Contents

Understanding the StorageGRID Webscale system ................................. 10
  What the StorageGRID Webscale system is ........................................ 10
  Working with the StorageGRID Webscale system .............................. 11
  Signing in to the NMS MI ................................................................. 13
  Signing out of the NMS MI ............................................................. 15
  Changing the NMS MI timeout period ............................................... 15
Managing storage tenant accounts ....................................................... 17
  Managing S3 tenant accounts ......................................................... 17
    Creating tenant accounts for S3 .................................................... 17
    Editing tenant accounts for S3 ...................................................... 18
    Editing group policies for S3 tenant accounts ............................... 18
    Editing S3 Root Keys for S3 tenant accounts ................................. 23
  Managing Swift tenant accounts ..................................................... 24
    Creating tenant accounts for Swift ................................................. 24
    Editing tenant accounts for Swift ................................................ 25
    Editing group policies for Swift tenant accounts ............................ 25
  Deleting tenant accounts ............................................................... 26
  Configuring LDAP for identity federation ....................................... 26
  OpenLDAP server configuration guidelines ...................................... 27
  Disabling LDAP for identity federation ......................................... 28
  Manually forcing synchronization with the LDAP server ................. 28
  Managing federated user S3 credentials ......................................... 28
StorageGRID Webscale Management API Overview ............................. 29
Monitoring the StorageGRID Webscale system ..................................... 32
  About alarms and e-mail notifications ........................................... 32
    Notification types ................................................................. 32
    Notification status and queues ................................................ 33
    Configuring notifications ......................................................... 33
    Sending test e-mails ............................................................... 38
    Suppressing email notifications for a mailing list ....................... 39
    Suppressing e-mail notifications system wide ............................ 39
    Selecting a preferred sender .................................................... 40
    Configuring a custom alarm notification .................................... 41
  Alarms management ................................................................. 41
    Alarm class types ................................................................. 42
    Alarm triggering logic ............................................................ 43
    Creating custom alarms .......................................................... 47
    Creating global custom alarms ................................................. 49
  Disabling alarms ................................................................. 51
  Alarms and tables ................................................................. 51
  Disabling default alarms for services ........................................... 51
Disabling default alarms system wide ........................................................... 52
Disabling global custom alarms for services ................................................. 52
Disabling global custom alarms system wide ............................................... 53
Clearing triggered alarms .............................................................................. 53

What AutoSupport is ................................................................................................. 54
Triggering AutoSupport messages ................................................................ 55
Disabling weekly AutoSupport messages ..................................................... 55
Troubleshooting AutoSupport ....................................................................... 56

Monitoring servers and grid nodes ................................................................. 56
What is the SSM service ............................................................................... 56
Monitoring StorageGRID Webscale Appliance Storage Nodes ................. 58

What information lifecycle management is ......................................................... 63
What an information lifecycle management policy is ........................................ 63
Order of ILM rules within an ILM policy ....................................................... 63
ILM policy updates ....................................................................................... 65
ILM policy version numbers ......................................................................... 66

What information lifecycle management rules are ........................................... 66
Types of ILM rules ........................................................................................ 67
ILM rule version numbers ............................................................................. 68

Determining storage locations ......................................................................... 69
What an Erasure Coding profile is ................................................................. 70
Matching criteria and filter evaluation ........................................................... 72
StorageGRID API metadata tags ................................................................... 72
CDMI metadata tags ...................................................................................... 75
S3 metadata tags ............................................................................................ 75
Swift metadata tags ....................................................................................... 75
Specifying time values for metadata ............................................................. 76

Reference time .................................................................................................... 76
Enabling or disabling Last Access Time ......................................................... 77
Content placement instructions ..................................................................... 77
Storage pools ................................................................................................. 78
Temporary copies if storage pool unavailable .............................................. 78
Copy age ........................................................................................................ 79

Retention diagram .......................................................................................... 79
Dual Commit ..................................................................................................... 80
Object deletions and purging ......................................................................... 80
How deletion protection works ..................................................................... 80

Configuring information lifecycle policies and rules ..................................... 84
Configuring information lifecycle management rules and policy ................. 84
Configure storage grades ............................................................................... 84
Configuring storage pools ............................................................................. 87
Configuring Erasure Coding profiles ............................................................ 89
Creating an ILM rule ..................................................................................... 91
Configure and activate an ILM policy ........................................................... 94

Verifying ILM policy ........................................................................................ 96
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working with ILM rules and ILM policies</td>
<td>98</td>
</tr>
<tr>
<td>Modifying ILM rules</td>
<td>98</td>
</tr>
<tr>
<td>Copying and creating a new ILM rule</td>
<td>99</td>
</tr>
<tr>
<td>Deleting an ILM rule</td>
<td>99</td>
</tr>
<tr>
<td>Viewing historical ILM policies</td>
<td>100</td>
</tr>
<tr>
<td>Viewing the ILM policy activity queue</td>
<td>100</td>
</tr>
<tr>
<td>Setting alarms on the ILM activity queue</td>
<td>101</td>
</tr>
<tr>
<td>Evaluating existing objects against new ILM policy</td>
<td>102</td>
</tr>
<tr>
<td>Example ILM policies</td>
<td>103</td>
</tr>
<tr>
<td>Single data center site ILM policy</td>
<td>104</td>
</tr>
<tr>
<td>Data center + data center and archive ILM policy</td>
<td>104</td>
</tr>
<tr>
<td>Example ILM rules</td>
<td>105</td>
</tr>
<tr>
<td>ILM rule to delete objects based on age</td>
<td>105</td>
</tr>
<tr>
<td>ILM rule to make copies in two storage pools (DC only)</td>
<td>106</td>
</tr>
<tr>
<td>ILM rule to archive erasure coded object data</td>
<td>107</td>
</tr>
<tr>
<td>Managing disk storage</td>
<td>109</td>
</tr>
<tr>
<td>What a Storage Node is</td>
<td>109</td>
</tr>
<tr>
<td>What the LDR service is</td>
<td>109</td>
</tr>
<tr>
<td>What the DDS service is</td>
<td>110</td>
</tr>
<tr>
<td>CMS service</td>
<td>111</td>
</tr>
<tr>
<td>ADC service</td>
<td>111</td>
</tr>
<tr>
<td>What the nodetool repair operation is</td>
<td>112</td>
</tr>
<tr>
<td>Managing Storage Nodes</td>
<td>112</td>
</tr>
<tr>
<td>Object stores</td>
<td>112</td>
</tr>
<tr>
<td>Storage capacity</td>
<td>113</td>
</tr>
<tr>
<td>Watermarks</td>
<td>114</td>
</tr>
<tr>
<td>Storage Node configuration settings</td>
<td>115</td>
</tr>
<tr>
<td>Manage full Storage Nodes</td>
<td>118</td>
</tr>
<tr>
<td>Monitoring storage</td>
<td>119</td>
</tr>
<tr>
<td>Monitoring storage capacity system-wide</td>
<td>119</td>
</tr>
<tr>
<td>Monitoring storage capacity per Storage Node</td>
<td>119</td>
</tr>
<tr>
<td>Configure settings for stored objects</td>
<td>120</td>
</tr>
<tr>
<td>Configuring stored object encryption</td>
<td>120</td>
</tr>
<tr>
<td>Configuring stored object hashing</td>
<td>121</td>
</tr>
<tr>
<td>Configuring stored object compression</td>
<td>122</td>
</tr>
<tr>
<td>Mount storage devices</td>
<td>123</td>
</tr>
<tr>
<td>Security partitions</td>
<td>124</td>
</tr>
<tr>
<td>Tuning for object size</td>
<td>124</td>
</tr>
<tr>
<td>Recommended optimization settings</td>
<td>124</td>
</tr>
<tr>
<td>Configuring object segmentation</td>
<td>125</td>
</tr>
<tr>
<td>Verifying object integrity</td>
<td>126</td>
</tr>
<tr>
<td>What background verification is</td>
<td>126</td>
</tr>
<tr>
<td>Configuring the background verification rate</td>
<td>127</td>
</tr>
<tr>
<td>What foreground verification is</td>
<td>128</td>
</tr>
<tr>
<td>Running foreground verification</td>
<td>129</td>
</tr>
</tbody>
</table>
Managing archival storage ................................................................. 132
  What an Archive Node is ................................................................. 132
  What the ARC service is ............................................................... 132
  About supported archive targets .................................................... 133
Managing connections to archival storage ...................................................... 133
  Configuring connection settings for S3 API ....................................... 134
  Modifying connection settings for S3 API .......................................... 135
  Configuring connections to Tivoli Storage Manager middleware .......... 137
Managing Archive Nodes .......................................................................................................................... 139
  Optimizing Archive Node’s TSM middleware sessions ....................... 139
  Managing an Archive Node when TSM server reaches capacity .......... 140
  Configuring Archive Node replication ............................................. 141
  Configuring retrieve settings .......................................................... 142
  Configuring the archive store ........................................................... 143
  Set custom alarms for the Archive Node ........................................... 144
What an Admin Node is ........................................................................... 145
  Admin Node redundancy .................................................................... 146
  Alarm acknowledgments .................................................................... 146
  E-mail notifications and AutoSupport messages .................................. 147
  Changing the name of an Admin Node .............................................. 148
  NMS entities ...................................................................................... 148
  Changing an NMS entity name .......................................................... 149
Managing StorageGRID Webscale networking ............................................. 151
  Viewing IP addresses ........................................................................ 151
  Changing IP addresses ..................................................................... 152
  Enabling Domain Name Service globally ......................................... 155
    Modifying the DNS configuration for a single grid node ................. 155
  Configure SNMP monitoring ............................................................ 156
    Management Information Base file ................................................. 157
    Detailed registry ............................................................................. 157
  Network Time Protocol configurations .............................................. 157
    Updating the Network Time Protocol external sources list .............. 158
    Adding, removing, or updating Network Time Protocol sources ....... 158
  Link costs ........................................................................................ 159
    Updating link costs ...................................................................... 160
  Changing network transfer encryption .............................................. 160
  Customize the SSH access point ...................................................... 161
    Configuring passwordless SSH access .......................................... 162
    Adding or changing the SSH private key password ......................... 162
    Removing the SSH private key ....................................................... 163
  Support for IPv6 and IPv4 ................................................................. 163
Configuring audit client access ............................................................... 166
  Configuring audit clients for CIFS ................................................... 166
  Configuring audit clients for Workgroup ........................................... 166
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What Server Manager is</td>
<td>203</td>
</tr>
<tr>
<td>Using the Server Manager graphical or command-line interface</td>
<td>203</td>
</tr>
<tr>
<td>Navigating the Server Manager graphical interface</td>
<td>203</td>
</tr>
<tr>
<td>Header</td>
<td>204</td>
</tr>
<tr>
<td>Service list</td>
<td>204</td>
</tr>
<tr>
<td>Command buttons</td>
<td>205</td>
</tr>
<tr>
<td>Grid node identification</td>
<td>206</td>
</tr>
<tr>
<td>Initiating an action</td>
<td>206</td>
</tr>
<tr>
<td>Changing the Server Manager password</td>
<td>206</td>
</tr>
<tr>
<td>Server Manager command shell procedures</td>
<td>207</td>
</tr>
<tr>
<td>Status information</td>
<td>207</td>
</tr>
<tr>
<td>Starting Server Manager and all services manually</td>
<td>208</td>
</tr>
<tr>
<td>Restarting Server Manager and all services</td>
<td>209</td>
</tr>
<tr>
<td>Stopping Server Manager and all services</td>
<td>209</td>
</tr>
<tr>
<td>Stopping individual services</td>
<td>209</td>
</tr>
<tr>
<td>Forcing services to terminate</td>
<td>210</td>
</tr>
<tr>
<td>Restarting individual services</td>
<td>210</td>
</tr>
<tr>
<td>Rebooting servers</td>
<td>210</td>
</tr>
<tr>
<td>Powering down servers</td>
<td>210</td>
</tr>
<tr>
<td>Service dependencies</td>
<td>211</td>
</tr>
<tr>
<td>DoNotStart file</td>
<td>211</td>
</tr>
<tr>
<td>Troubleshooting Server Manager</td>
<td>213</td>
</tr>
<tr>
<td>Log files</td>
<td>213</td>
</tr>
<tr>
<td>Service fails to start</td>
<td>213</td>
</tr>
<tr>
<td>Error state</td>
<td>213</td>
</tr>
<tr>
<td>tomcat service</td>
<td>214</td>
</tr>
<tr>
<td>Grid Deployment Utility</td>
<td>215</td>
</tr>
<tr>
<td>Starting the Grid Deployment Utility</td>
<td>215</td>
</tr>
<tr>
<td>How to use the Grid Deployment Utility</td>
<td>216</td>
</tr>
<tr>
<td>Entering commands</td>
<td>217</td>
</tr>
<tr>
<td>Quitting the Grid Deployment Utility</td>
<td>218</td>
</tr>
<tr>
<td>Troubleshooting the Grid Deployment Utility</td>
<td>218</td>
</tr>
<tr>
<td>Copying ISO files in a multi-site environment</td>
<td>219</td>
</tr>
<tr>
<td>About load_cds.py</td>
<td>221</td>
</tr>
<tr>
<td>Provisioning</td>
<td>222</td>
</tr>
<tr>
<td>Manually exporting a provisioned grid specification file</td>
<td>222</td>
</tr>
<tr>
<td>Manually provisioning the StorageGRID Webscale system</td>
<td>223</td>
</tr>
<tr>
<td>Changing the provisioning passphrase</td>
<td>224</td>
</tr>
<tr>
<td>Provisioning command reference</td>
<td>225</td>
</tr>
<tr>
<td>Preserving copies of the provisioning data</td>
<td>226</td>
</tr>
<tr>
<td>Troubleshooting provisioning</td>
<td>226</td>
</tr>
<tr>
<td>Provision command fails</td>
<td>227</td>
</tr>
<tr>
<td>About the Software Activation and Integration Data package</td>
<td>227</td>
</tr>
<tr>
<td>Viewing grid configuration files</td>
<td>228</td>
</tr>
<tr>
<td>Grid specification files</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. As well as information on how to configure the StorageGRID Webscale system to meet a deployment's unique operational requirements.

