your login name > Change password**.

2. Enter your current password.
3. Type a new password.
   Your password must contain between 8 and 32 characters and is case-sensitive.

4. Re-enter the new password.

5. Click Save.

**Changing the browser session timeout period**

You can specify the timeout period for the StorageGRID Webscale system's browser-based interface. If a user is inactive for the specified timeout period, the StorageGRID Webscale system times out and the Sign In page is displayed.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

The GUI Inactivity Timeout defaults to 900 seconds (15 minutes).

**Note:** To maintain the security of the system, a separate, non-configurable timer for each user's authentication token will expire 16 hours after the user signs in. When a user's authentication expires, that user is automatically signed out, even if the value for the GUI Inactivity Timeout has not been reached. To renew the token, the user must sign back in.

**Steps**

1. Select **Configuration > Display Options**.

2. For **GUI Inactivity Timeout**, enter a timeout period of 60 seconds or more.
   
   Set this field to 0 if you do not want to use this functionality. Users are signed out 16 hours after they sign in, when their authentication tokens expire.

3. Click **Apply Changes**.
   
   The new setting does not affect currently signed in users. Users must sign in again or refresh their browsers for the new timeout setting to take effect.

4. Sign out of the StorageGRID Webscale system.

5. Sign in again.
Viewing StorageGRID Webscale license information

You can view the license information for your StorageGRID Webscale system, such as the maximum storage capacity of your grid, whenever necessary.

Step

1. Select Maintenance > License.

The license information is displayed including the grid serial number, license serial number, licensed storage capacity of the grid, and the contents of the license text file. This information is read-only. For licenses issued before StorageGRID Webscale 10.3, the licensed storage capacity is not included in the license file, and a “See License Agreement” message is displayed instead of a value.

Updating StorageGRID Webscale license information

You must update the license information for your StorageGRID Webscale system any time the terms of your license change. For example, you must update the license information if you purchase additional storage capacity for your grid.

Before you begin

• You must have a new license file to apply to your StorageGRID Webscale system.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
• You must have the provisioning passphrase.

Steps

1. Select Maintenance > License.

2. Enter the provisioning passphrase for your StorageGRID Webscale system in the Provisioning Passphrase text box.

3. Click Browse.

4. In the Open dialog box, locate and select the new license file (.txt), and click Open.

The new license file is validated and displayed.

5. Click Save.

Understanding the StorageGRID Webscale management API

StorageGRID Webscale provides a REST API for performing system management tasks.

You access the StorageGRID Webscale management API over HTTPS. You can access the grid management API from the Grid Management Interface. You can access the tenant management API from the Tenant Management Interface.

StorageGRID Webscale Management API documentation

The StorageGRID Webscale Management API uses the Swagger open source API platform to provide the API documentation. Swagger allows both developers and non-developers to interact with the API in a user interface that illustrates how the API responds to parameters and options. This documentation assumes that you are familiar with standard web technologies and the JSON (JavaScript Object Notation) data format.
**Attention**: Any API operations you perform using the Swagger user interface are live operations. Be careful not to create, update, or delete configuration or other data by mistake.

You can access the Management API documentation by logging in to the Grid Management Interface and selecting **Help > API Docs** in the web application header.

**API**

Each REST API command includes the API’s URL, an HTTP action, any required or optional URL parameters, and an expected API response.

The Swagger UI provides details and documentation for each API operation, as in the following example. To get information about a local grid administrator group, you would enter that group’s unique name as the value for the `shortName` parameter and click **Try it out**.

The StorageGRID Webscale Management API includes the following sections:

- **accounts** – Operations to manage storage tenant accounts, including creating new accounts and retrieving storage usage for a given account.
- **alarms** – Operations to list current alarms, and return information about the health of the grid.
- **audit** – Operations to list and update the audit configuration.
- **auth** – Operations to perform user session authentication.

The Management API supports the Bearer Token Authentication Scheme. To login, you provide a username and password in the JSON body of the authentication request (that is, POST /api/v2/authorize). If the user is successfully authenticated, a security token is returned. This token must be provided in the header of subsequent API requests ("Authorization: Bearer token").
• **config** – Operations related to the product release and versions of the management API. You can list the product release version and the major versions of the management API supported by that release, and you can disable deprecated versions of the API.

• **deactivated-features** – Operations to view features that might have been deactivated.

• **dns-servers** – Operations to list and change configured external DNS servers.

• **endpoint-domain-names** – Operations to list and change endpoint domain names.

• **expansion** – Operations on expansion (procedure-level).

• **expansion-nodes** – Operations on expansion (node-level).

• **expansion-sites** – Operations on expansion (site-level).

• **grid-networks** – Operations to list and change the Grid Network List.

• **groups** – Operations to manage local Grid Administrator Groups and to retrieve federated Grid Administrator Groups from an external LDAP server.

• **identity-source** – Operations to configure an external identity source and to manually synchronize federated group and user information.

• **ilm** – Operations on information lifecycle management (ILM).

• **license** – Operations to retrieve or update the StorageGRID Webscale license.

• **ntp-servers** – Operations to list or update external Network Time Protocol (NTP) servers.

• **recovery** – Operations to list the grid nodes available for recovery.

• **recovery-package** – Operations to download the Recovery Package.

• **server certificates** – Operations to view and update Management Interface server certificates

• **users** – Operations to view and manage Grid Administrator users.

**Top-level resources**
The StorageGRID Webscale management API provides the following top level resources:

• **/grid**: Access is restricted to Grid Administrator users.

• **/org**: Access is restricted to users who belong to a local or federated LDAP group for a tenant account. See the *Tenant Administrator Guide* for more information.

• **/private**: Access is restricted to internal access to the StorageGRID Webscale system. This resource path is not publicly documented.

**Management API versioning**
The management API uses versioning to support non-disruptive upgrades. For example, this Request URL specifies version 2 of the API.

https://hostname_or_ip_address/api/v2/authorize

Changes in the management API that are backward incompatible bump the major version of the API. For example, an incompatible API change bumps the version from 1.1 to 2.0. Changes in the management API that are backward compatible bump the minor version instead. Backward-compatible changes include the addition of new endpoints or new properties. For example, a compatible API change bumps the version from 1.0 to 1.1.
When you install StorageGRID Webscale software for the first time, only the most recent version of the management API is enabled. However, when you upgrade to a new major version of StorageGRID Webscale, you continue to have access to the older API version for at least one major StorageGRID Webscale release.

**Note:** You can use the management API to configure the supported versions. See the “config” section of the Swagger API documentation for more information. You should deactivate support for the older version after updating all management API clients to use the newer version.

Outdated requests are marked as deprecated in the following ways:

- The response header is "Deprecated: true"
- The JSON response body includes "deprecated": true
- A deprecated warning is added to nms.log. For example:

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

**Determining which API versions are supported in the current release**

Use the following API request to return a list of the supported API major versions:

```
GET https://{{IP-Address}}/api/versions
```

```
{
   "responseTime": "2016-10-03T14:49:16.587Z",
   "status": "success",
   "apiVersion": "2.0",
   "data": [
      1,
      2
   ]
}
```

**Specifying an API version for a request**

You can specify the API version using a path parameter (/api/v1) or a header (Api-Version: 2). If you provide both values, the header value overrides the path value.

```
curl https://[IP-Address]/api/v2/grid/accounts

curl -H "Api-Version: 2" https://[IP-Address]/api/grid/accounts
```

**Related information**

*StorageGRID Webscale 10.4 Tenant Administrator Guide*
Managing storage tenant accounts

A storage tenant account allows you to specify who can use your StorageGRID Webscale system to store and retrieve objects.

A tenant account uses either the S3 client protocol or the Swift client protocol. You must create at least one tenant account for each client protocol (Swift or S3) that will be used to store objects on your StorageGRID Webscale system. If you want to use both the Swift client protocol and the S3 client protocol to store and retrieve objects, you must create at least two tenant accounts: one for Swift containers and objects and one for S3 buckets and objects.

Optionally, you can create additional tenant accounts if you want to segregate the objects stored on your system by different entities. Each tenant account has its own unique account ID, Tenant Management Interface, federated or local groups and users, and containers (buckets for S3) and objects.

For example, you might set up multiple tenant accounts in either of these use cases:

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

  **Note:** If you use the S3 client protocol, you can simply use S3 buckets and bucket policies to segregate objects between the departments in an enterprise. You do not need to use tenant accounts. See the StorageGRID Webscale S3 Implementation Guide for more information.

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

When you create a tenant account, you specify an account display name, the client protocol, and the password for the tenant account’s root user. Optionally, you can specify whether you want the tenant account to use the identity source that was configured for the grid. (By default, a tenant account must use its own identity source for identity federation.) Optionally, you can set a storage quota for each tenant account by specifying the maximum number of gigabytes, terabytes, or petabytes available for the tenant's objects.

Each tenant account has its own browser-based user interface and tenant API (referred to as the Tenant Management Interface). As soon as you save a new tenant account, you can sign in to the Tenant Management Interface to set up tenant groups and users. Or, if you are a service provider, you can provide the tenant's URL and the password for the tenant's root user to another person.

**Related information**

*StorageGRID Webscale 10.4 S3 (Simple Storage Service) Implementation Guide*

**Creating a tenant account**

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

**Before you begin**

• You must be signed in to the Grid Management Interface using a supported browser.
To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Tenants.

   The Tenant Accounts page appears.

   ![Tenant Accounts page](image)

2. Click Create.

   Step 1 - Create Tenant Account appears.

   ![Step 1 - Create Tenant Account](image)

3. Create the tenant account.

   a. In the Display Name text box, enter the display name for this tenant account.

      When the tenant account is created, it receives a unique, numeric Account ID; for this reason, display names are not required to be unique.

   b. Select the client protocol that will be used by this tenant account, either S3 or Swift.
c. Uncheck the **Uses Own Identity Source** checkbox if this tenant account will use the identity source that was configured for the Grid Management Interface. See “Configuring identity federation” for more information.

If this checkbox is selected (default), you must configure a unique identity source for this tenant if you want to use identity federation for tenant groups and users. See the *StorageGRID Webscale Tenant Administrator Guide* for instructions.

d. Optionally, enter the maximum number of gigabytes, terabytes, or petabytes that you want to make available for this tenant's objects in the **Storage Quota** text box. Then, select the units from the drop-down list.

Leave this field blank if you want this tenant to have an unlimited quota.

**Note:** ILM copies and erasure coding do not contribute to the amount of quota used. If the quota is exceeded, the tenant account cannot create new objects.

e. In the **Tenant Root User Password** section, enter a password for the tenant account's root user.

f. Click **Save**.

The tenant account is created, and Step 2 - Configure Tenant Account appears.

---

4. Decide whether to configure the tenant account now or later, as follows:

- If you are ready to specify who can access the new tenant account, go to step 5.
- If you or someone else will configure the new tenant later, go to step 7.

5. Click the **Sign in as root** button.

A green check mark appears on the button, indicating that you are now signed in to the tenant account as the root user.

6. Specify who can access the Tenant Management Interface.
a. If you want to set up an identity source for the tenant, select **Identity Federation**.

   **Note:** This link appears only if you left the **Uses Own Identity Source** checkbox selected in step 3.

   The Identity Federation page for the opens on a new tab. To complete this page, see the instructions in the *StorageGRID Webscale Tenant Administrator Guide*.

b. If you want to configure the groups who can access the tenant, select **Groups**.

   The Groups page for the Tenant Management Interface opens on a new tab. To complete this page, see the instructions in the *StorageGRID Webscale Tenant Administrator Guide*.

c. If you want to configure local users who can access the tenant, select **Users**.

   If you are using federated groups, you do not need to configure users.

   The Users page for the Tenant Management Interface opens on a new tab. To complete this page, see the instructions in the *StorageGRID Webscale Tenant Administrator Guide*.

7. Click **Finish**.

   The dialog closes. To access the Tenant Management Interface later, select **Tenants** from the menu, click the **Sign in** link, and sign in. Or, provide the URL for the **Sign in** link and the root user password to the tenant account’s administrator.

**Related concepts**

*Controlling system access with administration user accounts and groups* on page 175

**Related tasks**

*Configuring identity federation* on page 175

**Related information**

*StorageGRID Webscale 10.4 Tenant Administrator Guide*

### Editing a tenant account

You can edit a tenant account to change the display name, identity source setting, or storage quota.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Tenants**.

   The Tenant Accounts page appears.
2. Select the tenant account you want to edit.


4. Change the values for the fields as required.
   a. Change the display name for this tenant account.
   b. Change the setting of the Uses Own Identity Source checkbox to determine whether the tenant account will use its own identity source or the identity source that was configured for the Grid Management Interface.
      If the tenant has already enabled its own identity source, you cannot unselect the Uses Own Identity Source checkbox. A tenant must disable its identity source before it can use the identity source that was configured for the Grid Management Interface.
   c. For Storage Quota, change the number of maximum number of gigabytes, terabytes, or petabytes available for this tenant's objects, or leave the field blank if you want this tenant to have an unlimited quota.

5. Click Save.

Related concepts

Controlling system access with administration user accounts and groups on page 175
Changing the password for a tenant account's root user

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

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Tenants.
   
The Tenant Accounts page appears.

2. Select the tenant account you want to edit.

3. Select Change Root Password.

4. Enter the new password for the tenant account.

5. Click Save.

Related concepts

Controlling system access with administration user accounts and groups on page 175
Deleting tenant accounts

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

Before you begin

• You must be signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

• You must have removed all buckets (S3), containers (Swift), and objects associated with the tenant account.

Steps

1. Select Tenants.

2. Select the tenant account you want to delete.

3. Click Remove.

4. Click OK.

Related concepts

Controlling system access with administration user accounts and groups on page 175
Monitoring the StorageGRID Webscale system

The StorageGRID Webscale system provides you with the capabilities to monitor the daily activities of the system including its health. Alarms and notifications help you evaluate and quickly resolve trouble spots that sometimes occur during the normal operation of a StorageGRID Webscale system.

The StorageGRID Webscale system also includes support for NetApp’s AutoSupport feature.

The StorageGRID Webscale system also includes an auditing feature that retains a record of all system activities through audit logs. Audit logs are managed by the Audit Management System (AMS) service, which is found on Admin Nodes. The AMS service logs all audited system events to a text file on the Admin Node. For more information about auditing, see the Audit Message Reference Guide.

Related concepts
- Configuring audit client access on page 160
- What AutoSupport is on page 49

Related information
- StorageGRID Webscale 10.4 Audit Message Reference

About alarms and email notifications

An email notification is a message automatically sent by the StorageGRID Webscale system to configured recipients, which notifies recipients of a newly triggered alarm or service state change.
You can configure email notifications and set mailing lists to receive these email notifications for any particular alarm severity or state change.

If an email address (or list) belongs to multiple mailing lists, only one email notification is sent when a notification triggering event occurs. For example, one group of administrators within your organization can be configured to receive notifications for all alarms regardless of severity. Another group might only require notifications for alarms with a severity of Critical. You can belong to both lists. If a Critical alarm is triggered, you receive one notification, not two. For a general overview of alarms, see the Grid Primer.

Related information
- StorageGRID Webscale 10.4 Grid Primer

Alarm notification types

The StorageGRID Webscale systems sends out two types of alarm notifications: severity level and service state.

Severity level notifications

Severity level notifications are sent at the alarm level and are associated with attributes. A mailing list receives all notifications related to alarm for the selected severity: Notice, Minor, Major, and Critical.
A notification is sent when an event triggers an alarm for the selected alarm level. A notification is also sent when the alarm leaves the alarm level — either by being resolved or by entering a different alarm severity level.

Service state notifications

Service State notifications are sent at the services level and are associated with services; for example, the LDR service or CMS service. A mailing list receives all notifications related to changes in the
selected state: Unknown, or Administratively Down. A notification is sent when a service enters the selected Service State and when it leaves the selected Service State.

**Notification status and queues**

You can view the current status of the NMS service’s ability to send notifications to the mail server and the size of its notifications queue through the Interface Engine page.

To access the Interface Engine page, select **Grid**. Then, click **site > Admin Node > NMS > Interface Engine**.

Notifications are processed through the email notifications queue and are sent to the mail server one after another in the order they are triggered. If there is a problem (for example, a network connection error) and the mail server is unavailable when the attempt is made to send the notification, a best effort attempt to resend the notification to the mail server continues for a period of 60 seconds. If the notification is not sent to the mail server after 60 seconds, the notification is dropped from the notifications queue and an attempt to send the next notification in the queue is made. Because notifications can be dropped from the notifications queue without being sent, it is possible that an alarm can be triggered without a notification being sent. In the event that a notification is dropped from the queue without being sent, the MINS (E-mail Notification Status) Minor alarm is triggered.

For a StorageGRID Webscale system configured with multiple Admin Nodes (and thus multiple NMS services), if the “standby” sender detects a Server Connection Error with the preferred sender, it will begin sending notifications to the mail server. The standby sender will continue to send notifications until it detects that the preferred sender is no longer in an error state and is again successfully sending notifications to the mail server. Notifications in the preferred sender’s queue are not copied to the standby sender. Note that in a situation where the preferred sender and the standby sender are islanded from each other, duplicate messages can be sent.

**Related tasks**

*Selecting a preferred sender* on page 33

**Configuring notifications**

By default, notifications are not sent. You must configure the StorageGRID Webscale to send notifications when alarms are raised.

**Steps**

1. **Configuring email server settings** on page 28
2. Creating email templates on page 29
3. Creating mailing lists on page 30
4. Configuring global email notifications on page 31

Configuring email server settings

The E-mail Server page allows you to configure SMTP mail server settings that enable the sending of alarm notifications and AutoSupport messages. The StorageGRID Webscale system only sends email; it cannot receive email.

Before you begin

• You must be signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

Only the SMTP protocol is supported for the sending email.

Steps

1. Select Configuration > Email Setup.
2. From the Email menu, select Server.

3. Add the following SMTP mail server settings:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Server</td>
<td>IP address of the SMTP mail server. You can enter a hostname rather than an IP address if you have previously configured DNS settings on the Admin Node.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number to access the SMTP mail server.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Allows for the authentication of the SMTP mail server. By default, authentication is Off.</td>
</tr>
</tbody>
</table>
### Item | Description
---|---
Authentication Credentials | Username and Password of the SMTP mail server. If Authentication is set to On, a username and password to access the SMTP mail server must be provided.

4. **Under From Address**, enter a valid email address that the SMTP server will recognize as the sending email address. This is the official email address from which the alarm notification or AutoSupport message is sent.

5. Optionally, send a test email to confirm that your SMTP mail server settings are correct.
   a. In the Test E-mail > To box, add one or more addresses that you can access.
      You can enter a single email address, a mailing list previously configured on the Email Lists page, or a comma-delineated list of email addresses and mailing lists. Because the NMS service does not confirm success or failure when a test email is sent, you must be able to check the test recipient’s inbox.
   b. Select **Send Test E-mail**.

6. Click **Apply Changes**.
   The SMTP mail server settings are saved. If you entered information for a test email, that email is sent. Test emails are sent to the mail server immediately and are not sent through the notifications queue. In a system with multiple Admin Nodes, each Admin Node sends an email. Receipt of the test email confirms that your SMTP mail server settings are correct and that the NMS service is successfully connecting to the mail server. A connection problem between the NMS service and the mail server triggers the MINS (NMS Notification Status) Minor alarm.

**Related tasks**

*Creating mailing lists* on page 30

**Creating email templates**
Create an email template to customize the header, footer, and subject line of a notification. You can use email templates to send unique notifications that contain the same body text to different mailing lists.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**
Different mailing lists might require different contact information. Templates do not include the body text of the email message.

**Steps**
1. Select **Configuration > Email Setup**.
2. From the Email menu, select **Templates**.
3. Click **Edit** (or **Insert** if this is not the first template).
4. In the new row add the following:

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
</tr>
<tr>
<td>Unique name used to identify the template. Template names cannot be</td>
</tr>
<tr>
<td>duplicated.</td>
</tr>
<tr>
<td>Subject Prefix</td>
</tr>
<tr>
<td>Optional. Prefix that will appear at the beginning of an email’s subject</td>
</tr>
<tr>
<td>line. Prefixes can be used to easily configure email filters and organize</td>
</tr>
<tr>
<td>notifications.</td>
</tr>
<tr>
<td>Header</td>
</tr>
<tr>
<td>Optional. Header text that appears at the beginning of the email message</td>
</tr>
<tr>
<td>body. Header text can be used to preface the content of the email message</td>
</tr>
<tr>
<td>with information such as company name and address.</td>
</tr>
<tr>
<td>Footer</td>
</tr>
<tr>
<td>Optional. Footer text that appears at the end of the email message body.</td>
</tr>
<tr>
<td>Footer text can be used to close the email message with reminder information</td>
</tr>
<tr>
<td>such as a contact phone number or a link to a web site.</td>
</tr>
</tbody>
</table>

5. Click Apply Changes.

A new template for notifications is added.

Creating mailing lists

You can create mailing lists for notifications. A mailing list enables you to send one email message to multiple email addresses. These mailing lists are used to send notifications when an alarm is triggered or when a service state changes. You must create a mailing list before you can send notifications. To send a notification to a single recipient, create a mailing list with one email address.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Configuration > Email Setup.
2. From the Email menu, select Lists.
3. Click Edit (or Insert if this is not the first mailing list).
4. In the new row, add the following:

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
</table>
| **Group Name** | Unique name used to identify the mailing list. Mailing list names cannot be duplicated.  
  **Note:** If you change the name of a mailing list, the change is not propagated to the other locations that use the mailing list name. You must manually update all configured notifications to use the new mailing list name. |
| **Recipients** | Single email address, a previously configured mailing list, or a comma-delineated list of email addresses and mailing lists to which notifications will be sent. |
| **Template** | Optionally, select an email template to add a unique header, footer, and subject line to notifications sent to all recipients of this mailing list. |

5. Click **Apply Changes**.

A new mailing list is created.

**Related tasks**

*Creating email templates* on page 29

**Configuring global email notifications**

In order to receive global email notifications, recipients must be a member of a mailing list and that list must be added to the Notifications page. Notifications are configured to send email to recipients only when an alarm with a specified severity level is triggered or when a service state changes. Thus, recipients only receive the notifications they need to receive.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- You must have configured an email list.

**Steps**

1. Select **Configuration > Notifications**.

2. Click **Edit** (or **Insert**) if this is not the first notification).

3. Under **E-mail List**, add a mailing list.
4. Select one or more alarm severity levels and service states:

<table>
<thead>
<tr>
<th>Notification Type</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>Severity Level</td>
<td>An unusual condition exists that does not affect normal operation.</td>
</tr>
<tr>
<td>Minor</td>
<td>Severity Level</td>
<td>An abnormal condition exists that could affect operation in the future.</td>
</tr>
<tr>
<td>Major</td>
<td>Severity Level</td>
<td>An abnormal condition exists that is currently affecting operation.</td>
</tr>
<tr>
<td>Critical</td>
<td>Severity Level</td>
<td>An abnormal condition exists that has stopped normal operation.</td>
</tr>
<tr>
<td>Unknown</td>
<td>Service State</td>
<td>An unknown condition exists that has stopped normal service operation.</td>
</tr>
<tr>
<td>Administratively Down</td>
<td>Service State</td>
<td>A condition whereby a service has been purposefully stopped.</td>
</tr>
</tbody>
</table>

5. Click **Apply Changes**.

Notifications will be sent to the mailing list when alarms with the selected alarm severity level or service state are triggered or changed.

Related tasks

*Creating mailing lists* on page 30

### Suppressing email notifications for a mailing list

You can suppress notifications for a mailing list system-wide when you do not want a mailing list to receive notifications, for example while performing maintenance procedures.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Alarms**.
2. Select **Configuration > Notifications**.
3. Click **Edit** next to the mailing list for which you want to suppress notifications.
4. Under **Suppress**, select the check box next to the mailing list you want to suppress, or select **Suppress** at the top of the column to suppress all mailing lists.
5. Click **Apply Changes**.

Notifications are suppressed for the selected mailing lists.
Suppressing email notifications system wide

You can block the StorageGRID Webscale system’s ability to send notifications when an alarm is triggered.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Configuration > Display Options**.
2. From the Display Options menu, select **Options**.
3. Select **Notification Suppress All**.
4. Click **Apply Changes**.

The Notifications page (**Configuration > Notifications**) displays the following message:

**Selecting a preferred sender**

Each site in a StorageGRID Webscale deployment can include one or more Admin Nodes. If a deployment includes multiple Admin Nodes, one Admin Node is configured as the preferred sender.
of notifications and AutoSupport messages. Any Admin Node can be selected as the preferred sender and can be changed at any time.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

The Display Options page lists the Admin Node that is currently sending notifications. In most cases, this Admin Node is the same as the Preferred Sender; however, if an Admin Node is islanded from the rest of the system, it is unable to use the Preferred Sender and automatically updates to become the Current Sender. In the case of islanded Admin Nodes, multiple Admin Nodes will attempt to send notifications and AutoSupport message and thus it is possible that multiple copies of notifications will be received.

Steps

1. Select Configuration > Display Options.
2. From the Display Options menu, select Options.
3. Select Preferred Sender > Admin Node.
4. Click Apply Changes.
   The Admin Node is set as the preferred sender of notifications.

Alarms management

Customizing alarms lets you customize your StorageGRID Webscale system based on your unique monitoring requirements.

You can configure customized alarms either globally (Global Custom alarms) or for individual services (Custom alarms). You can create custom alarms with alarm levels that override default alarms, and you can create alarms for attributes that do not have a default alarm. Alarm customization is restricted to accounts with Maintenance permissions.

Important: Using the default alarm settings is recommended. Be very careful if you change alarm settings. For example, if you increase the threshold value for an alarm, you might not detect an underlying problem until it prevents a critical operation from completing. If you do need to change an alarm setting, you should discuss your proposed changes with technical support.
For a basic introduction to alarm monitoring, see the Grid Primer. For a list of alarm codes, see the Troubleshooting Guide.

Related concepts

Controlling system access with administration user accounts and groups on page 175

Related information

StorageGRID Webscale 10.4 Troubleshooting Guide
StorageGRID Webscale 10.4 Grid Primer

Alarm class types

Alarms are separated into three mutually exclusive alarm classes.

- **Default**: Standard alarm configurations. Default alarms are set during installation.
- **Global Custom**: Custom alarms that are set at a global level and that apply to all services of a given type in the StorageGRID Webscale system. Global Custom alarms are configured after installation to override default settings.
- **Custom**: Custom alarms that are set on individual services or components. Custom alarms are configured after installation to override default settings.

Default alarms

Default alarms are configured on a global basis and cannot be modified. However, Default alarms can be disabled or overridden by Custom alarms and Global Custom alarms.

Default alarms can be disabled both globally and at the services level. If a Default alarm is disabled globally, the Enabled check box appears with an adjacent asterisk at the services level on the Configuration page. The asterisk indicates that the Default alarm has been disabled through the Alarms > Custom page even though the Enabled check box is selected.

Default alarms for a particular service or component can be viewed on the Grid > service or component > Configuration > Alarms page.

Related tasks

Disabling default alarms for services on page 45
Disabling a default alarm system wide on page 46

Viewing all default alarms

You can view all default alarms that are standard alarm configurations set as part of the installation.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Configuration > Global Alarms**.
2. For **Filtered by** select **Attribute Code** or **Attribute Name**.
3. For **equals**, enter the wildcard symbol: *
4. Click the arrow 🔄 or press Enter. All default alarms are listed.

Global Custom alarms

Global Custom alarms monitor the status of conditions system-wide. By creating a Global Custom alarm, you can override a Default alarm system-wide. You can also create a new Global Custom alarm that will monitor status system-wide. This can be useful for monitoring any customized conditions of your StorageGRID Webscale system.

You can create Global Custom alarms, and disable Global Custom alarms system wide or for individual services.

Related tasks

Creating Global Custom alarms on page 42
Disabling Global Custom alarms for services on page 47
Disabling Global Custom alarms system wide on page 48
Custom alarms

Custom alarms can be created to override a default alarm or global custom alarm at the service or component level. You can also create new custom alarms based on the service’s unique requirements.

You can configure custom alarms by going to each service's Configuration > Alarms page in the Grid Topology tree.

Related tasks

Creating custom service or component alarms on page 40

Alarm triggering logic

Each alarm class is organized into a hierarchy of five severity levels from Normal to Critical. An alarm is triggered when a threshold value is reached that evaluates to true against a combination of alarm class and alarm severity level. Note that a severity level of Normal does not trigger an alarm.

The alarm severity and corresponding threshold value can be set for every numerical attribute. The NMS service on each Admin Node continuously monitors current attribute values against configured thresholds. When an alarm is triggered, a notification is sent to all designated personnel.

Attribute values are evaluated against the list of enabled alarms defined for that attribute in the Alarms table on the Alarms page for a specific service or component (for example, LDR > Storage > Alarms > Main). The list of alarms is checked in the following order to find the first alarm class with a defined and enabled alarm for the attribute:

1. Custom alarms with alarm severities from Critical down to Notice.
2. Global Custom alarms with alarm severities from Critical down to Notice.
3. Default alarms with alarm severities from Critical down to Notice.

After an enabled alarm for an attribute is found in the higher alarm class, the NMS service only evaluates within that class. The NMS service will not evaluate against the other lower priority classes. That is, if there is an enabled Custom alarm for an attribute, the NMS service only evaluates the attribute value against Custom alarms. Global Custom alarms and Default alarms are not evaluated. Thus, an enabled Global Custom alarm for an attribute can meet the criteria needed to trigger an alarm, but it will not be triggered because a Custom alarm (that does not meet the specified criteria) for the same attribute is enabled. No alarm is triggered and no notification is sent.

Related concepts

What an Admin Node is on page 146

Alarm triggering examples

You can use these example to understand how Custom alarms, Global Custom alarms, and Default alarms are triggered.

Example 1

For the following example, an attribute has a Global Custom alarm and a Default alarm defined and enabled as shown in the following table.

<table>
<thead>
<tr>
<th></th>
<th>Threshold Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Custom alarm (enabled)</td>
<td>Default alarm (enabled)</td>
</tr>
<tr>
<td>Notice</td>
<td>&gt;= 1500</td>
</tr>
<tr>
<td>Minor</td>
<td>&gt;= 15,000</td>
</tr>
</tbody>
</table>
Threshold Values

<table>
<thead>
<tr>
<th></th>
<th>Global Custom alarm (enabled)</th>
<th>Default alarm (enabled)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Major</td>
<td>&gt;=150,000</td>
<td>&gt;= 250,000</td>
</tr>
</tbody>
</table>

If the attribute is evaluated when its value is 1000, no alarm is triggered and no notification is sent.

The Global Custom alarm takes precedence over the Default alarm. A value of 1000 does not reach the threshold value of any severity level for the Global Custom alarm. As a result, the alarm level is evaluated to be Normal.

After the above scenario, if the Global Custom alarm is disabled, nothing changes. The attribute value must be evaluated again before a new alarm level is triggered.

With the Global Custom alarm disabled, when the attribute value is evaluated again, the attribute value is evaluated against the threshold values for the Default alarm. The alarm level triggers a Notice level alarm and an e-mail notification is sent to the designated personnel.

Note, however, that if there are custom alarms for an attribute, these alarms are still evaluated as custom alarms have a higher priority than Global Custom alarms.

**Example 2**

For the following example an attribute has a Custom alarm, a Global Custom alarm, and a Default alarm defined and enabled as shown in the following table.

<table>
<thead>
<tr>
<th></th>
<th>Custom alarm (enabled)</th>
<th>Global Custom alarm (enabled)</th>
<th>Default alarm (enabled)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>&gt;= 500</td>
<td>&gt;= 1500</td>
<td>&gt;=1000</td>
</tr>
<tr>
<td>Minor</td>
<td>&gt;= 750</td>
<td>&gt;= 15,000</td>
<td>&gt;=10,000</td>
</tr>
<tr>
<td>Major</td>
<td>&gt;=1,000</td>
<td>&gt;= 150,000</td>
<td>&gt;= 250,000</td>
</tr>
</tbody>
</table>

If the attribute is evaluated when its value is 1000, a Major alarm is triggered and an email notification is sent to the designated personnel. The Custom alarm takes precedence over both the Global Custom alarm and Default alarm. A value of 1000 reaches the threshold value of the Major severity level for the Custom alarm. As a result, the attribute value triggers a Major level alarm.

Within the same scenario, if the Custom alarm is then disabled and the attribute value evaluated again at 1000, the alarm level is changed to Normal. The attribute value is evaluated against the threshold values of the Global Custom alarm, the next alarm class that is defined and enabled. A value of 1000 does not reach any threshold level for this alarm class. As a result, the attribute value is evaluated to be Normal and no notification is sent. The Notice level alarm from the previous evaluation is cleared.

**Example 3**

For the following example, an attribute has a Custom alarm, Global Custom alarm, and Default alarm defined and enabled/disabled as shown below in the following table.

<table>
<thead>
<tr>
<th></th>
<th>Custom alarm (enabled)</th>
<th>Global Custom alarm (enabled)</th>
<th>Default alarm (enabled)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>&gt;= 500</td>
<td>&gt;= 1500</td>
<td>&gt;=1000</td>
</tr>
<tr>
<td>Minor</td>
<td>&gt;= 750</td>
<td>&gt;= 15,000</td>
<td>&gt;=10,000</td>
</tr>
<tr>
<td>Major</td>
<td>&gt;=1,000</td>
<td>&gt;= 150,000</td>
<td>&gt;= 250,000</td>
</tr>
</tbody>
</table>
If the attribute is evaluated when its value is 10,000, a Notice alarm is triggered and an e-mail notification is sent to the designated personnel.

The Custom alarm is defined, but disabled; therefore, the attribute value is evaluated against the next alarm class. The Global Custom alarm is defined, enabled, and it takes precedence over the Default alarm. The attribute value is evaluated against the threshold values set for the Global Custom alarm class. A value of 10,000 reaches the Notice severity level for this alarm class. As a result, the attribute value triggers a Notice level alarm.

If the Global Custom alarm is then disabled and the attribute value evaluated again at 10,000, a Minor level alarm is triggered. The attribute value is evaluated against the threshold values for the Default alarm class, the only alarm class in that is both defined and enabled.

A value of 10,000 reaches the threshold value for a Minor level alarm. As a result, the Notice level alarm from the previous evaluation is cleared and the alarm level changes to Minor. An e-mail notification is sent to the designated personnel.

**Alarms of same severity**

If two Global Custom or Custom alarms for the same attribute have the same severity, the alarms are evaluated with a “top down” priority.

For instance, if UMEM drops to 50MB, the first alarm is triggered (= 50000000), but not the one below it (<=100000000).

If the order is reversed, when UMEM drops to 100MB, the first alarm (<=100000000) is triggered, but not the one below it (= 50000000).
Alarm class overrides

To override a class of alarms, disable all alarms within that class. If all alarms within a class for an attribute are disabled, the NMS service interprets the class as having no alarms configured for the attribute and evaluates the next lower class for enabled alarms.

For example, if an alarm is triggered at the Global Custom alarm class level, it means that there are no enabled alarms at the Custom alarms class level for that attribute.

For example, to override a Default alarm, add a Global Custom alarm or Custom alarm for that attribute. This override is achieved because the NMS service does not evaluate lower priority alarm classes once an alarm setting is detected within a class. If this override is performed after an alarm has already been triggered, the override will not take effect until the alarm is triggered again.

Severity changes

If an alarm’s severity changes, the severity is propagated up the network hierarchy as needed. If there is a notification configured, a notification is sent. The notification is sent only at the time the alarm enters or leaves the new severity level.

Notifications

A notification reports the occurrence of an alarm or the change of state for a service. It is an email communication to designated personnel that the system requires attention.

To avoid multiple alarms and notifications being sent when an alarm threshold value is reached, the alarm severity is checked against the current alarm severity for the attribute. If there is no change, then no further action is taken. This means that as the NMS service continues to monitor the system, it will only raise an alarm and send notifications the first time it notices an alarm condition for an attribute. If a new value threshold for the attribute is reached and detected, the alarm severity changes and a new notification is sent. Alarms are cleared when conditions return to the Normal level.

The trigger value shown in the notification of an alarm state is rounded to three decimal places. Therefore, an attribute value of 1.9999 triggers an alarm whose threshold is less than (<) 2.0, although the alarm notification shows the trigger value as 2.0.

New services

As new services are added through the addition of new grid nodes or sites, they inherit Default alarms and Global Custom alarms.

Creating custom service or component alarms

Customizing alarm settings enables you to create a customized methodology for monitoring the StorageGRID Webscale system. You can create alarms on individual services or components in addition to creating global alarms.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

You should not change default alarm values unless absolutely necessary. By changing default alarms, you run the risk of concealing problems that might otherwise trigger an alarm.
Steps

1. Select Grid.

2. Select a service or component in the Grid Topology tree.

3. Click Configuration > Alarms.

4. Add a new row to the Custom alarms table:
   - Click Edit (if this is the first entry) or Insert to add a new alarm.
   - Copy an alarm from the Default alarms or Global Custom alarms tables. Click Copy next to the alarm you want to modify.