This guide is not indented 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 10.2 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 virtualized 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 10.2 Grid Primer*

## Working with the StorageGRID Webscale system

Most day-to-day activities are performed through the NMS Management Interface (NMS MI), which is accessed through a web browser. Broken into panes, the NMS MI provides access to the various levels of system functionality.

For more information about the NMS MI and its functional areas, see the *Grid Primer*.

### Grid Management tree

The Grid Management tree provides access to a number of configuration settings. These configurations are restricted to user accounts with Maintenance and/or Grid Management permissions.

### Grid Topology tree

The Grid Topology tree provides access to StorageGRID Webscale system elements: sites, grid nodes, services, and components.
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 detail description of grid nodes, see the Grid Primer.

A service is a software module, which 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 detail description of services, see the Grid Primer.

A sub-group of each service that performs a particular function for that service.

<table>
<thead>
<tr>
<th>StorageGRID Webscale 10.2 Administrator Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grid nodes</td>
</tr>
<tr>
<td>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 detail description of grid nodes, see the Grid Primer.</td>
</tr>
<tr>
<td>Services</td>
</tr>
<tr>
<td>A service is a software module, which 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 detail description of services, see the Grid Primer.</td>
</tr>
<tr>
<td>Components</td>
</tr>
<tr>
<td>A sub-group of each service that performs a particular function for that service.</td>
</tr>
</tbody>
</table>
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.

StorageGRID Webscale NAS Bridge

The StorageGRID Webscale NAS Bridge provides the StorageGRID Webscale system with the capability to connect clients to the system through the NFS and SMB protocols. It is managed through its own user interface, separate from the StorageGRID Webscale system’s user interface.

Related information

- StorageGRID Webscale 10.2 Grid Primer
- StorageGRID Webscale NAS Bridge 2.0 Installation and Setup Guide
- StorageGRID Webscale NAS Bridge 2.0 Administration Guide
- StorageGRID Webscale NAS Bridge 2.0 Management API Guide

Signing in to the NMS MI

You access the NMS Management Interface (NMS MI) by signing in through a supported web browser using the web address or domain name defined by your system administrator.

Before you begin

- You must have an authorized user name and password. If signing in to the NMS MI for the first time, note the NMS MI password for the Vendor account or the Admin account as listed in the Passwords.txt file.
- Cookies must be enabled in your web browser.
• Acquire the IP address or domain name to the NMS MI. If signing in to the NMS MI for the first time, note the IP address of the Admin Node as listed in the Configuration.txt file.

• Acquire access to a supported web browser.
  The following browsers have been tested with the StorageGRID Webscale system to verify compatibility:
  ◦ Google Chrome 43
  ◦ Microsoft Internet Explorer 11.0
  ◦ Mozilla Firefox 38.0.5

About this task
When you sign in to the NMS MI, you are connecting to a data center site's Admin Node. In a multi-site StorageGRID Webscale deployment, each site may include an Admin Node. You can connect to any Admin Node and each Admin Node displays a similar view of the StorageGRID Webscale system; however, alarm acknowledgments made at one Admin Node are not copied to the other Admin Node. It is therefore possible that the Grid Topology tree will not look the same for each Admin Node.

The NMS MI uses a self-signed certificate based on the StorageGRID Webscale system’s IP address. The expected URL to the NMS MI is this IP address and not a domain name. In cases where a domain name is used to connect to the NMS MI, your browser might not be able to match the self-signed certificate to the identity of the NMS server. For information about importing this certificate into a browser, see the browser’s documentation.

Steps
1. Launch a supported web browser.
2. In the browser’s address bar, enter the IP address or domain name of the NMS MI.
3. If you are prompted with a security alert, do one of the following:
   • Proceed with this session. The alert will appear again the next time you access this URL.
   • View and install the certificate using the browser’s installation wizard. The alert will not appear the next time you access this URL.

The Network Management System Sign In page appears.

4. Enter your case-sensitive username and password and click Sign In.
The NMS MI appears.

Signing out of the NMS MI

When you have completed your NMS MI session, to keep the system secure, you must log out of the NMS MI.

Step

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

   The logging out message appears.

   **Note:** Failure to log out can give unauthorized users access to your NMS MI session. Simply closing your browser is not sufficient to log out of the session.

Changing the NMS MI timeout period

You can specify the timeout period for the NMS MI. If there is no action within the set timeout period, the NMS MI times out and the NMS Login window appears.

About this task

You must log in to continue. The NMS GUI Timeout value defaults to 900 seconds (15 minutes).

Steps

1. Sign in to the NMS MI using the Admin or Vendor account.

2. Go to **Grid Management > NMS Management > General > Main**.

3. Under NMS GUI Timeout, enter a timeout period greater than or equal to 60 seconds.

   Entering a timeout period of 0 turns the timeout period functionality off.