5. Make any necessary changes to the custom alarm settings:

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Select or clear to enable or disable the alarm.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Select the name and code of the attribute being monitored from the list of all attributes applicable to the selected service or component.</td>
</tr>
<tr>
<td></td>
<td>To display information about the attribute, click Info next to the attribute’s name.</td>
</tr>
<tr>
<td>Severity</td>
<td>The icon and text indicating the level of the alarm.</td>
</tr>
<tr>
<td>Message</td>
<td>The reason for the alarm (connection lost, storage space below 10%, and so on).</td>
</tr>
<tr>
<td>Heading</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Operator</strong></td>
<td>Operators for testing the current attribute value against the Value threshold:</td>
</tr>
<tr>
<td></td>
<td>• = equals</td>
</tr>
<tr>
<td></td>
<td>• &gt; greater than</td>
</tr>
<tr>
<td></td>
<td>• &lt; less than</td>
</tr>
<tr>
<td></td>
<td>• &gt;= greater than or equal to</td>
</tr>
<tr>
<td></td>
<td>• &lt;= less than or equal to</td>
</tr>
<tr>
<td></td>
<td>• ≠ not equal to</td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td>The alarm’s threshold value used to test against the attribute’s actual value using the operator.</td>
</tr>
<tr>
<td></td>
<td>The entry can be a single number, a range of numbers specified with a colon (1:3), or a comma delineated list of numbers and/or ranges.</td>
</tr>
<tr>
<td><strong>Additional Recipients</strong></td>
<td>A supplementary list of email addresses to be notified when the alarm is triggered, in addition to the mailing list’s configuration on NMS Management &gt; Notifications &gt; Main. Lists are comma delineated.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Mailing lists require SMTP server setup in order to operate. Before adding mailing lists, confirm that SMTP is configured.</td>
</tr>
<tr>
<td></td>
<td>Notifications for custom alarms can override notifications from Global Custom or Default alarms.</td>
</tr>
<tr>
<td><strong>Actions</strong></td>
<td>Control buttons to:</td>
</tr>
<tr>
<td></td>
<td>🖌 Edit a row</td>
</tr>
<tr>
<td></td>
<td>✈ Insert a row</td>
</tr>
<tr>
<td></td>
<td>✖ Delete a row</td>
</tr>
<tr>
<td></td>
<td>🖇 Drag-and-drop a row up or down</td>
</tr>
<tr>
<td></td>
<td>☮ Copy a row</td>
</tr>
</tbody>
</table>

6. Click **Apply Changes**.

**Creating Global Custom alarms**

You can configure Global Custom alarms when you require a unique alarm that is the same for every service of the same type. Customizing alarm settings enables you to create a customized methodology for monitoring the StorageGRID Webscale system.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

Global alarms override default alarms. It is recommended that you do not change default alarm values unless absolutely necessary. By changing default alarms, you run the risk of concealing problems that might otherwise trigger an alarm.
Steps

1. Select Configuration > Global Alarms.

2. Add a new row to the Global Custom Alarms table. Click **Edit** (if this is the first entry) or **Insert** to add a new alarm.

3. Search for the Default alarm you want to modify.
   a. Under **Filter by**, select either Attribute Code or Attribute Name.
   b. Type a search string.
      Specify four characters or use wildcards (for example, A??? or AB*). Asterisks (*) represent multiple characters and question marks (?) represent a single character.
   c. Click the arrow or press **Enter**.

4. In the list of results, click **Copy** next to the alarm you want to modify. The default alarm is copied to the Global Custom alarms table.

5. Make any necessary changes to the Global Custom alarms settings:

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Select or clear to enable or disable the alarm.</td>
</tr>
<tr>
<td>Heading</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Attribute        | Select the name and code of the attribute being monitored from the list of all attributes applicable to the selected service or component.  
To display information about the attribute, click **Info** next to the attribute’s name. |
| Severity         | The icon and text indicating the level of the alarm.                      |
| Message          | The reason for the alarm (connection lost, storage space below 10%, and so on). |
| Operator         | Operators for testing the current attribute value against the Value threshold:  
• = equals  
• > greater than  
• < less than  
• >= greater than or equal to  
• <= less than or equal to  
• ≠ not equal to |
| Value            | The alarm’s threshold value used to test against the attribute’s actual value using the operator.  
The entry can be a single number, a range of numbers specified with a colon (1:3), or a comma delineated list of numbers and/or ranges. |
| Additional Recipients | A supplementary list of email addresses to be notified when the alarm is triggered. This is in addition to the mailing list’s configuration on the **Configuration > Notifications > Main** page. Lists are comma delineated.  
**Note:** Mailing lists require SMTP server setup in order to operate. Before adding mailing lists, confirm that SMTP is configured.  
Notifications for custom alarms can override notifications from Global Custom or Default alarms. |
| Actions          | Control buttons to:  
- Edit a row  
- Insert a row  
- Delete a row  
- Drag-and-drop a row up or down  
- Copy a row |

6. Click **Apply Changes**.

**Disabling alarms**

Alarms are enabled by default, but you can disable alarms that are not required.

Disabling an alarm for an attribute that currently has an alarm triggered does not clear the current alarm. The alarm will be disabled the next time the attribute crosses the alarm threshold, or you can clear the triggered alarm.
Warning: There are consequences to disabling alarms and extreme care should be taken. Disabling an alarm can result in no alarm being triggered. Because alarms are evaluated by alarm class and then severity level within the class, disabling an alarm at a higher class does not necessarily result in a lower class alarm being evaluated. All alarms for a specific attribute must be disabled before a lower alarm class will be evaluated.

Related tasks

Clearing triggered alarms on page 49

Alarms and tables

Alarm attributes displayed in tables can be disabled at the service, component, or system level. Alarms cannot be disabled for individual rows in a table.

For example, in the following figure, there are two critical Entries Available (VMFI) alarms. You can disable the VMFI alarm so that the Critical level VMFI alarm is not triggered (both currently Critical alarms would appear in the table as green); however, you cannot disable a single alarm in a table row so that one VMFI alarm displays as a Critical level alarm while the other remains green.

| Volumes |
|---|---|---|---|---|---|---|---|
| Mount Point | Device | Status | Size | Space Available | Total Entries | Entries Available | VMFI Cache |
| / | sda1 | Online | 19.5 GB | 7.46 GB | 555,763 | 555,763 | Enabled |
| /var/local | sda2 | Online | 53.4 GB | 53.4 GB | 3,910,460 | 3,910,460 | Unknown |
| /var/local/rangedb/ | | | | | | | |
| /var/local/rangedb/0 | sdc | Online | 53.4 GB | 53.4 GB | 52,427,800 | 52,427,800 | Enabled |
| /var/local/rangedb/1 | sdd | Online | 53.4 GB | 53.4 GB | 52,427,800 | 52,427,800 | Enabled |
| /var/local/rangedb/2 | | | | | | | |

Disabling default alarms for services

To temporarily stop alarms for a specific service, you can disable default alarms for that service.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Grid.
2. Select a service or component in the Grid Topology tree.
3. Click Configuration > Alarms.
4. In the Default Alarms table, click Edit next to the alarm you want to disable.
5. Clear the Enabled check box for the alarm.
6. Click **Apply Changes**.

   The Default alarm is disabled for the service or component.

**Disabling a default alarm system wide**

You can temporarily disable a default alarm system wide.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Click **Configuration > Global Alarms**.

2. Search for the default alarm to disable.
   a. In the Default Alarms section, select **Filter by > Attribute Code** or **Attribute Name**.
   b. Type a search string
      
      Specify four characters or use wildcards (for example, A??? or AB*). Asterisks (*) represent multiple characters and question marks (?) represent a single character.
   c. Click the arrow , or press **Enter**.
      
      **Note:** Selecting **Disabled Defaults** displays a list of all currently disabled Default Global alarms.

3. In the Default Alarms table, click the **Edit icon** next to the alarm you want to disable.
4. Clear the **Enabled** check box.

5. Click **Apply Changes**.

   The default alarm is disabled system wide.

### Disabling Global Custom alarms for services

You cannot disable a global alarm for a service unless you create another enabled global alarm for the attribute. This is because if all alarms within a class for an attribute are disabled, the NMS service interprets the class as having no alarms configured for the attribute and evaluates the next lower class for the enabled alarm.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.

- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

Instead of creating a Global Custom alarm and disabling it for selected services, reconfigure the alarms such that you create individual local custom alarms for the services that require the alarm. If you want to ensure that all these custom alarms have the same configuration, you can create a Global Custom alarm, disable it, and then enable it for selected services as a custom alarm.

If you want to create a Global Custom alarm and disable it for selected services, you must create a local custom alarm for that service that will never be triggered. Doing this overrides all global custom alarms for that service.

**Note:** Alarms cannot be disabled for individual rows in a table.

**Steps**

1. Create a local custom alarm for a service that will never be triggered.

2. Select **Grid**.
3. Select the service or component in the Grid Topology tree.

4. Click Configuration > Alarms.

5. In the Global Custom alarm table, click Copy next to the alarm you want to disable.
   The alarm is copied to the Custom Alarms table.


7. Click Apply Changes.

Related tasks

Creating custom service or component alarms on page 40

Disabling Global Custom alarms system wide

You can disable a Global Custom alarm for the entire system.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

Note: Alarms cannot be disabled for individual rows in a table.

Steps

1. Select Configuration > Global Alarms.

2. In the Global Custom Alarms table, click Edit next to the alarm you want to disable.

3. Clear the Enabled check box.

4. Click Apply Changes.
   The Global Custom alarm is disabled system wide.
Clearing triggered alarms

Disabling an alarm for an attribute that currently has an alarm triggered against it does not clear the alarm. The alarm will be disabled the next time the attribute changes. You can acknowledge the alarm or, if you want to immediately clear the alarm rather than wait for the attribute value to change, (resulting in a change to the alarm state), you can clear the triggered alarm. You might find this helpful if you want to clear an alarm immediately against an attribute whose value does not change often (for example, state attributes).

Before you begin

You must have the root/admin password as listed in the Passwords.txt file.

Steps

1. Disable the alarm.
   
   See the Grid Primer.

2. From the service laptop, log in to the primary Admin Node:
   
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   
   b. Enter the password listed in the Passwords.txt file.
   
   c. Enter the following command to switch to root: `su -`
   
   d. Enter the password listed in the Passwords.txt file.

   Once logged in as root, the prompt changes from `$_` to `#`.

3. Restart the NMS service:

   `/etc/init.d/nms restart`

4. Log out of the Admin Node:

   `exit`

   The alarm is cleared.

Related concepts

*Disabling alarms* on page 44

Related information

*StorageGRID Webscale 10.4 Grid Primer*

What AutoSupport is

AutoSupport enables technical support to proactively monitor the health of your StorageGRID Webscale system. In addition to the automatic weekly message, an AutoSupport message can be sent at any time by manually triggering AutoSupport’s “call home” mechanism.

The AutoSupport’s “call home” mechanism sends a message to technical support that includes the following information:

- StorageGRID Webscale software version
- Operating system version
By analyzing this information, technical support can help you determine the health and status of your StorageGRID Webscale system and troubleshoot any problems that might occur. This also includes monitoring the storage needs of the system, such as the need to expand.

For more information about AutoSupport, go to NetApp Support.

### Triggering AutoSupport messages

You can manually trigger an AutoSupport message at any time.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select Configuration > AutoSupport.

2. From the AutoSupport menu, select User-triggered.

3. Click Send.

   The StorageGRID Webscale system attempts to send an AutoSupport message to technical support. If the attempt is successful, the Last Attempt attribute updates to Successful. If there is a problem, the Last Attempt attribute updates to Failed. The StorageGRID Webscale system does not try again.

   If a failure occurs, check that the StorageGRID Webscale system’s email server is correctly configured and that your email server is running.
Disabling weekly AutoSupport messages

By default, the StorageGRID Webscale system is configured to send an AutoSupport message to NetApp Support once a week.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

To determine when the weekly AutoSupport message is sent, see the Next Scheduled Time attribute on the AutoSupport > Weekly page. You can disable the automatic sending of an AutoSupport message at any time.

Steps

1. Select Configuration > AutoSupport.
2. From the AutoSupport menu, select Weekly.
3. Clear the Enabled check box.
4. Click Apply Changes.

Troubleshooting AutoSupport

If the attempt to send the regularly scheduled AutoSupport message fails, the Most Recent Result attribute updates to Retrying.

The StorageGRID Webscale system attempts to resend the AutoSupport message 15 times every four minutes for one hour. If after one hour a message is not sent, the Most Recent Result attribute updates to Failed. The StorageGRID Webscale system will try again at the next scheduled time. If a failure occurs, check that the StorageGRID Webscale system’s email server is correctly configured and that your email server is running.

In the event that the NMS service is unavailable and thus an AutoSupport message cannot be sent, when the NMS service is once again available, if an AutoSupport message has not been sent in the past seven days, an AutoSupport message is immediately sent; otherwise, AutoSupport maintains its regular schedule.

Note: To send an AutoSupport message, the StorageGRID Webscale system’s email server must be correctly configured.
Related tasks

*Configuring email server settings* on page 28

### Monitoring servers and grid nodes

Various services hosted by the StorageGRID Webscale system's grid nodes provide you with mechanisms to monitor the system.

### What is the SSM service

The Server Status Monitor (SSM) service is present on all grid nodes and monitors the grid node’s status, services, and resources.

The SSM service monitors the condition of the server and related hardware, polls the server and hardware drivers for information, and displays the processed data. Information monitored includes:

- CPU information (type, mode, speed)
- Memory information (available, used)
- Performance (system load, load average, uptime, restarts)
- Volumes (status, available space)
- Network (addresses, interfaces, resources)
- Services
- NTP synchronization

### Services

The Services component tracks the services and support modules running on a grid node. It reports the service’s current version, status, the number of threads (CPU tasks) running, the current CPU load, and the amount of RAM being used.

The services are listed as well as the support modules (such as time synchronization). Also listed is the operating system and the StorageGRID Webscale software version installed on the grid node.
The status of a service is either Running or Not Running. A service is listed with a status of Not Running when its state is Administratively Down.

Related concepts

*Alarm notification types* on page 26

Resetting event counters

The Events component relays logged events. You can treat this data as a general indicator of problems with the system.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Grid.
2. Select a grid node in the Grid Topology tree.
3. Select SSM > Events.
4. Click Configuration > Main.
5. Select the Reset check boxes for the specific counters you want to reset.
6. Click Apply Changes.

Resources

The SSM service uses the standard set of resources attributes that report on the service health and all computational, disk device, and network resources. In addition, the Resources attributes report on memory, storage hardware, network resources, network interfaces, network addresses, and receive
and transmit information. The Resources component of the SSM service provides the ability to reset network error counters.

If the Storage Node is a StorageGRID Webscale appliance, appliance information appears in the Resources section. For details, see the StorageGRID Webscale Appliance Installation and Setup Guide.

**Timing**

The SSM service uses the set of timing attributes that report on the state of the grid node’s time and the time recorded by neighboring grid nodes. In addition, the SSM Timing attributes report on NTP Synchronization.

**Monitoring StorageGRID Webscale Appliance Storage Nodes**

You can view status information for every installed and operational StorageGRID Webscale Appliance Storage Nodes. This includes appliance hardware information, connectivity issues, alarm notifications, services, and disk device information.

**Viewing information about an appliance Storage Node**

You can view information about a StorageGRID Webscale appliance Storage Node at any time. For example, you might want to view the E-Series array name and review appliance-specific information to ensure correct configuration and status.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

Each StorageGRID Webscale appliance is represented as one Storage Node.

The StorageGRID Webscale appliance Storage Node lists information about service health and all computational, disk device, and network resources. You can also see memory, storage hardware, network resources, network interfaces, network addresses, and receipt and transmittal information.

**Steps**

1. Select **Grid**.
2. Select an appliance Storage Node.
3. Select **SSM > Resources**.
4. In the Memory section, note the information in the Installed Memory field.

5. In the Processors section, note the information in the Processor Number column.

   The appliance shows twelve E5-1428L v2 cores (six physical cores with 2:1 hyperthreading enabled).

6. In the Disk Devices section, note the Worldwide Names for the disks in the appliance.

   The Worldwide Name for each disk matches the volume world-wide identifier (WWID) that appears when you view standard volume properties in SANtricity Storage Manager (the management software connected to the E2700 controller).

   To help you interpret disk read and write statistics related to volume mount points, the first portion of the name shown in the Device column of the Disk Devices table (that is, sdc, sde, sdh, and so on) matches the value shown the Device column of the Volumes table on the SSM > Resources page.

7. Review the Storage Hardware section to see more about the StorageGRID Webscale appliance.
This section appears only if the Storage Node is an appliance.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Controller Name</td>
<td>Name of the E2700 controller, as shown in SANtricity Storage Manager.</td>
</tr>
<tr>
<td>Storage Controller Management IP</td>
<td>IP address for management port 1 on the E2700 controller. You can use this IP to connect SANtricity Storage Manager to the E2700 controller in the appliance to troubleshoot storage issues.</td>
</tr>
<tr>
<td>Storage Controller Model</td>
<td>The type of enclosure used for the appliance: 2u12 is two rack-units high with 12 drives, 4u60 is four rack-units high with 60 drives.</td>
</tr>
<tr>
<td>Storage Controller WWN</td>
<td>The worldwide identifier of the E2700 controller, as shown in SANtricity Storage Manager.</td>
</tr>
<tr>
<td>Storage Appliance Chassis Serial Number</td>
<td>The serial number for the appliance.</td>
</tr>
<tr>
<td>Software Platform</td>
<td>The software platform used to generate the storage hardware status and alarms.</td>
</tr>
<tr>
<td>Overall Power Supply Status</td>
<td>The status of power to the StorageGRID Webscale appliance enclosure.</td>
</tr>
<tr>
<td>Power Supply A and B Status</td>
<td>The status of power supply A and B in the StorageGRID Webscale appliance.</td>
</tr>
<tr>
<td>CPU Temperature</td>
<td>The temperature of CPU in the E5600SG controller.</td>
</tr>
<tr>
<td>Module Temperature</td>
<td>The temperature of the E5600SG controller.</td>
</tr>
<tr>
<td>Multipath State</td>
<td>The current multipath I/O state of the physical paths, for example, Simplex or Nominal. If one of the SAS connections on the appliance is not operational, then &quot;Simplex&quot; appears and performance and fault tolerance are impacted. If both paths are not operational, the appliance also stops working. For details about resolving performance or fault tolerance issues, refer to the E-Series documents.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Storage Controller Status | The overall status of the E2700 controller. If the Storage Node is a StorageGRID Webscale appliance and it needs attention, then both the StorageGRID Webscale and SANtricity systems indicate that the storage controller needs attention. If the status is “needs attention,” first check the E2700 controller using SANtricity Storage Manager. Then, ensure that no other alarms exist that apply to the E5600SG controller.

8. In the **Storage Hardware** section, confirm that all statuses are "Nominal."
The statuses in this section correspond to the following alarm codes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Alarm code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Power Supply Status</td>
<td>OPST</td>
</tr>
<tr>
<td>Power Supply A &amp; B Status</td>
<td>PSAS or PSBS</td>
</tr>
<tr>
<td>CPU Temperature</td>
<td>CPUT</td>
</tr>
<tr>
<td>Module (Board) Temperature</td>
<td>BRDT</td>
</tr>
<tr>
<td>Storage Controller Status</td>
<td>SOSS</td>
</tr>
</tbody>
</table>

For details about alarms in StorageGRID Webscale, see the *Troubleshooting Guide.*

9. Use the **Network Resources**, **Network Interfaces**, and **Network Addresses** sections to see IP addresses and status information for each network.

<table>
<thead>
<tr>
<th>Network</th>
<th>Interface name</th>
<th>Physical port name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grid</td>
<td>eth0</td>
<td>hic2 and hic4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Grid network connects to the 10-GbE (optical) network ports on the E5600SG controller. Port 2 is named hic2, and port 4 is named hic4.</td>
</tr>
<tr>
<td>Admin</td>
<td>eth1</td>
<td>mtc1 and mtc2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Admin network connects to the leftmost 1-Gb (RJ-45) Ethernet port on the E5600SG controller. Port 1 is named mtc1. Port 2 (mtc2) is used only for installation and service operations.</td>
</tr>
<tr>
<td>Client (optional)</td>
<td>eth2</td>
<td>hic1 and hic3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Client network connects to the 10-GbE (optical) network ports on the E5600SG controller. Port 1 is named hic1, and port 3 is named hic3.</td>
</tr>
</tbody>
</table>
You can use the **Speed** column in the Network Interfaces table to determine whether the 10-GbE network ports on the appliance were configured to use active/backup mode or LACP mode. In the following example, the Grid network (eth0, highlighted in blue) is using active/backup mode and has a speed of 10 gigabytes (equals the speed of hic2, the active port for that network). In contrast, the Client network (eth2, highlighted in yellow) is using LACP mode and has a speed of 20 gigabits (equals the combined speed of hic1 and hic3).

See the *Appliance Installation and Maintenance Guide* and the appropriate *Software Installation Guide* for more information about configuring the 10-GbE ports.

10. Use the **Receive** and **Transmit** sections to see how many bytes and packets have been sent and received across each network and to see various receive and transmission metrics.

The following example shows active/backup mode being used for the Grid network (see the eth0, hic2, and hic 4 entries, highlighted in blue), and LACP mode being used for the Client network (see the eth2, hic1, and hic3 entries, highlighted in yellow). Note that no bytes and packets were transmitted by hic4, all received packets on hic4 have been dropped, and the total packet counts for eth0 and hic2 are approximately the same. In contrast, data is being sent and received by hic1 and hic3.
You can view events related to a StorageGRID Webscale appliance Storage Node at any time. You might want to monitor events related to the E5600SG controller, the E2700 controller, the multipath state of the appliance connections, and the enclosure to ensure operational status. Some events trigger alarms.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

The StorageGRID Webscale appliance reports on events that impact the service health and all computational, disk devices, hardware, and network resources. For the appliance, you can gauge the hardware status of both the E5600SG controller and the E2700 controller by viewing storage hardware events.

For more information, see the *Troubleshooting Guide* and the *StorageGRID Webscale Appliance Installation and Maintenance Guide*. 
Steps
1. Select Grid.
2. Select an appliance Storage Node in the Grid Topology tree.
3. Select SSM > Events.
4. In the System Events section, note the count for Storage Hardware Events.
5. If a hardware event is noted here, identify the cause by completing the following steps:
   a. Select SSM > Resources.
   b. Look for abnormal conditions in the Storage Hardware section.

Related information
StorageGRID Webscale 10.4 Troubleshooting Guide
StorageGRID Webscale 10.4 Appliance Installation and Maintenance Guide
Managing objects through information lifecycle management

You manage objects through the configuration of information lifecycle management (ILM), which determines how the StorageGRID Webscale system creates and distributes copies of object data and then manages these copies over time.

Every object ingested into the StorageGRID Webscale is filtered against the system’s active ILM policy and the ILM rules that it contains. When the filtering process finds an ILM rule that matches the object, filtering stops and object data is processed and distributed according to the matching ILM rule's placement instructions.

Designing and implementing an ILM policy that manages objects in the manner that you intend requires careful planning and an understanding of ILM. You must define the logic for how objects are to be filtered, copied, and distributed throughout the system, taking into account the topology of the StorageGRID Webscale system, object protection requirements, and available storage types.

What an information lifecycle management policy is

An ILM policy is a set of prioritized ILM rules. It determines how the StorageGRID Webscale system manages object data over time.

The StorageGRID Webscale system's active ILM policy filters all ingested objects, copying object data to storage based on the matching ILM rule's placement instructions. To create an ILM policy, you must create ILM rules and then add them to the ILM policy. Once configured, your ILM policy does not start filtering objects until you activate it.

This diagram illustrates an ILM policy, which dictates that at ingest ILM rules store one copy at data center site one (DC1) on disk (Storage Nodes), one copy at data center site two (DC2) on disk (Storage Nodes), and one copy at DC2 (Archive Node). At the end of one year, ILM rules delete the copy on disk at DC2.

Related concepts

Order of ILM rules within an ILM policy on page 79
What an information lifecycle management rule is

An information lifecycle management (ILM) rule determines how the StorageGRID Webscale system stores object data over time. You configure ILM rules and then add them to an ILM policy.

ILM rules determine:

- Where an object’s data is stored (storage pools)
- The type of storage used to store object data (disk or archival media)
- The number and type of copies made (replicated and erasure coded)
- Which objects are stored
- How the object’s data is managed over time, where it is stored and how it is protected from loss (placement instructions)

How object storage locations are determined

You determine where the StorageGRID Webscale system stores object data by configuring storage pools.

A storage pool is a logical grouping of Storage Nodes (LDR services) or Archive Nodes (ARC services) and is used in ILM rules to determine where object data is stored. A storage pool has two attributes: storage grade and site. Storage grade refers to the type of storage; for example, flash. Site is the location to which object data is stored.

Related concepts

What an Erasure Coding profile is on page 62

How object data is protected from loss

ILM rules provide you with two mechanisms to protect object data from loss: replication and erasure coding.

Replication

Protecting object data from loss through replication means that exact copies of object data are made and stored to multiple Storage Nodes or Archive Nodes. ILM rules dictate the number of copies made, where those copies are made, and for how long they are retained by the system. If a copy is lost as a result of a Storage Node loss, the object is still available if a copy of it exists elsewhere in the StorageGRID Webscale system.

Erasure coding

Protecting object data from loss through erasure coding means that an erasure coding scheme is applied to object data. The erasure coding scheme breaks object data into data and parity fragments, which are distributed across multiple Storage Nodes. If fragments are lost, object data can still be recovered through the information encoded in the remaining fragments.

What an Erasure Coding profile is

You create an Erasure Coding profile by associating a storage pool with an erasure coding scheme. You then select this storage pool and its associated Erasure Coding profile when configuring an ILM rule’s content placement instructions. If an object matches an ILM rule that includes this
configuration, ILM functionality creates an erasure coded copy and distributes its fragments among the selected storage pool’s Storage Nodes.

Erasure coding protects object data from loss by breaking it into data and parity fragments. If fragments are lost, object data can still be recovered through the information encoded in the remaining fragments. A data fragment is a portion of the object’s data, while a parity fragment contains the information required to reconstruct object data if data fragments are lost. The number of data and parity fragments that object data is broken into depends on the selected erasure coding scheme.

An erasure code's parameters define its scheme. An erasure code's parameters are the number of data and parity fragments generated for each erasure coded object. This determines the maximum number of fragments that can be lost before an object is lost. For example, a 6+3 erasure coding scheme encodes an object's data into six data fragments and three parity fragments. The system distributes these nine fragments across nine Storage Nodes and a maximum of three fragments can be lost.

The following is an example of a 6+3 erasure coding scheme, detailing the number of fragments that object data is broken into and the maximum number of fragments that can be lost without impacting retrievals.

Any three fragments (data or parity) can be lost and object data is still recoverable. This is the erasure coding scheme’s fault tolerance.

However, if the erasure coding scheme’s fault tolerance is breached (four in the case of a 6+3 erasure coding scheme), the object is considered lost.
Object data protected from loss through erasure coding consumes less disk space than if it is protected through replication. For example, a 10 MB object that is replicated once consumes 20 MB of disk space, while an object that is erasure coded with a 6+3 scheme only consumes 15 MB of disk space. However, a StorageGRID Webscale deployment that creates erasure coded copies may initially require more Storage Nodes than a deployment that will create replicated copies and may also require more sites. For example, if using an erasure coding scheme of 6+3, to protect erasure coded object data from a site loss, a StorageGRID Webscale deployment must include a minimum of three sites. In contrast, to protect replicated object data from a site loss, a StorageGRID Webscale deployment requires a minimum of two sites.

Depending on the configuration of storage pools, it might take longer to retrieve an erasure coded copy than a replicated copy. A large object that is erasure coded and distributed across sites will take longer to retrieve than an object that is replicated and available locally (the same site to which the client connects). Due to the overhead of managing the number of fragments associated with an erasure coded copy, do not use Erasure Coding profiles for objects smaller than 200 KB.

Related concepts

How object storage locations are determined on page 62

Related tasks

Configuring storage pools on page 69
Configuring Erasure Coding profiles on page 72

Related information

StorageGRID Webscale 10.4 Grid Primer

How ILM rules filter objects

All objects ingested into the StorageGRID Webscale system have their metadata filtered against the active ILM policy and its ILM rules. When a metadata match is made, the content placement instructions for that rule distribute object data throughout the system.

Filtering logic

Within the active ILM policy, an object is evaluated against the first ILM rule and then against subsequent ILM rules until a metadata match is made. If a match is not found after evaluating all ILM rules, the default ILM rule is applied. This figure describes the filtering logic used to determine when an ILM rule applies to an object.
Advanced filtering

With advanced filtering, you can specify metadata against which objects are filtered. If metadata is not used to filter objects, the ILM rule applies to all objects ingested.

The table shows the metadata available for each API. Note that the API itself is also metadata. When you specify an API in an ILM rule, the rule applies only to objects ingested through that API. If you do not specify an API, the ILM rule applies to all objects ingested.

<table>
<thead>
<tr>
<th>Metadata</th>
<th>S3</th>
<th>Swift</th>
<th>CDMI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingest Time</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Key</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Last Access Time</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Object Size</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security Partition</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>User Metadata</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

When you use advanced filtering, you can specify multiple metadata fields and values. For example, if you wanted the rule to match objects between 10 MB and 100 MB in size, you would specify two metadata values.
Advanced filtering allows you to have precise control over which objects are matched. In the following example, the rule applies to objects that have a Brand A or Brand B as the value of the Camera Type user metadata. However, the rule only applies to Brand B objects if they are smaller than 10 MB.

**Note:** When creating ILM rules for erasure coding, you must type in a decimal value if you want to filter on object sizes less than 1 MB (for example, type 0.5 to specify 500 KB). It is recommended that you do not specify object sizes smaller than 200 KB.

**What Dual Commit is**

At ingest and before an object is evaluated against the active ILM policy, Dual Commit functionality synchronously creates two copies of object data and distributes these copies to two Storage Nodes.
The purpose of Dual Commit is to protect objects from accidental loss in the event that a storage location is lost before an object is evaluated against the active ILM policy.

Objects are simultaneously queued for ILM evaluation. When ILM rules are evaluated, additional copies might be made in different locations and initial Dual Commit copies deleted.

If the request to create initial copies fails (for example, because of a network issue that prevents the second initial copy from being made), the StorageGRID Webscale system does not retry and ingest fails.

Dual Commit is enabled by default. If ILM rules are configured to only store one instance of replicated object data, you can disable Dual Commit to avoid unnecessarily creating and then deleting copies generated by the Dual Commit operation.

For configuration information, see the appropriate StorageGRID Webscale API guide.

Related information

StorageGRID Webscale 10.4 S3 (Simple Storage Service) Implementation Guide
StorageGRID Webscale 10.4 Swift Implementation Guide
StorageGRID Webscale 10.3 Cloud Data Management Interface Implementation Guide

Configuring information lifecycle management rules and policy

When you configure your StorageGRID Webscale system's information lifecycle management rules and policy, there is a standard set of steps and related procedures that you work through in order to correctly configure your ILM.

Steps

1. Creating and assigning storage grades on page 67
2. Configuring storage pools on page 69
3. Configuring Erasure Coding profiles on page 72
4. Specifying time values for time based metadata on page 74
5. Creating an ILM rule on page 74
6. Configuring, simulating, and activating an ILM policy on page 78
7. Working with ILM rules and ILM policies on page 91

Creating and assigning storage grades

You can optionally create a unique storage grade and then associate this storage grade with a Storage Node. This allows for the easy identification of the Storage Node when configuring storage pools. If storage grade is not a concern (for example, your StorageGRID Webscale system includes only one type of disk storage), skip this procedure and instead use the system-generated storage grade “All Disks” when configuring a storage pool.

Before you begin

• You must be signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
About this task

A storage grade is the type of storage used by a Storage Node to store object data. Because a StorageGRID Webscale deployment can incorporate multiple spinning and archival media storage technologies, a label can be created for a storage grade and then attached to a Storage Node. This allows for the easy identification of the storage technology used by a Storage Node, which can then be used to select the correct Storage Node when configuring storage pools and determining where object data resides.

A storage grade refers to the storage media type; for example, flash. Creating a unique label for the storage grade and then assigning the storage grade to an LDR service helps you when configuring storage pools. This assignment lets you easily determine the storage type you are assigning to a storage pool.

When creating storage grades, follow these guidelines:

- Do not create more storage grades than necessary. For example, do not create one storage grade for each Storage Node. Instead, assign each storage grade to two or more nodes. Storage grades assigned to only one node can cause ILM backlogs if that node becomes unavailable.

  Note: You cannot configure storage grades for Archive Nodes.

Steps

1. Select ILM > Storage Grades.

2. Create a storage grade:

   a. For each storage grade you need to define, click Insert to add a row and enter a label for the storage grade.

      The Default storage grade cannot be modified. It is reserved for new LDR services added during a StorageGRID Webscale system expansion.
b. To edit an existing storage grade, click **Edit** and modify the label as required.

**Note:** You cannot delete storage grades.

c. Click **Apply Changes**.

These storage grades are now available for assignment to LDR services.

### 3. Assign a storage grade to an LDR service:

a. For each Storage Node's LDR service, click **Edit** and select a storage grade from the list.

![Storage Grades](image)

**Important:** Assign a storage grade to a given Storage Node only once. A Storage Node recovered from failure maintains the previously assigned storage grade. Do not change this assignment once the ILM policy is activated. If the assignment is changed, data is stored based on the new storage grade.

b. Click **Apply Changes**.

### Configuring storage pools

You configure storage pools to determine where object data is stored. You then select these storage pools when configuring Erasure Coding profiles and ILM rules. You can also change a storage pool that is already in use by an ILM rule.

### Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
About this task

When creating storage pools, follow these guidelines:

- Keep storage pool configurations as simple as possible. Do not create more storage pools than necessary. For example, do not create one storage pool for each LDR service.

- Create storage pools with as many nodes as possible. Storage pools should contain two or more nodes. Storage pools with only one node can cause ILM backlogs if that node becomes unavailable.

- Consider how the ILM rule will be configured for the type of copies made: replicated or erasure coded. Available erasure coding schemes are limited by the number of Storage Nodes a storage pool contains.

- Storage pools that will be associated with an erasure coding scheme should contain more than the minimum number of Storage Nodes. For example, if you use a 6+3 erasure coding scheme, you must have at least nine Storage Nodes; However, adding one additional Storage Node per site is recommended.

- If the storage pool will be associated with an erasure coding scheme, you should distribute Storage Nodes across sites as evenly as possible. For example, to support a scheme of 4+2, configure a storage pool that includes three Storage Nodes at three sites.

- Confirm that the storage pools you create have sufficient storage capacity.

- Consider whether or not copies will be archived. Archived copies require a storage pool that only includes Archive Nodes. You cannot create a storage pool that includes both Storage Nodes and Archive Nodes. A storage pool includes either disk or archive media, but not both. If an Archive Node's Target Type is Cloud Tiering - Simple Storage Service (S3), this Archive Node must be in its own storage pool.

A storage pool must include enough storage to satisfy content placement instructions. A replicated copy duplicates complete instances of object data to storage devices within the storage pool. One copy equals one Storage Node or Archive Node. An erasure coded copy distributes fragments to the various Storage Nodes within the storage pool. Storage pools are associated with erasure coding schemes through Erasure Coding profiles. Available erasure coding schemes are limited by the number of Storage Nodes a storage pool contains. There is a one-to-one relationship between the number of Storage Nodes in a storage pool and the erasure coding scheme that can be used.

Note: A storage pool cannot include both Storage Nodes and Archive Nodes.

When configuring storage pools with Archive Nodes, StorageGRID Webscale best practices are that you always maintain redundancy of object data to protect it from loss. Maintain at least one replicated or erasure-coded copy on Storage Nodes when keeping one copy in the Archive Node.

Steps

1. Select ILM > Storage Pools.

2. Create a storage pool:

   a. Click Insert at the end of the row for the last storage pool.
When creating a pool name, create a representative name for the storage pool. This makes for easy identification when configuring Erasure Coding profiles and ILM rules.

Select **Storage Grade > storage_grade** to set the type of storage to which object data will be copied if an ILM rule uses this storage pool. The values All Disks and Archive Nodes are system-generated.

Select **Site > site_name** to set the location to which object data will be copied if an ILM rule uses this storage pool. The value All Sites is system-generated.

When you select a Site, the number of grid nodes and storage capacity information (Installed, Used, and Available) are automatically updated. Make sure that storage pools have sufficient storage and Storage Nodes to support planned ILM rules and the types of copies that will be made.