4. Click **Apply Changes**.
5. Log out of the NMS MI.
Managing storage tenant accounts

StorageGRID Webscale supports the creation of tenant accounts to provide access to storage for S3 and Swift clients.

Access credentials are created within the context of the tenant account to provide S3 or Swift clients access to the buckets or containers and objects within the account. A tenant account is created with support for either S3 or Swift protocol access, but not both. LDAP federation can also be used to enable users belonging to configured LDAP groups to acquire access credentials for the tenant account. Configuration of tenant accounts is supported both in the NMS MI and through the REST API. Storage usage tracking is provided at the tenant account level, including the storage used by each bucket or container owned by that account.

Related concepts

StorageGRID Webscale Management API Overview on page 29

Managing S3 tenant accounts

You can create S3 tenant accounts to provide access to buckets and objects from authorized S3 client applications.

StorageGRID Webscale supports S3 v2 and v4 authentication, where the client’s request is authenticated by the AccessID provided, and the request header signature is validated with the secret key associated with that AccessID. Root S3 access keys may be created, providing full access to the account’s buckets and objects unless explicitly disabled by a bucket policy. Cross-account access is not permitted unless explicitly enabled by a bucket policy. Using LDAP identity federation, users belonging to configured LDAP groups can create user-level S3 access keys with access permissions defined by the configured group policy for the LDAP group.

Creating tenant accounts for S3

You can create an S3 tenant account for each group that requires access to the StorageGRID Webscale system using the S3 REST API. A tenant account can be created for an organization, division, department, or any other internal or external group you want to use to define access to storage in your StorageGRID Webscale system.

Steps

1. Sign in to the NMS MI using the Admin account.
2. Select Grid Management > Storage Tenants > Tenant Accounts.
3. Click Create.
4. Configure the tenant account in the Add Tenant Account dialog box:
   a. Select S3 as the protocol.
   b. In the Name text box enter the name to display in the NMS MI.
   c. Click Save.

Note: The Save Keys dialog box is displayed listing the Access Key ID and Secret Access Key for the tenant account. Do not close this dialog box until you have copied or downloaded this information.
5. In the **Save Keys** dialog box, note the Secret Access Key, or click **Download** to save a spreadsheet file (.csv) with the Access Key ID and Secret Access Key. The Secret Access Key is not displayed anywhere else in the user interface, and only the last four characters of the Access Key ID are displayed.

6. Click **Finish**.

The tenant account is created with a unique access key identifier. You can click on the **Login** link to sign in to the tenant account, or copy the link and send the URL to the users of the tenant account.

**Editing tenant accounts for S3**

You can edit the configuration settings associated with the tenant account, including the name and the LDAP group, if this information changes.

**Steps**

1. Sign in to the NMS MI using the Admin account.

2. Select **Grid Management > Storage Tenants > Tenant Accounts**.

3. Select the tenant account entry you want to edit.

4. Click **Edit Account**.

5. In the **Edit Tenant Account** dialog box, update the tenant details and click **Save**.

**Editing group policies for S3 tenant accounts**

You can manage permissions to access S3 tenant accounts by importing the group information from an external LDAP server and configuring policies for those groups.

**Steps**

1. Sign in to the NMS MI using the Admin account.

2. Select **Grid Management > Storage Tenants > Tenant Accounts**.

3. Select the S3 tenant account entry you want to edit the group policy for.

4. Click **Edit Group Policies**.

5. If you want to associate permissions with specific LDAP groups, you need to import each individual group you want to assign permissions to:
   a. Click **Import LDAP Group**.
   b. In the **Import LDAP Group** dialog box, enter the unique name of the LDAP group to import and click **Import**.
      For Active Directory, the unique name is associated with the “sAMAccountName” attribute. For OpenLDAP, the unique name is associated with the “uid” attribute.
   c. If you want to allow users that belong to the group to create and delete the S3 access keys associated with their tenant account, select the **Manage Your Own S3 Credentials** checkbox.
   d. If you want to create, update, or delete the S3 group policy, enter the group policy in the **S3 Policy** text box.

   The group policy must be entered using a valid JSON formatted string. The string is validated as it's entered, and you can only save valid group policy strings. See the information on S3 access control policies for the options and correct formatting for group policies.
For example, the following group policy grants the associated group permissions to perform all operations on all resources belonging to the tenant account:

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "urn:sgws:s3:::*"
    }
  ]
}
```

e. Click Save.

6. If you want to update the group policies for an existing group, select the group, click Edit Policies and make any necessary changes, and then click Save.

7. If you want to remove a group's permissions from the StorageGRID Webscale system, select the group and click Remove, and then click OK in the confirmation dialog box.

8. Click Close.

Due to caching, changes to access policies may take up to 15 minutes to take effect across all grid nodes.

**Related concepts**

*Group and bucket access policies* on page 19

**Group and bucket access policies**

The StorageGRID Webscale system implements a subset of the S3 API policy language that you can use to control access to buckets and objects within those buckets.

**Overview**

StorageGRID Webscale bucket and group policies contain statements. Statements contain the following elements, which you need to define:

- **Resources**
  You can allow or deny permissions to buckets and objects using the uniform resource name (URN) to identify the resource.

- **Principals**
  You can allow groups and accounts to access specific resources and perform specific actions. If no S3 signature is included in the request, anonymous access is allowed by specifying the wildcard character (*). Access to resources is granted to anonymous users through the permissions. By default anonymous users have no access to resources.
  You only need to specify the principal in a bucket policy. For group policies, the group to which the policy is attached is the implicit principal.

- **Permissions**
  When a group requests a resource they are either granted or denied access to the resource. Access is denied unless you specifically assign permissions, but you can also explicitly deny access to a resource, so that a group cannot access it even if a different policy grants access. Permissions have two components:
    - **Action**
      You need to identify operations you allow (or deny) on buckets or objects using the supported action keywords. You can use the wildcard character (*) to specify all operations, or a subset of operations (i.e. "s3:*Object").
Effect
You need to specify whether the specified operations are allowed or denied.

The following example policy shows a complete bucket policy that allows the admin and finance groups s3:ListBucket and s3:GetObject permissions for the mybucket bucket:

```json
{
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "SGWS": [
               "urn:sgws:identity::2723906934684427525:group/admin",
               "urn:sgws:identity::2723906934684427525:group/finance"
            ],
         "Action": ["s3:ListBucket","s3:GetObject"],
         "Resource": ["urn:sgws:s3:::mybucket", "urn:sgws:s3:::mybucket/*"]
      }
   ]
}
```

The bucket policy has a size limit of 20,480 bytes, and the group policy has a size limit of 5,120 bytes.

Due to caching, changes to group and bucket policies may take up to 15 minutes to take effect across all grid nodes.

Specify resources in a policy
You use the common uniform resource name (URN) format to identify any S3 resources or identity resources in the StorageGRID Webscale system:

- `urn:sgws:s3:::bucket_name`
- `urn:sgws:s3:::bucket_name/key_name`
- `urn:sgws:identity::2723906934684427525:root`
- `urn:sgws:identity::2723906934684427525:user/Bob`

- The StorageGRID Webscale REST API implementation of identity resources differs from Amazon's implementation:
  - For principals, the service component is “identity” instead of “iam”.
  - For principals, the `group-uuid` resource type is an additional StorageGRID Webscale specific resource type.
  - You need to specify the resource type and the UUID, instead of using a UUID alone.
    For example:
    ```
    urn:sgws:identity::2723906934684427525:group-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
    ```
  - For resources, the region component must be empty.
  - For resources, service component remains “s3”.
    For example:
    ```
    "Resource": "urn:sgws:s3:::mybucket/*"
    ```

- The principal value can specify a group name that does not yet exist when the bucket policy is created.
• The resource value can specify a bucket that does not yet exist when the group policy is created.
• The version value is not used; if you specify one it is ignored and does not affect the interpretation of policy variables.
• International characters, which can be specified in the object key, should be encoded using JSON UTF-8 or use JSON \u escape sequences. Percent-encoding, as outlined in RFC 2141 URN Syntax, is not supported. The request body for the PUT Bucket policy operation must be encoded as JSON UTF-8, and UTF-8 is always set as the content type.

**Specify a principal in a policy**

Account-based identities must be specified in one of the following formats:

- "SGWS": "account_ID"
- "SGWS": "account_URN"

You can specify an account using an ID. This example uses the ID 27233906934684427525, which includes the account root and all users in the account):

```
"Principal": { "SGWS": "27233906934684427525" }
```

You can specify just the account root:

```
"Principal": { "SGWS": "urn:sgws:identity::27233906934684427525:root" }
```

You can specify a specific federated user ("Bob"):

```
"Principal": { "SGWS": "urn:sgws:identity::27233906934684427525:federated-user/Bob" }
```

You can specify a specific federated group ("Managers"):

```
"Principal": { "SGWS": "urn:sgws:identity::27233906934684427525:federated-group/Managers" }
```

You can specify an anonymous principal:

```
"Principal": "*
```

The Canonical User ID is not supported.

**Specifying permissions in a policy**

There are a set of permissions that you can specify in a policy. Each of these keywords maps to specific S3 Rest API operations.

Permissions applicable to buckets:

<table>
<thead>
<tr>
<th>Permissions</th>
<th>S3 Rest API operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>s3:CreateBucket</td>
<td>PUT Bucket</td>
</tr>
<tr>
<td>s3:DeleteBucket</td>
<td>DELETE Bucket</td>
</tr>
<tr>
<td>s3:DeleteBucketPolicy</td>
<td>DELETE Bucket policy</td>
</tr>
<tr>
<td>s3:GetBucketAcl</td>
<td>GET Bucket acl</td>
</tr>
<tr>
<td>Permissions</td>
<td>S3 Rest API operations</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>s3:GetBucketPolicy</td>
<td>GET Bucket policy</td>
</tr>
<tr>
<td>s3:GetBucketVersioning</td>
<td>GET Bucket versioning</td>
</tr>
<tr>
<td>s3:ListAllMyBuckets</td>
<td>GET Service, GET Storage Usage</td>
</tr>
<tr>
<td>s3:ListBucket</td>
<td>GET Bucket (List Objects)</td>
</tr>
<tr>
<td>s3:ListBucketMultipartUploads</td>
<td>List Multipart Uploads</td>
</tr>
<tr>
<td>s3:PutBucketPolicy</td>
<td>PUT Bucket policy</td>
</tr>
</tbody>
</table>

Permissions applicable to objects:

<table>
<thead>
<tr>
<th>Permissions</th>
<th>S3 Rest API operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>s3:AbortMultipartUpload</td>
<td>Abort Multipart Upload</td>
</tr>
<tr>
<td>s3:DeleteObject</td>
<td>DELETE Object</td>
</tr>
<tr>
<td>s3:GetObject</td>
<td>GET Object</td>
</tr>
<tr>
<td>s3:GetObjectAcl</td>
<td>GET Object ACL</td>
</tr>
<tr>
<td>s3:ListMultipartUploadParts</td>
<td>List Parts</td>
</tr>
<tr>
<td>s3:PutObject</td>
<td>PUT Object</td>
</tr>
</tbody>
</table>

**Policies requiring special handling**

Sometimes a policy can grant permissions that are dangerous for security, or dangerous for continued operations. For example locking out the root user of the account. The StorageGRID Webscale S3 API implementation is less restrictive during policy validation than Amazon, but equally strict during policy evaluation.

<table>
<thead>
<tr>
<th>Policy description</th>
<th>Policy type</th>
<th>Special handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny self any permissions to the root account</td>
<td>Bucket</td>
<td>Valid and enforced, but root user account retains permission for all S3 bucket policy operations</td>
</tr>
<tr>
<td>Deny self any permissions to user/group</td>
<td>User/Group</td>
<td>Valid and enforced</td>
</tr>
<tr>
<td>Allow a foreign account group any permission</td>
<td>Bucket</td>
<td>Valid, but permissions for all S3 bucket policy operations return a 405 Method Not Allowed error when allowed by a policy</td>
</tr>
<tr>
<td>Allow a foreign account root or user any permission</td>
<td>Bucket</td>
<td>Valid, but permissions for all S3 bucket policy operations return a 405 Method Not Allowed error when allowed by a policy</td>
</tr>
<tr>
<td>Policy description</td>
<td>Policy type</td>
<td>Special handling</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow everyone permissions to all actions</td>
<td>Bucket</td>
<td>Valid, but permissions for all S3 bucket policy operations return a 405 Method Not Allowed error for the foreign account root and users</td>
</tr>
<tr>
<td>Deny everyone permissions to all actions</td>
<td>Bucket</td>
<td>Valid and enforced, but root user account retains permission for all S3 bucket policy operations</td>
</tr>
<tr>
<td>Principal is a non-existent user or group</td>
<td>Bucket</td>
<td>Valid, differs from Amazon behavior, which is to treat this as an invalid principal</td>
</tr>
<tr>
<td>Resource is a non-existent S3 bucket</td>
<td>User/Group</td>
<td>Valid</td>
</tr>
<tr>
<td>Principal is a local group</td>
<td>Bucket</td>
<td>Valid, differs from Amazon behavior, which is to treat this as an invalid principal</td>
</tr>
</tbody>
</table>

### Editing S3 Root Keys for S3 tenant accounts

You can create or remove the S3 root keys used by a tenant account to connect to the StorageGRID Webscale system using client applications developed to use S3 web services.

**About this task**

The S3 account information is used in the authentication process. When you later configure an S3 client, you need the Access Key ID and Secret Access Key information.

**Steps**

1. Sign in to the NMS MI using the Admin account.

2. Select Grid Management > Storage Tenants > Tenant Accounts.

3. Select the tenant account entry you want to modify S3 Root Keys for.

4. Click Edit S3 Root Keys.

5. If you want to create a new key:
   a. Click Create.
   b. Use the calendar control to select the expiration date and then set the time, or leave the default value of Never, and click Save.

   **Note:** The Save Keys dialog box is displayed listing the Access Key ID and Secret Access Key for the account. Do not close this dialog box until you have copied or downloaded this information.
c. In the **Save Keys** dialog box, note the Secret Access Key, or click **Download** to save a spreadsheet file (.csv) with the Access Key ID and Secret Access Key. The Secret Access Key is not displayed anywhere else in the user interface, and only the last four characters of the Access Key ID are displayed.

d. Click **Finish**.

6. If you want to remove an existing key:
   a. Select the entry to remove.
   b. Click **Remove**.
   c. Click **OK** in the confirmation dialog box.

   Due to caching, access keys may remain valid for up to 15 minutes after you remove them.

### Managing Swift tenant accounts

You can create Swift tenant accounts to provide access to Swift containers and objects from authorized Swift client applications.

#### Creating tenant accounts for Swift

You can create a Swift tenant account for each group that requires access to the StorageGRID Webscale system using the Swift REST API. A tenant account can be created for an organization, division, department, or any other internal or external group you want to use to define access to storage in your StorageGRID Webscale system. If you configured LDAP for this account, all groups and users in the LDAP domain can access Swift via this account.

**About this task**

The Swift tenant account information is used in the authentication process. Configuring a Swift client requires one of the following sets of user credentials:

- If Identity Federation is enabled for the tenant account (for Active Directory or LDAP configurations), you should provide the username and password of the federated user from the AD or LDAP server. Alternatively, LDAP users can be referred to with their domain name, for example, `X-Auth-User: <Tenant_Account_ID>:<Username@Domain_Name>`

- For local accounts when LDAP is not configured, you should use the "swiftadmin" as the user name and the password provided during tenant account creation.

**Steps**

1. Sign in to the NMS MI using the Admin account.
2. Select **Grid Management > Storage Tenants > Tenant Accounts**.
3. Click **Create**.
4. Configure the tenant account in the **Add Tenant Account** dialog box:
   a. Select **Swift** as the protocol.
   b. In the **Name** text box enter the name to display in the NMS MI.
   c. If you want to use the local Swift Administrator account, instead of or in addition to LDAP authentication, enter the password to use in the **Password** and **Confirm Password** text boxes.
The password must be between 8 and 32 characters. You must enter a strong password to ensure the security of your StorageGRID Webscale system.

d. Click Save.

**Editing tenant accounts for Swift**

You can edit the configuration settings associated with the tenant account, including the name and the password for the Swift Administrator account, if this information changes.

**Steps**

1. Sign in to the NMS MI using the Admin account.
2. Select **Grid Management > Storage Tenants > Tenant Accounts**.
3. Select the tenant account entry you want to edit.
4. Click **Edit Account**.
5. In the **Edit Tenant Account** dialog box, you can update the tenant details:
   a. To rename the tenant account, enter the new name in the **Name** text box.
   b. To change the password for the local Swift Administrator account, enter the new password in the **New Password** and **Confirm Password** text boxes.
      The password must be between 8 and 32 characters. You must enter a strong password to ensure the security of your StorageGRID Webscale system.
   c. Click **Save**.

**Editing group policies for Swift tenant accounts**

You can manage permissions to access Swift tenant accounts by importing the group information from an external LDAP server and configuring policies for those groups. You can also define which groups have Administrator permissions for the Swift REST API.

**Steps**

1. Sign in to the NMS MI using the Admin account.
2. Select **Grid Management > Storage Tenants > Tenant Accounts**.
3. Select the Swift tenant account entry you want to edit the group policy for.
4. Click **Edit Group Policies**.
5. If you want to associate permissions with specific LDAP groups, you need to import each individual group you want to assign permissions to:
   a. Click **Import LDAP Group**.
   b. In the **Import LDAP Group** dialog box, enter the unique name of the LDAP group to import and click **Import**.
      For Active Directory, the unique name is associated with the “sAMAccountName” attribute. For OpenLDAP, the unique name is associated with the “uid” attribute.
   c. If you want to grant Administrator permissions to members of the LDAP group, select the **Administrator** checkbox.
   d. Click **Save**.
6. If you want to update the group policies for an existing group, select the group, click Edit Policies and make any necessary changes, and then click Save.

7. If you want to remove a group's permissions from the StorageGRID Webscale system, select the group and click Remove, and then click OK in the confirmation dialog box.

8. Click Close.

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 have removed all buckets and objects associated with the tenant account before you can delete it.

Steps
1. Sign in to the NMS MI using the Admin account.
2. Select Grid Management > Storage Tenants > Tenant Accounts.
3. Select the tenant account entry you want to delete.
4. Click Remove.
5. Click OK in the confirmation dialog box.

Configuring LDAP for identity federation
You can configure LDAP if you want to use an external LDAP server to authenticate tenant accounts.

Steps
1. Sign in to the NMS MI using the Admin account.
2. Select Grid Management > Storage Tenants > Identity Federation.
3. Select the Enable LDAP checkbox.
4. Select the type of LDAP server to configure from the Service Type drop-down list.
   The options are Active Directory, OpenLDAP, or Other. If you select Other, you need to enter additional information in the LDAP Attributes section:
   - Unique User Name: The LDAP attribute that uniquely identifies each LDAP user relative to the User Base DN. This will be the name the user provides when authenticating (uid/sAMAccountName)
   - User UUID: The LDAP attribute that uniquely identifies each LDAP user, permanently (entryUUID/objectGUID)
   - Group Unique Name: The LDAP attribute that uniquely identifies each LDAP group (uid/sAMAccountName)
   - Group UUID: The LDAP attribute that uniquely identifies each LDAP group, permanently (entryUUID/objectGUID)
5. Enter the required LDAP server and network connection information:
- **Hostname**: The server hostname or IP address of the identity source.
- **Port**: The port to use to connect to the identity source.
- **Username**: The username to use to access the identity source.
  The credentials for the specified user account must be sufficient to list group and users, and access the following attributes: cn, sAMAccountName/uid, objectGUID/entryUUID, memberOf.
- **Password**: The password to use to access the identity source.
- **Group Base DN**: The fully qualified Distinguished Name (DN) of an LDAP subtree you want to search for tenant groups.
  The Unique User 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 tenant users.
- **Transport Layer Security**: Specifies if TLS is used to secure communications with the identity server. Select the appropriate security setting from the drop-down list:
  - **Use operating system CA certificate**: Use the default CA certificate installed on the operating system to secure connections.
  - **Use custom CA certificate**: Cut and paste the contents of the custom security certificate to use in the text area.
  - **Do not use**: The network traffic between the StorageGRID Webscale system and the LDAP server will not be secured.

6. Optional. Click **Test Connection** to validate your connection settings for the identity server.

7. Click **Save**.

**OpenLDAP server configuration guidelines**

If you are configuring OpenLDAP server for use with StorageGRID Webscale Identity Federation, you need to configure specific settings on the OpenLDAP server.

**Memberof overlay**

The memberof overlay 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:

```plaintext
olcDbIndex: objectClass eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: cn eq,pres,sub
olcDbIndex: entryUUID eq
```

For more information on the olcDBIndex directive used for indexing attributes, see the *OpenLDAP Software Administrator's Guide*.

[http://www.openldap.org/doc/admin24/slapdconf2.html](http://www.openldap.org/doc/admin24/slapdconf2.html)
Disabling LDAP for identity federation

You can temporarily or permanently disable LDAP authentication for tenant accounts. Any settings you have configured are retained while LDAP is disabled, but there is no communication between the StorageGRID Webscale system and the LDAP server.

**About this task**

Before you disable LDAP, you should be aware of the following:

- Federated users will be unable to log in.
- Federated users who are currently logged in will retain access to the StorageGRID Webscale system until their session expires, but they will be unable to log in after their session expires.
- Synchronization between the StorageGRID Webscale system and the LDAP server will not occur, and alarms will not be raised for accounts that have not been synchronized.

**Steps**

1. Sign in to the NMS MI using the Admin account.
2. Select **Grid Management > Storage Tenants > Identity Federation**
3. Deselect the **Enable LDAP** checkbox.
4. Click **Save**.

Manually forcing synchronization with the LDAP server

The StorageGRID Webscale system periodically synchronizes federated groups and users from the LDAP server. You can manually force synchronization to start if you want changes to be reflected as soon as possible to enable or restrict user permissions to the system.

**Steps**

1. Sign in to the NMS MI using the Admin account.
2. Select **Grid Management > Storage Tenants > Identity Federation**.
3. Click **Synchronize**.
   
   A confirmation message is displayed indicating that synchronization started successfully.

Managing federated user S3 credentials

Federated users can manage their S3 credentials for storage tenant accounts, which allows them to control API client access to objects stored in the StorageGRID Webscale system.

**About this task**

You can create and remove S3 access keys as required.

**Steps**

1. Log in to the NetApp StorageGRID Webscale web application:
• Click the tenant account link, or cut and paste the URL, provided by the StorageGRID Webscale administrator.

• If you have Admin or Vendor access to the NMS MI, select Grid Management > Storage Tenants > Tenant Accounts and click the Login link next to the S3 tenant account you want to access.

2. Enter the Username and Password for the tenant account and click Sign In.

3. If you want to create a new key:
   a. Click Create.
   b. Use the calendar control to select the expiration date and then set the time, or leave the default value of Never, and click Save.

   Note: The Save Keys dialog box is displayed listing the Access Key ID and Secret Access Key for the federated user. Do not close this dialog box until you have copied or downloaded this information. The Secret Access Key is not displayed anywhere else in the user interface, and only the last four characters of the Access Key ID are displayed.

   c. In the Save Keys dialog box, note the Secret Access Key, or click Download to save a spreadsheet file (.csv) with the Access Key ID and Secret Access Key.
   d. Click Finish.

4. If you want to remove an existing key:
   a. Select the entry to remove.
   b. Click Remove.
   c. Click OK in the confirmation dialog box.

StorageGRID Webscale Management API Overview

StorageGRID Webscale provides a REST API for performing grid and tenant management tasks for S3 and Swift accounts, and for managing S3 credentials for tenant user access.

The StorageGRID Webscale Management API is accessed through the NMS service over HTTPS and all operations require authorization.

StorageGRID Webscale Management API Documentation

You can access the StorageGRID Webscale Management API documentation in two places depending on the APIs you want more information on:

• For grid level APIs, log in to the NMS MI and select API docs in the web application header.
• For tenant user APIs, log in to the Tenant UI and select Help > API Docs in the web application header.

StorageGRID Webscale uses Swagger for the REST API documentation. Swagger allows both developers and non-developers to interact with the API in a UI 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: Operations performed via the Swagger documentation UI are real operations and perform real actions on the grid.
Each of the REST API commands is comprised of the API's URL, an HTTP action, a URL parameter, and an expected API response.

In the Swagger output, you see API details similar to the following:

The StorageGRID Webscale Management API is separated into the following sections:

- **accounts**: Operations to perform management of storage tenant accounts.
  
  The Management API allows the user to list the current storage tenant accounts, create new accounts or delete empty accounts. An account is created with a descriptive name and a set of capabilities including which protocol is supported. Individual accounts, referenced by their ID, may be modified after creation but the supported protocol may not be changed. Storage usage, comprised of the number of objects and the number of bytes of object data, may be retrieved for a given account and the buckets or containers in that account.

- **auth**: Operations to perform user session authentication.
  
  The Management API supports the Bearer Token Authentication Scheme. To login, the client provides username and password in the JSON body of the authentication request (i.e., POST /api/v1/authorize) and a security token is returned if successfully authenticated. The returned token must be provided with subsequent API requests, with ‘Bearer’ for Authorization followed by the token. For grid APIs, the username and password provided is that of the ‘Vendor’ account for the StorageGRID Webscale NMS MI.

- **groups**: Operations to perform management of LDAP federated groups for a given account.
The Management API allows the user to list the currently configured LDAP groups associated with a given account, and associate new groups with the account. Group names and user membership are validated against the configured LDAP server. For S3 tenant accounts, the group can be configured with permissions to enable access to the tenant UI/API for authenticated members of this group to create S3 access keys. The group may also be configured with an S3 policy to control access to buckets within this account, for access keys belonging to this group.

- **identity-source**: Operations to interact with an external LDAP server.

  The Management API allows the user to configure, or manually start synchronization between the LDAP server and the StorageGRID Webscale system.

- **s3**: Operations to perform management of S3 root access keys for a given account.

  The Management API allows the user to create new root access keys, delete existing access keys, or list the existing access keys. Access keys may be created with an optional expiry time. Root access keys have full access to buckets in the account.

### Top level resources

The StorageGRID Webscale Management API provides the following top level resources.

- **/grid**: Access is restricted to NMS user accounts with Grid Management or Maintenance permissions. Grid Management permissions are required for APIs which perform modifications. Grid Maintenance permissions enable read-only access. Sub-resources available include `identity-source` for LDAP configuration, and tenant accounts for storage tenant account management including group and `s3-access-key` root access keys.

- **/org**: Access is restricted to LDAP federated users belonging to a group enabled for the given tenant account. Sub-resources available include `s3-access-keys` for the current authenticated user.

- **/private**: Access is restricted to internal access by the NMS MI. This resource path is not publically documented.

### Versioning

The current REST API version is shown in the URL. For example, below is version 1 of the API.

https://hostname_or_ip_address/api/v1/grid/accounts/001122334455/usage

**Note:**

- For a minor release (for example, 1.x), the API will be backwards compatible. That is, functions will be added; however, these updates will not affect existing contracts.

- For a major release (for example, 2.x), the API may not be backwards compatible; you may have to rework the client code.
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 the Admin Node. The AMS service logs all audited system events to a text file on the Admin Node. For more information about auditing, the Audit Message Reference Guide.

Related concepts
- Configuring audit client access on page 166
- What AutoSupport is on page 54

Related information
- StorageGRID Webscale 10.2 Audit Message Reference

About alarms and e-mail notifications

An e-mail notification is a message automatically e-mailed by the StorageGRID Webscale system to configured recipients, which alerts recipients that an alarm has been triggered or that a service state has changed. The NMS MI allows you to easily configure e-mail notifications and set mailing lists to receive these e-mail notifications for a particular alarm severity or state change.

If an e-mail address (or list) belongs to multiple mailing lists, only one e-mail notification is sent when an e-mail 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 need to receive notifications for alarms with a severity of Critical. You can belong to both lists. If a Critical 2 alarm is triggered, you will receive one notification, not two. For a general overview about alarms, see the Grid Primer.

Related information
- StorageGRID Webscale 10.2 Grid Primer

Notification types

There are two types of notifications e-mailed by the StorageGRID Webscale system, severity level and service state notifications.

Severity Level notifications

Severity Level notifications are sent at the alarm level and are associated with attributes. A mailing list will receive all notifications related to alarms of the selected severity: Notice, Minor, Major, and Critical. A notification is sent when an alarm is triggered for the selected alarm level and when it leaves the alarm level — either by being resolved (an alarm severity of “Normal”) 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 will receive 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**

The current status of the NMS service’s ability to send notifications to the mail server and the size of its notifications queue is displayed at Admin Node > NMS > Interface Engine > Overview > Main.

Notifications are processed through the e-mail 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 40

**Configuring notifications**

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

**Steps**

1. **Configuring e-mail server settings** on page 34

   The E-Mail Server page allows you to configure SMTP mail server settings that enable the sending of e-mail for alarm notifications and AutoSupport messages. The StorageGRID Webscale system only sends e-mail; it cannot receive e-mail. Only the SMTP protocol is supported.
2. Creating e-mail templates on page 35
   Templates allow you to customize the content of the header, footer, and subject line of a
   notification. Templates can be used to send unique notifications that contain the same body text to
   different mailing lists.

3. Creating mailing lists on page 36