To add another storage grade/site combination to the storage pool, click **Insert** next to Site. You cannot create storage pools that include LDR and ARC services in the same storage pool. A storage pool includes either disks or archive media, but not both.

To remove a storage grade/site combination, click **Delete** next to Site.

To delete a storage pool, click **Delete** next to the storage pool name. You cannot delete a storage pool that is used in a saved ILM rule.

Click **Apply Changes**.

**Note:** Changes made to a storage pool that is currently in use by an ILM policy do not take effect until the ILM policy is reactivated.

**Related tasks**

*Creating and assigning storage grades* on page 67

*Activating the ILM policy* on page 87
Viewing current storage pools

You can view the current configuration of storage pools at any time.

Before you begin

You must be signed in to the Grid Management Interface using a supported browser.

Steps

1. Select ILM > Storage Pools.

   For each storage pool, you can view the number of Storage Nodes or Archive Nodes as well as the amount of storage installed, used, and available.

   **Note:** For Archive Nodes, storage installed and available is not shown.

   If you have just run expansion grid tasks for Storage Nodes, the total number of LDR services is displayed correctly. However, information related to available storage capacity, storage grade, and site will not be accurate until the new grid nodes are started (services enabled).

2. Click Expand All to display the storage grade and site defined for each storage pool. Click Close All to hide details.

Configuring Erasure Coding profiles

Before you can create an ILM rule that erasure codes object data, you must first create an Erasure Coding profile.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- You must have configured storage pools.
About this task

To create an Erasure Coding profile, associate a storage pool with an erasure coding scheme. This association determines the number of fragments created and where the system distributes these fragments.

**Note:** Once created, an Erasure Coding profile cannot be changed or deleted.

After you create the profile, you can create ILM rules for erasure coding.

**Attention:** When creating ILM rules for erasure coding, do not erasure code objects 200 KB or smaller.

Steps

1. Select ILM > Erasure Coding.

2. If this is not the first profile, click **Insert** to add a new profile.
   
   **Note:** You must update the default Erasure Coding profile listed on the page before adding a new profile.

3. Enter a representative name for the Erasure Coding profile.
   
   Create a name that enables easy identification when you configure ILM rules.

4. Select a storage pool.
   
   When selecting a storage pool, remember that the number of Storage Nodes associated with a storage pool determine which erasure coding schemes are made available for that profile.

5. Select an available erasure coding scheme.
   
   **Note:** Available erasure coding schemes are limited by the number of Storage Nodes available in the selected storage pool.

   When selecting an erasure coding scheme, the profile automatically updates Storage Overhead, Storage Node Redundancy, and Site Redundancy values.
6. To add another profile, click **Insert**. Once created, an Erasure Coding profile cannot be changed or deleted.

7. Click **Apply Changes**.

**Related concepts**

- *What an Erasure Coding profile is* on page 62
- *How object storage locations are determined* on page 62

**Related tasks**

- *Configuring storage pools* on page 69
- *Creating an ILM rule* on page 74

**Specifying time values for time based metadata**

When you configure an ILM rule's advanced filtering, you can select Ingest Time or Last Access Time metadata.

**About this task**

ILM rules apply retroactively to all data in the system. If you want to create rules that only apply to new data, you must specify Ingest Time or Last Access Time metadata. Ingest Time and Last Access Time metadata are specified in microseconds since Unix Epoch.

**Steps**

1. Determine the UTC date and time to filter against.
   - You might need to convert from your local time zone to UTC.

2. Convert the UTC date and time to microseconds since Unix Epoch.
   - For example, use `date` from a Linux command prompt.

**Example**

```
# date -d '2015-03-14 00:00:00 UTC' +%s000000
1426291200000
```

3. If Last Access Time is used, enable last access time updates on each S3 bucket or Swift container, as required.
   - See the appropriate StorageGRID Webscale API guide.

**Related information**

- *StorageGRID Webscale 10.4 S3 (Simple Storage Service) Implementation Guide*
- *StorageGRID Webscale 10.3 Cloud Data Management Interface Implementation Guide*

**Creating an ILM rule**

To manage the placement of object data over time, you must create ILM rules, which is achieved through the Create New ILM Rules wizard.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

• You have configured storage pools.

• To use last access time metadata, Last Access Time must be enabled by bucket for S3, by container for Swift, or by client for CDMI.

• If you are creating erasure coded copies, you must have configured Erasure Coding profiles.

• When creating ILM rules for erasure coding, use advanced filtering to ensure that you do not erasure code objects 200 KB or smaller.

**About this task**

Objects are first evaluated against the ILM rule’s filtering criteria and then, if there is a match, object data is copied and placed based on the matching ILM rule’s placement instructions. Object metadata is not managed by ILM rules. Metadata is kept in the distributed key value store, which makes three copies of an object’s metadata in each data center.

Placement instructions determine where, when, and how object data is stored. If more than one placement instruction is configured, when a set time expires, the content placement instructions for the next time period are applied to objects at the next ILM evaluation time.

**Warning:** Although it is possible to create an ILM rule that creates one replicated copy only, it is not recommended. If the only replicated copy is lost or corrupted, data will be irrevocably lost.

**Steps**

1. Select ILM > Rules.

   The ILM Rules page appears.

2. Click **Create**.

   The Create ILM Rule wizard opens. The screen shots in this section show an example rule named “Finance Records.”
3. Complete Step 1 of the Create ILM Rule wizard.
   
a. Complete the Name and Description fields.
   
b. If a tenant account is configured, select from the Tenant Account field the account ID to which the rule applies. Otherwise, select Ignore.
   
c. Choose the bucket configuration in the Bucket Name fields.
   
d. In the Object Type field, choose the data type to which the rule applies (All, CDMI, or S3/Swift).
   
e. Optionally, click Advanced filtering and configure metadata against which the ILM rule filters object data.
      
      If you do not configure advanced filtering for your ILM rule, the ILM rule matches all objects ingested within the currently configured scope (tenants, buckets, and object type), if any.
      
      **Note:** When creating ILM rules for erasure coding, do not erasure code objects with an Object Size of 200 KB (0.20 MB) or smaller.
   
   f. Click Save.
   
g. Click Next.
      
      Step 2 of the wizard displays.
4. For **Reference Time**, select a time from which the ILM calculates the start time for a placement instruction.

   a. Choose **Ingest Time** to use the time of object ingest.

   b. Choose **Last Access Time** to use the time the object was last modified or viewed.
      
      **Note:** To use this option, Last Access Time must be enabled.

   c. Choose **Noncurrent Time** to use the time an object version becomes noncurrent when a new version is ingested and replaces it as the current version.
      
      One example of using this option can include reducing the storage impact of versioned objects by filtering for noncurrent object versions updated with a new current version or delete marker.
      
      **Note:** The Noncurrent Time applies only to S3 objects in versioning-enabled buckets.

   d. Choose **User Defined Creation Time** to use a time specified in user-defined metadata.
      
      **Note:** The User Defined Creation Time applies only to S3 and Swift objects.

5. Under **Placements**, set the storage location, length of time, and type of copy made for matching object data.

   When you select a storage location (storage pool) for erasure coded object data, the selected storage pool also indicates the erasure coding profile used (in parentheses).
For replicated copies, in addition to the preferred storage pool, you can specify a temporary storage pool. This location is used temporarily if the preferred storage pool is unavailable.

**Warning:** Using a temporary storage pool is strongly recommended. Failure to specify a temporary storage pool puts object data at risk if the preferred pool is unavailable.

6. Click **Refresh** to update the Retention Diagram. Use the retention diagram to confirm your placement instructions.

Each line represents a copy of object data and when the copy is placed in the selected storage pool. Each storage location type is depicted by the following icons:

- Erasure coded
- Replicated

7. Click **Save**.

The ILM rule is saved. The rule is not active until it is added to an ILM policy and that policy is activated.

**Related concepts**

- *How ILM rules filter objects* on page 64
- *Configuring, simulating, and activating an ILM policy* on page 78

**Related tasks**

- *Configuring storage pools* on page 69

**Configuring, simulating, and activating an ILM policy**

After you have created ILM rules, you add them to an ILM policy and then simulate and activate the ILM policy. You should then verify the active policy by ingesting test objects.

Before you create an ILM policy, determine the following:

- The number and type of copies required (replicated or erasure coded), and their placement over time.
- The metadata used in the applications that connect to the StorageGRID Webscale system. Objects are filtered against metadata.
- The StorageGRID Webscale system’s topology and storage configurations.

Keep the ILM policy as simple as possible. This avoids potentially dangerous situations where object data is not protected as intended when changes are made to the StorageGRID Webscale system over time.

**Warning:** An ILM policy that has been incorrectly configured can result in unrecoverable data loss. Before activating an ILM policy, carefully review the ILM policy and its ILM rules, and then simulate the ILM policy. Always confirm that the ILM policy will work as intended.

Policy configuration consists of these main tasks:

1. Creating or updating the ILM policy by adding ILM rules and reordering the rules as needed
2. Simulating the policy
3. Activating the policy
4. Verifying the active policy
Order of ILM rules within an ILM policy

The order in which you place ILM rules within an ILM policy determines how ILM rules are applied. The object is first evaluated against the top priority ILM rule and then subsequent ILM rules until a match is made. To match an ILM rule’s filter, an object must match all of the filter’s criteria. If an object does not have the metadata tag specified in the criteria, the object does not match the filter.

One ILM rule must be set as the default ILM rule. If none of the other ILM rules match the object, the placement instructions specified in the default rule are applied. When the StorageGRID Webscale system is first installed, the stock ILM rule “Make 2 Copies” is the default ILM rule.

Configuring an ILM policy

Use the ILM policy configuration page to create or update ILM policies.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- To configure an ILM policy, you must include at least one ILM rule:
  - You can configure a new policy using the stock ILM rule “Make 2 Copies.”
  - You can create the rules before you create the policy or while you are creating the policy.
    
    **Note:** If you go back to configuring rules, you lose any simulation objects you have added to the simulation page and must add them back in after returning to the configuration page.
  - You know the order you want the ILM rules to be applied.

About this task

You can create or update policies using the configuration page. Typical reasons for updating an ILM policy include:

- The current ILM policy has an error.
- Changes have been made to a storage pool.
- An Archive Node was added to the StorageGRID Webscale system.
- New client application connections were added.
- New storage retention requirements were defined (for example, there was a change in regulatory requirements).
Steps

1. Select ILM > Policies.

2. Select the Configure tab.
   The configuration page initializes and displays the active policy.

3. If you want to create a new ILM policy, enter the name of the new ILM policy in the Name field.
   If you are updating an existing policy, changing the name is optional, but recommended if significant changes are made to the policy.

4. Click the icon next to each rule in the policy to view the settings for each rule.
   Note: This icon is available on each dialog where rules are displayed.

5. If you want to add rules to the policy, click Select Rules.
   The Select Rules for Policy dialog displays.

6. Select the ILM rules you want to add to the policy.
   Rules that are already in the policy remain checked. As required, you can uncheck rules in this dialog to remove them from the policy.
   Note: Rules created using StorageGRID Webscale version 10.2 or earlier can only be included in the proposed policy if they are already included in the active policy.

7. Click Apply to close the dialog.

8. Change the order of ILM rules within the policy by dragging and dropping rules in the list.
   Warning: The order of ILM rules within an ILM policy is extremely important. Objects are filtered against ILM rules as they are listed in the table: from top to bottom.
9. Select Default next to the ILM rule you want to be applied as the default. Every ILM policy must contain a default ILM rule.

10. If a tenant account was configured for a rule, confirm that the Tenant Account column includes the correct account ID.

11. Confirm that the Object Type column identifies the correct object type for each rule.

12. Click Save to save the configured policy and enable the Simulate and Activate buttons. The policy is saved but not yet active. At this point, the policy is a proposed policy.

Related concepts

How ILM rules filter objects on page 64

Simulating an ILM policy

If you are changing a rule or policy, you must simulate the new rule or policy on objects before applying it to production data. The simulation window provides a standalone environment that is safe for testing policies before they are activated and applied to data in the production environment.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- You must know which objects you are going to simulate the policy on and have already ingested the objects.

About this task

You must carefully select previously ingested objects for use with the simulation environment. To thoroughly simulate a policy, you must have at least one object for each criteria the rules will be matching against.

For example, if you have one rule matching bucket A and another rule matching bucket B, you would need at least one object from bucket A and one object from bucket B to validate the ILM. In the case a default rule is relied upon say for bucket C, you would need at least one additional object to validate the ILM.

When simulating a policy change, the following considerations apply:

- After you make changes to a policy, save the proposed policy. Then, simulate the saved proposed policy. If a proposed policy does not exist, the active policy is used for simulation instead.
- Simulation filters the specified objects against the ILM rules you are testing. Simulation does not modify data, rules, or policies in any way.
- If you do not close or refresh the Policy creation page, then the Simulation page retains your selected objects when closed.
- Simulation returns the name of the matched rule. To determine which Storage Pool or EC Profile is in effect, reference the Retention Diagram for that rule.
- When entering the Object ID, use the identifier specific to the protocol selected. If S3 is selected, use the bucket and key such as "<bucket> / <key>" in the Object ID field.
- If S3 Versioning is enabled, the policy is only simulated against the current version of the object.
Steps

1. Click **Simulate** to test the policy by specifying existing objects that are in the grid and confirming that the correct rule matches the object.

   The objects must have been previously ingested into the grid before you can specify them for simulation.

   The Simulation Results dialog appears.

2. Under Simulation Results, verify that each object matches the appropriate rule.

   **Note:** If an object is entered for simulation that has not been ingested, then the Object Not Found error message displays.

![Error](image)

Examples for simulating ILM policies

These examples show how you can verify ILM rules by simulating the ILM policy before activating it.

Choices

- Example 1: Verifying rules when simulating a proposed ILM policy on page 82
- Example 2: Reordering rules when simulating a proposed ILM policy on page 84
- Example 3: Correcting a rule when simulating a proposed ILM policy on page 86

**Example 1: Verifying rules when simulating a proposed ILM policy**

This example shows how to verify rules when simulating a proposed policy.

Steps

1. Click **Save** on the proposed policy to be simulated.

   In this example, there is a bucket "photos" with ingested objects, and a new rule "X-men" has been created that tests for `metadata=x-men`. A second rule has been created that includes "png" file types. The rules have been added to the policy, and the policy has been saved.
2. Click **Simulate**.

   The Simulation Results dialog appears.

3. Under Simulation Results, verify that each object matches the appropriate rule.

   In this example, the Fullsteam image metadata does not match the X-men metadata rule, but it does match the png filename rule. Both Havok and Warpath files match the X-men metadata rule, which is evaluated first. Next, the objects would match the png/jpg rules respectively because of their object type, even though they do not match the metadata rules. The default rule would only be used if, for example, Havok.png were named Havok.tiff and did not match the remaining PNGs/JPGs rules.

4. Update the policy by entering the new title, click **Select Rules**, add rules to the updated policy, and click **Save**.

   In this example, there is a bucket "photos" with ingested objects, and a new rule "X-men" has been created that tests for metadata=x-men. A second rule has been created that includes "png" file types. The rules have been added to the policy, and the policy has been saved.

5. Click **Simulate** to test the policy by specifying existing objects that are in the grid and confirming that the correct rule matches the object.

   The objects must have been previously ingested into the grid before you can specify them for simulation.

   The Simulation Results dialog appears.
6. Under Simulation Results, verify that each object matches the appropriate rule.

   In this example, the Fullsteam image metadata does not match the X-men metadata rule, but it does match the png filename rule. Both Havok and Warpath files match the X-men metadata rule, which is evaluated first. If these files did not match the default rule, then the respective PNGs or JPG rule would be evaluated next.

   **Note:** If an object is entered for simulation that has not been ingested, then the Object Not Found error message displays.

**Example 2: Reordering rules when simulating a proposed ILM policy**

This example shows how to reorder rules when simulating a proposed policy.

**About this task**

In this example, the Demo policy is testing the rule for objects with `metadata=x-men` and a key name ending with "png."

**Steps**

1. Drag and drop the rules so that the rule testing for PNGs is at the top.
2. Select **Save** and then **Simulate**.

The simulation result shows the Havok.png object matches the PNGs rule.

```plaintext
   Name: Demo

Select the rules which will be part of the new policy. Drag and drop rows to re-order rules. Rules are evaluated top-down.

<table>
<thead>
<tr>
<th>Default</th>
<th>Rule Name</th>
<th>Tenant Account</th>
<th>Object Type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PNGs</td>
<td>Ignore</td>
<td>S3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>X-men</td>
<td>Ignore</td>
<td>S3:Swift</td>
<td></td>
</tr>
<tr>
<td></td>
<td>X-men</td>
<td>Ignore</td>
<td>All</td>
<td></td>
</tr>
</tbody>
</table>

The simulation result shows the Havok.png object matches the PNGs rule.
```

However, in this case, the rule that the Havok.png object is meant to be testing is the X-men rule.

3. Drag and drop the rules so that the rule testing for X-men is at the top. Select **Save** and then **Simulate**.

```plaintext
   Name: Demo

Select the rules which will be part of the new policy. Drag and drop rows to re-order rules. Rules are evaluated top-down.

<table>
<thead>
<tr>
<th>Default</th>
<th>Rule Name</th>
<th>Tenant Account</th>
<th>Object Type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X-men</td>
<td>Ignore</td>
<td>S3:Swift</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PNGs</td>
<td>Ignore</td>
<td>S3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Make 2 Copies</td>
<td>Ignore</td>
<td>All</td>
<td></td>
</tr>
</tbody>
</table>

The simulation result shows the Havok.png object matching the X-men rule.
**Example 3: Correcting a rule when simulating a proposed ILM policy**

This example shows how to simulate a policy, correct a rule in the policy, and continue the simulation.

**Steps**

1. Select **Save** and then **Simulate**.

   In this example, the Demo policy is testing the rule for objects with `metadata=x-men` and using the Beast.jpg object to test the rule. However, the Simulation results show the object matches the default rule for Make 2 Copies.

2. For each rule in the policy, view the rule settings by selecting the information icon on any dialog where the rules are displayed. Notice that the metadata matching for the rule is incorrect. The rule is matching `metadata=x-men1` instead of `metadata=x-men`.

---

86 | StorageGRID Webscale 10.4 Administrator Guide
Correct the rule by using the **Configure > ILM Rules** screen. After the rule is corrected, perform the simulation again.

**Note:** The objects for simulation that were previously entered are no longer displayed when you navigate away from the Policy page. Re-enter the objects on the Simulation screen as necessary.

Now that the rule has been corrected, the Beast.jpg object matches the expected rule in the policy.

### Activating the ILM policy

After you have added ILM rules to a proposed ILM policy and simulated the policy, you are ready to activate the proposed policy.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

You must have saved and simulated the proposed ILM policy.

**Warning:** Errors in an ILM policy can cause unrecoverable data loss. Carefully review and simulate the policy before activating it to confirm that it will work as intended. When a new ILM policy goes into effect, the StorageGRID Webscale system immediately uses it to manage all objects in the grid, including existing objects and newly ingested objects.

### About this task

When you activate an ILM policy, the system distributes the new policy to all nodes. However, the new active policy might not actually take effect until all grid nodes are available to receive the new policy. In some cases, the system waits to implement a new active policy to ensure that grid objects are not accidentally removed.

- If you make policy changes that increase data redundancy or durability, those changes are implemented immediately. For example, if you activate a new policy that uses a Make 3 Copy rule instead of a Make 2 Copy rule, that policy will be implemented right away because it increases data redundancy.

- If you make policy changes that could decrease data redundancy or durability, those changes will not be implemented until all grid nodes are available. For example, if you activate a new policy that uses a Make 2 Copy rule instead of a Make 3 Copy rule, the new policy will be marked as “Active,” but it will not take effect until all nodes are online and available.

### Steps

1. When you are ready to activate a new policy, click **Activate** on the ILM Policies > Configure page.

   Clicking **Revert** causes the proposed policy to be discarded and reverts to the active policy.

2. Click **OK** to confirm you want to change the ILM policy.

### Result

When a new ILM policy has been activated, it appears in the ILM Policy > Active page. It is also listed on the CMS > Content > Overview > Main page.

The previously active policy appears in the ILM Policy > Historical page.

Each ILM policy is automatically assigned a version number in the form `major.minor` (for example, 2.5). The change of a name such that no other policy previously existed with that name triggers a major revision. If a policy previously existed with that name, then it triggers a minor revision.

### Verifying an ILM policy

After you have activated a new ILM policy, you should ingest test objects into the StorageGRID Webscale system. You can perform an “object lookup” to confirm that copies are being made as intended and placed in the correct locations.

### Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.

- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

- You must have an object identifier, which can be one of the following:
- **S3 bucket and key:** When an object is ingested through the S3 interface, the client application uses a bucket and key combination to store and identify the object. For details, see the *S3 Implementation Guide*.

- **Swift container and object:** When an object is ingested through the Swift interface, the client application uses a container and object combination to store and identify the object. For details, see the *Swift Implementation Guide*.

- **CDMI data object ID:** When an object is ingested through the CDMI interface, the StorageGRID Webscale system returns a CDMI data object ID to the client application. For details, see the *Cloud Data Management Interface Implementation Guide*.

- **CBID:** You can obtain an object’s CBID from the latest audit log, which is located on the Admin Node at /var/local/audit/export.

**Steps**

1. Ingest an object.
   Before ingesting the object, confirm that you have the object’s identifier.
2. Select Grid.
3. Select *primary Admin Node > CMN > Object Lookup*.
4. Click *Configuration > Main*.
5. Type the object's S3 bucket/key, Swift container/object, CDMI data object ID, or CBID in the *Object Identifier* field.
6. Press Enter, or click *Apply Changes*.
7. From the Grid Options menu, click *Overview*.
   The Object Lookup page displays the current location of the object and any metadata associated with the object.
8. Confirm that the object is stored in the correct location or locations and that it is the correct type of copy.

**Note:** If the Audit option is enabled, you can also monitor the audit log for the “ORLM Object Rules Met” message. The ORLM audit message can provide you with more information about the status of the ILM evaluation process, but it cannot give you information about the
correctness of the object data’s placement or the completeness of the ILM policy. You must evaluate this yourself. For more information, see the Audit Message Reference.

Related concepts
Configuring audit client access on page 160

Related information
StorageGRID Webscale 10.4 Audit Message Reference
StorageGRID Webscale 10.3 Cloud Data Management Interface Implementation Guide
StorageGRID Webscale 10.4 S3 (Simple Storage Service) Implementation Guide
StorageGRID Webscale 10.4 Swift Implementation Guide

Working with ILM rules and ILM policies
Once you have created ILM rules and an ILM policy, you can continue to work with them, modifying their configuration as your storage requirements change.

Deleting an ILM rule
To keep the list of current ILM rules manageable, delete any ILM rules that you are not likely to use. You cannot delete the stock ILM rule (“Make 2 Copies”), ILM rules listed in the active policy, or ILM rules currently listed in the proposed policy.

Before you begin
• You must be signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps
1. Select ILM > Rules.
2. Select the ILM rule you want to delete and click Remove.
3. Click OK to confirm that you want to delete the ILM rule.
   The ILM rule is deleted.

Related concepts
Configuring, simulating, and activating an ILM policy on page 78

Editing an ILM rule
After creating an ILM rule, and before adding it to the active ILM policy, you can edit it. You cannot edit the stock ILM rule (“Make 2 Copies”), ILM rules listed in the active policy, ILM rules currently listed in the proposed policy, or ILM rules created before StorageGRID Webscale version 10.3.

Before you begin
• You must be signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
Steps

1. Select ILM > Rules.

   The ILM Rules page appears.

   ![ILM Rules page](image)

2. Select the appropriate rule and click **Edit**.

   The Edit ILM Rule wizard opens.

   ![Edit ILM Rule wizard](image)

3. Complete the pages of the **Edit ILM Rule** wizard, following the steps for creating an ILM rule as necessary.

   When editing an ILM rule, you cannot change its name.

4. Click **Save**.

Cloning an ILM rule

You can clone an existing ILM rule and use it to create a new rule. You cannot clone ILM rules created before StorageGRID Webscale version 10.3.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select ILM > Rules.

   The ILM Rules page appears.
2. Select the ILM rule you want to clone and click **Clone**.
   The Create ILM Rule wizard opens.

3. Follow the steps for creating an ILM rule. Edit the cloned ILM rule as necessary and click **Save**.
   The new ILM rule is created.

### Viewing historical ILM policies

You can view historical ILM rules at any time. These are ILM rules that have been at some point in time included in an active ILM policy.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

Historical ILM policies include ILM policies that are no longer active. Historical ILM policies cannot be deleted.

**Steps**

1. Select **ILM > Policies**.
2. Select **ILM Policies > Historical**.
3. To view the ILM rules and storage pools associated with an ILM policy, click **Expand**. All policies are displayed with start and end dates.
4. Within an ILM rule, click **Expand** to display more information about its configuration.
Viewing the ILM policy activity queue

You can view the number of objects that are in queue to be evaluated against the ILM policy at any time. You might want to monitor the ILM processing queue to determine system performance. A large queue might indicate that the system is not able to keep up with the ingest rate, the load from the client is too great, or that some abnormal condition exists.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Dashboard.

2. Monitor the Information Lifecycle Management (ILM) section.
   You can click the title of each item in the ILM section (for example, Awaiting - Client) to see a description of the item.

Example ILM rules and policies

You can use the following examples as starting points for defining your own ILM rules and policy.

- Example 1: ILM rules and policy for object storage
- Example 2: ILM rules and policy for EC object size filtering on page 98
- Example 3: ILM rules and policy for better protection for image files on page 101

Example 1: ILM rules and policy for object storage

You can use the following example rules and policy as a starting point when defining an ILM policy to meet your object protection and retention requirements.

Warning: The following ILM rules and policy are only examples. There are many ways to configure ILM rules. Carefully analyze your ILM rules before adding them to an ILM policy to confirm that they will work as intended to protect content from loss.
ILM rule 1 for example 1: Copy object data to two data centers

This example ILM rule copies object data to storage pools in two data centers.

<table>
<thead>
<tr>
<th>Rule definition</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Pools</td>
<td>Two storage pools, each at different data centers, named Storage Pool DC1 and Storage Pool DC2.</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Two Copies Two Data Centers</td>
</tr>
<tr>
<td>Reference Time</td>
<td>Ingest Time</td>
</tr>
</tbody>
</table>
| Content Placement | • On Day 0, keep a replicated copy in Storage Pool DC1 forever; temp copies in Storage Pool DC2  
                    • On Day 0, keep a replicated copy in Storage Pool DC2 forever; temp copies in Storage Pool DC1 |

Create ILM Rule

Configure placement instructions to determine where the system stores matching object data, for how long, and the type of copy made (replicated or transient coded).

Two Copies Two Data Centers

| Reference Time | Ingest Time |

Placements

Create 1 copies as replicated in Storage Pool DC1 or temporarily in Storage Pool DC2

Create 1 copies as replicated in Storage Pool DC2 or temporarily in Storage Pool DC1

Retention Diagram

Storage Pool DC1

Storage Pool DC2

Duration

Forever
ILM rule 2 for example 1: Erasure Coding profile with bucket matching

This example ILM rule uses an Erasure Coding profile and an S3 bucket to determine where and how long the object is stored.

<table>
<thead>
<tr>
<th>Rule definition</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erasure Coding Profile</td>
<td>• One storage pool across three data centers</td>
</tr>
<tr>
<td></td>
<td>• Use 4+2 Erasure Coding scheme</td>
</tr>
<tr>
<td>Rule Name</td>
<td>EC for S3 Bucket FinanceRecords</td>
</tr>
<tr>
<td>Reference Time</td>
<td>Ingest Time</td>
</tr>
<tr>
<td>Content Placement</td>
<td>For objects in the S3 Bucket FinanceRecords, create one Erasure Coded copy in the pool specified by the Erasure Coding profile. Keep this copy forever.</td>
</tr>
</tbody>
</table>

ILM rule 3 for example 1: Store object to DC1 and Archive

This example ILM rule creates two copies. One copy is stored in Data Center 1 for one year, and the second copy is stored in an Archive Node forever.

<table>
<thead>
<tr>
<th>Rule definition</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Pools</td>
<td>A disk storage pool and an archive storage pool.</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Archive</td>
</tr>
<tr>
<td>Reference Time</td>
<td>Ingest Time</td>
</tr>
</tbody>
</table>
### ILM policy for example 1

The StorageGRID Webscale system allows you to design sophisticated and complex ILM policies; however, in practice, most ILM policies are simple.

A typical ILM policy for a multi-site topology might include ILM rules such as the follows:

- At ingest, use 4+2 Erasure Coding to store all objects belonging to the S3 Bucket FinanceReports across three data centers.

- If an object does not match the first ILM rule, use the default ILM rule to store a copy of that object in two data centers, DC1 and DC2.
Example 2: ILM rules and policy for EC object size filtering

You can use the following example rules and policy as starting points to define an ILM policy that filters by object size to meet recommended EC requirements.

**Warning:** The following ILM rules and policy are only examples. There are many ways to configure ILM rules. Carefully analyze your ILM rules before adding them to an ILM policy to confirm that they will work as intended to protect content from loss.

**ILM rule 1 for example 2: Use EC for all objects larger than 200 KB**

This example ILM rule erasure codes all objects larger than 200 KB (0.20 MB).

<table>
<thead>
<tr>
<th>Rule definition</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>EC only objects &gt; 200 KB</td>
</tr>
<tr>
<td>Reference Time</td>
<td>Ingest Time</td>
</tr>
<tr>
<td>Advanced Filtering for Object Size</td>
<td>Object Size (MB) greater than 0.20</td>
</tr>
<tr>
<td>Content Placement</td>
<td>Create 1 erasure coded copy in all Storage Nodes</td>
</tr>
</tbody>
</table>
The placement instructions specify that one erasure coded copy be created in all Storage Nodes.

### ILM rule 2 for example 2: Make 2 copies

This example ILM rule creates two replicated copies and does not filter by object size. This rule is the second rule in the policy. Because ILM rule 1 for example 2 filters out all objects larger than 200 KB, ILM rule 2 for example 2 only applies to objects that are 200 KB or smaller.

<table>
<thead>
<tr>
<th>Rule definition</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Make 2 Copies</td>
</tr>
<tr>
<td>Reference Time</td>
<td>Ingest Time</td>
</tr>
<tr>
<td>Advanced Filtering for Object Size</td>
<td>None</td>
</tr>
<tr>
<td>Content Placement</td>
<td>Create 2 replicated copies in all Storage Nodes</td>
</tr>
</tbody>
</table>
ILM policy for example 2: Use EC for objects larger than 200 KB

In this example policy, objects larger than 200 KB are erasure coded, and any other objects that are smaller than 200 KB are replicated using the default catch-all Make 2 Copies rule.

This example ILM policy includes the following ILM rules:

- Erasure code all objects larger than 200 KB.
- If an object does not match the first ILM rule, use the default ILM rule to create two replicated copies of that object. Because objects larger than 200 KB have been filtered out by rule 1, rule 2 only applies to objects that are 200 KB or smaller.
Example 3: ILM rules and policy for better protection for image files

You can use the following example rules and policy to ensure that images larger than 200 KB are erasure coded and that three copies are made of smaller images.

**Warning:** The following ILM rules and policy are only examples. There are many ways to configure ILM rules. Carefully analyze your ILM rules before adding them to an ILM policy to confirm that they will work as intended to protect content from loss.

ILM rule 1 for example 3: Use EC for image files larger than 200 KB

This example ILM rule uses advanced filtering to erasure code all image files larger than 200 KB. Because this rule is configured as the first rule in the policy, it catches all image files larger than 200 KB.

<table>
<thead>
<tr>
<th>Rule definition</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>EC image files &gt; 200 KB</td>
</tr>
<tr>
<td>Reference Time</td>
<td>Ingest Time</td>
</tr>
<tr>
<td>Advanced Filtering for User Metadata</td>
<td>User Metadata type equals image files</td>
</tr>
<tr>
<td>Advanced Filtering for Object Size</td>
<td>Object Size (MB) greater than 0.2</td>
</tr>
<tr>
<td>Content Placement</td>
<td>Create 1 erasure coded copy in all Storage Nodes</td>
</tr>
</tbody>
</table>

Advanced Filtering

Select metadata to determine how this ILM rule filters objects for the selected API. If you do not configure advanced filtering, this ILM rule applies to all objects ingested through the selected API.
ILM rule 2 for example 3: Replicate 3 copies for all remaining image files

This example ILM rule uses advanced filtering to specify that image files be replicated. Because the first rule in the policy will have already matched image files larger than 200 KB, this rule will only apply to image files 200 KB or smaller.

<table>
<thead>
<tr>
<th>Rule definition</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>3 copies for image files</td>
</tr>
<tr>
<td>Reference Time</td>
<td>Ingest Time</td>
</tr>
<tr>
<td>Advanced Filtering for User Metadata</td>
<td>User Metadata type equals image files</td>
</tr>
<tr>
<td>Content Placement</td>
<td>Create 3 replicated copies in all Storage Nodes</td>
</tr>
</tbody>
</table>
ILM policy for example 3: Better protection for image files

In this example, the ILM policy uses three ILM rules to create a policy that guarantees EC of image files larger than 200 KB (0.2 MB) and separately handles image files 200 KB or smaller and other file types.

This example ILM policy includes the following ILM rules:

1. Erasure code all image files larger than 200 KB.
2. Then, create three copies of any remaining image files (that is, images that are 200 KB or smaller).
3. Finally, apply the default Make 2 Copy rule to any remaining objects (that is, all non-image files).

When you first create the ILM policy, it appears on the Configure tab with the rules in the specified order and the default rule selected.
After the ILM policy has been simulated and activated, it appears on the **Active** tab with the rules in the specified order and the default rule indicated.
Managing disk storage

Storage Nodes provide disk storage capacity and services.

What a Storage Node is

A Storage Node includes the services and processes required to store, move, verify, and retrieve object data and metadata on disk.

What the LDR service is

Hosted by a Storage Node, the Local Distribution Router (LDR) service handles content transport for the StorageGRID Webscale system. Content transport encompasses many tasks including data storage, routing, and request handling. The LDR service does the majority of the StorageGRID Webscale 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 data transfers from another LDR service (Storage Node)
- Object deleting
- Object data storage
- Object data transfers from another LDR service (Storage Node)
- Data storage management
- Protocol interfaces (S3 and Swift)

For general information about the LDR service’s role in the management of objects, see the Grid Primer.
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 key data 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 time out is high, that might indicate that the data store is 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 distributed key value stores at the time a query is performed through the specific LDR service.

ILM Activity

Information Lifecycle Management (ILM) metrics allow you to monitor the rate at which objects are evaluated for ILM implementation. These metrics are also visible on the Dashboard.

Related information

StorageGRID Webscale 10.4 Grid Primer
Object stores

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

Object stores are identified by a hexadecimal number from 0000 to 000F, which is known as the volume ID. Replicated copies and erasure coded fragments are stored to all available object stores within a Storage Node, while object metadata is stored only to volume 0000.

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.

Monitoring ILM activity

You can monitor the number of objects waiting or being queued for ILM evaluation.

Information Lifecycle Management (ILM) metrics allow you to monitor the rate at which objects are evaluated for ILM implementation. These metrics are also visible on the Dashboard.

To monitor ILM activity, click Grid. Then, select Storage Node > LDR > Data Store > Overview > Main.

This table summarizes the ILM Activity statistics.
<table>
<thead>
<tr>
<th>Service/Component</th>
<th>Attribute Name</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDR &gt; Data Store &gt; ILM Activity</td>
<td>ILM Implementation</td>
<td>ILMN</td>
<td>The ILM policy currently in use.</td>
</tr>
<tr>
<td></td>
<td>ILM Version</td>
<td>ILMV</td>
<td>The version number of the ILM policy currently in use.</td>
</tr>
<tr>
<td></td>
<td>Awaiting - All</td>
<td>QUSZ</td>
<td>The total number of objects on this node awaiting ILM evaluation.</td>
</tr>
<tr>
<td></td>
<td>Awaiting - Client</td>
<td>CQUZ</td>
<td>The total number of objects on this node awaiting ILM evaluation from client operations (for example, ingest).</td>
</tr>
<tr>
<td></td>
<td>Awaiting - Background Scan</td>
<td>BQUZ</td>
<td>The total number of objects on this node awaiting ILM evaluation from the scan.</td>
</tr>
<tr>
<td></td>
<td>Scan Rate</td>
<td>SCRT</td>
<td>The rate at which objects owned by this node are scanned and queued for ILM.</td>
</tr>
<tr>
<td></td>
<td>Scan Period - Estimated</td>
<td>SCTM</td>
<td>The estimated time to complete a full ILM scan on this node. <strong>Note:</strong> A full scan does not guarantee that ILM has been applied to all objects owned by this node.</td>
</tr>
<tr>
<td></td>
<td>Awaiting - Evaluation Rate</td>
<td>EVRT</td>
<td>The current rate at which objects are evaluated against the ILM policy on this node.</td>
</tr>
<tr>
<td></td>
<td>Repairs Attempted</td>
<td>REPA</td>
<td>The total number of object repair operations for replicated data that have been attempted on this node. This count increments each time an LDR tries to repair a high-risk object. High-risk ILM repairs are prioritized if the grid becomes busy. <strong>Note:</strong> The same object repair might increment again if replication failed after the repair.</td>
</tr>
</tbody>
</table>

This table summarizes the Object Transfer statistics.

<table>
<thead>
<tr>
<th>Service/Component</th>
<th>Attribute Name</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDR &gt; Data Store &gt; Object Transfer</td>
<td>Active Transfers</td>
<td>DCdA</td>
<td>The total number of objects being transferred to another storage device (Storage Node or Archive Node).</td>
</tr>
<tr>
<td></td>
<td>Transfer Rate</td>
<td>DCdR</td>
<td>The rate at which objects are currently being transferred to another storage device (Storage Node or Archive Node).</td>
</tr>
<tr>
<td></td>
<td>Total Transfers</td>
<td>DCdT</td>
<td>The total number of object transfers generated by this service.</td>
</tr>
</tbody>
</table>

This table summarizes the Object Deleting statistics.
What the DDS service is

Hosted by a Storage Node, the Distributed Data Store (DDS) service interfaces with the distributed key value store and manages metadata stored in the StorageGRID Webscale system. Included in this management is the distribution of metadata copies to multiple instances of the distributed key value store so that metadata is always protected against loss.

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

Object counts

The DDS service lists the total number of objects ingested into the StorageGRID Webscale system as well as the total number of objects ingested through each of the system’s supported interfaces (S3, Swift, and CDMI).

Because object metadata synchronization occurs over time, object count attributes (see DDS > Data Store > Overview > Main) can differ between DDS services. Eventually, all distributed key value stores will synchronize and counts should become the same.
Queries
You can identify the average time that it takes to run a query against the distributed key value data 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 key data 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 time out is high, that might indicate that the data store is 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 distributed key value stores at the time a query is performed through the specific DDS service.

Consistency guarantees and controls
StorageGRID Webscale 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.

Metadata protection
Object metadata is information related to or a description of an object; for example, object modification time, or storage location. Metadata is stored in a distributed key value store maintained by the StorageGRID Webscale system’s DDS services.

To ensure redundancy and thus protection against loss, the StorageGRID Webscale system stores copies of the object metadata in different distributed key value stores throughout the StorageGRID Webscale system including between sites. This replication is non-configurable and performed automatically by the DDS service.

What the nodetool repair operation is
Periodically, the StorageGRID Webscale system runs the nodetool repair operation on Storage Nodes checking for and repairing metadata replication inconsistencies that may occur over time.

Nodetool repair is run every 12 to 14 days at random times on different Storage Nodes, so that it does not run on every Storage Node at the same time. The nodetool repair operation is a seamless activity that occurs in the background of normal system operations.

CMS service
The Content Management System (CMS) service manages objects to ensure that the StorageGRID Webscale system’s information lifecycle management (ILM) policy is satisfied.

The CMS service carries out the operations of the active ILM policy’s ILM rules, determining how object data is protected over time. For general information about the role of the CMS service when content is ingested and copied, see the Grid Primer.

Related tasks
Configuring information lifecycle management rules and policy on page 67

Related information
StorageGRID Webscale 10.4 Grid Primer
ADC service

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 Webscale deployment’s configuration bundles, allowing any grid node to retrieve current configuration information.

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 Webscale 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 Webscale system.

Managing Storage Nodes

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

Monitoring Storage Node capacity

To monitor the amount of usable space available on a Storage Node go to Storage Node > LDR > Storage > Overview > Main and note the current value for the attribute Total Usable Space (STAS).
Total Usable Space (STAS) is calculated by adding together the available space of all object stores for a Storage Node. A Storage Node does not become read-only until all object stores are filled to configured watermark settings.

Total Usable Space = Useable Space 0 + Useable Space 1 + Useable Space 2 + Useable Space 3

Related concepts

*Watermarks* on page 113
Watermarks

You use watermark settings to globally manage a Storage Node’s usable storage space. Watermarks settings trigger alarms that assist you in monitoring available storage and determine when adding Storage Nodes is required.

A Storage Node becomes read-only when all of a Storage Node’s object stores reach the Storage Volume Hard Read-Only Watermark. If available space falls below this configured watermark amount, a Notice alarm is triggered for the Storage Status (SSTS) attribute. This allows you to manage storage proactively and add capacity only when necessary.

The StorageGRID Webscale system’s current watermark values can be obtained at any time. Go to Configuration > Storage Options > Overview.

Watermark related attributes
<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Default Setting</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
</table>
| Storage Volume Soft Read-Only Watermark           | 10 GB           | VHWM  | Indicates when a Storage Node transitions to soft read-only mode. Soft read-only mode means that the Storage Node advertises read-only services to the rest of the StorageGRID Webscale system, but fulfills all pending write requests. The Storage Volume Soft Read-Only Watermark value is calculated against the Total Space value for the Storage Node, but measured against the Total Usable Space value for the Storage Node. When the value of Total Usable Space falls below the value of Storage Volume Soft Read-Only Watermark, the Storage Node transitions to soft read-only mode:  
  • The Storage State – Current (SSCR) changes to Read-Only. If Storage State – Desired is set to Online, Storage Status (SSTS) changes to Insufficient Free Space and a Notice alarm is triggered.  
  • An alarm for Total Usable Space (Percent) (SAVP) can be triggered, depending on the relationship between the watermark setting (in bytes) and the alarm settings (in percent). The Storage Node is writable again if Total Usable Space (STAS) becomes greater than Storage Volume Soft Read-Only Watermark. |
| Storage Volume Hard Read-Only Watermark           | 5 GB            | VROM  | Indicates when a Storage Node transitions to hard read-only mode. Hard read-only mode means that the Storage Node is read-only and no longer accepts write requests. The Storage Volume Hard Read-Only Watermark value is calculated against the Total Space value for the Storage Node, but measured against the Total Usable Space value for the Storage Node. When the value of Total Usable Space falls below the value of Storage Volume Hard Read-Only Watermark, the Storage Node transitions to hard read-only mode. The Storage Volume Hard Read-Only Watermark value must be less than value for The Storage Volume Soft Read-Only Watermark. |
| Metadata Reserved Space Watermark                  | 2 TB            | CAWM  | The amount of free space reserved on object store volume 0 for metadata storage. If the storage capacity of volume 0 is less than 500 GB, only 10% of the storage volume’s capacity is reserved for metadata. |

**Related concepts**

*Managing full Storage Nodes* on page 117

**Storage Node configuration settings**

Depending on your requirements, there are several configuration settings for Storage Nodes that you can apply.

This table summarizes Storage Node configuration settings.
<table>
<thead>
<tr>
<th>Service/ Component</th>
<th>Attribute Name</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
</table>
| LDR                | HTTP/CDMI State | HSTE   | Set the LDR service to one of:  
- 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.  
- Online: Operation continues normally |
| Auto-Start HTTP    |                | HTAS   | Enable the HTTP component when the LDR service is restarted. If not selected, the HTTP interface remains Offline until explicitly enabled.  
If Auto-Start HTTP is selected, the state of the system on restart depends on the state of the LDR > Storage component. If the LDR > Storage component is Read-only on restart, the HTTP interface is also Read-only. If the LDR > Storage component is Online, then HTTP is also Online. Otherwise, the HTTP interface remains in the Offline state. |
| LDR > Storage      | Storage State – Desired | SSDS   | 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.  
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.  
The attribute can take one of the following values:  
- Offline: When the desired state is Offline, the LDR service takes the LDR > Storage component offline.  
- 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.  
- 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. |
<p>| 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. |</p>
<table>
<thead>
<tr>
<th>Service/Component</th>
<th>Attribute Name</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDR &gt; Verification</td>
<td>Reset Missing Objects Count</td>
<td>VCMII</td>
<td>Resets the count of Missing Objects Detected (OMIS). Use only after foreground verification completes. Missing replicated object data is restored automatically by the StorageGRID Webscale system.</td>
</tr>
<tr>
<td></td>
<td>Verify</td>
<td>FVOV</td>
<td>Select object stores on which to perform foreground verification.</td>
</tr>
<tr>
<td></td>
<td>Verification Priority</td>
<td>VPRI</td>
<td>Set the priority rate at which background verification takes place. See Configuring the background verification rate on page 126.</td>
</tr>
<tr>
<td></td>
<td>Reset Corrupt Objects Count</td>
<td>VCCR</td>
<td>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 more information, see the StorageGRID Webscale 10.4 Troubleshooting Guide.</td>
</tr>
<tr>
<td>LDR &gt; Erasure Coding</td>
<td>Reset Writes Failure Count</td>
<td>RSWF</td>
<td>Reset to zero the counter for write failures of erasure coded object data to the Storage Node.</td>
</tr>
<tr>
<td></td>
<td>Reset Reads Failure Count</td>
<td>RSRF</td>
<td>Reset to zero the counter for read failures of erasure coded object data from the Storage Node.</td>
</tr>
<tr>
<td></td>
<td>Reset Deletes Failure Count</td>
<td>RSDF</td>
<td>Reset to zero the counter for delete failures of erasure coded object data from the Storage Node.</td>
</tr>
<tr>
<td></td>
<td>Reset Corrupt Copies Detected Count</td>
<td>RSCC</td>
<td>Reset to zero the counter for the number of corrupt copies of erasure coded object data on the Storage Node.</td>
</tr>
<tr>
<td></td>
<td>Reset Corrupt Fragments Detected Count</td>
<td>RSCD</td>
<td>Reset to zero the counter for corrupt fragments of erasure coded object data on the Storage Node.</td>
</tr>
<tr>
<td>Service/ Component</td>
<td>Attribute Name</td>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>LDR &gt; Replication</td>
<td>Reset Inbound Replication Failure Count</td>
<td>RICR</td>
<td>Reset to zero the counter for inbound replication failures. This can be used to clear the RIRF (Inbound Replication – Failed) alarm.</td>
</tr>
<tr>
<td></td>
<td>Reset Outbound Replication Failure Count</td>
<td>ROCR</td>
<td>Reset to zero the counter for outbound replication failures. This can be used to clear the RORF (Outbound Replications – Failed) alarm.</td>
</tr>
<tr>
<td></td>
<td>Disable Inbound Replication</td>
<td>DSIR</td>
<td>Select to disable inbound replication as part of a maintenance or testing procedure. Leave unchecked during normal operation. When inbound replication is disabled, objects can be retrieved from the Storage Node for copying to other locations in the StorageGRID Webscale system, but objects cannot be copied to this Storage Node from other locations: the LDR service is read-only.</td>
</tr>
<tr>
<td></td>
<td>Disable Outbound Replication</td>
<td>DSOR</td>
<td>Select to disable outbound replication (including content requests for HTTP retrievals) as part of a maintenance or testing procedure. Leave unchecked during normal operation. 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 Webscale system. The LDR service is write-only.</td>
</tr>
<tr>
<td>LDR &gt; CDMI</td>
<td>Reset CDMI Counts</td>
<td>CACR</td>
<td>Reset to zero the counter for all CDMI transactions.</td>
</tr>
<tr>
<td>LDR &gt; HTTP</td>
<td>Reset HTTP Counts</td>
<td>LHAC</td>
<td>Reset to zero the counter for all HTTP transactions.</td>
</tr>
</tbody>
</table>

**Related information**

*StorageGRID Webscale 10.4 Troubleshooting Guide*

**Managing full Storage Nodes**

As Storage Nodes reach capacity, you must be expand the StorageGRID Webscale system through the addition of new storage. There are two options available when considering how to increase storage capacity: adding Storage Nodes and adding storage volumes.

**Adding Storage Nodes**

You can increase storage capacity by adding Storage Nodes. Careful consideration of currently active ILM rules and capacity requirement must be taken when adding storage. For more information about how to add storage volumes and Storage Nodes, see the *Expansion Guide*.

**Adding storage volumes**

Each Storage Node supports a maximum of 16 storage volumes. If a Storage Node includes fewer than 16 storage volumes, you can increase its capacity by adding storage volume up to the maximum of 16.
Related information

StorageGRID Webscale 10.4 Expansion Guide for VMware Deployments
StorageGRID Webscale 10.4 Expansion Guide for OpenStack Deployments
StorageGRID Webscale 10.4 Expansion Guide for Red Hat Enterprise Linux Deployments

Monitoring storage

Monitoring storage includes looking at total storage capacity, consumed storage, and usable storage. You might want to monitor storage capacity to determine your usable storage for the entire StorageGRID Webscale system or for select data center sites.

Monitoring storage capacity system-wide

At the deployment level, you can monitor installed storage capacity, used storage capacity, and usable storage capacity.

Before you begin

You must be signed in to the Grid Management Interface using a supported browser.

Step

1. Select Dashboard.

Note the values for the StorageGRID Webscale system’s storage capacity.

Monitoring storage capacity per Storage Node

You can track the amount of usable space available on a Storage Node through the Total Usable Space (STAS) attribute, which is calculated by adding together the available space of all object stores for a Storage Node.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.

About this task

A Storage Node does not become read-only until all object stores are filled to configured watermark settings.

Steps

1. Select Grid.
2. Select **Storage Node > LDR > Storage**.

3. Note the current value for the attribute Total Usable Space (STAS).

![Overview: LDR (dc1-s4-100-116) - Storage](image)

**Utilization**
- Total Space: 160 GB
- Total Usable Space: 155 GB
- Total Data: 634 GB
- Total Data (Percent): 98.5%
- Total Data (Percent): 3.35%

**Replication**
- Block Reads: 3,392
- Block Writes: 3,567
- Objects Retrieved: 1,197
- Objects Committed: 675
- Objects Deleted: 673
- Delete Source State: Enabled

**Object Stores**

<table>
<thead>
<tr>
<th>ID</th>
<th>Total</th>
<th>Available</th>
<th>Stored Data</th>
<th>Stored (%)</th>
<th>Cached Data</th>
<th>Cached (%)</th>
<th>Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>0080</td>
<td>53.4 GB</td>
<td>48 GB</td>
<td>53.4 GB</td>
<td>10.002%</td>
<td>32.3 MB</td>
<td>0.006%</td>
<td>No Errors</td>
</tr>
<tr>
<td>0081</td>
<td>53.4 GB</td>
<td>53.4 GB</td>
<td>727 KB</td>
<td>0.801%</td>
<td>34 MB</td>
<td>0.864%</td>
<td>No Errors</td>
</tr>
<tr>
<td>0082</td>
<td>53.4 GB</td>
<td>53.4 GB</td>
<td>552 KB</td>
<td>0.802%</td>
<td>83.5 MB</td>
<td>0.151%</td>
<td>No Errors</td>
</tr>
</tbody>
</table>

**Related concepts**
- Watermarks on page 113

**Configuring settings for stored objects**

You can configure the settings for stored objects, including stored object encryption, stored object hashing, and stored object compression. You can also enable the Prevent Client Modify setting to override the permissions defined for HTTP profiles and to deny specific HTTP client operations.

**Choices**
- Configuring stored object encryption on page 119
- Configuring stored object hashing on page 120
- Configuring stored object compression on page 121
- Enabling Prevent Client Modify on page 122

**Configuring stored object encryption**

Stored object encryption enables the encryption of stored object data so that if an object store is compromised data cannot be retrieved in a readable form. By default, objects are not encrypted.

**Before you begin**
- You must be signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

Objects can also be encrypted using the AES-128 or AES-256 encryption algorithm. Stored object encryption enables the encryption of all object data ingested through S3, Swift, or CDMI. If disabled, currently encrypted objects remain encrypted. For S3 objects, the Stored Object Encryption setting can be overridden by the `x-amz-server-side-encryption` header. If you use the `x-amz-server-side-encryption` header, you must specify the AES-256 encryption algorithm in the request.

**Note:** If you change this setting, it may take a short period of time for the new setting to be applied. The configured value is cached for performance and scaling. If you want to ensure that the new setting is applied immediately, you need to restart the StorageGRID Webscale system.

**Steps**

1. Select **Configuration > Grid Options**.
2. From the Grid Options menu, select **Configuration**.
3. Change Stored Object Encryption to **Disabled, AES-256, or AES-128**.
4. Click **Apply Changes**.

**Configuring stored object hashing**

The Stored Object Hashing option specifies the hashing algorithm used by the LDR service to hash data when new content is stored. These hashes are verified during retrieval and verification to protect the integrity of data.

**Before you begin**

• You must be signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
About this task

By default, object data is hashed using the SHA-1 algorithm. Object data can also be hashed using the SHA-256 algorithm.

Steps

1. Select Configuration > Grid Options.
2. From the Grid Options menu, select Configuration.
3. Change Stored Object Hashing to SHA-256 or SHA-1.
4. Click Apply Changes.

Configuring stored object compression

Stored Object Compression uses lossless compression of object data to reduce the size of objects and thus consume less storage.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

Applications saving an object to the StorageGRID Webscale system can compress the object before saving it; however, if a client application compresses an object before saving it to the StorageGRID Webscale system, enabling Stored Object Compression does not further reduce an object’s size.

Stored Object Compression is disabled by default.
Steps

1. Select **Configuration > Grid Options**.
2. From the Grid Options menu, select **Configuration**.
3. Change Stored Object Compression to **Enabled**.
4. Click **Apply Changes**.

Enabling Prevent Client Modify

You can set the Prevent Client Modify option to **Enabled** to override the permissions defined for HTTP profiles and to deny specific HTTP client operations.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

When the Prevent Client Modify option is enabled, the following requests are denied:

- **S3 REST API**
  - Delete Bucket requests
  - Requests to modify any existing object. For example, the following operations are denied: Put Overwrite, Delete, Metadata Update, and so on.
    
    **Note:** This setting does not apply to buckets with versioning enabled because they already prevent the modification of existing data.
• **Swift REST API**
  - Delete Container requests
  - Requests to modify any existing object. For example, the following operations are denied: Put Overwrite, Delete, Metadata Update, and so on.

• **CDMI**
  - Delete requests
  - Metadata Update requests
  - Last Access Time Update

Prevent Client Modify is a system wide setting.

**Steps**
1. Select Configuration > Grid Options.
2. From the Grid Options menu, select Configuration.
3. Change Prevent Client Modify to Enabled.
4. Click Apply Changes.

**Mounted storage devices**

At installation, each storage device is assigned a file system UUID and is mounted to a rangedb directory on the Storage Node using that file system UUID. The file system UUID and the rangedb directory are captured in the `/etc/fstab` file.

The device name, rangedb directory, and the size of the mounted volume are displayed at Storage Node > SSM > Resources > Overview > Main.
In the following example, device `/dev/sdb` has a volume size of 830 GB, is mounted to `/var/local/rangedb/0`, using the device name `dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba` in the `/etc/fstab` file.

What security partitions are

Security partitions is a system-wide setting that restricts CDMI client access to objects. A security partition prevents CDMI client applications from retrieving objects ingested through another CDMI client application. CDMI client applications are only permitted read-write access to a specific security partition, but can be configured with read-only access to other security partitions.

**Note:** Security partitions are ignored for objects ingested through the S3 and Swift interfaces.

Objects ingested before security partitions are enabled are not assigned a security partition and can be retrieved, queried, and deleted by any client application. If security partitions are enabled, objects ingested by a client application that is not assigned a security partition can be retrieved, queried, and deleted by any other client application—client applications are not automatically assigned a security partition.

**Related information**

*StorageGRID Webscale 10.3 Cloud Data Management Interface Implementation Guide*
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 Webscale system, the LDR service splits the object into segments, and creates a segment container that lists the header information of all segments as content. For CDMI clients, the OID of the segment container is returned as the ingest result.

If your StorageGRID Webscale 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 Webscale 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 Webscale 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 10Gbps 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.
Verifying object integrity

The StorageGRID Webscale system verifies the integrity of object data on Storage Nodes, checking for both corrupt and missing objects.

There are two verification processes: background verification and foreground verification. Background verification runs automatically and continuously checks for corrupt object data. Foreground verification is manually triggered to detect missing objects.

Related concepts

What background verification is on page 126
What foreground verification is on page 128

Related information

StorageGRID Webscale 10.4 Troubleshooting Guide

What background verification is

The background verification process automatically and continuously checks Storage Nodes to determine if there are corrupt copies of replicated object data or corrupt fragments of erasure coded object data. If problems are found, the StorageGRID Webscale system automatically attempts to replace the missing or corrupt object data from copies stored elsewhere in the system. Background verification does not run on Archive Nodes.

If the background verification process detects that a copy of replicated object data is corrupt, that corrupt copy is removed from its location and quarantined elsewhere on the Storage Node. The Storage Node's LDR service then sends a request to the DDS service to create a new uncorrupted copy. The DDS service fulfills this request by running an existing copy through an ILM evaluation, which will determine that the current ILM policy is no longer being met for this object because the corrupt object no longer exists at the expected location. A new copy is generated and placed to satisfy the system's active ILM policy. This new copy may not be placed in the same location that the corrupt copy was stored. Corrupt object data is quarantined rather than deleted from the system, so that it can still be accessed. For more information on accessing quarantined object data, contact Support.

If the background verification process detects that a fragment of erasure coded object data is corrupt, that missing erasure coded fragment is rebuilt in place on the same Storage Node from the remaining fragments for that copy of erasure coded object data.

If background verification cannot replace the corrupted object because it cannot locate another copy, a LOST (Lost Object) alarm is triggered. Note that for erasure coded copies, if an object cannot be retrieved from the expected location, an ECOR (Corrupt Copies Detected) alarm is triggered on the Storage Node from which the retrieval was attempted and an attempt is made to retrieve another copy. Only when no other copies are found, the LOST (Lost Objects) alarm is also triggered.

Background verification cannot be stopped; however, the rate at which it runs can be changed.

Configuring the background verification rate

For each Storage Node, you can change the rate that background verification checks replicated object data.

Before you begin

• You must be signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

You can change the rate at which background verification takes place by adjusting the Verification Priority value:

• Adaptive: Default setting. The task is designed to verify at a maximum of four MB/s or 10 objects/s (whichever is exceeded first).

• High: Storage verification proceeds quickly, at a rate that can slow ordinary system activities. Use the High verification priority only when you suspect that a hardware or software fault might have corrupted replicated object data. After the High priority background verification completes, the Verification Priority value automatically resets to Adaptive.

Steps

1. Select Grid.

2. Select Storage Node > LDR > Verification.

3. Click Configuration > Main.

4. Go to LDR > Verification > Configuration > Main.

5. Under Background Verification, select Verification Priority > High or Verification Priority > Adaptive.

6. Click Apply Changes.

7. Monitor the results of background verification. Go to LDR > Verification > Overview > Main and monitor the attribute Corrupt Objects Detected.
If background verification finds corrupt replicated object data, the attribute Corrupt Objects Detected is incremented. The LDR service recovers by quarantining the corrupt object data and sending a message to the DDS service to create a new copy of the object data. The new copy can be made anywhere in the StorageGRID Webscale system that satisfies the active ILM policy.

8. If corrupt object data is found, contact Support to clear the quarantined copies from the StorageGRID Webscale system and determine the root cause of the corruption.

What foreground verification is

The foreground verification process allows you to manually verify the existence of replicated object data on a Storage Node. Foreground verification does not check for missing fragments of erasure coded object data. If a copy of replicated object data is found to be missing, the StorageGRID Webscale system automatically attempts to replace the missing object data from copies stored elsewhere in the system. The Storage Node's LDR service sends a request to the DDS service to create a new copy. The DDS service fulfills this request by running an existing copy through an ILM evaluation, which will determine that the current ILM policy is no longer being met for this object because the missing object no longer exists at the expected location. A new copy is generated and placed to satisfy the system's active ILM policy. This new copy may not be placed in the same location that the missing copy was stored.

Running foreground verification

Foreground verification enables you to verify the existence of replicated object data on a Storage Node. This foreground verification process can help you to determine if there are integrity issues with a storage device. Missing objects might indicate an issue with the underlying storage, which the LDR service uses.

Before you begin

• You must be signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
• Ensure that the following grid tasks are not running:
  ◦ Grid Expansion: Add Server (GEXP), when adding a Storage Node
  ◦ Storage Node Decommissioning (LDCM) on the same Storage Node

If these grid tasks are running, wait for them to complete or release their lock, or abort them as appropriate.
• Storage must be online.

About this task

Foreground verification only checks for missing replicated object data and does not check for missing fragments of erasure coded object data.

You can configure foreground verification to check all of a Storage Node's object stores or only specific object stores. If foreground verification determines that a copy of replicated object data is missing, the count for the Missing Objects Detected (OMIS) attribute (see Grid > site > Storage Node > LDR > Verification > Overview > Main) goes up by one. A replacement copy is automatically created by the system and stored to a location that satisfies the active ILM policy. The replacement copy is not necessarily stored on the Storage Node from which it originally went missing. If a replacement copy cannot be made, the LOST (Lost Object) alarm might be triggered.
Foreground verification generates an LDR Foreground Verification grid task that, depending on the number of objects stored on a Storage Node, can take days or weeks to complete. It is possible to select multiple Storage Nodes at the same time; however, these grid tasks are not run simultaneously, but rather queued and run one after the other until completion. When foreground verification is in progress on a Storage Node, you cannot start another foreground verification task on that same Storage Node even though the option to verify additional volumes might appear to be available for the Storage Node.

If a Storage Node other than the one where foreground verification is being run goes offline, the grid task continues to run until the % Complete attribute reaches 99.99 percent. The % Complete attribute then falls back to 50 percent and waits for the Storage Node to return to online status. When the Storage Node's state returns to online, the LDR Foreground Verification grid task continues until it completes.

Steps
1. Select Grid.
2. Select Storage Node > LDR > Verification.
3. Click Configuration > Main.
4. Under Foreground Verification, select ID for the storage volume or volumes to verify.
5. Click Apply Changes.
   Wait until the page auto-refreshes and reloads before you leave the page. Once refreshed, object stores become unavailable for selection on that Storage Node.
   An LDR Foreground Verification grid task is generated and runs until it completes or is aborted. To view its progress, go to Grid > site > Admin Node > CMN > Grid Task > Overview > Main. If object data is found to be missing, the missing object data is automatically replicated.
6. Monitor missing objects:
a. Select **Storage Node > LDR > Verification**.

b. From the Grid Options menu, click **Overview**.

c. Under **Verification Results** note the value of **Missing Objects Detected**.

   If the count for the attribute **Missing Objects Detected** is large (if there are hundreds of missing objects), there is likely an issue with the Storage Node's storage. In this case, cancel foreground verification by aborting the Foreground Verification grid task, resolve the storage issue, and then rerun foreground verification for the Storage Node.

   If foreground does not detect a significant number of replicated objects are missing, then the storage is operating normally.

**After you finish**

If foreground verification finds no (or few) missing objects, and you still have concerns about data integrity, it is recommended that you verify the integrity of the stored objects on the LDR by increasing the priority of the background verification process.

**How load balancing works**

To balance ingest and retrieval workloads, optionally deploy the StorageGRID Webscale system with API Gateway Nodes, or integrate a third-party load balancer.

**API Gateway Node**

The API Gateway Node provides load balancing functionality to the StorageGRID Webscale system and distributes the workload when multiple client applications perform ingest and retrieval operations.

The Connection Load Balancer (CLB) service directs incoming requests to the optimal LDR service, based on availability and system load. When the optimal LDR service is chosen, the CLB service establishes an outgoing connection and forwards the traffic to the chosen grid node.

HTTP connections from the StorageGRID Webscale system to a client application use the CLB service to act as a proxy unless the client application is configured to connect through an LDR service. The CLB services operates as a connection pipeline between the client application and an LDR service.
Managing archival storage

Optionally, each of your StorageGRID Webscale system's data center sites can be deployed with an Archive Node, which allows you to connect to a targeted external archival storage system.

What an Archive Node is

The Archive Node provides an interface through which you can target an external archival storage system for the long term storage of object data. The Archive Node also monitors this connection and the transfer of object data between the StorageGRID Webscale system and the targeted external archival storage system.

Object data that cannot be deleted, but is not regularly accessed, can at any time be moved off of a Storage Node's spinning disks and onto external archival storage such as the cloud or tape. This archiving of object data is accomplished through the configuration of a data center site's Archive Node and then the configuration of ILM rules where this Archive Node is selected as the "target" for content placement instructions. The Archive Node does not manage archived object data itself; this is achieved by the external archive device.

Note: Object metadata is not archived, but remains on Storage Nodes.

What the ARC service is

The Archive Node's Archive (ARC) service provides the management interface with which you configure connections to external archival storage such as the cloud through the S3 API or tape through TSM middleware.

It is the ARC service that interacts with an external archival storage system, sending object data for nearline storage and performing retrievals when a client application requests an archived object. When a client application requests an archived object, a Storage Node requests the object data from the ARC service. The ARC service makes a request to the external archival storage system, which retrieves the requested object data and sends it to the ARC service. The ARC service verifies the object data and forwards it to the Storage Node, which in turn returns the object to the requesting client application.

Requests for object data archived to tape through TSM middleware are managed for efficiency of retrievals. Requests can be ordered so that objects stored in sequential order on tape are requested in