   The Lists page allows you to create mailing lists for notifications. A mailing list allows you to
   send one e-mail message to multiple e-mail 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 e-mail address.

4. Configuring global e-mail notifications on page 37
   In order to receive global e-mail notifications, recipients must be a member of a mailing list and
   that list must be added to Notifications > Main. Notifications are configured to send e-mail 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.

Configuring e-mail server settings

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

Steps
1. Log in to the NMS MI using the Admin or Vendor account.
2. Go to Grid Management > NMS Management > E-mail > Server.

3. Configure 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>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authentication</td>
<td>Allows for the authentication of the SMTP mail server. By default, authentication is Off.</td>
</tr>
<tr>
<td>Authentication Credentials</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

5. Optionally, in the Test E-mail section:
   - Under To, add an e-mail addresses you want to send a confirmation message to, confirming that your SMTP mail server settings are correct. E-mail addresses can be any single address, multiple e-mail addresses comma delineated, or mailing list as configured on the Lists page. Test e-mails are sent from all NMS services. This includes the standby sender (if the system includes a second Admin Node). Thus, multiple test e-mails can be sent.
   - Select **Send Test E-mail**.
     A test e-mail will be sent when Apply Changes is clicked. This test e-mail can be used to confirm that the SMTP mail server is configured correctly and that the NMS service can connect to the mail server.

6. Click **Apply Changes**.
   SMTP mail server settings are saved. If configured, a test e-mail is immediately sent.

**Related tasks**

*Enabling Domain Name Service globally* on page 155

*Creating mailing lists* on page 36

The Lists page allows you to create mailing lists for notifications. A mailing list allows you to send one e-mail message to multiple e-mail 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 e-mail address.

**Creating e-mail templates**

Templates allow you to customize the content of the header, footer, and subject line of a notification. Templates can be used to send unique notifications that contain the same body text to different mailing lists.

**About this task**

For example, different mailing lists might require different contact information. Templates do not include the body text of the e-mail message.

**Steps**

1. Log in to the NMS MI using the Admin or Vendor account.
2. Go to Grid Management > NMS Management > E-mail > Template.
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><strong>Template Name</strong></td>
</tr>
<tr>
<td><strong>Subject Prefix</strong></td>
</tr>
<tr>
<td><strong>Header</strong></td>
</tr>
<tr>
<td><strong>Footer</strong></td>
</tr>
</tbody>
</table>

5. Click **Apply Changes**.

A new template for notifications is added to the NMS MI.

Creating mailing lists

The Lists page allows you to create mailing lists for notifications. A mailing list allows you to send one e-mail message to multiple e-mail 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 e-mail address.

**Steps**

1. Log in to the NMS MI using the Admin or Vendor account.
2. Go to Grid Management > NMS Management > E-mail > 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>
<th>Group Name</th>
<th>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 in the NMS MI that use the mailing list name. You must manually update all configured notifications to use the new mailing list name.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Recipients</td>
<td>Single e-mail address, a mailing list already defined, or a comma delineated list of e-mail addresses and mailing lists to which notifications will be sent.</td>
</tr>
<tr>
<td>E-mail Template</td>
<td>Optionally, select a Template to add a unique header, footer, and subject line to notifications sent to all recipients of this mailing list.</td>
<td></td>
</tr>
</tbody>
</table>

5. Click Apply Changes.
A new mailing list is created.

**Related tasks**

*Creating e-mail templates* on page 35
Templates allow you to customize the content of the header, footer, and subject line of a notification. Templates can be used to send unique notifications that contain the same body text to different mailing lists.

**Configuring global e-mail notifications**

In order to receive global e-mail notifications, recipients must be a member of a mailing list and that list must be added to Notifications > Main. Notifications are configured to send e-mail 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.

**Steps**

1. Go to Grid Management > NMS Management > Notifications > Main.
2. Click Edit (or Insert if this is not the first notification).
3. Under E-mail List, add a new mailing list. Mailing lists are configured on E-mail > Lists.
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 change.

**Related tasks**

*Creating mailing lists* on page 36

The Lists page allows you to create mailing lists for notifications. A mailing list allows you to send one e-mail message to multiple e-mail 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 e-mail address.

**Sending test e-mails**

To confirm that you have configured the e-mail server connection correctly, you can send a test e-mail. When you send a test e-mail, a message is sent from all NMS services. The test also attempts to send a test e-mail from the standby sender (if the system includes a second Admin Node). Thus, multiple test e-mails can be sent.

**About this task**

When a test e-mail is sent, the NMS MI does not confirm success or failure. You must check the test recipient’s inbox. Make sure, when sending a test e-mail, that it will be sent to an address you can access. Test e-mails are sent to the mail server immediately and are not sent through the notifications queue. Note that if there is a connection problem between the NMS service and the mail server, the MINS (NMS Notification Status) Minor alarm is triggered.

**Steps**

1. Log in to the NMS MI using the Admin or Vendor account.

2. Go to **Grid Management > NMS Management > E-mail > Server**.

3. In the Test E-mail section:
   a. Under To, type e-mail addresses you want to send a confirmation message to. E-mail addresses are comma delineated.
   b. Select **Send Test E-mail**.
4. Click Apply Changes.
   A test e-mail is immediately sent to designated personnel.
   Receipt of this test e-mail confirms that your SMTP mail server settings are correct and that the NMS service is successful connecting to the mail server.

Related tasks

Configuring e-mail server settings on page 34
   The E-Mail Server page allows you to configure SMTP mail server settings that enable the sending of e-mail for alarm notifications and AutoSupport messages. The StorageGRID Webscale system only sends e-mail; it cannot receive e-mail. Only the SMTP protocol is supported.

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.

Steps

1. Go to Grid Management > NMS Management > Notifications > Main.

2. Click Edit next to the mailing list for which you want to suppress notifications.

3. 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.

4. Click Apply Changes.
   Notifications are suppressed for the selected mailing lists.

Suppressing e-mail notifications system wide

Suppressing notifications for the entire StorageGRID Webscale system overrides any notifications that are configured. If you suppress notifications system-wide, the notice “All e-mail notifications are now suppressed” is displayed on Notifications > Main.

Steps

1. Go to Grid Management > NMS Management > General > Main.

2. Select Notification Suppress All.
3. Click **Apply Changes**.

Notifications are suppressed system-wide. This configuration is viewable from **Grid Management > NMS Management > General > Main**.

![Notifications: NMS Management](image)

All e-mail notifications are now suppressed.

<table>
<thead>
<tr>
<th>E-mail List</th>
<th>Severity Levels</th>
<th>Service States</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test</td>
<td>Notice</td>
<td>Minor</td>
<td>Critical</td>
</tr>
</tbody>
</table>

Selecting a preferred sender

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

**About this task**

For a list of available Admin Nodes, go to **Grid Management > NMS Management > Overview > Main**. Select a preferred sender based on the name of the Admin Node as listed here. Note that when selecting a preferred sender, the name of the Admin Node is used.

![Overview: NMS Management](image)

NMS Information

<table>
<thead>
<tr>
<th>NMS Service</th>
<th>Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center 1/DC1-ADM1-99-160/NMS</td>
<td>Consolidated</td>
<td>ADMIN-DC1-ADM1-99-160</td>
</tr>
</tbody>
</table>

On the **Grid Management > NMS Management > Overview > Main** page, the Current Sender is read-only and displays the Admin Node that is currently acting as the preferred sender. In most cases, this Admin Node is the same as the Admin Node displayed for Preferred Sender; however, in rare instances an Admin Node can become separated or “islanded” from the rest of the system and be unable to use the Preferred Sender. In this case, the islanded Admin Node will update 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. Go to **Grid Management > NMS Management > Overview > Main**.
2. Select **Preferred Sender > Admin Node**.
   For a list of available Admin Nodes, see [Grid Management > NMS Management > Overview > Main](#).

3. Click **Apply Changes**.
   The selected Admin Node and its NMS service is set as the preferred sender of notifications.

**Configuring a custom alarm notification**

Along with global notifications, you can create custom alarms and notifications for a specific service.

For example, if you want to monitor the LDR service on a specific Storage Node, you can create a custom alarm and notification for that LDR service, which notifies a specific set of people (for example, administrators) if the alarm is triggered. Customized alarms are configured on **component** > **Configuration** > **Alarms**.

**Related tasks**

* [Creating custom alarms](#) on page 47

**Alarms management**

Customizing alarms enables you to optimize the NMS MI for your StorageGRID Webscale system’s unique requirements. You can configure these customized alarms either globally (Global Custom alarms) or for individual services (Custom alarms). You can create alarms to set a new alarm level that overrides an existing Default alarm, or you can create alarms for attributes that do not have a Default alarm.

Alarm customization is restricted to accounts with Maintenance permissions.

**Warning:** Alarm settings are enabled as part of your installation. You should not make changes to alarm settings for simple convenience. Changing alarm settings can conceal underlying problems that should be resolved. If you find an alarm is persistent, discuss the situation with technical support before making changes.

For a basic introduction to alarm monitoring, see the *Grid Primer*. For a list of alarm codes, see the *Troubleshooting Guide*.

**Related concepts**

* [Managing user and group accounts](#) on page 180
Alarm class types

Alarms are separated into three mutually exclusive alarm classes.

- Default: Standard alarm configurations set at installation
- Global Custom: Configured after installation to override default settings, custom alarms are set at a global level so that they apply to all services of a given type anywhere in the StorageGRID Webscale system