that same sequential order. Requests are then queued for submission to the storage device. Depending upon the archival device, multiple requests for objects on different volumes can be processed simultaneously.

**Related information**

*StorageGRID Webscale 10.4 Grid Primer*

**About supported archive targets**

When you configure the Archive Node to connect with an external archive, you must select the target type.

The StorageGRID Webscale system supports the archiving of object data to the cloud through an S3 interface or to tape through TSM middleware.

**Archiving to the cloud through the S3 API**

You can configure an Archive Node to target any external archival storage system that is capable of interfacing with the StorageGRID Webscale system through the S3 API.

The Archive Node's ARC service can be configured to connect directly to Amazon Web Services (AWS) or to any other system that can interface to the StorageGRID Webscale system through the S3 API; for example, another instance of the StorageGRID Webscale system.

**Archiving to tape through TSM middleware**

You can configure an Archive Node to target a Tivoli Storage Manager (TSM) server which provides a logical interface for storing and retrieving object data to random or sequential access storage devices, including tape libraries.

The Archive Node's ARC service acts as a client to the TSM server, using Tivoli Storage Manager as middleware for communicating with the archival storage system.

**Tivoli Storage Manager Management Classes**

Management classes defined by the TSM middleware outline how the TSM's backup and archive operations function, and can be used to specify rules for content that are applied by the TSM server. Such rules operate independently of the StorageGRID Webscale system's ILM policy, and must be consistent with the StorageGRID Webscale system's requirement that objects are stored permanently and are always available for retrieval by the Archive Node. After object data is sent to a TSM server by the Archive Node, the TSM lifecycle and retention rules are applied while the object data is stored to tape managed by the TSM server.

The TSM management class is used by the TSM server to apply rules for data location or retention after objects are sent to the TSM server by the Archive Node. For example, objects identified as database backups (temporary content that can be overwritten with newer data) could be treated differently than application data (fixed content that must be retained indefinitely).

**Managing connections to archival storage**

You can configure an Archive Node to connect to an external archival storage system through either the S3 API or TSM middleware.

Once the type of archival target is configured for an Archive Node, the target type cannot be changed.
Configuring connection settings for S3 API

There are a number of settings you must configure, before the Archive Node can communicate with an external archival storage system that connects to the StorageGRID Webscale system through the S3 API.

Before you begin

• You must be signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

• You need to create a bucket on the target archival storage system:
  ◦ The bucket must be dedicated to a single Archive Node. It cannot be used by other Archive Nodes or other applications.
  ◦ The bucket must have the appropriate region selected for your location.
  ◦ The bucket should be configured with versioning suspended.

• Object Segmentation must be enabled and the Maximum Segment Size must be less than or equal to 4.5 GiB (4,831,838,208 bytes). S3 API requests that exceed this value will fail if Simple Storage Service (S3) is used as the external archival storage system.

About this task

Until these settings are configured, the ARC service remains in a Major alarm state as it is unable to communicate with the external archival storage system.

Steps

1. Select Grid.

2. Select Archive Node > ARC > Target.

3. Click Configuration > Main.
4. Select *Cloud Tiering - Simple Storage Service (S3)* from the *Target Type* drop-down list.  
   **Note:** Configuration settings are unavailable until you select a Target Type.

5. Configure the cloud tiering (S3) account through which the Archive Node will connect to the target external S3 capable archival storage system.  
   Most of the fields on this page are self-explanatory. The following describes fields for which you might need guidance.
   
   • **Region:** Only available if Use AWS is selected. The region you select must match the bucket’s region.
   
   • **Endpoint and Use AWS:** For Amazon Web Services (AWS), select Use AWS. Endpoint is then automatically populated with an endpoint URL based on the Bucket Name and Region attributes. For example, `https://bucket.region.amazonaws.com`  
     For a non-AWS target, enter the URL of the system hosting the bucket, including the port number. For example, `https://system.com:1080`
   
   • **Endpoint Authentication:** Enabled by default. Clear to disable endpoint SSL certificate and hostname verification for the targeted external archival storage system. Only clear the checkbox if the network to the external archival storage system is trusted. If another instance of a StorageGRID Webscale system is the target archival storage device and the system is configured with publicly signed certificates, you do not need to clear the checkbox.
   
   • **Storage Class:** Select Standard, the default value, for regular storage, or Reduced Redundancy, which provides lower cost storage with less reliability for objects that can be easily recreated. If the target archival storage system is another instance of the StorageGRID Webscale system, Storage Class controls the target system’s dual-commit behavior.

6. Click **Apply Changes**.
   
   The specified configuration settings are validated and applied to your StorageGRID Webscale system. Once configured, the target cannot be changed.
Modifying connection settings for S3 API

After the Archive Node is configured to connect to an external archival storage system through the S3 API, you can modify some settings should the connection change.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

If you change the Cloud Tiering (S3) account, you must ensure that the user access credentials have read/write access to the bucket, including all objects that were previously ingested by the Archive Node to the bucket.

Steps

1. Select Grid.
2. Select Archive Node > ARC > Target.
3. Click Configuration > Main.
4. Modify account information, as necessary.
   
   If you change the storage class, new object data is stored with the new storage class. Existing object continue to be stored under the storage class set when ingested.
   
   **Note:** Bucket Name, Region, and Endpoint, use AWS values and cannot be changed.
5. Click Apply Changes.
Modifying the Cloud Tiering Service state

You can control the Archive Node's ability read and write to the targeted external archival storage system that connects through the S3 API by changing the state of the Cloud Tiering Service.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- The Archive Node must be configured.

About this task

You can effectively take the Archive Node offline by changing the Cloud Tiering Service State to Read-Write Disabled.

Steps

1. Select Grid.
2. Select Archive Node > ARC.
3. Click Configuration > Main.
4. Select a Cloud Tiering Service State.
5. Click Apply Changes.

Configuring connections to Tivoli Storage Manager middleware

Before the Archive Node can communicate with Tivoli Storage Manager (TSM) middleware, you must configure a number of settings.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

Until these settings are configured, the ARC service remains in a Major alarm state as it is unable to communicate with the Tivoli Storage Manager.
Steps

1. Select Grid.

2. Select Archive Node > ARC > Target.

3. Click Configuration > Main.

4. Select Tivoli Storage Manager (TSM) from the Target Type drop-down list.

5. By default, the Tivoli Storage Manager State is set to Online, which means that the Archive Node is able to retrieve object data from the TSM middleware server. Select Offline to prevent retrievals from the TSM middleware server.

6. Complete the following information:

   - Server IP or Hostname: Specify the IP address or Fully Qualified Domain Name (FQDN) of the TSM middleware server used by the ARC service. The default IP address is 127.0.0.1.
   - Server Port: Specify the port number on the TSM middleware server that the ARC service will connect to. The default is 1500.
   - Node Name: Specify the name of the Archive Node. You must enter the name (arc-user) that you registered on the TSM middleware server.
   - User Name: Specify the user name the ARC service uses to log in to the TSM server. Enter the default user name (arc-user) or the administrative user you specified for the Archive Node.
   - Password: Specify the password used by the ARC service to log in to the TSM server. Re-enter the password when you are prompted to confirm it.
   - Management Class: Specify the default management class to use if a management class is not specified when the object is being save to the StorageGRID Webscale system, or the specified management class is not defined on the TSM middleware server.

      - If the specified management class does not exist on the TSM server, the object cannot be saved to the TSM archive. The object remains in the queue on the StorageGRID Webscale...
system and the CMS > Content > Overview > Objects with ILM Evaluation Pending count is incremented.

- Number of Sessions: Specify the number of tape drives on the TSM middleware server that are dedicated to the Archive Node. The Archive Node concurrently creates a maximum of one session per mount point plus a small number of additional sessions (less than five). You need to change this value to be the same as the value set for MAXNUMMP (maximum number of mount points) when the Archive Node was registered or updated. (In the register command, the default value of MAXNUMMP used is 1, if no value is set.) You must also change the value of MAXSESSIONS for the TSM server to a number that is at least as large as the Number of Sessions set for the ARC service. The default value of MAXSESSIONS on the TSM server is 25.

- Maximum Retrieve Sessions: Specify the maximum number of sessions that the ARC service can open to the TSM middleware server for retrieve operations. In most cases, the appropriate value is Number of Sessions minus Maximum Store Sessions. If you need to share one tape drive for storage and retrieval, specify a value equal to the Number of Sessions.

- Maximum Store Sessions: Specify the maximum number of concurrent sessions that the ARC service can open to the TSM middleware server for archive operations. This value should be set to one except when the targeted archival storage system is full and only retrievals can be performed. Set this value to zero to use all sessions for retrievals.

7. Click Apply Changes.

Managing Archive Nodes

You can configure an Archive Node to optimize Tivoli Storage Manager performance, take an Archive Node offline when a TSM server is nearing capacity or unavailable, and configure replication and retrieve settings. You can also set custom alarms for the Archive Node.

Choices

- Optimizing Archive Node's TSM middleware sessions on page 138
- Managing an Archive Node when TSM server reaches capacity on page 139
- Configuring Archive Node replication on page 141
- Configuring retrieve settings on page 142
- Configuring the archive store on page 143
- Setting custom alarms for the Archive Node on page 144

Optimizing Archive Node's TSM middleware sessions

Typically, the number of concurrent sessions that the Archive Node has open to the TSM middleware server is set to the number of tape drives the TSM server has dedicated to the Archive Node. One tape drive is allocated for storage while the rest are allocated for retrieval.

However, in situations where a Storage Node is being rebuilt from Archive Node copies or the Archive Node is operating in Read-only mode, you can optimize TSM server performance by setting the maximum number of retrieve sessions to be the same as number of concurrent sessions. The result is that all drives can be used concurrently for retrieval, and, at most, one of these drives can also be used for storage if applicable.
Optimizing Archive Node for TSM middleware sessions

You can optimize the performance of an Archive Node that connects to an external archival storage system through the S3 API by configuring the Archive Node's sessions.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Grid.
2. Select Archive Node > ARC > Target.
3. Click Configuration > Main.
4. Change Maximum Retrieve Sessions to be the same as Number of Sessions.

5. Click Apply Changes.

Managing an Archive Node when TSM server reaches capacity

The TSM server has no way to notify the Archive Node when either the TSM database or the archival media storage managed by the TSM server is nearing capacity. The Archive Node continues to accept object data for transfer to the TSM server after the TSM server stops accepting new content. This content cannot be written to media managed by the TSM server. An alarm is triggered if this happens. This situation can be avoided through proactive monitoring of the TSM server.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task
To prevent the ARC service from sending further content to the TSM server, you can take the Archive Node offline by taking its ARC > Store component offline. This procedure can also be useful in preventing alarms when the TSM server is unavailable for maintenance.

Steps
1. Select Grid.
2. Select Archive Node > ARC > Store.
3. Click Configuration > Main.
4. Change Archive Store State to Offline.
5. Select Archive Store Disabled on Startup.
6. Click Apply Changes.

Setting Archive Node to read-only if TSM middleware reaches capacity
If the targeted TSM middleware server reaches capacity, the Archive Node can be optimized to only perform retrievals.

Before you begin
• You must be signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps
1. Select Grid.
2. Select Archive Node > ARC > Target.
3. Click Configuration > Main.
4. Change Maximum Retrieve Sessions to be the same as the number of concurrent sessions listed in Number of Sessions.
5. Change Maximum Store Sessions to 0.
Note: Changing Maximum Store Sessions to 0 is not necessary if the Archive Node is Read-only. Store sessions will not be created.

6. Click Apply Changes.

Configuring Archive Node replication

You can configure the replication settings for an Archive Node and disable inbound and outbound replication, or reset the failure counts being tracked for the associated alarms.

Before you begin

• You must be signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Grid.

2. Select Archive Node > ARC > Replication.

3. Click Configuration > Main.

4. Modify the following settings, as necessary:

   • Reset Inbound Replication Failure Count: Select to reset the counter for inbound replication failures. This can be used to clear the RIRF (Inbound Replications – Failed) alarm.

   • Reset Outbound Replication Failure Count: Select to reset the counter for outbound replication failures. This can be used to clear the RORF (Outbound Replications – Failed) alarm.

   • Disable Inbound Replication: Select to disable inbound replication as part of a maintenance or testing procedure. Leave cleared during normal operation. When inbound replication is disabled, object data can be retrieved from the ARC service for replication to other locations in the StorageGRID Webscale system, but objects cannot be replicated to this ARC service from other system locations. The ARC service is read-only.
• Disable Outbound Replication: Select the checkbox to disable outbound replication (including content requests for HTTP retrievals) as part of a maintenance or testing procedure. Leave unchecked during normal operation. When outbound replication is disabled, object data can be copied to this ARC service to satisfy ILM rules, but object data cannot be retrieved from the ARC service to be copied to other locations in the StorageGRID Webscale system. The ARC service is write-only.

5. Click Apply Changes.

Configuring retrieve settings

You can configure the retrieve settings for an Archive Node to set the state to Online or Offline, or reset the failure counts being tracked for the associated alarms.

Before you begin

• You must be signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Grid.

2. Select Archive Node > ARC > Retrieve.

3. Click Configuration > Main.

4. Modify the following settings, as necessary:

• Archive Retrieve State: Set the component state to either:
  ◦ Online: The grid node is available to retrieve object data from the archival media device.
  ◦ Offline: The grid node is not available to retrieve object data.

• Reset Request Failures Count: Select the checkbox to reset the counter for request failures. This can be used to clear the ARRF (Request Failures) alarm.

• Reset Verification Failure Count: Select the checkbox to reset the counter for verification failures on retrieved object data. This can be used to clear the ARRV (Verification Failures) alarm.

5. Click Apply Changes.
Configuring the archive store

You can configure store setting for an Archive Node.

About this task

Store settings differ based on the configured target type for the Archive Node.

Related tasks

* Managing an Archive Node when TSM server reaches capacity on page 139

Configuring the archive store for TSM middleware connection

If your Archive Node connects to a TSM middleware server, you can configure an Archive Node’s archive store state to Online or Offline. You can also disable the archive store when the Archive Node first starts up, or reset the failure count being tracked for the associated alarm.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Grid.
2. Select Archive Node > ARC > Store.
3. Click Configuration > Main.

4. Modify the following settings, as necessary:
   - Archive Store State: Set the component state to either:
     - Online: The Archive Node is available to process object data for storage to the archival storage system.
     - Offline: The Archive Node is not available to process object data for storage to the archival storage system.
   - Archive Store Disabled on Startup: When selected, the Archive Store component remains in the Read-only state when restarted. Used to persistently disable storage to the targeted the archival storage system. Useful when the targeted the archival storage system is unable to accept content.
- Reset Store Failure Count: Reset the counter for store failures. This can be used to clear the ARVF (Store Failures) alarm.

5. Click **Apply Changes**.

**Configuring store settings for S3 API connection**

If your Archive Node connects to an archival storage system through the S3 API, you can reset the Store Failures count, which can be used to clear the ARVF (Store Failures) alarm.

**Before you begin**
- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Grid**.
2. Select **Archive Node > ARC > Store**.
3. Click **Configuration > Main**.
4. Select **Reset Store Failure Count**.
5. Click **Apply Changes**.

The Store Failures attribute resets to zero.

**Setting custom alarms for the Archive Node**

You should establish custom alarms for the ARQL and ARRL attributes that are used to monitor the speed and efficiency of object data retrieval from the archival storage system by the Archive Node.

- **ARQL**: Average Queue Length. The average time, in microseconds, that object data is queued for retrieval from the archival storage system.
- **ARRL**: Average Request Latency. The average time, in microseconds, needed by the Archive Node to retrieve object data from the archival storage system.

The acceptable values for these attributes depend on how the archival storage system is configured and used. (Go to **ARC > Retrieve > Overview > Main**.) The values set for request timeouts and the number of sessions made available for retrieve requests are particularly influential.

After integration is complete, monitor the Archive Node's object data retrievals to establish values for normal retrieval times and queue lengths. Then, create custom alarms for ARQL and ARRL that will trigger if an abnormal operating condition arises.
Related tasks

*Creating custom service or component alarms* on page 40
What an Admin Node is

You perform most day-to-day activities using the Grid Management Interface, which resides on Admin Nodes. Admin Nodes provide services for the web interface, system configuration, and audit logs. Each site in a StorageGRID Webscale deployment can have one or more Admin Nodes.

Admin Nodes use the AMS service, the CMN service, and the NMS service.

What the AMS service is

The Audit Management System (AMS) service tracks system activity and events.

What the CMN service is

The Configuration Management Node (CMN) service manages system-wide configurations of connectivity and protocol features needed by all services. In addition, the CMN service is used to run and monitor grid tasks. One Admin Node per StorageGRID Webscale hosts the CMN service and is known as the primary Admin Node. No other Admin Node hosts the CMN service. There is only one per StorageGRID Webscale deployment.

What the NMS service is

The Network Management System (NMS) service powers the monitoring, reporting, and configuration options that are displayed through the StorageGRID Webscale system's browser-based interface.

Related concepts

Monitoring grid tasks on page 188

Related tasks

Verifying an ILM policy on page 88
Admin Node redundancy

A StorageGRID Webscale system can include multiple Admin Nodes. This provides you with the redundancy of multiple IP addresses from which you can sign in to StorageGRID Webscale system and perform various monitoring and configuration procedures.

Having multiple Admin Nodes provides you with the capability to continuously monitor and configure your StorageGRID Webscale system in the event that an Admin Node fails. If an Admin Node becomes unavailable, web clients can reconnect to any other available Admin Node and continue to view and configure the system. Meanwhile, attribute processing continues, alarms are still triggered, and related notifications sent. However, multiple Admin Nodes do not provide failover protection except for notifications and AutoSupport messages. Alarm acknowledgments made from one Admin Node are not copied to other Admin Nodes.

Related concepts

Alarm acknowledgments on page 147

Alarm acknowledgments

Alarm acknowledgments made from one Admin Node are not copied to any other Admin Node. Because acknowledgments are not copied to other Admin Nodes, it is possible that the Grid Topology tree will not look the same for each Admin Node.

This difference can be useful when connecting web clients. Web clients can have different views of the StorageGRID Webscale system based on the administrator needs.
Note that notifications are sent from the Admin Node where the acknowledgment occurs.

Email notifications and AutoSupport messages

In a multi-site StorageGRID Webscale system, one Admin Node is configured as the preferred sender of notifications and AutoSupport messages. This preferred sender can be any Admin Node. All other Admin Nodes become “standby” senders.

Under normal system operations, only the preferred sender sends notifications and AutoSupport messages. The standby sender monitors the preferred sender and if it detects a problem, the standby sender switches to online status and assumes the task of sending notifications and AutoSupport messages.

Preferred and standby senders

There are two scenarios in which both the preferred sender and the standby sender can send notifications and AutoSupport messages:

- It is possible that while the StorageGRID Webscale system is running in this “switch-over” scenario, where the standby sender assumes the task of sending notifications and AutoSupport messages, the preferred sender will maintain the ability to send notifications and AutoSupport messages. If this occurs, duplicate notifications and AutoSupport messages are sent: one from the preferred sender and one from the standby sender. When the Admin Node configured as the standby sender no longer detects errors on the preferred sender, it switches to “standby” status and stops sending notifications and AutoSupport messages. Notifications and AutoSupport messages are once again sent only by the preferred sender.

- If the standby sender cannot detect the preferred sender, the standby sender switches to online and sends notifications and AutoSupport messages. In this scenario, the preferred sender and standby senders are “islanded” from each other. Each sender (Admin Node) can be operating and monitoring the system normally, but because the standby sender cannot detect the other Admin Node of the preferred sender, both the preferred sender and the standby sender send notifications and AutoSupport messages.

When sending a test email, all NMS services send a test email.

Related concepts

About alarms and email notifications on page 26
What AutoSupport is on page 49

Related tasks

Selecting a preferred sender on page 33
Changing the name of an Admin Node

You can change the display name that is shown for an Admin Node on various browser-based interface pages; however, this operation is not recommended. Any display name changes are lost when you run the provision command (for example, during grid expansion).

Related concepts

NMS entities on page 149

Related tasks

Selecting a preferred sender on page 33

NMS entities

NMS entities refer to elements of the Grid Topology tree that appear above the component level (the names of the StorageGRID Webscale deployment, locations, grid nodes, and services).

NMS entity settings determine the name that appears in the Grid Topology tree and elsewhere in the Grid Management Interface.

Attention: Never change these setting unless advised by technical support.

Names are allocated to each entity through Object IDs (OIDs) that are unique to each entity while being hierarchically organized. Each row in the NMS Entities table allocates a name to an entity OID. The combination of OID hierarchy and position in the table determines the sequence of appearance in the Grid Topology tree.
Managing networking

Because the topology of your StorageGRID Webscale system is that of a group of interconnected servers, over time as your system changes and grows you may be required to perform various updates to the system's networking.

You can change the configuration of the Grid, Client, or Admin networks, or you can add new Client and Admin networks. You can also update external NTP source IP addresses and DNS IP addresses at any time.

*Note:* To use the Grid network editor to modify or add a network for a grid node, see the *Maintenance Guide*. For more information about network topology, see the *Grid Primer*.

### Grid network

Required. The Grid network is the communication link between grid nodes. All hosts on the Grid network must be able to talk to all other hosts. This network is used for all internal StorageGRID Webscale system communications.

### Admin network

Optional. The Admin network allows for restricted access to the StorageGRID Webscale system for maintenance and administration.

### Client network

Optional. The Client network can communicate with any subnet reachable through the local gateway.

### Guidelines

- A StorageGRID Webscale grid node requires a dedicated network interface, IP address, subnet mask, and gateway for each network it is assigned to.
- A grid node is not permitted to have more than one interface on a network.
- A single gateway, per network, per grid node is supported, and it has to be on the same subnet as the node. You can implement more complex routing in the gateway, if required.
- On each node, each network maps to a specific network interface.

<table>
<thead>
<tr>
<th>Network</th>
<th>Interface name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grid</td>
<td>eth0</td>
</tr>
<tr>
<td>Admin (optional)</td>
<td>eth1</td>
</tr>
<tr>
<td>Client (optional)</td>
<td>eth2</td>
</tr>
</tbody>
</table>

- If the node is connected to a StorageGRID Webscale appliance, specific ports are used for each network
  - Grid network or eth0: hic2 and hic4 (10-GbE network ports)
  - Admin network or eth1: mtc1 (the leftmost 1-GbE port)
  - Client network or eth2: hic1 and hic3 (10-GbE network ports)
- The default route is generated automatically, per node. If eth2 is enabled, then 0.0.0.0/0 uses the Client network on eth2. If eth2 is not enabled, then 0.0.0.0/0 uses the Grid network on eth0.
- The Client network does not become operational until the grid node has joined the grid
- The Admin network can be configured during VM deployment to allow access to the installation UI before the grid is fully installed.

**Related information**

- StorageGRID Webscale 10.4 Maintenance Guide for VMware Deployments
- StorageGRID Webscale 10.4 Maintenance Guide for OpenStack Deployments
- StorageGRID Webscale 10.4 Maintenance Guide for Red Hat Enterprise Linux Deployments
- StorageGRID Webscale 10.4 Grid Primer
- StorageGRID Webscale 10.4 Appliance Installation and Maintenance Guide

**Viewing IP addresses**

You can view the IP address for each grid node that makes up your StorageGRID Webscale system. You can then use this IP address to log into the grid node at the command line and perform various maintenance procedures.

**Before you begin**

You must be signed in to the Grid Management Interface using a supported browser.

**About this task**

For information on changing IP addresses, see the *Maintenance Guide*.

**Steps**

1. Select **Grid**.
2. Select **SSM > Resources**.
3. From the Grid Options menu, click **Overview**.
   - IP addresses are listed in the Network Addresses table.

**Example**

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>10.96.30.39</td>
</tr>
<tr>
<td>eth0</td>
<td>fe80:259:56ff:fe00:5227</td>
</tr>
</tbody>
</table>

For VM-based deployments, the IP address assigned to eth0 is always the grid node’s grid network IP address. For StorageGRID Webscale appliance-based deployments, the IP address assigned to hic2 and hic4 is always the grid node’s grid network IP address.

The Network Addresses table always displays link-local IPv6 addresses beginning with fe80::, which are automatically assigned by Linux.

**Related information**

- StorageGRID Webscale 10.4 Maintenance Guide for VMware Deployments
- StorageGRID Webscale 10.4 Maintenance Guide for OpenStack Deployments
- StorageGRID Webscale 10.4 Maintenance Guide for Red Hat Enterprise Linux Deployments
Configuring SNMP monitoring

A Simple Network Management Protocol (SNMP) agent is installed with each grid node during the installation process. SNMP is used to monitor system status. StorageGRID Webscale’s SNMP agent sends StorageGRID Webscale system status through object identifier (OID) data values to a third party monitoring server.

The StorageGRID Webscale system provides a custom management information base (MIB) file that can be installed on the monitor server to translate OID data into a readable form displayed by the monitor.

The StorageGRID Webscale system supports version v2c of the SNMP protocol (SNMPv2c).

For information about how to install and configure a third-party monitor and have it receive SNMP status from the StorageGRID Webscale system, refer to documentation specific to the SNMP monitor employed.

Management Information Base file

A Management Information Base (MIB) file is needed by the monitor to translate SNMP data from the StorageGRID Webscale system into readable text.

Copy the StorageGRID Webscale MIB file (BYCAST-STORAGWRID-MIB.mib) to the monitor server.

The StorageGRID Webscale MIB file is available on the StorageGRID Webscale Admin node at /usr/share/snmp/mibs/BYCAST-STORAGEGRID-MIB.mib.

Detailed registry

The OID is displayed on third-party monitor servers.

This OID reports the overall system status of the StorageGRID Webscale system.

<table>
<thead>
<tr>
<th>Element</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>1.3.6.1.4.1.28669.1.0.1.1.1</td>
</tr>
<tr>
<td>Hierarchy</td>
<td>iso.org.dod.internet.mgmt.private.enterprises.bycast.version1.common.nmsmi.system.status</td>
</tr>
<tr>
<td>Values</td>
<td>One of the following values is displayed:</td>
</tr>
<tr>
<td></td>
<td>1 = unknown</td>
</tr>
<tr>
<td></td>
<td>11 = adminDown</td>
</tr>
<tr>
<td></td>
<td>21 = normal</td>
</tr>
<tr>
<td></td>
<td>31 = notice</td>
</tr>
<tr>
<td></td>
<td>41 = minor</td>
</tr>
<tr>
<td></td>
<td>51 = major</td>
</tr>
<tr>
<td></td>
<td>61 = critical</td>
</tr>
<tr>
<td></td>
<td>The MIB contains this enumeration mapping. If the monitor uses SNMP GET, the textual value will appear instead of the numerical value.</td>
</tr>
</tbody>
</table>

This OID is the system label.

<table>
<thead>
<tr>
<th>Element</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>1.3.6.1.4.1.28669.1.0.1.1.2</td>
</tr>
</tbody>
</table>
Link costs

Link costs refers to the relative costs of communicating between data center sites. Link costs are used to determine which grid nodes should provide a requested service.

For example, link cost information is used to determine which LDR services are used to retrieve objects. All else being equal, the service with the lowest link cost is preferred.

In the example shown below, if a client application at data center site two (DC2) retrieves an object that is stored both at data center site one (DC1) and at data center site three, the LDR service at DC1 is responsible for sending the object because the link cost from DC1 to DC2 is 0, which is lower than the link cost from the DC3 site to the DC2 site (25).

The table shows example link costs.

<table>
<thead>
<tr>
<th>Link</th>
<th>Link cost</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Between physical data center sites</td>
<td>25 (default)</td>
<td>Usually a high-speed WAN link exists between sites.</td>
</tr>
<tr>
<td>Between logical data center sites</td>
<td>0</td>
<td>Logical data centers at the same physical site connected by a LAN.</td>
</tr>
</tbody>
</table>

Updating link costs

You can update the link costs between data center sites.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
Steps

1. Select Configuration > Link Cost.

2. Select a site under Link Source and enter a cost value between 0 and 100 under Link Destination.

   You cannot change the link cost if the source is the same as the destination.

   To cancel changes, click Revert.

3. Click Apply Changes.

Changing network transfer encryption

The StorageGRID Webscale system uses Transport Layer Security (TLS) to protect internal control traffic between grid nodes. The Network Transfer Encryption option sets the algorithm used by TLS to encrypt control traffic between grid nodes. This setting does not affect data encryption.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

By default, network transfer encryption uses the AES256-SHA algorithm. Control traffic can also be encrypted using the AES128-SHA algorithm.
Steps

1. Select Configuration > Grid Options.
2. From the Grid Options menu, select Configuration.
3. Change Network Transfer Encryption to AES256-SHA or AES128-SHA.

4. Click Apply Changes.

Configuring passwordless SSH access

The primary Admin Node acts as an SSH access point for other grid nodes. This means that after you log in to the command shell of the primary Admin Node, you can access any other grid node through SSH without entering the grid node’s password.

About this task

You are only prompted to enter the SSH Access Password. Optionally, you can enable passwordless access to grid nodes by starting ssh-agent. In this case, you are only prompted for the SSH Access Password once.

To connect to a grid node through SSH, you can:

- From any grid node, use the remote server password.
- From the primary Admin Node, use the SSH private key password (SSH Access Password listed in the Passwords.txt file).
- From the primary Admin Node, without entering any password except the SSH Access Password once.

To enable passwordless SSH access to remote grid nodes, you need:

- The password for the SSH private key (SSH Access Password in the Passwords.txt file).
  By default the SSH access point is installed with a password.
• The SSH private key to be on the primary Admin Node.
  By default, the private key is located on the primary Admin Node. However, it might have been
  removed to prevent the Admin Node from acting as an SSH access point.

• The private key added to the SSH agent.
  This must be done each time you log in to the primary Admin Node at the command line.

**Steps**

1. From the service laptop, log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.
   
   Once logged in as root, the prompt changes from `$` to `#`.

2. Add the SSH private key to the ssh agent to allow the primary Admin Node passwordless access
   to the StorageGRID Webscale system’s other grid nodes. Enter: `ssh-add`
   
   You need to add the ssh private key to the ssh agent each time you log in at the command line.

3. When prompted, enter the SSH Access Password listed in the `Passwords.txt` file or the one
   created in “Adding or changing the SSH private key password” on page 186.
   
   You can now access any grid node from the primary Admin Node through ssh without entering
   additional passwords.

4. When you no longer require passwordless access to other servers, remove the private key from the
   ssh agent. Enter: `ssh-add -D`

5. Log out of the primary Admin Node. Enter: `exit`

**Configuring certificates**

You can customize the certificates used by the StorageGRID Webscale system.

The StorageGRID Webscale system uses security certificates for two distinct purposes:

• Management Interface Server Certificates: Used to secure access to the Management Interface,
  which end-users access through their web browser, or the Management API.

• Storage API Server Certificates: Used to secure access to the Storage Nodes and API Gateway
  Nodes, which API client applications use to upload and download object data.

You can use the default certificates created during installation, or you can replace either, or both, of
these default types of certificates with your own custom certificates.

**Configuring custom server certificates for the Grid Management Interface**

You can replace the default Grid Management Interface server certificates with custom certificates
that allows users to access the interface without encountering security warnings.

**About this task**

You need to complete configuration on the server, and depending on the root Certificate Authority
(CA) you are using, users may also need to install a client certificate in the web browser they will use
to access the Grid Management Interface.
Steps
1. Select Configuration > Server Certificates.
2. In the Management Interface Server Certificate section, click Install Custom Certificate.
3. Upload the required server certificate files:
   - CA Bundle: A single file containing the certificates from each intermediate issuing Certificate Authority (CA). The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.
4. Click Save.
   The custom server certificates are used for all subsequent new client connections.
5. Refresh the page to ensure the web browser is updated.

Restoring the default server certificates for the Grid Management Interface
You can revert to using the default server certificates for the Grid Management Interface.

Steps
1. Select Configuration > Server Certificates.
2. In the Manage Interface Server Certificate section, click Use Default Certificates.
3. Click OK in the confirmation dialog box.
   When you restore the default Management Interface server certificates, the custom server certificate files you configured are deleted and cannot be recovered from the system. The default server certificates are used for all subsequent new client connections.
4. Refresh the page to ensure the web browser is updated.

Configuring custom server certificates for storage API endpoints
You can replace the default object storage API service endpoint server certificates with a single custom server certificate that is specific to your organization.

About this task
API service endpoints on Storage Nodes are secured and identified by X.509 server certificates. By default, every Storage Node is issued a certificate signed by the grid CA. These CA signed certificates can be replaced by a single common custom server certificate and corresponding private key.

You need to complete configuration on the server, and depending on the root Certificate Authority (CA) you are using, users may also need to install a client certificate in the API client they will use to access the system.

Steps
1. Select Configuration > Server Certificates.
2. In the Object Storage API Service Endpoints Server Certificate section, click Install Custom Certificate.
3. Upload the required server certificate files:
• **Server Certificate**: The custom server certificate file (.crt).

• **Server Certificate Private Key**: The custom server certificate private key file (.key).

• **CA Bundle**: A single file containing the certificates from each intermediate issuing Certificate Authority (CA). The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.

4. Click **Save**.

   The custom server certificates are used for all subsequent new API client connections.

5. Refresh the page to ensure the web browser is updated.

**Restoring the default server certificates for storage API endpoints**

You can revert to using the default server certificates for the storage API endpoints.

**Steps**

1. Select **Configuration > Server Certificates**.

2. In the **Object Storage API Service Endpoints Server Certificate** section, click **Use Default Certificates**.

3. Click **OK** in the confirmation dialog box.

   When you restore the default object storage API service endpoints server certificates, the custom server certificate files you configured are deleted and cannot be recovered from the system. The default server certificates are used for all subsequent new API client connections.

4. Refresh the page to ensure the web browser is updated.

**Copying the StorageGRID Webscale system's CA certificate**

You can copy the StorageGRID Webscale system's certificate authority (CA) certificate from the StorageGRID Webscale system for client applications that require server verification. If a custom server certificate has been configured, then client applications should verify the server using the root CA certificate that issues the custom server certificate, rather than copy the CA certificate from the StorageGRID Webscale system.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Configuration > Grid Options**.

2. From the Grid Options menu, click **Overview**.

3. Under **API Server Certificates**, expand **CA Certificate**.

4. Select the CA certificate.

   Include the “-----BEGIN CERTIFICATE-----” and the “-----END CERTIFICATE-----” in your selection.
5. Right-click the selected certificate, and then select **Copy**.

6. Refresh the page to ensure the web browser is updated.
Configuring audit client access

The Admin Node, through the Audit Management System (AMS) service, logs all audited system events to a log file available through the audit share, which is added to each Admin Node at installation. For easy access to audit logs, you can configure client access to audit shares for both CIFS and NFS.

The StorageGRID Webscale system uses positive acknowledgment to prevent loss of audit messages before they are written to the log file or audit feed. A message remains queued at a service until the AMS service or an intermediate audit relay service has acknowledged control of it.

For information about audit messages, see the Audit Message Reference.

Related concepts

What an Admin Node is on page 146

Related information

StorageGRID Webscale 10.4 Audit Message Reference

Configuring audit clients for CIFS

The procedure used to configure an audit client depends on the authentication method: Windows Workgroup or Windows Active Directory (AD). When added, the audit share is automatically enabled as a read-only share.

Configuring audit clients for Workgroup

Perform this procedure for each Admin Node in a StorageGRID Webscale deployment from which you want to retrieve audit messages.

Before you begin

• You must have the Passwords.txt file with the root/admin account password (available in the SAID package).

• You must have the Configuration.txt file (available in the SAID package).

Steps

1. From the service laptop, log in to the primary Admin Node:
   a. Enter the following command: ssh admin@primary_Admin_Node_IP
   b. Enter the password listed in the Passwords.txt file.
   c. Enter the following command to switch to root: su -
   d. Enter the password listed in the Passwords.txt file.
      Once logged in as root, the prompt changes from $ to #.

2. Confirm that all services have a state of Running or Verified: storagegrid-status
   If all services are not Running or Verified, resolve issues before continuing.

3. Return to the command line, press Ctrl+C.
4. Start the CIFS configuration utility: `config_cifs.rb`

<table>
<thead>
<tr>
<th>Shares</th>
<th>Authentication</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>add-audit-share</td>
<td>set-authentication</td>
<td>validate-config</td>
</tr>
<tr>
<td>enable-disable-share</td>
<td>set-netbios-name</td>
<td>help</td>
</tr>
<tr>
<td>add-user-to-share</td>
<td>join-domain</td>
<td>exit</td>
</tr>
<tr>
<td>remove-user-from-share</td>
<td>add-password-server</td>
<td></td>
</tr>
<tr>
<td>modify-group</td>
<td>add-wins-server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>remove-wins-server</td>
<td></td>
</tr>
</tbody>
</table>

5. Set the authentication for the Windows Workgroup:
   If authentication has already been set, an advisory message appears. If authentication has already
   been set, go to step 6.
   
   a. Enter: `set-authentication`
   
   b. When prompted for Windows Workgroup or Active Directory installation, enter: `workgroup`
   
   c. When prompted, enter a name of the Workgroup:
      
      `workgroup_name`
   
   d. When prompted, create a meaningful NetBIOS name:
      
      `workgroup_name`
      
      or
      
      Press Enter to use the Admin Node’s hostname as the NetBIOS name.
      
      The script restarts the Samba server and changes are applied. This should take less than one
      minute. After setting authentication, add an audit client.
   
   e. When prompted, press Enter.
      
      The CIFS configuration utility is displayed.

6. Add an audit client:
   
   a. Enter: `add-audit-share`
      
      Note: The share is automatically added as read-only.
   
   b. When prompted, add a user or group: `user`
   
   c. When prompted, enter the audit user name: `audit_user_name`
   
   d. When prompted, enter a password for the audit user: `password`
   
   e. When prompted, re-enter the same password to confirm it: `password`
   
   f. When prompted, press Enter.
      
      The CIFS configuration utility is displayed.
      
      Note: There is no need to enter a directory. The audit directory name is predefined.

7. If more than one user or group is permitted to access the audit share, add the additional users:
   
   a. Enter: `add-user-to-share`
      
      A numbered list of enabled shares is displayed.
   
   b. When prompted, enter the number of the audit-export share: `share_number`
c. When prompted, add a user or group:
   user
   or
   group

d. When prompted, enter the name of the audit user or group: audit_user or audit_group

e. When prompted, press Enter.
   The CIFS configuration utility is displayed.

f. Repeat step 7 for each additional user or group that has access to the audit share.

8. Optionally, verify your configuration: validate-config
   The services are checked and displayed. You can safely ignore the following messages:

   Can't find include file /etc/samba/includes/cifs-interfaces.inc
   Can't find include file /etc/samba/includes/cifs-filesystem.inc
   Can't find include file /etc/samba/includes/cifs-custom-config.inc
   Can't find include file /etc/samba/includes/cifs-shares.inc
   rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)

   a. When prompted, press Enter.
      The audit client configuration is displayed.

   b. When prompted, press Enter.
      The CIFS configuration utility is displayed.

9. Close the CIFS configuration utility: exit

10. If the StorageGRID Webscale deployment is a single site, go to step 11.
   or
   Optionally, if the StorageGRID Webscale deployment includes Admin Nodes at other sites, enable these audit share as required:

   a. Remotely log in to a site’s Admin Node:
      i. Enter the following command: ssh admin@grid_node_IP
      ii. Enter the password listed in the Passwords.txt file.
      iii. Enter the following command to switch to root: su -
      iv. Enter the password listed in the Passwords.txt file.

   b. Repeat steps 4 through 9 to configure the audit share for each additional Admin Node.

   c. Close the remote secure shell login to the remote Admin Node: exit

11. Log out of the command shell: exit

### Configuring audit clients for Active Directory

**Before you begin**
- You must have the Passwords.txt file with the root/admin account password (available in the SAID package).
- You must have the CIFS Active Directory username and password.
• You must have the Configuration.txt file (available in the SAID package).

**About this task**
Perform this procedure for each Admin Node in a StorageGRID Webscale deployment from which you want to retrieve audit messages.

**Steps**
1. From the service laptop, log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   b. Enter the password listed in the Passwords.txt file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the Passwords.txt file.
      Once logged in as root, the prompt changes from `$` to `#`.
2. Confirm that all services have a state of Running or Verified: `storagegrid-status`
   If all services are not Running or Verified, resolve issues before continuing.
3. Return to the command line, press Ctrl-C.
4. Start the CIFS configuration utility: `config_cifs.rb`

<table>
<thead>
<tr>
<th>Shares</th>
<th>Authentication</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>add-audit-share</td>
<td>set-authentication</td>
<td>validate-config</td>
</tr>
<tr>
<td>enable-disable-share</td>
<td>set-netbios-name</td>
<td>help</td>
</tr>
<tr>
<td>add-user-to-share</td>
<td>join-domain</td>
<td>exit</td>
</tr>
<tr>
<td>remove-user-from-share</td>
<td>add-password-server</td>
<td></td>
</tr>
<tr>
<td>modify-group</td>
<td>remove-password-server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>add-wins-server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>remove-wins-server</td>
<td></td>
</tr>
</tbody>
</table>

5. Set the authentication for Active Directory: `set-authentication`
   In most deployments, you must set the authentication before adding the audit client. If authentication has already been set, an advisory message appears. If authentication has already been set, go to step 6.
   a. When prompted for Workgroup or Active Directory installation: `ad`
   b. When prompted, enter the name of the AD domain (short domain name).
   c. When prompted, enter the domain controller’s IP address or DNS hostname.
   d. When prompted, enter the full domain realm name.
      Use uppercase letters.
   e. When prompted to enable winbind support, type `y`.
      Winbind is used to resolve user and group information from AD servers.
   f. When prompted, enter the NetBIOS name.
   g. When prompted, press **Enter**.
      The CIFS configuration utility is displayed.
6. Join the domain:
   a. If not already started, start the CIFS configuration utility: `config_cifs.rb`
   b. Join the domain: `join-domain`
   c. You are prompted to test if the Admin Node is currently a valid member of the domain. If this Admin Node has not previously joined the domain, enter: `no`
   d. When prompted, provide the Administrator’s username: `administrator_username`
      where `administrator_username` is the CIFS Active Directory username, not the StorageGRID Webscale username.
   e. When prompted, provide the Administrator’s password: `administrator_password`
      were `administrator_password` is the CIFS Active Directory username, not the StorageGRID Webscale password.
   f. When prompted, press `Enter`.
      The CIFS configuration utility is displayed.

7. Verify that you have correctly joined the domain:
   a. Join the domain: `join-domain`
   b. When prompted to test if the server is currently a valid member of the domain, enter: `y`
      If you receive the message “Join is OK,” you have successfully joined the domain. If you do not get this response, try setting authentication and joining the domain again.
   c. When prompted, press `Enter`.
      The CIFS configuration utility is displayed.

8. Add an audit client: `add-audit-share`
   a. When prompted to add a user or group, enter: `user`
   b. When prompted to enter the audit user name, enter the audit user name.
   c. When prompted, press `Enter`.
      The CIFS configuration utility is displayed.

9. If more than one user or group is permitted to access the audit share, add additional users: `add-user-to-share`
   A numbered list of enabled shares is displayed.
   a. Enter the number of the audit-export share.
   b. When prompted to add a user or group, enter: `group`
      You are prompted for the audit group name.
   c. When prompted for the audit group name, enter the name of the audit user group.
   d. When prompted, press `Enter`.
      The CIFS configuration utility is displayed.
   e. Repeat step 9 for each additional user or group that has access to the audit share.

10. Optionally, verify your configuration: `validate-config`
    The services are checked and displayed. You can safely ignore the following messages:
    - Can't find include file `/etc/samba/includes/cifs-interfaces.inc`
• Can't find include file /etc/samba/includes/cifs-filesystem.inc
• Can't find include file /etc/samba/includes/cifs-interfaces.inc
• Can't find include file /etc/samba/includes/cifs-custom-config.inc
• Can't find include file /etc/samba/includes/cifs-shares.inc
• rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)

Warning: Do not combine the setting 'security=ads' with the 'password server' parameter. (by default Samba will discover the correct DC to contact automatically).

a. When prompted, press **Enter** to display the audit client configuration.

b. When prompted, press **Enter**.
   The CIFS configuration utility is displayed.

11. Close the CIFS configuration utility: **exit**

12. If the StorageGRID Webscale deployment is a single site, go to step **13**.
   or
   Optionally, if the StorageGRID Webscale deployment includes Admin Nodes at other sites, enable these audit shares as required:

   a. Remotely log in to a site’s Admin Node:
      i. Enter the following command: `ssh admin@grid_node_IP`
      ii. Enter the password listed in the **Passwords.txt** file.
      iii. Enter the following command to switch to root: `su -`
      iv. Enter the password listed in the **Passwords.txt** file.

   b. Repeat steps **4** through **11** to configure the audit shares for each Admin Node.

   c. Close the remote secure shell login to the Admin Node: **exit**

13. Log out of the command shell: **exit**

### Adding a user or group to a CIFS audit share

You can add a user or group to a CIFS audit share that is integrated with AD authentication.

**Before you begin**

- You must have the **Passwords.txt** file with the root/admin account password (available in the SAID package).
- You must have the **Configuration.txt** file (available in the SAID package).

**About this task**

The following procedure is for an audit share integrated with AD authentication.

**Steps**

1. From the service laptop, log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
b. Enter the password listed in the `Passwords.txt` file.

c. Enter the following command to switch to root: `su -`

d. Enter the password listed in the `Passwords.txt` file.

   Once logged in as root, the prompt changes from `$` to `#`.

2. Confirm that all services have a state of Running or Verified. Enter: `storagegrid-status`

   If all services are not Running or Verified, resolve issues before continuing.

3. Return to the command line, press `Ctrl+C`.

4. Start the CIFS configuration utility: `config_cifs.rb`

<table>
<thead>
<tr>
<th>Shares</th>
<th>Authentication</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>add-audit-share</td>
<td>set-authentication</td>
<td>validate-config</td>
</tr>
<tr>
<td>enable-disable-share</td>
<td>set-netbios-name</td>
<td>help</td>
</tr>
<tr>
<td>add-user-to-share</td>
<td>join-domain</td>
<td>exit</td>
</tr>
<tr>
<td>remove-user-from-share</td>
<td>add-password-server</td>
<td></td>
</tr>
<tr>
<td>modify-group</td>
<td>remove-password-server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>add-wins-server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>remove-wins-server</td>
<td></td>
</tr>
</tbody>
</table>

5. Start adding a user or group: `add-user-to-share`

   A numbered list of audit shares that have been configured is displayed.

6. When prompted, enter the number for the audit share (audit-export): `audit_share_number`

   You are asked if you would like to give a user or a group access to this audit share.

7. When prompted, add a user or group: `user` or `group`

8. When prompted for the user or group name for this AD audit share, enter the name.

   The user or group is added as read-only for the audit share both in the server’s operating system and in the CIFS service. The Samba configuration is reloaded to enable the user or group to access the audit client share.


   The CIFS configuration utility is displayed.

10. Repeat steps 5 to 8 for each user or group that has access to the audit share.

11. Optionally, verify your configuration: `validate-config`

   The services are checked and displayed. You can safely ignore the following messages:

   - Can't find include file `/etc/samba/includes/cifs-interfaces.inc`
   - Can't find include file `/etc/samba/includes/cifs-filesystem.inc`
   - Can't find include file `/etc/samba/includes/cifs-custom-config.inc`
   - Can't find include file `/etc/samba/includes/cifs-shares.inc`

   a. When prompted, press `Enter` to display the audit client configuration.

   b. When prompted, press `Enter`. 
12. Close the CIFS configuration utility: **exit**

13. Determine if you need to enable additional audit shares, as follows:
   - If the StorageGRID Webscale deployment is a single site, go to step 14.
   - If the StorageGRID Webscale deployment includes Admin Nodes at other sites, enable these audit shares as required:
     a. Remotely log in to a site’s Admin Node:
        i. Enter the following command: `ssh admin@grid_node_IP`
        ii. Enter the password listed in the `Passwords.txt` file.
        iii. Enter the following command to switch to root: `su -`
        iv. Enter the password listed in the `Passwords.txt` file.
     b. Repeat steps 4 through 12 to configure the audit shares for each Admin Node.
     c. Close the remote secure shell login to the remote Admin Node: **exit**

14. Log out of the command shell: **exit**

**Removing a user or group from a CIFS audit share**

You cannot remove the last user or group permitted to access the audit share.

**Before you begin**
- You must have the `Passwords.txt` file with the root account passwords (available in the SAID package).
- You must have the `Configuration.txt` file (available in the SAID package).

**Steps**

1. From the service laptop, log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.
      Once logged in as root, the prompt changes from `$` to `#`.

2. Start the CIFS configuration utility: **config_cifs.rb**