- Custom: Configured after installation to override default settings, custom alarms are set on individual services or components.

Default alarms

Default alarms are configured on a global basis and cannot be modified; however, they 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, at the services level on the Configuration page, the Enabled check box appears with an asterisk adjacent to it. The asterisk indicates that the Default alarm has been disabled through the Grid Management > NMS Management > Alarms > Custom page even though the Enabled check box is selected.

Default alarms for a particular service or service component can be viewed on Service/Component > Configuration > Alarms.

Related tasks

- Disabling default alarms for services on page 51
- Disabling default alarms system wide on page 52

Viewing all default alarms

Steps

1. Go to Grid Management > NMS Management > Alarms > Custom.
2. Select Filtered by > Attribute Code or Attribute Name.
3. For equals, enter the wildcard symbol: *.
4. Under Default Alarms, click Apply Changes.
   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.

The configuration of Global Custom alarms is performed on Go to Grid Management > NMS Management > Alarms > Custom. You can create global custom alarms, and disable global custom alarms for services or system wide.

Related tasks

Creating global custom alarms on page 49
Disabling global custom alarms for services on page 52
Disabling global custom alarms system wide on page 53

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.

The configuration of Custom alarms is performed on Service > Configuration > Alarms.

Related tasks

Creating custom alarms on page 47

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 145

Alarm triggering examples

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>Threshold Values</th>
<th>Global Custom alarm (enabled)</th>
<th>Default alarm (enabled)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>&gt;= 1500</td>
<td>&gt;= 1000</td>
</tr>
<tr>
<td>Minor</td>
<td>&gt;= 15,000</td>
<td>&gt;= 1000</td>
</tr>
<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.
Threshold Values

<table>
<thead>
<tr>
<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>
</tr>
<tr>
<td>Minor</td>
<td>&gt;= 750</td>
<td>&gt;= 15,000</td>
</tr>
<tr>
<td>Major</td>
<td>&gt;= 1,000</td>
<td>&gt;= 150,000</td>
</tr>
</tbody>
</table>

If the attribute is evaluated when its value is 1000, a Major alarm is triggered and an e-mail 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>Threshold Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom alarm (enabled)</td>
</tr>
<tr>
<td>Notice</td>
</tr>
<tr>
<td>Minor</td>
</tr>
<tr>
<td>Major</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 “top down.”

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 ($\leq 100000000$) 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 e-mail 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 alarms

Customizing alarm settings allows you to create a customized methodology for monitoring the StorageGRID Webscale system. 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 a service or component in the Grid Topology tree.
2. Go to Configuration > Alarms.
3. 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.
4. 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>Operator</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>Value</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>Additional Recipients</td>
<td>A supplementary list of e-mail 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>Actions</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>

5. 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 allows you to create a customized methodology to monitoring the StorageGRID Webscale system.

About this task

Global Custom 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. Go to Grid Management > NMS Management > Alarms > Custom.

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.
   - Copy Default alarms to the table.
     
     **Note:** Selecting Disabled Defaults displays a list of all currently disabled default global alarms.

     To copy Default alarms:
     - Search for the Default alarm. Under Filter by, select eitherAttribute Code or Attribute Name, type a search string, and then click Submit.
     - You can use the wildcards * (for multiple characters) and ? (for single characters) in the search string.

3. 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.
4. 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>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. 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>Operator</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>Value</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>Additional Recipients</td>
<td>A supplementary list of e-mail 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>Actions</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>

5. Click **Apply Changes**.
Disabling alarms

By default, all alarms are enabled. You can selectively 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 53

Alarms and tables

Alarm attributes displayed in tables can only be disabled at the service level, component level, or system wide. 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

<table>
<thead>
<tr>
<th>Mount Point</th>
<th>Device</th>
<th>Status</th>
<th>Size</th>
<th>Space Available</th>
<th>Total Entries</th>
<th>Entries Available</th>
<th>Write Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>sda1</td>
<td>Online</td>
<td>19.6 GB</td>
<td>7.45 GB</td>
<td>655,360</td>
<td>559,263</td>
<td>Enabled</td>
</tr>
<tr>
<td>/var/local</td>
<td>sda2</td>
<td>Online</td>
<td>63.4 GB</td>
<td>59.4 GB</td>
<td>3,932,160</td>
<td>3,931,842</td>
<td>Unknown</td>
</tr>
<tr>
<td>/var/local/rangedb0</td>
<td>sdc</td>
<td>Online</td>
<td>53.4 GB</td>
<td>53.4 GB</td>
<td>52,428,800</td>
<td>52,427,856</td>
<td>Enabled</td>
</tr>
<tr>
<td>/var/local/rangedb1</td>
<td>sdd</td>
<td>Online</td>
<td>53.4 GB</td>
<td>53.4 GB</td>
<td>52,428,800</td>
<td>52,427,848</td>
<td>Enabled</td>
</tr>
<tr>
<td>/var/local/rangedb2</td>
<td>sde</td>
<td>Online</td>
<td>53.4 GB</td>
<td>53.4 GB</td>
<td>52,428,800</td>
<td>52,427,866</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Disabling default alarms for services

**Steps**

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

The Default alarm is disabled for the service or component.

**Note:** Alarms cannot be disabled for individual rows in a table.
Disabling default alarms system wide

Steps
1. Go to Grid Management > NMS Management > Alarms > Custom.
2. Search for the Default alarm to disable:
   a. In the Default Alarms section, select Filtered by > Attribute Code or Attribute Name.
   b. Type a search string, and then click Submit.
   You can use the wildcards * and ? in the search string. Asterisks (*) represent multiple characters
      and question marks (?) represent a single character.
   Note: Selecting Disabled Defaults displays a list of all currently disabled Default Global
      alarms.
3. In the Default Alarms table, click Edit 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 enabled alarms.

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 that service that will never be triggered.
2. Select the service or component in the Grid Topology tree.
3. Go to Configuration > Alarms.
4. 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.
5. Clear Enabled for the alarm.
6. Click Apply Changes.

Related tasks
Creating custom alarms on page 47

Disabling global custom alarms system wide

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

Steps
1. Go to Grid Management > NMS Management > Alarms > Custom.
2. In the Global Custom Alarms table, click Edit next to the alarm you want to disable.
3. Clear Enabled for the alarm.
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 (as described in the Grid Primer) or, if you want to immediately clear the alarm rather than wait for the attribute value to change (which will result in a change to the alarm state), you can clear the triggered alarm.

About this task
The following procedure is useful for immediately clearing an alarm against an attribute whose value does not change often (for example, state attributes).
Steps

1. Disable the alarm, as described earlier in this section.

2. At the Admin Node, access a command shell and log in as root using the password listed in the Passwords.txt file.

3. Restart the NMS service:
   `/etc/init.d/nms restart`

4. Log out of the Admin Node:
   `exit`
   The current triggered alarm is cleared from the NMS MI.

Related concepts

`Disabling alarms` on page 51

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.

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

- StorageGRID Webscale software version
- Operating system version
- System-level and location-level attribute information
- All alarms raised in the last seven days
- Current status of all grid tasks, including historical data
- Events information as listed on the SSM > Events > Overview page
- Admin Node database usage
- Number of lost replicated objects (zero or more)
- Number of missing replicated objects (zero or more)
- Number of lost copies of erasure coded object data (zero or more)
- Grid configuration settings
- NMS entities
- Active ILM policy
- Provisioned grid specification file.

By analyzing this information, technical support can help you determine the health and status of your StorageGRID Webscale system, proactively troubleshooting 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, see the technical support site.

NetApp Support
Triggering AutoSupport messages

You can manually trigger an AutoSupport message at any time.

Steps

1. Log in to the NMS MI using the Admin or Vendor Account.
2. Go to Grid Management > NMS Management > AutoSupport > 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 e-mail server is correctly configured and that your e-mail server is running.

Related tasks

Configuring e-mail server settings on page 34

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

Disabling weekly AutoSupport messages

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

About this task

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

Steps

1. Log in to the NMS MI using the Admin or Vendor Account.
2. Go to Grid Management > NMS Management > AutoSupport > 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 e-mail server is correctly configured and that your e-mail 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 e-mail server must be correctly configured.

**Related tasks**

*Configuring e-mail server settings* on page 34

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

**Monitoring servers and grid nodes**

**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 through the NMS MI. 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

Notification types on page 32

Resetting event counters

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

Steps

1. Go to SSM > Events > Configuration > Main.
2. Select the **Reset** check boxes for the specific counters to be reset.
3. 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 information about the status of StorageGRID Webscale Appliance Storage Nodes in the NMS MI, such as appliance hardware, connectivity issues, alarm notifications, node services, and disk device information.