```
<table>
<thead>
<tr>
<th>Shares</th>
<th>Authentication</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>add-audit-share</td>
<td>set-authentication</td>
<td>validate-config</td>
</tr>
<tr>
<td>enable-disable-share</td>
<td>set-netbios-name</td>
<td>help</td>
</tr>
<tr>
<td>add-user-to-share</td>
<td>join-domain</td>
<td>exit</td>
</tr>
<tr>
<td>remove-user-from-share</td>
<td>add-password-server</td>
<td></td>
</tr>
<tr>
<td>modify-group</td>
<td>remove-password-server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>add-wins-server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>remove-wins-server</td>
<td></td>
</tr>
</tbody>
</table>
```
3. Start removing a user or group: `remove-user-from-share`
   
   A numbered list of available audit shares for the Admin Node is displayed. The audit share is labeled audit-export.

4. Enter the number of the audit share: `audit_share_number`

5. When prompted to remove a user or a group:
   
   `user`
   
   or `group`

   A numbered list of users or groups for the audit share is displayed.

6. Enter the number corresponding to the user or group you want to remove: `number`
   
   The audit share is updated, and the user or group is no longer permitted access to the audit share. For example:

   ```
   Enabled shares
   1. audit-export
   Select the share to change: 1
   Remove user or group? [User/group]: User
   Valid users for this share
   1. audituser
   2. newaudituser
   Select the user to remove: 1
   Removed user "audituser" from share "audit-export".
   Press return to continue.
   ```

7. Close the CIFS configuration utility: `exit`

8. If the StorageGRID Webscale deployment includes Admin Nodes at other sites, disable the audit share at each site as required.

9. Log out of each command shell when configuration is complete: `exit`

**Changing a CIFS audit share user or group name**

**Steps**

1. Add a new user or group with the updated name to the audit share.

2. Delete the old user or group name.

**Related tasks**

*Adding a user or group to a CIFS audit share* on page 165

*Removing a user or group from a CIFS audit share* on page 167

**Verifying CIFS audit integration**

The audit share is read-only. Log files are intended to be read by computer applications and verification does not include opening a file. It is considered sufficient verification that the audit log files appear in a Windows Explorer window. Following connection verification, close all windows.
Configuring the audit client for NFS

The audit share is automatically enabled as a read-only share.

Before you begin

- You must have the `Passwords.txt` file with the root/admin password (available in the SAID package).
- You must have the `Configuration.txt` file (available in the SAID package).
- The audit client must be using NFS Version 3 (NFSv3).

About this task

Perform this procedure for each Admin Node in a StorageGRID Webscale deployment from which you want to retrieve audit messages.

Steps

1. From the service laptop, log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.
      Once logged in as root, the prompt changes from `$` to `#`.

2. Confirm that all services have a state of Running or Verified. Enter: `storagegrid-status`
   If any services are not listed as Running or Verified, resolve issues before continuing.

3. Return to the command line, press `Ctrl+C`.

4. Start the NFS configuration utility. Enter: `config_nfs.rb`

<table>
<thead>
<tr>
<th>Shares</th>
<th>Clients</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>add-audit-share</td>
<td>add-ip-to-share</td>
<td>validate-config</td>
</tr>
<tr>
<td>enable-disable-share</td>
<td>remove-ip-from-share</td>
<td>refresh-config</td>
</tr>
<tr>
<td></td>
<td></td>
<td>help</td>
</tr>
<tr>
<td></td>
<td></td>
<td>exit</td>
</tr>
</tbody>
</table>

5. Add the audit client: `add-audit-share`
   a. When prompted, enter the audit client’s IP address or IP address range for the audit share: `client_IP_address`
      IP address ranges must be expressed using a subnet mask in CIDR notation (that is, in a form such as 192.168.110.0/24).
   b. When prompted, press Enter.

6. If more than one audit client is permitted to access the audit share, add the IP address of the additional user: `add-ip-to-share`
a. Enter the number of the audit share: `audit_share_number`

b. When prompted, enter the audit client’s IP address or IP Address range for the audit share:
   `client_IP_address`
   IP address ranges must be expressed using a subnet mask in CIDR notation (that is, in a form such as 192.168.110.0/24).

c. When prompted, press **Enter**.
   The NFS configuration utility is displayed.

d. Repeat step 6 for each additional audit client that has access to the audit share.

7. Optionally, verify your configuration.
   a. Enter the following: `validate-config`
      The services are checked and displayed.
   b. When prompted, press **Enter**.
      The NFS configuration utility is displayed.
   c. Close the NFS configuration utility: `exit`

8. Determine if you must enable audit shares at other sites.
   • If the StorageGRID Webscale deployment is a single site, go to step 9.
   • If the StorageGRID Webscale deployment includes Admin Nodes at other sites, enable these audit shares as required:
     a. Remotely log in to the site’s Admin Node:
        i. Enter the following command: `ssh admin@grid_node_IP`
        ii. Enter the password listed in the `Passwords.txt` file.
        iii. Enter the following command to switch to root: `su -`
        iv. Enter the password listed in the `Passwords.txt` file.
     b. Repeat steps 4 through 7.c to configure the audit shares for each additional Admin Node.
     c. Close the remote secure shell login to the remote Admin Node. Enter: `exit`

9. Log out of the command shell: `exit`

NFS audit clients are granted access to an audit share based on their IP address. Grant access to the audit share to a new NFS audit client by adding its IP address to the share, or remove an existing audit client by removing its IP address.

**Adding an NFS audit client to an audit share**

NFS audit clients are granted access to an audit share based on their IP address. Grant access to the audit share to a new NFS audit client by adding its IP address to the audit share.

**Before you begin**

• You must have the `Passwords.txt` file with the root/admin account password (available in the SAID package).

• You must have the `Configuration.txt` file (available in the SAID package).

• The audit client must be using NFS Version 3 (NFSv3).
Steps

1. From the service laptop, log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

   Once logged in as root, the prompt changes from `$` to `#`.

2. Start the NFS configuration utility: `config_nfs.rb`

<table>
<thead>
<tr>
<th>Shares</th>
<th>Clients</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>add-audit-share</td>
<td>add-ip-to-share</td>
<td>validate-config</td>
</tr>
<tr>
<td>enable-disable-share</td>
<td>remove-ip-from-share</td>
<td>refresh-config</td>
</tr>
<tr>
<td></td>
<td></td>
<td>help</td>
</tr>
<tr>
<td></td>
<td></td>
<td>exit</td>
</tr>
</tbody>
</table>

3. Enter: `add-ip-to-share`
   A list of NFS audit shares enabled on the Admin Node is displayed. The audit share is listed as: `/var/local/audit/export`

4. Enter the number of the audit share: `audit_share_number`

5. When prompted, enter the audit client’s IP address or IP Address range for the audit share: `client_IP_address`

   IP address ranges must be expressed using a subnet mask in CIDR notation (form such as `192.168.110.0/24`).

   The audit client is added to the audit share.

   The NFS configuration utility is displayed.

7. Repeat from step 3 for each audit client that should be added to the audit share.

8. Optionally, verify your configuration: `validate-config`
   The services are checked and displayed.

   a. When prompted, press `Enter`.

   The NFS configuration utility is displayed.

9. Close the NFS configuration utility: `exit`

10. If the StorageGRID Webscale deployment is a single site, go to step 11.
    — or —

    Optionally, if the StorageGRID Webscale deployment includes Admin Nodes at other sites, enable these audit shares as required:

    a. Remotely log in to a site’s Admin Node:

    i. Enter the following command: `ssh admin@grid_node_IP`
ii. Enter the password listed in the `Passwords.txt` file.

iii. Enter the following command to switch to root: `su -`

iv. Enter the password listed in the `Passwords.txt` file.

b. Repeat steps 2 through 9 to configure the audit shares for each Admin Node.

c. Close the remote secure shell login to the remote Admin Node: `exit`

11. Log out of the command shell: `exit`

**Verifying NFS audit integration**

After you configure an audit share and add an NFS audit client, you can mount the audit client share and verify that the files are available from the audit share.

**Steps**

1. Verify connectivity (or variant for the client system) using the client-side IP address of the Admin Node hosting the AMS service. Enter: `ping IP_address`

   Verify that the server responds, indicating connectivity.

2. Mount the audit read-only share using a command appropriate to the client operating system. A sample Linux command is (enter on one line):

   ```bash
   mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export myAudit
   ```

   Use the IP address of the Admin Node hosting the AMS service and the predefined share name for the audit system. The mount point can be any name selected by the client (for example, `myAudit` in the previous command).

3. Verify that the files are available from the audit share. Enter: `ls myAudit /*`

   where `myAudit` is the mount point of the audit share. There should be at least one log file listed.

**Removing an NFS audit client from the audit share**

NFS audit clients are granted access to an audit share based on their IP address. You can remove an existing audit client by removing its IP address.

**Before you begin**

- You must have the `Passwords.txt` file with the root/admin account password (available in the SAID package).
- You must have the `Configuration.txt` file (available in the SAID package).

**About this task**

You cannot remove the last IP address permitted to access the audit share.

**Steps**

1. From the service laptop, log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
d. Enter the password listed in the `Passwords.txt` file.

Once logged in as root, the prompt changes from `$` to `#`.

2. Start the NFS configuration utility: `config_nfs.rb`

3. Remove the IP address from the audit share: `remove-ip-from-share`

A numbered list of audit shares configured on the server is displayed. The audit share is listed as: `/var/local/audit/export`

4. Enter the number corresponding to the audit share: `audit_share_number`

A numbered list of IP addresses permitted to access the audit share is displayed.

5. Enter the number corresponding to the IP address you want to remove.

The audit share is updated, and access is no longer permitted from any audit client with this IP address.


The NFS configuration utility is displayed.

7. Close the NFS configuration utility: `exit`

8. If your StorageGRID Webscale deployment is a multiple data center site deployment with additional Admin Nodes at the other sites, disable these audit shares as required:

   a. Remotely log in to each site’s Admin Node:

      i. Enter the following command: `ssh admin@grid_node_IP`

      ii. Enter the password listed in the `Passwords.txt` file.

      iii. Enter the following command to switch to root: `su -`

      iv. Enter the password listed in the `Passwords.txt` file.

   b. Repeat steps 2 through 7 to configure the audit shares for each additional Admin Node.

   c. Close the remote secure shell login to the remote Admin Node: `exit`

9. Log out of the command shell: `exit`

**Changing the IP address of an NFS audit client**

**Steps**

1. Add a new IP address to an existing NFS audit share.

2. Remove the original IP address.
Related tasks

- Adding an NFS audit client to an audit share on page 170
- Removing an NFS audit client from the audit share on page 172
Controlling system access with administration user accounts and groups

By managing administration user accounts and administration groups, you can control access to the StorageGRID Webscale system. Each administration group account is assigned permissions that control access to StorageGRID Webscale features and functionality. You then add administration users to one or more administration group accounts to control individual user access.

You can perform the following tasks related to users and groups:

- Configure a federated identity source (such as Active Directory or OpenLDAP) so you can import administration groups and users.
- Create, edit, clone, and remove local and federated groups.
- Create, edit, clone, and remove local users.
- Change local users' passwords.

Additionally, local users can change their own passwords.

Configuring identity federation

You can use identity federation to import admin groups and users. Using identity federation makes setting up groups and users faster, and it allows users to sign in to their accounts using familiar credentials.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

The identity source you configure for the Grid Management Interface allows you to import the following types of federated groups:

- Administration (or “admin”) groups. The users in these groups can sign in to the Grid Management Interface and perform tasks, based on the management permissions assigned to the group. See “About administration user groups.”
- Tenant account groups, assuming that the tenant is not using its own identity source (that is, assuming the Uses Own Identity Source checkbox is unchecked for the tenant account). Users in tenant account groups can sign in to the Tenant Management Interface and perform tasks, based on the permissions assigned to the group. See information about creating tenant accounts and the StorageGRID Webscale Tenant Administrator Guide.

Note: When using identity federation, be aware that users who only belong to a primary group on Active Directory are not allowed to sign in to the Grid Management Interface or the Tenant Management Interface. To allow these users to sign in, grant them membership in a user-created group.

Steps

1. Select Configuration > Identity Federation.
2. Select Enable Identity Federation.
   LDAP service configuration information appears.

3. Select the type of LDAP service you want to configure from the LDAP Service Type drop-down list.
   You can select Active Directory, OpenLDAP, or Other.
   
   **Note:** If you select OpenLDAP, you must configure the OpenLDAP server. See “Guidelines for configuring an OpenLDAP server” in this guide.

4. If you selected Other, complete the fields in the LDAP Attributes section.
   - **Unique User Name:** The name of the attribute that contains the unique identifier of an LDAP user. This attribute is equivalent to sAMAccountName for Active Directory and uid for OpenLDAP.
   - **User UUID:** The name of the attribute that contains the permanent unique identifier of an LDAP user. This attribute is equivalent to objectGUID for Active Directory and entryUUID for OpenLDAP.
   - **Group Unique Name:** The name of the attribute that contains the unique identifier of an LDAP group. This attribute is equivalent to sAMAccountName for Active Directory and cn for OpenLDAP.
   - **Group UUID:** The name of the attribute that contains the permanent unique identifier of an LDAP group. This attribute is equivalent to objectGUID for Active Directory and entryUUID for OpenLDAP.

5. Enter the required LDAP server and network connection information:
   - **Hostname:** The hostname or IP address of the LDAP server.
   - **Port:** The port used to connect to the LDAP server. This is typically 389.
   - **Username:** The username used to access the LDAP server, including the domain. The specified user must have permission to list groups and users and to access the following attributes:
     - cn
     - sAMAccountName or uid
     - objectGUID or entryUUID
     - memberOf
   - **Password:** The password associated with the username.
   - **Group Base DN:** The fully qualified Distinguished Name (DN) of an LDAP subtree you want to search for groups. In the example, all groups whose Distinguished Name is relative to the base DN (DC=storagegrid,DC=example,DC=com) can be used as federated groups.
     - **Note:** The Unique Group Name values must be unique within the Group Base DN they belong to.
   - **User Base DN:** The fully qualified Distinguished Name (DN) of an LDAP subtree you want to search for users.
     - **Note:** The Unique User Name values must be unique within the User Base DN they belong to.
6. Select a security setting from the **Transport Layer Security (TLS)** drop-down list to specify if TLS is used to secure communications with the LDAP server.

- **Use operating system CA certificate**: Use the default CA certificate installed on the operating system to secure connections.

- **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.

- **Do not use TLS**: The network traffic between the StorageGRID Webscale system and the LDAP server will not be secured.

**Example**

The following screen shot shows example configuration values for an LDAP server that uses Active Directory.

![Example Configuration](image)

7. Optionally, click **Test Connection** to validate your connection settings for the LDAP server.

8. Click **Save**.
Guidelines for configuring an OpenLDAP server

If you want to use an OpenLDAP server for identity federation, you must configure specific settings on the OpenLDAP server.

**Memberof and refint overlays**

The memberof and refint overlays should be enabled. For more information, see the “Reverse Group Membership Maintenance” section in the *OpenLDAP Software Administrator’s Guide*.

**Indexing**

You must configure the following OpenLDAP attributes with the specified index keywords:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

In addition, ensure the fields mentioned in the help for Username are indexed for optimal performance.

For more information on the `olcDBIndex` directive used for indexing attributes, see the *OpenLDAP Software Administrator’s Guide*.

Forcing synchronization with the identity source

The StorageGRID Webscale system periodically synchronizes federated groups and users from the identity source. You can force synchronization to start if you want to enable or restrict user permissions as quickly as possible.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- The identity source must be enabled.

**Steps**

1. Select **Configuration > Identity Federation**.
2. Click **Synchronize**.
   A confirmation message is displayed indicating that synchronization started successfully.

**Disabling identity federation**

You can temporarily or permanently disable identity federation for groups and users. When identity federation is disabled, there is no communication between the StorageGRID Webscale and the identity source. However, any settings you have configured are retained, allowing you to easily re-enable identity federation in the future.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

Before you disable identity federation, you should be aware of the following:

- Federated users will be unable to sign in.
- Federated users who are currently signed in will retain access to the StorageGRID Webscale system until their session expires, but they will be unable to sign in after their session expires.
- Synchronization between the StorageGRID Webscale system and the identity source will not occur, and alarms will not be raised for accounts that have not been synchronized.

**Steps**

1. Select **Configuration > Identity Federation**.
2. Deselect the **Enable Identity Federation** checkbox.
3. Click **Save**.

**About admin group permissions**

When creating administration user groups, you select one or more permissions to control access to specific features of the StorageGRID Webscale system. You can then assign each user to one or more of these admin groups to determine which tasks that user can perform.

You must assign at least one permission to each group; otherwise, users belonging to that group will not be able to sign in to the StorageGRID Webscale system.

By default, any user who belongs to a group that has at least one permission can perform the following tasks:

- Sign in to the StorageGRID Webscale system
- View the dashboard
- Monitor grid topology
- Monitor alarms
- Change their own password

The table shows the permissions you can assign when creating or editing an admin group.
Note: You can use the StorageGRID Webscale Management API to completely deactivate certain features. When a feature has been deactivated, the corresponding Management Permission no longer appears on the Groups page.

<table>
<thead>
<tr>
<th>Management permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Access</td>
<td>Provides access to all grid administration features.</td>
</tr>
<tr>
<td>Acknowledge Alarms</td>
<td>Provides access to acknowledge and respond to alarms. All signed-in users can monitor alarms. If you want a user to monitor grid topology and acknowledge alarms only, you should assign this permission.</td>
</tr>
<tr>
<td>Change Tenant Root Password</td>
<td>Provides access to the Change Root Password button on the Tenant Accounts page, allowing you to control who can change the password for the tenant account's root user. Users who do not have this permission cannot see the Change Root Password button. Note: You must assign the Tenant Accounts permission to the group before you can assign this permission.</td>
</tr>
<tr>
<td>Grid Topology Page Configuration</td>
<td>Provides access to the Configuration tabs in Grid Topology.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Provides access to maintenance options. Users who do not have this permission:</td>
</tr>
<tr>
<td></td>
<td>• Do not see the following options in the menu:</td>
</tr>
<tr>
<td></td>
<td>◦ Software upgrade</td>
</tr>
<tr>
<td></td>
<td>◦ Grid expansion</td>
</tr>
<tr>
<td></td>
<td>◦ Grid decommission</td>
</tr>
<tr>
<td></td>
<td>◦ Recovery package creation</td>
</tr>
<tr>
<td></td>
<td>◦ Recovery</td>
</tr>
<tr>
<td></td>
<td>• Can see the following options in the menu and the pages, but cannot make changes in these pages:</td>
</tr>
<tr>
<td></td>
<td>◦ DNS Servers</td>
</tr>
<tr>
<td></td>
<td>◦ NTP Servers</td>
</tr>
<tr>
<td></td>
<td>◦ License update</td>
</tr>
</tbody>
</table>
### Management permission

<table>
<thead>
<tr>
<th>Management permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other Grid Configuration</td>
<td>Provides access to all other grid configuration options, such as:</td>
</tr>
<tr>
<td></td>
<td>• Configuration &gt; System Settings &gt; Domain Names, Grid Options, Link Cost Groups, Storage Options, Display Options, CDMI</td>
</tr>
<tr>
<td></td>
<td>• Configuration &gt; Monitoring &gt; Global Alarms, Notifications, Email Setup, AutoSupport, Audit, Events</td>
</tr>
<tr>
<td></td>
<td>• Configuration &gt; Access Control &gt; Admin Users, Admin Groups, Identity Federation</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Access to these items also requires the Grid Topology Page Configuration permission.</td>
</tr>
<tr>
<td>Tenant Accounts</td>
<td>Provides access to the Tenant Accounts page from the Tenants option, allowing you to control who can add, edit, or remove tenant accounts. Users who do not have this permission do not see the Tenants option in the menu.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Version 1 of the management API (which has been deprecated) uses this permission to manage tenant group policies, reset Swift admin passwords, and manage root user S3 access keys.</td>
</tr>
</tbody>
</table>

### Related tasks

*Deactivating features from the StorageGRID Webscale management API* on page 181

### Deactivating features from the StorageGRID Webscale management API

You can use the StorageGRID Webscale management API to completely deactivate certain features in the StorageGRID Webscale system. When a feature is deactivated, no one can be assigned permissions to perform the tasks related to that feature.

### About this task

The Deactivated Features system allows you to prevent access to certain features in the StorageGRID Webscale system. Deactivating a feature is the only way to prevent the root user or users who belong to admin groups with the Root Access permission from being able to use that feature.

To understand how this functionality might be useful, consider the following scenario:

*Company A is a service provider who leases the storage capacity of their StorageGRID Webscale system by creating tenant accounts. To protect the security of their leaseholders' objects, Company A wants to ensure that its own employees can never access any tenant account after the account has been deployed.*

*Company A can accomplish this goal by using the Deactivate Features system in the StorageGRID Webscale management API. By completely deactivating the Change Tenant Root Password feature in the Grid Management Interface (both the UI and the API), Company A can ensure that no Admin user—including the root user and users belonging to groups with the Root Access permission—can change the password for any tenant account's root user.*

### Reactivating deactivated features
By default, you can use the management API to reactivate a feature that has been deactivated. However, if you want to prevent deactivated features from ever being reactivated, you can deactivate the activateFeatures feature itself.

**Caution:** The activateFeatures feature cannot be reactivated. If you decide to deactivate this feature, be aware that you will permanently lose the ability to reactivate any other deactivated features. You must contact technical support to restore any lost functionality.

See the management API documentation for additional information.

**Steps**

1. Access the Swagger documentation for the API.
2. Locate the Deactivate Features end point.
3. To deactivate a feature, such as Change Tenant Root Password, send a body to the API like this:

   ```json
   { "grid": {"changeTenantRootPassword": true} }
   ```

   When the request is complete, the Change Tenant Root Password feature is disabled. The Change Tenant Root Password management permission no longer appears in the user interface, and any API request that attempts to change the root password for a tenant will fail with "403 Forbidden."

4. To reactivate all features, send a body to the API like this:

   ```json
   { "grid": null }
   ```

   When this request is complete, all features, including the Change Tenant Root Password feature, are reactivated. The Change Tenant Root Password management permission now appears in the user interface, and any API request that attempts to change the root password for a tenant will succeed.

   **Note:** The previous example causes all deactivated features to be reactivated. If other features have been deactivated that should remain deactivated, you must explicitly specify them in the PUT request. For example, to reactivate the Change Tenant Root Password feature and continue to deactivate the Alarm Acknowledgment feature, send this PUT request:

   ```json
   { "grid": { "alarmAcknowledgment": true } }
   ```

**Related concepts**

*Understanding the StorageGRID Webscale management API* on page 15

**About admin user accounts**

You can manage admin user accounts in the StorageGRID Webscale system and also add them to one or more admin groups that govern access to system features. The StorageGRID Webscale system includes one predefined local user, named “root.”

**Note:** If you upgraded from a previous version of StorageGRID Webscale you will also retain the built-in “Vendor” and “Admin” accounts. The best practice is to switch from using the “Vendor” account to the “root” account.

StorageGRID Webscale can be accessed by local and federated users:
• Local users: You can create admin user accounts that are local to StorageGRID Webscale system and add these users to StorageGRID Webscale local admin groups.

• Federated users: You can use a federated identity source (such as Active Directory or OpenLDAP) to import administration groups and users. The identity source manages the groups to which users belong, so you cannot add federated users to local groups. Also, you cannot edit federated user information; this information is synchronized with the external identity source.

Although you can add and delete users, you cannot delete the root user. After creating groups, you assign users to one or more groups.

Creating admin groups

You can create admin groups to manage the security permissions for a group of admin user accounts.

Before you begin

• You must be signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Configuration > Admin Groups.

2. Click Add.

3. Select either Local or Federated as the type of group.

4. For local groups, enter the group’s name that will appear to users, for example, “Development US”.

5. Enter a unique name without spaces for the group, for example, “Dev_US”.

6. Select a set of permissions. See information about admin group permissions.

7. Click Save.

A new group is created and added to the list of group names available for user accounts. User accounts can now be associated with the new group.

Related concepts

About admin group permissions on page 179
Modifying an admin group

You can modify an admin group to update the display name or permissions associated with the group.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Configuration > Admin Groups.
2. Select the name of the group and click Edit.
3. For local groups, enter the group’s name that will appear to users, for example, “Development US”.
   You cannot change the unique name, which is the internal group name.
4. Select a set of permissions.
   See information about admin group permissions.
5. Click Save.

Related concepts

- About admin group permissions on page 179

Deleting an admin group

You can delete an admin group when you want to remove the group from the system, and remove all permissions associated with the group. Deleting an admin group removes any admin users from the group, but does not delete the admin users.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

When you delete a group, users assigned to that group will lose all access privileges to the StorageGRID Webscale system, unless they are granted privileges by a different group.

Steps

1. Select Configuration > Admin Groups.
2. Select the name of the group.
3. Click **Remove**.
4. Click **OK**.

**Creating an admin users account**

You can create a new local user and assign the user to a defined admin group with permissions that govern access to system features. If an admin group with the necessary permission settings does not exist, you must first create an admin groups account.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

You can create only local users. Federated user details are automatically synchronized with the external identity source, for example, the LDAP server.

**Steps**

1. Select **Configuration > Admin Users**.
2. Click **Create**.
   
   The list of group names is generated from the Groups table.
3. Enter the user's display name, unique name, and password.
4. Assign the user to one or more groups that govern the access permissions.
5. Click **Save**.

   New settings are applied the next time you sign out and then sign back in to the StorageGRID Webscale system.

**Related tasks**

*Creating admin groups* on page 183

**Modifying an admin users account**

You can modify a local admin users account to update the full display name or group membership that governs access to system features. You can also temporarily prevent the user from accessing the system.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

You can edit only local users. Federated user details are automatically synchronized with the external identity source, for example, the LDAP server.
Steps
1. Select **Configuration > Admin Users**.
2. Select the user account you want to edit.
3. Click **Edit**.
4. Make changes to the name or group membership.
5. To prevent the user from accessing the system temporarily, check **Deny Access**.
6. Click **Save**.

   The new settings are applied the next time the user signs out and then signs back in to the StorageGRID Webscale system.

Deleting an admin users account

You can delete accounts for local users that no longer require access to the StorageGRID Webscale system.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Configuration > Admin Users**.
2. Select the user account you want to delete.
   
   **Note:** You cannot delete StorageGRID Webscale system’s built-in root user.
3. Click **Remove**.
4. Click **OK** to confirm the deletion.

Changing local users' passwords

While local users can change their own passwords using the **Change Password** option in the StorageGRID Webscale header, users with access to the Admin Users page can change passwords for any local user.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

You can change passwords only for local users. Federated users must change their own passwords in the external identity source (such as Active Directory or OpenLDAP).
Steps

1. Select Configuration > Admin Users.

2. From the Users page, select a user and click Change Password.

3. Enter and confirm the password, and click Save.
Monitoring and managing grid tasks

Grid tasks are scripts that implement specific changes to the StorageGRID Webscale system.

You can monitor the grid tasks that run automatically during maintenance procedures; however, you should not perform any of the other manual grid task operations unless you are instructed to do so by technical support or by the specific instructions for another procedure.

Steps
1. Monitoring grid tasks on page 188
2. Running a grid task on page 190
3. Pausing an active grid task on page 191
4. Resuming a paused grid task on page 192
5. Cancelling a grid task on page 192
6. Aborting a grid task on page 193
7. Submitting a Task Signed Text Block on page 194
8. Removing grid tasks from the Historical table on page 195
9. Troubleshooting grid tasks on page 196

Monitoring grid tasks

You can monitor grid tasks to ensure that a maintenance procedure is completing successfully.

For example, when you add grid nodes or a new data center site in an expansion, you can monitor the expansion grid tasks.
To view the status of grid tasks, select Grid > primary Admin Node > CMN > Grid Tasks > Overview > Main.

Each grid task goes through three phases:

1. **Pending**: The grid task has been submitted, but not started yet.

2. **Active**: The grid task has been started.
   
   An active grid task can be either actively running or temporarily paused. If a grid task’s status changes to Error, the task is continuously retried until it completes or it is aborted.
   
   Grid tasks might report an error when a grid node becomes unavailable (lost connection or crash) or when another grid task is running. When the issue causing the error is resolved, grid tasks with a status of Error automatically start running again.

3. **Historical**: The grid task has been submitted, but is no longer active.
   
   The Historical phase includes grid tasks that completed successfully, have been canceled or aborted, or have failed.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task ID</td>
<td>Unique identifier assigned when the task is created.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the grid task’s purpose. A description can include a revision number, which is used to determine the order in which grid tasks have been created and must be run. If you are running grid tasks manually for some reason, you should always run the earliest generated grid task first.</td>
</tr>
<tr>
<td>Valid From</td>
<td>For pending tasks, the date from which the grid task is valid and can be run. The grid task fails if it is submitted before this date.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Valid To</td>
<td>For pending tasks, the date until which the grid task is valid and can be run. The grid task fails if it is submitted after this date.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Date and time when the grid task was started.</td>
</tr>
<tr>
<td>Duration</td>
<td>Amount of time since the grid task was started.</td>
</tr>
<tr>
<td>Stage</td>
<td>Description of the current stage of the active grid task.</td>
</tr>
<tr>
<td>% Complete</td>
<td>Progress indicator for the current stage of the active grid task.</td>
</tr>
</tbody>
</table>

**Status—Active grid tasks**

- Starting
- Running
- Pausing
  - Paused: The grid task was paused, either automatically or by the user.
  - Error: An error has been encountered. User action might be required. Grid task retries until successful or aborted.
- Aborting
- Abort Paused: Grid task failed to be aborted and is paused in error.
- Retrying

**Status—Historical grid tasks**

- Successful: The grid task completed normally.
- Aborted: The grid task did not complete normally and had to be aborted.
- Rollback Failed: The grid task did not complete normally and failed to be aborted.
- Cancelled: The grid task was cancelled before being started.
- Expired: The grid task expired before completing.
- Invalid: The grid task was not valid.
- Unauthorized: The grid task failed authorization.
- Duplicate: The grid task was a duplicate.

**Message**

Information about the current status of the active grid task.

**Completion time**

For Historical tasks, the date and time on which the grid task completed (or when it expired or was cancelled or aborted).

---

### Running a grid task

You might need to run a grid task manually to complete some maintenance procedures.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task
Under normal circumstances, the grid tasks required for maintenance procedures appear in the Pending table automatically and are run automatically. However, in some cases, you might need to run a pending grid task manually.

Important: Do not run a grid task unless you are instructed to do so by technical support or by the specific instructions for another procedure.

If the Pending table includes grid tasks from multiple provisioning revisions, you must run grid tasks from the earliest revision (lowest revision number) first. If there is an active grid task currently listed with a status of Error, do not run any other grid tasks until either the problem is resolved and the grid task begins running again or the grid task is aborted.

Steps
1. Select Grid.
2. Select primary Admin Node > CMN > Grid Tasks.
3. Click Configuration > Main.
4. Under Actions, select Start for the grid task you want to run.
   Note: If there is an error after starting and the grid task updates to a status of Error, the grid task continuously retries until it completes successfully or is aborted.
5. Click Apply Changes.
   The grid task moves from the Pending table to the Active table. You must wait for the page to refresh before the change is visible. Do not submit the change again. The grid task continues to run until it completes or you pause or abort it. When the grid task completes successfully, it moves to the Historical table with a Status of Successful.
   Note: The Configuration page does not update automatically. To monitor the progress of a grid task, go to the Overview page. Then, if necessary, go back to the Configuration page to make changes.

Pausing an active grid task
You might need to pause an active grid task before it finishes. Pausing a grid task might be necessary if the StorageGRID Webscale system becomes particularly busy and you need to free resources used by the grid task operation.

Before you begin
- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task
Do not pause an active grid task unless you are instructed to do so by technical support or by the specific instructions for another procedure.
Steps
1. Select Grid.
2. Select primary Admin Node > CMN > Grid Tasks.
3. Click Configuration > Main.
4. Under Actions, select Pause for the Active grid task you want to suspend temporarily.
5. Click Apply Changes.

The grid task remains on the Active table with its Status changed to Paused. You can confirm this by returning to primary Admin Node > CMN > Grid Tasks > Overview > Main.

Resuming a paused grid task

If a grid task has been paused, you can resume the task when conditions permit.

Before you begin
• You must be signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps
1. Select Grid.
2. Select primary Admin Node > CMN > Grid Tasks.
3. Click Configuration > Main.
4. Under Actions, select Run for the Paused grid task you want to resume.
5. Click Apply Changes.

The grid task remains in the Active table with its status changed to Running. You can confirm this by returning to primary Admin Node > CMN > Grid Tasks > Overview > Main.

Cancelling a grid task

You can cancel a grid task from the Pending table so that it is no longer available to be run.

Before you begin
• You must be signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task
Do not cancel an active grid task unless you are instructed to do so by technical support or by the specific instructions for another procedure.

Steps
1. Select Grid.
2. Select primary Admin Node > CMN > Grid Tasks.

3. Click Configuration > Main.

4. Under Actions, select Cancel for the Pending grid task that you want to cancel.

5. Click Apply Changes.

   The grid task is moved to the Historical table with its status changed to Cancelled. You can confirm this by returning to primary Admin Node > CMN > Grid Tasks > Overview > Main.

Aborting a grid task

You can abort an active grid task while it is running.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

Not all grid tasks can be aborted. To determine whether a grid task can be aborted, follow the guidelines in the procedures where the grid task is discussed.

   Important: Do not abort an active grid task unless you are instructed to do so by technical support or by the specific instructions for another procedure.

Aborting an active grid task causes it to leave affected entities in a reliable state. This might require you to roll back some actions or reset device states. The result is that the grid task can remain on the Active table with a status of Aborting for an extended period of time. When the programmed abort process is complete, the grid task moves to the Historical table.

Steps

1. Select Grid.

2. Select primary Admin Node > CMN > Grid Tasks.

3. Click Configuration > Main.

4. Under Actions, select Pause for the Active grid task you want to abort.

5. Click Apply Changes.

   When the page refreshes, the status of the grid task changes to Paused.

6. Under Actions, select Abort.

7. Click Apply Changes.

   While the task is aborting, it remains in the Active table with a status of Aborting. When the operation is complete, the grid task moves to the Historical table with its status changed to Aborted. You can confirm this by returning to primary Admin Node > CMN > Grid Tasks > Overview > Main.

After you finish

You can run an aborted grid task again by resubmitting it with a Task Signed Text Block.
Submitting a Task Signed Text Block

If the grid task you need to run is not in the Pending table, you can manually load the grid task by submitting the Task Signed Text Block.

Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

Do not submit a task signed text block unless you are instructed to do so by technical support or by the specific instructions for another procedure.

Steps

1. Retrieve the grid task from the Grid_Tasks folder of the SAID package.
2. Copy the Task Signed Text Block file to the same computer that you will use to access the StorageGRID Webscale system.
3. Open the file that contains the grid task (Task Signed Text Block) using a text editor.
4. Copy the Task Signed Text Block to the clipboard:
   a. Select the text, including the opening and closing delimiters:
      
      ```
      -----BEGIN TASK-----
      AAAAAH1RTSUJDT05UAAANB1RCTEtjbmN0AAAM+1RCTEtDT05UAAAA
      EF5wRVjVSTMyAAAABAABBUU01EVEUzMoEecsEAAAAAYVFNSQONTV
      ...
      s5zJz1795J3x7TWeqBAInHDVEMKg95095VJUW5kQij5SRjtoWLAYXC
      -----END TASK-----
      ```
      If the Task Signed Text Block has a readable description above the opening delimiter, it can be included but is ignored by the StorageGRID Webscale system.
      
      b. Copy the selected text.

5. Select Grid.
6. Click Configuration > Main.
7. Under Submit New Task, paste the Task Signed Text Block.

8. Click Apply Changes.

The StorageGRID Webscale system validates the Task Signed Text Block and either rejects the grid task or adds it to the table of pending grid tasks.

## Removing grid tasks from the Historical table

You can manually remove grid tasks listed in the Historical table.

### Before you begin

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

### Steps

1. Select Grid.

2. Select `primary Admin Node > CMN > Grid Tasks`.

3. Click Configuration > Main.

4. Select the Remove check box for the grid task.

5. Click Apply Changes.

The grid task is removed from the Historical table. You can confirm this by returning to `primary Admin Node > CMN > Grid Tasks > Overview > Main`.

---

**Configuration: CMN (DC1-ADM1) - Grid Tasks**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task Type</th>
<th>Description</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>4235363152</td>
<td>VFOV</td>
<td>LDR Foreground Verification: Node ID 12123456</td>
<td>Successful</td>
<td>□</td>
</tr>
</tbody>
</table>

**Pending:**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task Type</th>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
</table>

**Active:**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task Type</th>
<th>Description</th>
<th>Stage</th>
<th>% Complete</th>
<th>Status</th>
<th>Message</th>
<th>Actions</th>
</tr>
</thead>
</table>

**Historical:**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task Type</th>
<th>Description</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>4235363152</td>
<td>VFOV</td>
<td>LDR Foreground Verification: Node ID 12123456</td>
<td>Successful</td>
<td>□</td>
</tr>
</tbody>
</table>
Troubleshooting grid tasks

If a grid task is not successful, you can perform basic troubleshooting to help technical support resolve the issue.

Note: Do not run, pause, cancel, or abort grid tasks unless you are instructed to do so by technical support or by the specific instructions for another procedure.

Choices

• Grid task fails to complete and moves to Historical table on page 196
• Grid task retries multiple times on page 196
• Grid task has Error status on page 197

Grid task fails to complete and moves to Historical table

In some cases, you might observe that a grid task moves to the Historical table without completing successfully.

If a grid task fails to finish successfully, it moves to the Historical table with one of the following statuses:

• Aborted: The grid task did not complete normally and had to be aborted.
• Rollback Failed: The grid task did not complete normally and failed to be aborted.
• Cancelled: The grid task was cancelled before being started.
• Expired: The grid task expired before completing.
• Invalid: The grid task was not valid.
• Unauthorized: The grid task failed authorization.
• Duplicate: The grid task was a duplicate.

Grid task expiration is most common reason for a grid task to fail. If a grid task expires, it can never be run. A new grid task must be created and run.

Note that a grid task failure is not the same as a grid task error. If a grid task encounters an error, it remains in the Active table. Its status changes to Error and then to Retrying as it attempts to finish. A grid task that has an error does not move to the Historical table unless it is aborted.

Grid task retries multiple times

You might observe that a grid task does not complete successfully, but that the StorageGRID Webscale system tries to run the grid task multiple times. You should identify and solve this issue to conserve system resources.

About this task

If you notice that the StorageGRID Webscale system is retrying the same grid task multiple times, contact technical support. Technical support might advise you to pause and restart the grid task manually or to abort the grid task, remove it from the Historical table, and resubmit it.
Grid task has Error status

If the status of a grid task changes to Error, that task is retried until it runs successfully or it is aborted.

When the status of a grid task changes to Error, a Grid Task Status alarm (SCAS) is triggered. Do not run any other grid tasks until the grid task with a status of Error completes successfully or is aborted.

For information about the error, go to Grid > primary Admin Node > CMN > Grid Tasks > Overview > Main and look up the grid task message. This message displays information about the error (for example, check failed on node 12130011). After you have investigated and corrected the problem, the grid task moves out of the Error state and continues to a successful completion.
What data migration is

You can migrate large amounts of data to the StorageGRID Webscale system while simultaneously using the StorageGRID Webscale system for day-to-day operations.

The following section is a guide to understanding and planning a migration of large amounts of data into the StorageGRID Webscale system. It is not a general guide to data migration, and it does not include detailed steps for performing a migration. Follow the guidelines and instructions in this section to ensure that data is migrated efficiently into the StorageGRID Webscale system without interfering with its day-to-day operations, and that the migrated data is handled appropriately by the StorageGRID Webscale system.

Confirming capacity of the StorageGRID Webscale system

Before migrating large amounts of data into the StorageGRID Webscale system, confirm that the StorageGRID Webscale system has the disk capacity to handle the anticipated volume.

If the StorageGRID Webscale system includes an Archive Node and a copy of migrated objects has been saved to nearline storage (such as tape), ensure that the Archive Node’s storage has sufficient capacity for the anticipated volume of migrated data.

As part of the capacity assessment, look at the data profile of the objects you plan to migrate and calculate the amount of disk capacity required. For information about monitoring the disk capacity of your StorageGRID Webscale system, see the Grid Primer.

Related information

StorageGRID Webscale 10.4 Grid Primer

Determining the ILM policy for migrated data

The StorageGRID Webscale system’s ILM policy determines how many copies are made, the locations to which copies are stored, and for how long these copies are retained. An ILM policy consists of a set of ILM rules that describe how to filter objects and manage object data over time.

Depending on how migrated data is used and your requirements for migrated data, you might want to define unique ILM rules for migrated data that are different from the ILM rules used for day-to-day operations. For example, if there are different regulatory requirements for day-to-day data management than there are for the data that is included in the migration, you might want a different number of copies of the migrated data on a different grade of storage.

You can configure rules that apply exclusively to migrated data if it is possible to uniquely distinguish between migrated data and object data saved from day-to-day operations.

If you can reliably distinguish between the types of data using one of the metadata criteria, you can use this criteria to define an ILM rule that applies only to migrated data.

Before beginning data migration, ensure that you understand the StorageGRID Webscale system’s ILM policy and how it will apply to migrated data, and that you have made and tested any changes to the ILM policy.

Warning: An ILM policy that has been incorrectly specified can cause unrecoverable data loss. Carefully review all changes you make to an ILM policy before activating it to make sure the policy will work as intended.
Impact of migration on operations

A StorageGRID Webscale system is designed to provide efficient operation for object storage and retrieval, and to provide excellent protection against data loss through the seamless creation of redundant copies of object data and metadata.

However, data migration must be carefully managed according to the instructions in this chapter to avoid having an impact on day-to-day system operations, or, in extreme cases, placing data at risk of loss in case of a failure in the StorageGRID Webscale system.

Migration of large quantities of data places additional load on the system. When the StorageGRID Webscale system is heavily loaded, it responds more slowly to requests to store and retrieve objects. This can interfere with store and retrieve requests which are integral to day-to-day operations. Migration can also cause other operational issues. For example, when a Storage Node is nearing capacity, the heavy intermittent load due to batch ingest can cause the Storage Node to cycle between read-only and read-write, generating notifications.

If the heavy loading persists, queues can develop for various operations that the StorageGRID Webscale system must perform to ensure full redundancy of object data and metadata.

Data migration must be carefully managed according to the guidelines in this document to ensure safe and efficient operation of the StorageGRID Webscale system during migration. When migrating data, ingest objects in batches or continuously throttle ingest. Then, continuously monitor the StorageGRID Webscale system to ensure that various attribute values are not exceeded. Controlling the rate of migration of data into the system is outside of the scope of StorageGRID Webscale functionality.

Scheduling data migration

Avoid migrating data during core operational hours. Limit data migration to evenings, weekends, and other times when system usage is low.

If possible, do not schedule data migration during periods of high activity. However, if it is not practical to completely avoid the high activity period, it is safe to proceed as long as you closely monitor the relevant attributes and take action if they exceed acceptable values.

Related concepts

*Monitoring data migration* on page 199

Monitoring data migration

Data migration must be monitored and adjusted as necessary to ensure data is placed according to the ILM policy within the required timeframe.

This table lists the attributes you must monitor during data migration, and the issues that they represent.
<table>
<thead>
<tr>
<th>Monitor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of objects waiting for ILM evaluation</td>
<td>1. Select Grid.</td>
</tr>
<tr>
<td></td>
<td>2. Select deployment &gt; Overview &gt; Main.</td>
</tr>
<tr>
<td></td>
<td>3. In the ILM Activity section, monitor the number of objects shown for the following attributes:</td>
</tr>
<tr>
<td></td>
<td>• Awaiting - All (XQUZ): The total number of objects awaiting ILM evaluation.</td>
</tr>
<tr>
<td></td>
<td>• Awaiting - Client (XCQZ): The total number of objects awaiting ILM evaluation from client operations (for example, ingest).</td>
</tr>
<tr>
<td></td>
<td>4. If the number of objects shown for either of these attributes exceeds 100,000, throttle the ingest rate of objects to reduce the load on</td>
</tr>
<tr>
<td></td>
<td>the StorageGRID Webscale system.</td>
</tr>
<tr>
<td>Targeted archival system's storage capacity</td>
<td>If the ILM policy saves a copy of the migrated data to a targeted archival storage system (tape or the cloud), monitor the capacity of</td>
</tr>
<tr>
<td></td>
<td>the targeted archival storage system to ensure that there is sufficient capacity for the migrated data.</td>
</tr>
<tr>
<td>Archive Node &gt; ARC &gt; Store &gt; Store Failures (ARVF)</td>
<td>If an alarm for this attribute is triggered, the targeted archival storage system might have reached capacity. Check the targeted archival</td>
</tr>
<tr>
<td></td>
<td>storage system and resolve any issues that triggered an alarm.</td>
</tr>
</tbody>
</table>

### Creating custom notifications for migration alarms

You might want to configure the StorageGRID Webscale system to send a notification email to the system administrator responsible for monitoring migration if the attribute values exceed their recommended maximum values.

**Before you begin**

- You must be signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- You must have configured email settings.
- You must have a mailing list.

**Steps**

1. Create an email list that includes all administrators responsible for monitoring the data migration.
   
   Optionally, you can create a template to customize the subject line, header, and footer of data migration notification emails.

2. Create a Global Custom alarm for each attribute you need to monitor during data migration.
   
   a. Select Configuration > Global Alarms.

   b. Under Default Alarms, search for the default alarms for the first attribute. Under Filter by, select Attribute Code, then type the four letter code for the attribute. For example, ARVF.
c. Click **Submit**.

d. In the results list, click **Copy** next to the alarm you want to modify.
The alarm moves to the Global Custom Alarms table.

e. Under Global Custom Alarms, in the Mailing List column for the copied attribute, add the mailing list.

f. Repeat for each remaining attribute.

g. When finished creating Global Custom alarms, click **Apply Changes**.

**After you finish**

Administrators responsible for monitoring data migration now receive an email notification if the values of key attributes exceed their maximum acceptable levels during migration.

Remember to disable these notifications after data migration is complete. Note that global custom alarms override default alarms. If there are any, enable custom alarms at the grid node level as global custom alarms cannot be triggered.

**Related tasks**

- *Configuring email server settings* on page 28
- *Creating mailing lists* on page 30
What Server Manager is

The Server Manager application runs on every grid node, supervising the starting and stopping of services, and ensuring services gracefully join and leave the StorageGRID Webscale system. Server Manager also monitors every grid node’s services and automatically attempts to restart any that report faults.

During system start-up, Server Manager is automatically started by the operating system (OS), executing a sequential series of scripts to verify that support services are running, and starting them as needed. The start-up and shut-down sequences are reversed, ensuring that dependent services are in place as needed, and are not removed prematurely.

Server Manager provides the following capabilities:

- Stopping and starting of services to:
  - Restart services that have gone offline
  - Bring up the services after a reconfiguration
- Monitoring of services on an ongoing basis and restarting them as needed.
- Automatically starting of services if a server is power cycled or reset, and to recover from unintentional restarts.
- Detection of OS shutdown and gracefully closing of services.
- Restarting a grid node (bring down everything, including the OS, and rebooting the machine from the BIOS up).
- Shutting down a grid node to the point where it must be manually restarted. This enables you to safely power down a server for hardware maintenance.

Server Manager command shell procedures

You access Server Manager through the command line of any grid node.

Always remember to log out after you are finished with Server Manager, which is accomplished by closing the current command shell session. Enter: `exit`

Viewing Server Manager status and version

For each grid node, you can view the current status and version of Server Manager running on that grid node. You can also obtain the current status of all services running on that grid node.

Before you begin

You must have the `Passwords.txt` file.

Steps

1. From the service laptop, log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
d. Enter the password listed in the `Passwords.txt` file.

Once logged in as root, the prompt changes from `$` to `#`.

2. View the current status of Server Manager running on a grid node: `/etc/init.d/servermanager status`

The current status of Server Manager running on the grid node is reported (running or not). If Server Manager’s status is `running`, the time it has been running since last it was started is listed. For example,

```
servermanager running for 1d, 13h, 0m, 30s
```

This status is the equivalent of the status shown in the header of the local console display.

3. View the current version of Server Manager running on a grid node: `/etc/init.d/servermanager version`

The current version of Server Manager running on the grid node is reported. For example,

```
10.3.0-20160125.2055.fe1efd1
```

This information can be useful when updating the StorageGRID Webscale system.

4. Log out of the command shell: `exit`

**Viewing current status of all services**

You can view the current status of all services running on a grid node at any time.

**Before you begin**

You must have the `Passwords.txt` file.

**Steps**

1. From the service laptop, log in to the grid node:
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

   Once logged in as root, the prompt changes from `$` to `#`.

2. View a continuously updated report of status for all services running on the grid node: `storagegrid-status`

   The current status of all service running on the grid node is reported (running or not). For example,

<table>
<thead>
<tr>
<th>Host Name</th>
<th>DC1-ADM1-104-80</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.0.2.64</td>
</tr>
<tr>
<td>Operating System Kernel</td>
<td>3.16.0</td>
</tr>
<tr>
<td>Verified</td>
<td></td>
</tr>
<tr>
<td>Operating System Environment</td>
<td>Debian 8.2</td>
</tr>
<tr>
<td>Verified</td>
<td></td>
</tr>
<tr>
<td>StorageGRID Webscale Release</td>
<td>10.3.0</td>
</tr>
<tr>
<td>Verified</td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td>Verified</td>
</tr>
<tr>
<td>Storage Subsystem</td>
<td>Verified</td>
</tr>
<tr>
<td>Database Engine</td>
<td>5.5.46</td>
</tr>
<tr>
<td>Running</td>
<td></td>
</tr>
<tr>
<td>Time Synchronization</td>
<td>1:4.2.6.p5+dfs</td>
</tr>
</tbody>
</table>

   The current status of all service running on the grid node is reported (running or not). For example,
If the status of a service changes, the report is immediately updated to reflect the change in status.

3. Return to the command line, press Ctrl+C.

4. View a static report of status for all services running on the grid node: /usr/local/servermanager/reader.rb

   The current status of all service running on the grid node is reported (running or not). For example,

<table>
<thead>
<tr>
<th>Host Name</th>
<th>DC1-ADM1-104-80</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.0.2.64</td>
</tr>
<tr>
<td>Operating System Kernel</td>
<td>3.16.0         Verified</td>
</tr>
<tr>
<td>Operating System Environment</td>
<td>Debian 8.2     Verified</td>
</tr>
<tr>
<td>StorageGRID Webscale Release</td>
<td>10.3.0         Verified</td>
</tr>
<tr>
<td>Networking</td>
<td>Verified</td>
</tr>
<tr>
<td>Storage Subsystem</td>
<td>Verified</td>
</tr>
<tr>
<td>Database Engine</td>
<td>5.5.46          Running</td>
</tr>
<tr>
<td>Time Synchronization</td>
<td>1:4.2.6.p5+dfsg  Running</td>
</tr>
<tr>
<td>Network Monitoring</td>
<td>10.3.0         Running</td>
</tr>
<tr>
<td>ams</td>
<td>10.3.0          Running</td>
</tr>
<tr>
<td>cmn</td>
<td>10.3.0          Running</td>
</tr>
<tr>
<td>nms</td>
<td>10.3.0          Running</td>
</tr>
<tr>
<td>ssm</td>
<td>10.3.0          Running</td>
</tr>
<tr>
<td>mi</td>
<td>10.3.0          Running</td>
</tr>
<tr>
<td>tomcat</td>
<td>5.5.35.5        Running</td>
</tr>
<tr>
<td>mgmt api</td>
<td>10.3.0          Running</td>
</tr>
<tr>
<td>attrDownPurge</td>
<td>10.3.0          Running</td>
</tr>
<tr>
<td>attrDownSamp1</td>
<td>10.3.0          Running</td>
</tr>
<tr>
<td>attrDownSamp2</td>
<td>10.3.0          Running</td>
</tr>
</tbody>
</table>

If the status of a service changes, the report does not update to reflect the change in status.

5. Log out of the command shell: exit

Starting Server Manager and all services

There may be times when might have to start Server Manager, which also starts all services on the grid node.

Before you begin

You must have the Passwords.txt file.

About this task

Starting Server Manager on a grid node where it is already running results in a restart of Server Manager and all services on the grid node.

Steps

1. From the service laptop, log in to the grid node:
a. Enter the following command: `ssh admin@grid_node_IP`
b. Enter the password listed in the `Passwords.txt` file.
c. Enter the following command to switch to root: `su -`
d. Enter the password listed in the `Passwords.txt` file.

Once logged in as root, the prompt changes from `$` to `#`.

2. Start Server Manager: `/etc/init.d/servermanager start`

3. Log out of the command shell: `exit`

**Restarting Server Manager and all services**

You might need to restart server manager and all services running on a grid node.

**Before you begin**

You must have the `Passwords.txt` file.

**Steps**

1. From the service laptop, log in to the grid node:
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

   Once logged in as root, the prompt changes from `$` to `#`.

2. Restart Server Manager and all services on the grid node: `/etc/init.d/servermanager restart`

   Server Manager and all services on the grid node are stopped and then restarted.

   **Note:** Using the `restart` command is the same as using the `stop` command followed by the `start` command.

3. Log out of the command shell: `exit`

**Stopping Server Manager and all services**

Server Manager is intended to run at all times, but there might be a time when you need to stop Server Manager and all services running on a grid node.

**Before you begin**

You must have the `Passwords.txt` file.

**About this task**

The only scenario that requires you to stop Server Manager while keeping the operating system running is when you need to integrate Server Manager to other services. If there is a requirement to stop the Server Manager for servicing of the hardware or reconfiguration of the server, the entire server should be halted.
Steps

1. From the service laptop, log in to the grid node:
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the Passwords.txt file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the Passwords.txt file.

   Once logged in as root, the prompt changes from $ to #.

2. Stop Server manager and all services running on the grid node: `/etc/init.d/servermanager stop`

   Server Manager and all services running on the grid node are gracefully terminated.

3. Log out of the command shell: `exit`

Viewing current status of a service

You can view the current status of a services running on a grid node at any time.

Before you begin

You must have the Passwords.txt file.

Steps

1. From the service laptop, log in to the grid node:
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the Passwords.txt file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the Passwords.txt file.

   Once logged in as root, the prompt changes from $ to #.

2. View the current status of a service running on a grid node: `/etc/init.d/service status`

   The current status of the requested service running on the grid node is reported (running or not). For example,

   ```
   cmn running for 1d, 14h, 21m, 2s
   ```

3. Log out of the command shell: `exit`

Stopping a service

Some maintenance procedures require you to stop a single service while keeping other services on the grid node running. Only stop individual services when directed to do so by a maintenance procedure.

Before you begin

You must have the Passwords.txt file.
About this task
When a service is “administratively stopped” in this way, Server Manager does not automatically restart the service. You must either restart the single service manually or restart Server Manager.

Steps
1. From the service laptop, log in to the grid node:
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

   Once logged in as root, the prompt changes from `$` to `#`.

2. Stop an individual service:
   `/etc/init.d/service stop`
   For example,
   `/etc/init.d/ldr stop`
   
   Note: If the service fails to stop after 15 minutes, perform a manual termination of the service.

3. Log out of the command shell: `exit`

Related tasks
   Forcing a service to terminate on page 207

Forcing a service to terminate
Occasionally, a service will not stop after you have run the `stop` command (`/etc/init.d/service stop`). This failure to stop can be the result of an unusual software state or other unexpected condition within the system.

Before you begin
You must have the `Passwords.txt` file.

Steps
1. From the service laptop, log in to the grid node:
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

   Once logged in as root, the prompt changes from `$` to `#`.

2. Manually force a service to terminate: `sv -w time force-stop service`
   
   where `time` is the number of seconds to wait before executing the command. For example,
sv -w30 force-stop ldr

The system waits 30 seconds before terminating the ldr service.

3. Log out of the command shell: exit

### Restarting a service

Some maintenance procedures require you to stop a single service while keeping other services on the grid node running. After you have completed tasks that required you to stop a service, restart that service.

**Before you begin**

You must have the `Passwords.txt` file.

**Steps**

1. From the service laptop, log in to the grid node:
   
   a. Enter the following command: `ssh admin@grid_node_IP`
   
   b. Enter the password listed in the `Passwords.txt` file.
   
   c. Enter the following command to switch to root: `su -`
   
   d. Enter the password listed in the `Passwords.txt` file.

   Once logged in as root, the prompt changes from `$` to `#`.

2. Restart a manually stopped service: `/etc/init.d/service start`

   For example,
   
   `/etc/init.d/ldr start`

3. Restart a running service: `/etc/init.d/service restart`

4. Log out of the command shell: `exit`

### Rebooting a grid node

When you reboot a grid node, all services are started automatically.

**Before you begin**

You must have the `Passwords.txt` file.

**Steps**

1. From the service laptop, log in to the grid node:
   
   a. Enter the following command: `ssh admin@grid_node_IP`
   
   b. Enter the password listed in the `Passwords.txt` file.
   
   c. Enter the following command to switch to root: `su -`
   
   d. Enter the password listed in the `Passwords.txt` file.

   Once logged in as root, the prompt changes from `$` to `#`.  

---

208 | StorageGRID Webscale 10.4 Administrator Guide
2. Optionally, stop services: `/etc/init.d/servermanager stop`
   This is an optional, but recommended step.

3. Reboot the grid node: `reboot`
   If a `reboot` command is directly issued to the system, you might not be able to log in to the system remotely to monitor the shutdown process. Services can take some time to shut down.

4. Log out of the command shell: `exit`

### Powering down servers

Before you power down a server, stop services on all grid nodes hosted by that server.

**Steps**

1. From the service laptop, log in to the grid node:
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

   Once logged in as root, the prompt changes from `$` to `#`.

2. Stop services: `/etc/init.d/servermanager stop`

3. Repeat steps 1 and 2 for each grid node hosted on the server to be shut down.

4. Shutdown the server: `shutdown -h now`

5. Log out of the command shell: `exit`

### Using a DoNotStart file

When performing various maintenance or configuration procedures, you might want to use an interlock DoNotStart file to prevent services from starting when Server Manager is started or restarted.

To prevent a service from starting, place a DoNotStart file in the directory of the service you want to prevent from starting. At start-up, Server Manager looks for the DoNotStart file. If the file is present, the service (and any services dependent upon it) is prevented from starting. When the DoNotStart file is removed, the previously stopped service will start on the next start or restart of Server Manager. Services are not automatically started when the DoNotStart file is removed.

The most efficient way to prevent all services from restarting is to prevent the NTP service from starting. All services are dependent on the NTP service and cannot run if the NTP service is not running.

**Adding a DoNotStart file for a service**

You can prevent an individual service from starting by adding a DoNotStart file to that service's directory on a grid node.

**Before you begin**

You must have the `Passwords.txt` file.
Steps

1. From the service laptop, log in to the grid node:
   
a. Enter the following command: `ssh admin@grid_node_IP`
   
b. Enter the password listed in the Passwords.txt file.
   
c. Enter the following command to switch to root: `su -`
   
d. Enter the password listed in the Passwords.txt file.

Once logged in as root, the prompt changes from `$` to `#`.

2. Add a DoNotStart file:
   
   `touch /etc/sv/service/DoNotStart`
   
   where `service` is the name of the service to be prevented from starting. For example,

   ```
   touch /etc/sv/ldr/DoNotStart
   ```
   
   A DoNotStart file is created. No file content is needed.

   When Server Manager or the grid node is restarted, Server Manager restarts, but the `service` does not.

3. Log out of the command shell: `exit`

Removing a DoNotStart file for a service

When you remove a DoNotStart file that is preventing a service from starting, you must start that service.

Before you begin

You must have the Passwords.txt file.

Steps

1. From the service laptop, log in to the grid node:
   
a. Enter the following command: `ssh admin@grid_node_IP`
   
b. Enter the password listed in the Passwords.txt file.
   
c. Enter the following command to switch to root: `su -`
   
d. Enter the password listed in the Passwords.txt file.

   Once logged in as root, the prompt changes from `$` to `#`.

2. Remove the DoNotStart file from the service directory: `rm /etc/sv/service/DoNotStart`

   where `service` is the name of the service. For example,

   ```
   rm /etc/sv/ldr/DoNotStart
   ```

3. Start the service: `/etc/init.d/service start`

   where `service` is the name of the service.

4. Log out of the command shell: `exit`
Troubleshooting Server Manager

There are several tasks you can follow to help determine the source of Server Manager related problems.

Accessing the Server Manager log file

If a problem arises when using Server Manager, check its log file. Error messages related to Server Manager are captured in the Server Manager log file, which is located at: /var/local/log/servermanager.log

Check this file for error messages regarding failures. Escalate the issue to technical support if required. You might be asked to forward log files to technical support.

Service fails to start

While running normally, Server Manager is constantly monitoring services. If a service fails, Server Manager attempts to restart it. If there are three failed attempts to start a service within five minutes, the service goes down and Server Manager does not attempt another restart.

Before you begin

You must have the Passwords.txt file.

About this task

The following procedure can be used if Server Manager fails to start a service or appears to halt execution for an extended period (more than ten minutes).

Steps

1. From the service laptop, log in to the grid node:
   a. Enter the following command: ssh admin@grid_node_IP
   b. Enter the password listed in the Passwords.txt file.
   c. Enter the following command to switch to root: su -
   d. Enter the password listed in the Passwords.txt file.
   Once logged in as root, the prompt changes from $ to #.

2. Determine the status of a service: /etc/init.d/service status
   For example,
   
   /etc/init.d/ldr status
   
   Status information is displayed. For example,
   
   nms running for 2h, 59m, 29s
   
   A status of disabled indicates the presence of a DoNotStart file.

3. If status is disabled, check for the service directory for a DoNotStart file: /etc/sv/service/DoNotStart
4. If the DoNotStart file is present:
   a. Delete the file: `rm /etc/sv/service/DoNotStart exit`  
   b. Start the service: `/etc/init.d/service start` 

5. Log out of the command shell: `exit`

**Service with an error state**

If you detect that a service has entered an error state, attempt to restart the service.

**Before you begin**

You must have the `Passwords.txt` file.

**About this task**

Server Manager monitors services and restarts any that have stopped unexpectedly. If a service fails, Server Manager attempts to restart it. If there are three failed attempts to start a service within five minutes, the service goes down, fails to start, and enters an error state. Server Manager does not attempt another restart.

**Steps**

1. From the service laptop, log in to the grid node:
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

   Once logged in as root, the prompt changes from `$` to `#`.

2. Confirm error state of a service: `/etc/init.d/service status`

   For example,

   ```
   /etc/init.d/ldr status
   ```

   If the service is in an error state, the following message is returned:
   
   `service in error state`

   For example,

   ```
   ldr in error state
   ```

3. Attempt to remove the error state by restarting the service: `/etc/init.d/service restart`

   If the service fails to restart contact support.

4. Log out of the command shell: `exit`
Integrating Tivoli Storage Manager

This section includes best practices and set-up information for integrating an Archive Node with a Tivoli Storage Manager (TSM) server, including Archive Node operational details that impact the configuration of the TSM server.

Archive Node configuration and operation

Your StorageGRID Webscale system manages the Archive Node as a location where objects are stored indefinitely and are always accessible.

When an object is ingested, copies are made to all required locations, including Archive Nodes, based on the Information Lifecycle Management (ILM) rules defined for your StorageGRID Webscale system. The Archive Node acts as a client to a TSM server, and the TSM client libraries are installed on the Archive Node by the StorageGRID Webscale software installation process. Object data directed to the Archive Node for storage is saved directly to the TSM server as it is received. The Archive Node does not stage object data before saving it to the TSM server, nor does it perform object aggregation. However, the Archive Node can submit multiple copies to the TSM server in a single transaction when data rates warrant.

After the Archive Node saves object data to the TSM server, the object data is managed by the TSM server using its lifecycle/retention policies. These retention policies must be defined to be compatible with the operation of the Archive Node. That is, object data saved by the Archive Node must be stored indefinitely and must always be accessible by the Archive Node, unless it is deleted by the Archive Node.

There is no connection between the StorageGRID Webscale system’s ILM rules and the TSM server’s lifecycle/retention policies. Each operates independently of the other; however, as each object is ingested into the StorageGRID Webscale system, you can assign it a TSM management class. This management class is passed to the TSM server along with object data. Assigning different management classes to different object types permits you to configure the TSM server to place object data in different storage pools, or to apply different migration or retention policies as required. For example, objects identified as database backups (temporary content than can be overwritten with newer data) might be treated differently than application data (fixed content that must be retained indefinitely).

The Archive Node can be integrated with a new or an existing TSM server; it does not require a dedicated TSM server. TSM servers can be shared with other clients, provided that the TSM server is sized appropriately for the maximum expected load. TSM must be installed on a server or virtual machine separate from the Archive Node.

It is possible to configure more than one Archive Node to write to the same TSM server; however, this configuration is only recommended if the Archive Nodes write different sets of data to the TSM server. Configuring more than one Archive Node to write to the same TSM server is not recommended when each Archive Node writes copies of the same object data to the archive. In the latter scenario, both copies are subject to a single point of failure (the TSM server) for what are supposed to be independent, redundant copies of object data.

Archive Nodes do not make use of the Hierarchical Storage Management (HSM) component of TSM.

Configuration best practices

When you are sizing and configuring your TSM server there are best practices you should apply to optimize it to work with the Archive Node.

When sizing and configuring the TSM server, you should consider the following factors:
Because the Archive Node does not aggregate objects before saving them to the TSM server, the TSM database must be sized to hold references to all objects that will be written to the Archive Node.

Archive Node software cannot tolerate the latency involved in writing objects directly to tape or other removable media. Therefore, the TSM server must be configured with a disk storage pool for the initial storage of data saved by the Archive Node whenever removable media are used.

You must configure TSM retention policies to use event-based retention. The Archive Node does not support creation-based TSM retention policies. Use the following recommended settings of retmin=0 and retver=0 in the retention policy (which indicates that retention begins when the Archive Node triggers a retention event, and is retained for 0 days after that). However, these values for retmin and retver are optional.

The disk pool must be configured to migrate data to the tape pool (that is, the tape pool must be the NXTSTGPOLL of the disk pool). The tape pool must not be configured as a copy pool of the disk pool with simultaneous write to both pools (that is, the tape pool cannot be a COPYSTGPOLL for the disk pool). To create offline copies of the tapes containing Archive Node data, configure the TSM server with a second tape pool that is a copy pool of the tape pool used for Archive Node data.

Completing the Archive Node setup

The Archive Node is not functional after you complete the installation process. Before the StorageGRID Webscale system can save objects to the TSM Archive Node, you must complete the installation and configuration of the TSM server and configure the Archive Node to communicate with the TSM server.

For more information about optimizing TSM retrieval and store sessions, see Managing archival storage on page 131.

Refer to the following IBM documentation, as necessary, as you prepare your TSM server for integration with the Archive Node in a StorageGRID Webscale system:

- IBM Tape Device Drivers Installation and User’s Guide

- IBM Tape Device Drivers Programming Reference

Installing a new TSM server

You can integrate the Archive Node with either a new or an existing TSM server. If you are installing a new TSM server, follow the instructions in your TSM documentation to complete the installation.

**Note:** An Archive Node cannot be co-hosted with a TSM server.

Configuring the TSM server

This section includes sample instructions for preparing a TSM server following TSM best practices. The following instructions guide you through the process of:

- Defining a disk storage pool, and a tape storage pool (if required) on the TSM server
- Defining a domain policy that uses the TSM management class for the data saved from the Archive Node, and registering a node to use this domain policy

These instructions are provided for your guidance only; they are not intended to replace TSM documentation, or to provide complete and comprehensive instructions suitable for all configurations. Deployment specific instructions should be provided by a TSM administrator who is familiar both with your detailed requirements, and with the complete set of TSM Server documentation.
Defining TSM tape and disk storage pools

The Archive Node writes to a disk storage pool. To archive content to tape, you must configure the disk storage pool to move content to a tape storage pool.

About this task

For a TSM server, you must define a tape storage pool and a disk storage pool within Tivoli Storage Manager. After the disk pool is defined, create a disk volume and assign it to the disk pool. A tape pool is not required if your TSM server uses disk-only storage.

You must complete a number of steps on your TSM server before you can create a tape storage pool. (Create a tape library and at least one drive in the tape library. Define a path from the server to the library and from the server to the drives, and then define a device class for the drives.) The details of these steps can vary depending upon the hardware configuration and storage requirements of the site. For more information, see the TSM documentation.

The following set of instructions illustrates the process. You should be aware that the requirements for your site may be different depending on the requirements of your deployment. For configuration details and for instructions, see the TSM documentation.

Note: You must log onto the server with administrative privileges and use the dsmadmc tool to execute the following commands.

Steps

1. Create a tape library.

   ```bash
   define library tapelibrary libtype=scsi
   ```
   Where `tapelibrary` is an arbitrary name chosen for the tape library, and the value of `libtype` can vary depending upon the type of tape library.

2. Define a path from the server to the tape library.

   ```bash
   define path servername tapelibrary srctype=server desttype=librarydevice=lib-devicename
   ```
   • `servername` is the name of the TSM server
   • `lib-devicename` is the device name for the tape library

3. Define a drive for the library.

   ```bash
   define drive tapelibrary drivename
   ```
   `drivename` is the name you want to specify for the drive.

   You might want to configure an additional drive or drives, depending upon your hardware configuration. (For example, if the TSM server is connected to a Fibre Channel switch that has two inputs from a tape library, you might want to define a drive for each input.)

4. Define a path from the server to the drive you defined.

   ```bash
   define path servername drivename srctype=server desttype=drive
   library=tapelibrary device=drive-dname
   ```
   `drive-dname` is the device name for the drive, and `tapelibrary` is the name of the tape library

   Repeat for each drive that you have defined for the tape library, using a separate `drivename` and `drive-dname` for each drive.

5. Define a device class for the drives.
define devclass DeviceClassName devtype=lto library=tapelibrary format=ultrium3

- DeviceClassName is the name of the device class
- lto describes the type of drive connected to the server
- tapelibrary is the tape library name you defined
- substitute the appropriate value for ultrium3 in the format=parameter to match your tape type

6. Add tape volumes to the inventory for the library.

   checkin libvolume tapelibrary
tapelibrary is the tape library name you defined.

7. Create the primary tape storage pool.

   define stgpool BycastTapePool DeviceClassName description=description
collocates=filespace maxscratch=XX

   - BycastTapePool is the name of the Archive Node’s tape storage pool. You can select any name for the tape storage pool (as long as the name uses the syntax conventions expected by the TSM server).
   - DeviceClassName is the name of the device class name for the tape library.
   - description is a description of the storage pool that can be displayed on the TSM server using the ‘query stgpool’ command. For example: “Tape storage pool for the Archive Node”.
   - collocate=filespace specifies that the TSM server should write objects from the same filespace into a single tape.
   - XX is one of the following:
     - The number of empty tapes in the tape library (in the case that the Archive Node is the only application using the library).
     - The number of tapes allocated for use by the StorageGRID Webscale system (in instances where the tape library is shared).

8. On a TSM server, create a disk storage pool. At the TSM server’s administrative console, enter

   define stgpool BycastDiskPool disk description=description
maxsize=maximum_file_size nextstgpool=BycastTapePool
highmig=percent_high lowmig=percent_low

   - BycastDiskPool is the name of the Archive Node’s disk pool. You can select any name for the disk storage pool (as long as the name uses the syntax conventions expected by the TSM).
   - description is a description of the storage pool that can be displayed on the TSM server using the ‘query stgpool’ command. For example, “Disk storage pool for the Archive Node”.
   - maximum_file_size forces objects larger than this size to be written directly to tape, rather than being cached in the disk pool. It is recommended to set maximum_file_size to 10 GB.
   - nextstgpool=BycastTapePool refers the disk storage pool to the tape storage pool defined for the Archive Node.
   - percent_high sets the value at which the disk pool begins to migrate its contents to the tape pool. It is recommended to set percent_high to 0 so that data migration begins immediately
   - percent_low sets the value at which migration to the tape pool stops. It is recommended to set percent_low to 0 to clear out the disk pool.
On a TSM server, create a disk volume (or volumes) and assign it to the disk pool.

```bash
define volume BycastDiskPool volume_name formatsize=size
```

- `BycastDiskPool` is the disk pool name.
- `volume_name` is the full path to the location of the volume (for example `/var/local/arc/stage6.dsm`) on the TSM server where it writes the contents of the disk pool in preparation for transfer to tape.
- `size` is the size, in MB, of the disk volume.

For example, to create a single disk volume such that the contents of a disk pool fill a single tape, set the value of `size` to 200000 when the tape volume has a capacity of 200 GB.

However, it might be desirable to create multiple disk volumes of a smaller size, as the TSM server can write to each volume in the disk pool. For example, if the tape size is 250 GB, create 25 disk volumes with a size of 10 GB (10000) each.

The TSM server preallocates space in the directory for the disk volume. This can take some time to complete (more than three hours for a 200 GB disk volume).

### Defining a domain policy and registering a node

You need to define a domain policy that uses the TSM management class for the data saved from the Archive Node, and then register a node to use this domain policy.

**Note:** Archive Node processes can leak memory if the client password for the Archive Node in Tivoli Storage Manager (TSM) expires. Ensure that the TSM server is configured so the client username/password for the Archive Node never expires.

When registering a node on the TSM server for the use of the Archive Node (or updating an existing node), you must specify the number of mount points that the node can use for write operations by specifying the MAXNUMMP parameter to the REGISTER NODE command. The number of mount points is typically equivalent to the number of tape drive heads allocated to the Archive Node. The number specified for MAXNUMMP on the TSM server must be at least as large as the value set for the **ARC > Target > Configuration > Main > Maximum Store Sessions** for the Archive Node, which is set to a value of 0 or 1, as concurrent store sessions are not supported by the Archive Node.

The value of MAXSESSIONS set for the TSM server controls the maximum number of sessions that can be opened to the TSM server by all client applications. The value of MAXSESSIONS specified on the TSM must be at least as large as the value specified for **ARC > Target > Configuration > Main > Number of Sessions** in the NMS for the Archive Node. The Archive Node concurrently creates at most one session per mount point plus a small number (< 5) of additional sessions.

The TSM node assigned to the Archive Node uses a custom domain policy `tsm-domain`. The `tsm-domain` domain policy is a modified version of the “standard” domain policy, configured to write to tape and with the archive destination set to be the StorageGRID Webscale system’s storage pool (`BycastDiskPool`).

**Note:** You must log in to the TSM server with administrative privileges and use the dsmadmc tool to create and activate the domain policy.

### Creating and activating the domain policy

You must create a domain policy and then activate it to configure the TSM server to save data sent from the Archive Node.

**Steps**

1. Create a domain policy.

```bash
copy domain standard tsm-domain
```
2. If you are not using an existing management class, enter one of the following:
   
   ```
   define policyset tsm-domain standard
   define mgmtclass tsm-domain standard default
   ```

   `default` is the default management class for the deployment.

3. Create a copygroup to the appropriate storage pool. Enter (on one line):
   
   ```
   define copygroup tsm-domain standard default type=archive
   destination=BycastDiskPool retinit=event retmin=0 retver=0
   ```

   `default` is the default Management Class for the Archive Node. The values of retinit, retmin, and retver have been chosen to reflect the retention behavior currently used by the Archive Node.

   **Note:** Do not set retinit to retinit=create. Setting retinit=create blocks the Archive Node from deleting content since retention events are used to remove content from the TSM server.

4. Assign the management class to be the default.
   
   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Set the new policy set as active.
   
   ```
   activate policyset tsm-domain standard
   ```

   Ignore the “no backup copy group” warning that appears when you enter the activate command.

6. Register a node to use the new policy set on the TSM server. On the TSM server, enter (on one line):
   
   ```
   register node arc-user arc-password passexp=0 domain=tsm-domain
   MAXNUMMP=number-of-sessions
   ```

   arc-user and arc-password are same client node name and password as you define on the Archive Node, and the value of MAXNUMMP is set to the number of tape drives reserved for Archive Node store sessions.

   **Note:** By default, registering a node creates an administrative user ID with client owner authority, with the password defined for the node.
Glossary

ACL
Access control list. Specifies which users or groups of users are allowed to access an object and what operations are permitted, for example, read, write, and execute.

active-backup mode
A method for bonding two physical ports together for redundancy.

ADC service
Administrative Domain Controller. The ADC service maintains topology information, provides authentication services, and responds to queries from the LDR, CMN, and CLB services. The ADC service is present on each of the first three Storage Nodes installed at a site.

ADE
Asynchronous Distributed Environment. Proprietary development environment used as a framework for services within the StorageGRID Webscale system.

Admin Node
The Admin Node provides services for the web interface, system configuration, and audit logs. See also, primary Admin Node.

Amazon S3
Proprietary web service from Amazon for the storage and retrieval of data.

AMS service
Audit Management System. The AMS service monitors and logs all audited system events and transactions to a text log file. The AMS service is present on the Admin Node.

API Gateway Node
An API Gateway Node provides load balancing functionality to the StorageGRID Webscale system and is used to distribute the workload when multiple client applications are performing ingest and retrieval operations. API Gateway Nodes include a Connection Load Balancer (CLB) service.

ARC service
Archive. The ARC service provides the management interface with which you configure connections to external archival storage such as the cloud through an S3 interface or tape through TSM middleware. The ARC service is present on the Archive Node.

Archive Node
The Archive Node manages the archiving of object data to an external archival storage system.

atom
Atoms are the lowest level component of the container data structure, and generally encode a single piece of information.

audit message
Information about an event occurring in the StorageGRID Webscale system that is captured and logged to a file.

Base64
A standardized data encoding algorithm that enables 8-bit data to be converted into a format that uses a smaller character set, enabling it to safely pass through legacy systems
that can process only basic (low order) ASCII text excluding control characters. See RFC 2045 for more details.

**bundle**
A structured collection of configuration information used internally by various components of the StorageGRID Webscale system. Bundles are structured in container format.

**Cassandra**
An open-source database that is scalable and distributed, provides high availability, and handles large amounts of data across multiple servers.

**CBID**
Content Block Identifier. A unique internal identifier of a piece of content within the StorageGRID Webscale system.

**CDMI**
Cloud Data Management Interface. An industry-standard defined by SNIA that includes a RESTful interface for object storage. For more information, see [www.snia.org/cdmi](http://www.snia.org/cdmi).

**CIDR**
Classless Inter-Domain Routing. A notation used to compactly describe a subnet mask used to define a range of IP addresses. In CIDR notation, the subnet mask is expressed as an IP address in dotted decimal notation, followed by a slash and the number of bits in the subnet. For example, 192.0.2.0/24.

**CLB service**
Connection Load Balancer. The CLB service provides a gateway into the StorageGRID Webscale system for client applications connecting through HTTP. The CLB service is part of the API Gateway Node.

**Cloud Data Management Interface**
See **CDMI**.

**CMN service**
Configuration Management Node. The CMN service manages system-wide configurations and grid tasks. The CMN service is present on the primary Admin Node.

**CMS service**
Content Management System. The CMS service carries out the operations of the active ILM policy’s ILM rules, determining how object data is protected over time. The CMS service is present on the Storage Node.

**command**
In HTTP, an instruction in the request header such as GET, HEAD, DELETE, OPTIONS, POST, or PUT. Also known as an HTTP method.

**container**
Created when an object is split into segments. A container object lists the header information for all segments of the split object and is used by the LDR service to assemble the segmented object when it is retrieved by a client application.

**content block ID**
See **CBID**.

**content handle**
See **UUID**.

**CSTR**
Null-terminated, variable-length string.
DC
Data Center site.

**DDS service**
Distributed Data Store. The DDS service interfaces with the distributed key-value store and manages object metadata. It distributes metadata copies to multiple instances of the distributed key-value store so that metadata is always protected against loss.

**distributed key value store**
Data storage and retrieval that unlike a traditional relational database manages data across grid nodes.

**DNS**
Domain Name System.

**enablement layer**
Used during installation to customize the Linux operating system installed on each grid node. Only the packages needed to support the services hosted on the grid node are retained, which minimizes the overall footprint occupied by the operating system and maximizes the security of each grid node.

**Fibre Channel**
A networking technology primarily used for storage.

**Grid ID signed text block**
A Base64 encoded block of cryptographically signed data that contains the grid ID. See also, provisioning.

**grid node**
The basic software building block for the StorageGRID Webscale system, for example, Admin Node or Storage Node. Each grid node type consists of a set of services that perform a specialized set of tasks.

**grid task**
System-wide scripts used to trigger various actions that implement specific changes to the StorageGRID Webscale system. For example, most maintenance and expansion procedures involve running grid tasks. Grid tasks are typically long-term operations that span many entities within the StorageGRID Webscale system. See also, Task Signed Text Block.

**ILM**
Information Lifecycle Management. A process of managing content storage location and duration based on content value, cost of storage, performance access, regulatory compliance, and other factors. See also, Admin Node and storage pool.

**LACP**
Link Aggregation Control Protocol. A method for bundling two or more physical ports together to form a single logical channel.

**LAN**
Local Area Network. A network of interconnected computers that is restricted to a small area, such as a building or campus. A LAN can be considered a node to the Internet or other wide area network.

**latency**
Time duration for processing a transaction or transmitting a unit of data from end to end. When evaluating system performance, both throughput and latency need to be considered. See also, throughput.
**LDR service**

Local Distribution Router. The LDR service manages the storage and transfer of content within the StorageGRID Webscale system. The LDR service is present on the Storage Node.

**LUN**

See *object store*.

**mDNS**

Multicast Domain Name System. A system for resolving IP addresses in a small network where no DNS server has been installed.

**metadata**

Information related to or describing an object stored in the StorageGRID Webscale system; for example, ingest time.

**MLAG**

Multi-Chassis Link Aggregation Group. A type of link aggregation group that uses two (and sometimes more) switches to provide redundancy in case one of the switches fails.

**MTU**

Maximum transmission unit. The largest size packet or frame that can be sent in any transmission.

**namespace**

A set whose elements are unique names. There is no guarantee that a name in one namespace is not repeated in a different namespace.

**nearline**

A term describing data storage that is neither “online” (implies that it is instantly available, like spinning disk) nor “offline” (which can include offsite storage media). An example of a nearline data storage location is a tape that is loaded in a tape library, but is not mounted.

**NFS**

Network File System. A protocol (developed by SUN Microsystems) that enables access to network files as if they were on local disks.

**NMS service**

Network Management System. The NMS service provides a web-based interface for managing and monitoring the StorageGRID Webscale system. The NMS service is present on the Admin Node. See also, *Admin Node*.

**node ID**

An identification number assigned to a service within the StorageGRID Webscale system. Each service (such as an NMS service or ADC service) must have a unique node ID. The number is set during system configuration and tied to authentication certificates.

**NTP**

Network Time Protocol. A protocol used to synchronize distributed clocks over a variable latency network, such as the Internet.

**object**

An artificial construct used to describe a system that divides content into data and metadata.

**object segmentation**

A StorageGRID Webscale process that splits a large object into a collection of small objects (segments) and creates a segment container to track the collection. The segment container contains the UUID for the collection of small objects as well as the header.
information for each small object in the collection. All of the small objects in the collection are the same size. See also, segment container.

**object storage**
An approach to storing data where the data is accessed by unique identifiers and not by a user-defined hierarchy of directories and files. Each object has both data (for example, a picture) and metadata (for example, the date the picture was taken). Object storage operations act on entire objects as opposed to reading and writing bytes as is commonly done with files, and provided via APIs or HTTP instead of NAS (CIFS/NFS) or block protocols (iSCSI/FC/FCOE).

**object store**
A configured file system on a disk volume. The configuration includes a specific directory structure and resources initialized at system installation.

**OID**
Object Identifier. The unique identifier of an object.

**primary Admin Node**
Admin Node that hosts the CMN service. Each StorageGRID Webscale system has only one primary Admin Node. See also, Admin Node.

**provisioning**
The process of generating a new or updated Recovery Package and GPT repository. See also, SAID.

**quorum**
A simple majority: 50% + 1. Some system functionality requires a quorum of the total number of a particular service type.

**Recovery Package**
A .zip file containing deployment-specific files and software needed to install, expand, upgrade, and maintain a StorageGRID Webscale system. The package also contains system-specific configuration and integration information, including server hostnames and IP addresses, and highly confidential passwords needed during system maintenance, upgrade, and expansion. See also, SAID.

**SAID**
Software Activation and Integration Data. The component in the Recovery Package that includes the *Passwords.txt* file.

**SATA**
Serial Advanced Technology Attachment. A connection technology used to connect server and storage devices.

**SCSI**
Small Computer System Interface. A connection technology used to connect servers and peripheral devices, such as storage systems.

**segment container**
An object created by the StorageGRID Webscale system during the segmentation process. Object segmentation splits a large object into a collection of small objects (segments) and creates a segment container to track the collection. A segment container contains the UUID for the collection of segmented objects as well as the header information for each segment in the collection. When assembled, the collection of segments creates the original object. See also, object segmentation.

**server**
Used when specifically referring to hardware. Might also refer to a virtual machine.
service
A unit of the StorageGRID Webscale system, such as the ADC service, NMS service, or SSM service. Each service performs unique tasks critical to the normal operations of a StorageGRID Webscale system.

SQL
Structured Query Language. An industry-standard interface language for managing relational databases. An SQL database is one that supports the SQL interface.

ssh
Secure Shell. A UNIX shell program and supporting protocols used to log in to a remote computer and run commands over an authenticated and encrypted channel.

SSL
Secure Socket Layer. The original cryptographic protocol used to enable secure communications over the Internet. See also, TLS.

SSM service
Server Status Monitor. A component of the StorageGRID Webscale software that monitors hardware conditions and reports to the NMS service. Every grid node runs an instance of the SSM service.

Storage Node
The Storage Node provides storage capacity and services to store, move, verify, and retrieve objects stored on disks.

storage pool
The element of an ILM rule that determines the location where an object is stored.

storage volume
See object store

StorageGRID
A registered trademark of NetApp, Inc., used for an object storage grid architecture and software system.

Task Signed Text Block
A Base64 encoded block of cryptographically signed data that provides the set of instructions that define a grid task.

TCP/IP

throughput
The amount of data that can be transmitted or the number of transactions that can be processed by a system or subsystem in a given period of time. See also, latency.

Tivoli Storage Manager
IBM storage middleware product that manages storage and retrieval of data from removable storage resources.

TLS
Transport Layer Security. A cryptographic protocol used to enable secure communications over the Internet. See RFC 2246 for more details.

transfer syntax
The parameters, such as the byte order and compression method, needed to exchange data between systems.
URI
Universal Resource Identifier. A generic set of all names or addresses used to refer to resources that can be served from a computer system. These addresses are represented as short text strings.

UTC
A language-independent international abbreviation, UTC is neither English nor French. It means both “Coordinated Universal Time” and “Temps Universel Coordonné.” UTC refers to the standard time common to every place in the world.

UUID
Universally Unique Identifier. Unique identifier for each piece of content in the StorageGRID Webscale system. UUIDs provide client applications with a content handle that permits them to access content in a way that does not interfere with the StorageGRID Webscale system’s management of that same content. A 128-bit number that is guaranteed to be unique. See RFC 4122 for more details.

virtual machine (VM)
A software platform that enables the installation of an operating system and software, substituting for a physical server and permitting the sharing of physical server resources among several virtual servers.

VLAN
Virtual local area network (or virtual LAN). A group of devices that are located on different LAN segments but are configured to communicate as if they were attached to the same network switch.

WAN
Wide area network. A network of interconnected computers that covers a large geographic area, such as a country.

XFS
A scalable, high-performance journaled file system originally developed by Silicon Graphics.

XML
Extensible Markup Language. A text format for the extensible representation of structured information; classified by type and managed like a database. XML has the advantages of being verifiable, human readable, and easily interchangeable between different systems.
Copyright information

Copyright © 1994–2017 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).
Trademark information

Active IQ, AltaVault, Arch Design, ASUP, AutoSupport, Campaign Express, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Element, Fitness, Flash Accel, Flash Cache, Flash Pool, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, Fueled by SolidFire, GetSuccessful, Helix Design, LockVault, Manage ONTAP, MetroCluster, MultiStore, NetApp, NetApp Insight, OnCommand, ONTAP, ONTAP, RAID DP, RAID-TEC, SANscreen, SANshare, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, SolidFire, SolidFire Helix, StorageGRID, SyncMirror, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

• NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
• Telephone: +1 (408) 822-6000
• Fax: +1 (408) 822-4501
• Support telephone: +1 (888) 463-8277
Index

/etc/fstab file 123

A

aborting grid tasks
  procedure for 193
accounts, group
  deleting 184
accounts, user
  adding 185
  creating 185
  deleting 186
Acknowledge Alarms permission 179
Active Directory
  adding users or groups to audit share 165
  audit clients 162
  changing audit client share user or group name 168
  configuring audit clients 162
  removing users from audit share 167
ADC service 111
add-audit-share command, in config_cifs.rb 160, 162
add-ip-to-share command, in config_nfs.rb 170
add-user-to-share command 165
add-user-to-share command in config_cifs.rb 165
add-user-to-share command, in config_cifs.rb 160
adding
  Storage Nodes 117
  storage volumes 117
admin groups
  managing 175
  permissions 179
Admin Node
  changing display name 149
  defined 146
  passwordless access 155
  redundancy 147
admin users
  managing 175
Administrative Domain Controller
  See ADC
AES-128 119
AES-256 119
alarms
  acknowledgments 147
  by code
    SAVP Total Usable Space (Percent) 113
    SSTS Storage Status 113
  class overrides 40
  clearing triggered alarms 49
  configuring email notifications 28
  creating custom alarms 40
  creating email mailing lists 30
  creating Global Custom alarms 42
  custom 37
  custom notification migration 200
  customizing alarms 34
  default 35
  disabling 44
  disabling default alarms 45, 46
  disabling Global Custom alarms, service level 47
  disabling Global Custom alarms, system wide 48
  email notifications 26
  examples of how triggered 37
  Global Custom 36
  monitoring 37
  new services 40
  notifications 26, 27
  of same severity 39
  overriding higher priority alarm 40
  severity changes 40
  table, displayed in 45
  triggering evaluation order 37
  triggering logic 37
  types 35
  viewing default 35
All Storage Nodes storage pool 69
API
  management 15
API Gateway Node
  description of 130
appliance
  viewing events 59
  viewing Storage Nodes 54
ARC
  archive read-only on startup 143
  archive store state 143
  configuration
    Target component 136
  description of service 131
  optimizing for Tivoli Storage Manager 138
  resetting store failure count 143, 144
  retrieve component 142
  Tivoli Storage Manager
    unavailable 139
archive
  read-only on startup 143
  retrieve state 142
  store set 143, 144
Archive Node
  capacity, full 140
  configurations described 213
  configure replication settings 141
  configure target 132
  configuring cloud connections 133
  configuring S3 connections 133
  description 131
  destination 132
  optimizing for Tivoli Storage Manager middleware 138–140
  setting custom alarms 144
  target 132
attributes
  by code
    BQUZ Awaiting - Background Scan 107
    CQUZ Awaiting - Client 107
    EVRT Awaiting - Evaluation Rate 107
    ILMN ILM Implementation 107
ILMV ILM Version 107
QUSZ Awaiting - All 107
REPA Repairs Attempted 107
ROMK Hard Read-Only Watermark 113
SCRT Scan Rate 107
SCTM Scan Period - Estimated 107
SSCR Storage Status - Current 113
STAS Total Usable Space 111
VHWM Storage Volume Soft Read-Only Watermark 113
VROM Storage Volume Hard Read-Only Watermark 113
XCQZ Awaiting - Client 199
XQUZ Awaiting - All 199

by name
Awaiting - All (QUSZ) 107
Awaiting - All (XQUZ) 199
Awaiting - Background Scan (BQUZ) 107
Awaiting - Client (CQUZ) 107
Awaiting - Client (XCQZ) 199
Awaiting - Evaluation Rate (EVRT) 107
Hard Read-Only Watermark ROMK 113
ILM Implementation (ILMN) 107
ILM Version (ILMV) 107
Repairs Attempted (REPA) 107
Scan Period - Estimated (SCTM) 107
Scan Rate (SCRT) 107
Storage Status - Current SSCR 113
Storage Volume Soft Read-Only Watermark 113
Total Usable Space STAS 111

described 9

audit client configuration
CIFS, Active Directory 162
CIFS, Windows Workgroup 160
NFS 169

AutoSupport
described 49
disabling 51
preferred sender 148
sending 50
triggering 50
troubleshooting 51

B
background verification
adaptive 126
configuring 126
high verification priority 126
LDR 126
priority 126
reset corrupt objects count 114
verification priority 114
Baseline 2 Copy Rule policy 61
browsers
changing inactivity timeout period 14
supported 11

C
capacity

Archive Node 140
of storage 111
Cassandra database
node tool repair 110
CBID
defined 88
obtain 88
CDMI
effect of Prevent Client Modify option 122
CDMI data object ID 88
certificate authority (CA) certificates
copying for StorageGRID Webscale system 158
Change Tenant Root Password permission 179
changing password for tenant accounts 179
CIFS
audit file share configuration 160
audit share 160
CIFS audit share
adding groups 165
adding users 165
CLB service
defined 130
client file shares
CIFS
audit directory, AD 162
configuring audit clients 160
CIFS audit share
changing group name 168
changing user name 168
removing users 167
NFS audit share
adding clients 170
changing client IP address 173
CMN service
defined 146
CMS service
described 110
command shell
accessing 202
logging in 202
logging out 202
comments
how to send feedback about documentation 228
components
described 9
compression
lossless 121
configuring
Archive Node 133, 213
configuring identity federation 175
content block identifier
See CBID
content placement instructions 74
content protection
security partition 124
content verification 126
corrupt objects 114
CPU status 52
creating tenant accounts 19
custom alarms
creating 40
triggering logic 37
Dashboard described 9

data center topology, example ILM policy 97, 100, 103
data migration
  attributes, monitoring
    ARVF 199
    Awaiting - All (XQUZ) 199
    Awaiting - Client (XCQZ) 199
  creating custom alarms 200
  grid capacity, check 198
  ILM policy 198
  impact on grid operations 199
  notifications 200
  schedule time of day 199

Data Store
  ILM Activity statistics 107
  Object Deleting statistics 107
  Object Transfer statistics 107

DDS service
  described 109
  object count 109
  object metadata 110
  queries 110

default alarms
  disable 45
  triggering logic 37

deleting tenant accounts 25

Device Model ID 149
Device Model Version 149
disable inbound replication 114
disable outbound replication 114
disabling identity federation 179
documentation
  how to receive automatic notification of changes to 228
  how to send feedback about 228
domain policy
  activating for TSM 217
  creating for TSM 217

DoNotStart file
  creating for individual service 209
  defined 209
  remove for service 210

Dual Commit 66

severity level in notifications 26
suppressing for entire system 33
suppressing for mailing lists 32
template 29
test email 28

email server
  configuring 28
email template 29
encryption
  disabling 119
  network transfer 154

erasure codes, storage pool 62
erasure coding
  configure 72
error state 212
eth0 151
eth1 151
eth2 151
events
  alarms 26
  events, hardware
    viewing 59
example policies 97, 100, 103
examples
  alarm triggering 37

failed grid tasks
  types of status shown in Historical table 196

feedback
  how to send comments about documentation 228

file system
  UUID 123

force-stop 207

foreground verification
  missing replicated object data 128

Global Custom alarms
  creating 42
  disabling 47
  disabling for entire system 48
  triggering logic 37

grid capacity
  data migration 198

grid configuration
  network transfer encryption 154
  Prevent Client Modify option 122

Grid Management Interface
  customizing server certificates 156
  described 9
  restoring server certificates 157
  signing in 12
  signing out 13

Grid network IP addresses 150

grid node
  IP address 150

grid nodes
  described 9
  monitor 52

editing tenant accounts 24

email notifications
  configure global notification 31
  configuring email server 28
  create global notification 31
  create mailing lists 30
  create templates 29
  description 26
  events 27
  for alarms 40
  islanded Admin Nodes 33
  mail server settings 28
  preferred sender 33, 148
  service state notifications 26
reboot 208
viewing appliance 54
grid tasks
  aborting 193
  active 188
  cancelling 192
  description 188
  historical 188
  LDR foreground verification 128
  managing 188
  monitoring 188
  pausing 191
  pending 188
  progress 188
  reasons for failure 196
  removing from the Historical table 195
  resuming 192
  running 190
  status 188
  task signed text block 194
  troubleshooting 196, 197
Grid Topology Page Configuration permission 179
Grid Topology tree
  described 9
grids
  access permissions 179
groups
  authenticating with identity federation 175
  changing 184
  creating 183
  deleting 184
  updating 184
groups, in ILM policies 62
GUI Inactivity Timeout
  updating 14
H
hardware
  viewing events 59
hashing, stored object 120
health check timeout
  LDR 114
historical ILM policies 93
Historical table
  status of failed grid tasks 196
HSTE
HTTP/CDMI State 114
HTTP
  auto-start 114
HTTP/CDMI State, set 114
HTTPS connections
  copying CA certificates 158
I
identity federation
  configuring 175
  configuring OpenLDAP for 178
  disabling 179
  synchronization of identity source 178
identity source
  forcing synchronization of 178
ILM
  Activity statistics 107
  content placement instructions 74
defined 62
  Dual Commit 66
evaluation logic 61
  example policies for simulating 82
  example rules and policy for EC object size filtering 98
  example rules and policy for image files 101
  example rules and policy for object storage 94
  filters 64, 74
groups 62
  historical policies 93
  Last Access Time 74
  metadata 64
  object identifier 88
  object not referenced by API 66
  overview 61
  policies
    activating 87
    configuring 79
    example policies 97, 100, 103
    historical policies 93
    order of rules 79
    simulating 81
    simulation examples 82, 84, 86
    verifying 88
    view historical 93
    viewing activity queue 94
reference time
  ingest time 74
  Last Access Time 74
rules
  cloning 92
  content placement instructions 74
  creating 74, 92
  deleting 91
  editing 91
  examples 95, 96, 98, 99, 101, 102
  Last Access Time 74
  Make 2 Copies rule 69
  modifying 91
storage 62, 67
  grade
    assign to LDR 67
    configuring 62, 67
  locations 62
  pools
    built-in 69
    configure 69
guidelines 69
  view existing 72
time values 74
ILM criteria evaluation 64
ILM policy
  activating 87
  configuring 79
  example for EC object size filtering 98
  example for image files 101
  example for object storage 94
  examples for simulating 82
order of rules 79
simulating 81
verifying 88
viewing activity queue 94

ILM rules
archival media 131
default rule 79
elements 95, 96, 98, 99, 101, 102
examples for EC object size filtering 98
examples for image files 101
examples for object storage 94
last access time 74
order of 79

inactivity timeout
changing 14

information
how to send feedback about improving
documentation 228

Interface Engine page
NMS service 27

IP address
Grid network 150
supplementary network 150
view 151

J
join-domain command, in config_cifs.rb 162

L
last access time
ILM rules 74
Last Access Time 74
LDR
assign storage grade 67
background verification 114
configuration
Storage component 114
content balancing 107
corrupt objects 114
Data Store 107
encryption 114
full 126
health check timeout 114
HTTP/CDMI State 114
monitor available space 111
object mapping 107
object stores 107
replication 114
reset missing copies count, erasure coding 114
reset read failures, erasure coding 114
reset write failures, erasure coding 114
service 105
storage grade 67
storage state-desired 114
verification 126
volume ID 107

license
updating 15
viewing details for 15

link costs

default values 153
updating 153

lists, mailing
suppressing email notifications from 32

Local Distribution Router service
See LDR

log files
servermanager.log 211
logging in
Grid Management Interface 12
logging out
Grid Management Interface 13

M
mailing lists
suppressing email notifications from 32

Maintenance permission 179
Make 2 Copies rule, ILM 61, 69
management API
overview 15
management class, Tivoli Storage Manager 132
metadata
in ILM rules 64

MIB
OID values 152
SNMP 152

MINS E-mail Notification Status alarm 27
monitoring
storage 118
storage capacity per Storage Node 118
system capacity
system-wide 118

N
NetBIOS name
file share configuration 162
network connections
viewing for appliance 54
network transfer encryption
disable 154
enable 154

NFS audit share
removing clients 172
verifying integration 172

NFS share configuration
adding client to an audit share 170
changing client IP address 173
configure the audit client 169
removing client from the audit share 172

NMS entities
device model ID 149
device model version 149
language 149
name 149
OID 149
settings 149

NMS service
defined 146
Interface Engine page 27

nodetool repair
Storage Nodes 110

notifications
  configuring 27
  suppressing for entire system 33
  suppressing for mailing lists 32

O

object count
  DDS service 109
object data
  corrupt 126
  missing 126, 128
  verify 128
  verify integrity 126
object lookup
  view 88
object metadata
  DDS service 110
object not referenced by API 66
object segmentation 125
object store
  volume ID 107
object stores 107
OID
  defined 149
  values 152
OpenLDAP
  configuration guidelines for 178
optimizing performance, middleware sessions
  Tivoli Storage Manager 132
optimizing storage 125
ORLM 88
Other Grid Configuration permission 179

P

password for tenant account 19
passwordless access, ssh 155
passwords
  changing 13
  changing for others 186
  changing for tenant account’s root user 24
permissions
  setting for groups 183
policies
  activating 78, 87
  baseline 61
  configuring 78, 79
  migrated data 198
  order of rules 79
  simulating 81
  verifying 78, 88
preferred sender, notifications 33
Prevent Client Modify
  effect of enabling 122
primary Admin Node
  passwordless access 155
product overview 8

R

RAM usage 52
reboot
  grid node 208
remove-ip-from-share command, in config_nfs.rb 172
remove-user-from-share command, in config_cifs.rb 167
removing tenant accounts 25
reset counters
  CDMI counts 114
  HTTP counts 114
  inbound replication failure count 114
  outbound replication failure count 114
  SSM events 53
resetting corrupt objects count 114
resetting missing copies count, erasure coding 114
resetting read failure count 114
resetting writes failure count 114
reties, grid task
  troubleshooting 196
Root Access permission 179
root user 179
rules
  Make 2 Copies rule 61

S

S3
  effect of Prevent Client Modify option 122
  modify Archive Node settings 135
  modifying Cloud Tiering Service 136
  modifying settings 135
  obtaining bucket/key 88
  tenant account for 19
SA VP Total Usable Space (Percent)
  alarm 113
scripts
  servermanager restart 205
  servermanager start 204
  servermanager stop 205
security
  StorageGRID Webscale CA certificate 158
security partitions 124
server certificates
  copying 158
  customizing for Grid Management Interface 156
  restoring for Grid Management Interface 157
  storage API endpoints
    configuring 157
    restoring 158
Server Connection Error 27
Server Manager
  accessing remotely 202
  capabilities 202
  current status 202
  individual service, current status 206
  overview 202
  power down server 209
  remote access 202
  restart 205
  scripts
    service, terminate 207
    terminate service 207
services, current status 203
services, restart all 205
services, start all 204
services, stop individual 206, 208
start services 204
start, manually 204
troubleshooting
error state 212
version 202
Server Status Monitor
See SSM
servermanager.log 211
servers
power down 209
service
status 203, 206
stop 206
services
creating alarms 40
described 9
disable Global Custom alarm 47
disabling default alarms 44, 45
restarting 208
stop 205
terminate 207
set-authentication command, in config_cifs.rb 160, 162
setting custom Archive Node 144
share configuration
add-audit-share command 160, 162
add-ip-to-share command 170
add-user-to-share command 160
audit share (CIFS) 160
audit share (NFS) 169
join-domain command 162
NetBIOS name 162
remove-ip-from-share command 172
remove-user-from-share command 167
set-authentication command 160, 162
signing in
Grid Management Interface 12
signing out
Grid Management Interface 13
Simple Storage Service 132
SMTP mail server settings 28
SNMP
agent 152
configure 152
system status 152
SNMP monitoring
configure 152
MIB 152
OID 152
SNMPv2c 152
SSCR Storage Status - Current 113
ssh
passwordless access 155
private key 155
SSM
components
events 53
resources 53
timing 54
configuration
Resources component 53
reset event counters 53
services 52
SSTS Storage Status alarm 113
STAS Total Usable Space
attribute 111
status
grid tasks 188
of failed grid tasks 196
storage
background verification 126
calculate capacity 111
ILM 62, 67
storage capacity
monitoring per Storage Node 118
monitoring system-wide 118
watermarks 113
storage grade
assign to LDR 67
configuring 67
creating a list 67
Storage Node
background verification 126
cryptography 119
foreground verification 126, 128
LDR 107
nodetool repair 110
object mapping 107
viewing appliance information 54
watermarks 113
storage pools
configure 69
ILM 62, 67
view existing 72
Storage Status - Current SSCR 113
Storage Status SSTS alarm 113
StorageGRID Webscale system
copying CA certificates 158
defined 8
stored object
configuring encryption 119
configuring hashing 120
enabling compression 121
suggestions
how to send feedback about documentation 228
supplementary network IP addresses 150
Swift clients
effect of Prevent Client Modify option 122
tenant account for 19
synchronization
identity source 178
system events 26
system status
OID 152
SNMP 152
T
template 29
tenant accounts
changing password for root user 24
creating 19
deleting 25
U

user accounts
  adding 185
  changing password 13
  creating 185
  deleting 186
  modifying 185
  permissions 13, 182
users
  authenticating with identity federation 175
  changing passwords for 186
UUID
  obtaining 88

V

verifying
  CIFS audit integration 168
version information 52
volume ID 107

W

watermarks
  view values 113
web browsers
  signing in 12
  signing out 13
  supported 11
Workgroup share configuration
  adding users or groups to audit share 165
  audit clients 160
  changing audit client share user or group name 168
  removing user from audit share 167