**Viewing the appliance Storage Node in the NMS Management Interface**

You can view the StorageGRID Webscale appliance Storage Node in the Network Management System (NMS) Management Interface (MI). You might want to view the E-Series array name and review appliance-specific information to ensure correct configuration and status.

**About this task**

Each StorageGRID Webscale appliance is represented as one Storage Node in the NMS MI.

The appliance Storage Node information appears in the NMS MI SSM > Resources view, which reports on the service health and all computational, disk device, and network resources. In the Resources view, you can also see memory, storage hardware, network resources, network interfaces, network addresses, and receipt and transmittal information.

**Steps**

1. From the NMS MI Grid Topology tree, select `site > Storage Node > SSM > Resources`.
2. In the **Resources** view, click the **Overview** tab:
3. In the **Memory** section, note the information in the **Installed Memory** field.

   The Installed Memory for the appliance version shows 25.3 GB of RAM.

4. 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).

5. In the **Disk Devices** section, note the device names.

   These LUN names match the LUN names you see if you connect SANtricity to the E2700 controller. To help you interpret disk read and write statistics related to volume mount points, the names in the Disk Devices section match the device names in the Volumes section on this page:

6. In the **Storage Hardware** section, note the information in these fields.

   This section appears only if the Storage Node is an appliance. If not, all the attributes and alarms associated with storage hardware do not display on tabs within **SSM > Resources**.
### Storage Hardware

<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</td>
</tr>
</tbody>
</table>
| Storage Controller Management IP | Management IP address of the E2700 controller  
You can use this IP to connect SANtricity to the E2700 controller in this StorageGRID Webscale appliance to troubleshoot storage issues. |
| Storage Controller Model       | The physical type of Storage Node controller: for example, 2u12 or 4u60                                                                    |
| Storage Controller WWN         | The worldwide identifier of the E2700 controller, as shown in SANtricity                                                                    |
| Storage Appliance Chassis Serial Number | Serial number associated with the appliance.                                                                                          |
| Software Platform              | The software platform used to generate the storage hardware status and alarms.                                                            |
| Overall Power Supply Status    | The status of power to a StorageGRID Webscale appliance enclosure                                                                       |

### Network Resources

- **Received Data Rate:** 5.97 Mbps
- **Transmitted Data Rate:** 6.94 Mbps
- **Received Bytes:** 96.7 GB
- **Transmitted Bytes:** 97 GB

### Network Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>Hardware Address</th>
<th>Speed</th>
<th>Duplex</th>
<th>Auto Negotiate</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>hlc2</td>
<td>00:A8:98:68:61:09</td>
<td>10 Gigabit</td>
<td>Off</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>hlc4</td>
<td>00:A8:98:68:01:09</td>
<td>10 Gigabit</td>
<td>Off</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>mtc2</td>
<td>00:96:54:29:59:45</td>
<td>Not in use</td>
<td>Not in use</td>
<td>Not in use</td>
<td></td>
</tr>
</tbody>
</table>

### Network Addresses

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>hlc2</td>
<td>172.26.121.267</td>
</tr>
<tr>
<td>hlc2</td>
<td>fe80::2a8:98ff:fe98:109</td>
</tr>
<tr>
<td>hlc4</td>
<td>172.26.121.267</td>
</tr>
<tr>
<td>hlc4</td>
<td>fe80::2a8:98ff:fe98:109</td>
</tr>
<tr>
<td>mtc2</td>
<td>169.254.6.1</td>
</tr>
</tbody>
</table>

### Receive

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
<th>Errors</th>
<th>Dropped</th>
<th>Frame Overruns</th>
<th>Frames</th>
</tr>
</thead>
<tbody>
<tr>
<td>hlc2</td>
<td>96.5 GB</td>
<td>482,160,023</td>
<td>0</td>
<td>13</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>hlc4</td>
<td>1.474,082</td>
<td>0</td>
<td>1,474,082</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mtc2</td>
<td>0 B</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supply A and B Status</td>
<td>The status of power supply A or B in the StorageGRID Webscale appliance</td>
</tr>
<tr>
<td>CPU Temperature</td>
<td>The temperature of E5600SG controller CPU</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>
<tr>
<td>Storage Controller Status</td>
<td>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. Then, ensure that no other alarms exist that apply to the E5600SG controller.</td>
</tr>
</tbody>
</table>

7. In the **Storage Hardware** section, note that each of status fields have associated alarms:

<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*.

8. In the **Network Resources**, **Network Interfaces**, and **Network Addresses** sections, note the information in these fields.

The interface names encode the port numbers: for example, a hic2 and hic4 could be 10 GB ports. These two ports might exist in an active/standby bond, rather than operating independently, and they would appear with the same IP address. To distinguish the active port, note the bytes and packets received in the Receive table.

**Related information**

*StorageGRID Webscale 10.2 Troubleshooting Guide*

*NetApp Documentation: SANtricity Storage Manager*

**Resolving hardware-based events in the NMS MI**

You can view the events related to the StorageGRID Webscale appliance in the NMS Management Interface (MI). 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 raise alarms in the NMS MI.

About this task

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

For details about the events and alarms, refer to the alarms reference and troubleshooting information.

Steps

1. From the NMS MI Grid Topology tree, select `<site> > <Storage Node> > SSM > Events`.
2. In the **System Events** section, note the count for Storage Hardware Events.
3. If a hardware event is noted here, identify the cause by completing the following steps:
   a. Select `<Storage Node> > SSM > Resources`.
   b. In the **Resources** view, select the **Overview** tab.
   c. Look for abnormal conditions in the **Storage Hardware** section.
What information lifecycle management is

Information lifecycle management (ILM) settings determine how an object’s data is managed and protected from loss over time. These settings are applied through an active ILM policy, which is made up of ILM rules.

Every object ingested into the StorageGRID Webscale system is evaluated against the system’s active ILM policy and then its object data is copied and distributed based on the active ILM policy’s ILM rules. An object’s metadata is managed by the DDS service and not through ILM rules.

What an information lifecycle management policy is

An ILM policy is a set of prioritized ILM rules that specify the instructions for managing object data over time. More than one ILM policy can be created; however, only one is ever active. The active ILM policy is the policy against which objects are evaluated.

When the StorageGRID Webscale system is first installed, the active ILM policy is the built-in policy Baseline 2 Copy Rule v1.0. This ILM policy contains the built-in ILM rules Make 2 copies v1.0 and Purge Deleted Objects v1.0.

Order of ILM rules within an ILM policy

The order of ILM rules within an ILM policy determines how ILM rules are applied. An object’s metadata is used to filter against matching criteria configured in ILM rules. When a match is found, the ILM rule is applied.

The following figure shows the default ILM policy with ordered ILM rules.

The following figure describes the logic used to determine if an ILM rule applies to an object.
The object is first evaluated against the top priority ILM rule and then subsequent ILM until a match is made. If a match is not found after evaluating all ILM rules, the default ILM rule is applied. 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 so that, if after evaluating all ILM rules and a match is not made, the default ILM rule is applied. When the StorageGRID Webscale system is first installed, the built-in ILM rule Make 2 Copies is the default ILM rule.

The example shown in the following figure illustrates the importance of ordering ILM rules correctly.
The ILM rules shown in this figure should store three copies for objects ingested through the S3 interface that match both specific Key and Bucket Name metadata and should store only two copies ingested through the S3 interface that only match the specified Key metadata. In the example shown on the left, the three-copy ILM rule for S3 objects with Key and Bucket Name metadata is not the top priority ILM rule and therefore is never applied because all objects ingested that match the Key metadata match the first ILM rule and Bucket Name metadata is never evaluated. In the case shown on the right, the ILM rules are ordered correctly for what is intended, which is to make three copies for objects ingested through S3 that match both specified Key and Bucket Name metadata.

**ILM policy updates**

**Warning:** Errors in an ILM policy can cause unrecoverable data loss. Carefully review the policy before activating it to make sure it will work as intended.

Typical reasons for updating an ILM policy include:

- An error exists in the current ILM policy
- Changes to a storage pool
- An Archive Node is added to the StorageGRID Webscale system
- New client application connections
- New storage retention requirements (for example, a change in regulatory requirements) are defined.

If you change the ILM policy, objects that have completed ILM evaluation are not re-evaluated against the updated ILM policy and object data stays “as is”. Any object that has been ingested, but not yet evaluated, is managed according to the new ILM policy.

After you activate an updated ILM policy, the StorageGRID Webscale system immediately starts applying that ILM policy to all newly ingested objects. To verify the ILM policy, you might want to activate and verify it with test objects at a time when normal ingest does not occur.
If the updated ILM policy includes an ILM rule to move object data to a new storage pool after a set period of time, it might not be practical to wait to verify this future placement. You might want to activate and verify an ILM policy with a temporary or test ILM rule that uses shorter time periods, but is otherwise identical to the current ILM policy, before activating the final version of your ILM policy for regular operations.

**ILM policy version numbers**

Each ILM policy is automatically assigned a version number in the form major.minor (for example, 2.5). A change to the ILM policy triggers a major revision. A change to an ILM rule that is part of the ILM policy triggers a minor revision.

**What information lifecycle management rules are**

Information lifecycle management (ILM) rules are used by ILM policies to determine how and where object data is stored over time.

ILM rules determine:

- Location: where an object’s data is stored
- Storage: the type of storage used to store object data (disc or archival media)
- Loss protection: how copies are made and the number
- Retention: the changes over time to how an object’s data is managed, where it is stored and how it is protected from loss.

Every object ingested into the StorageGRID Webscale system is evaluated against ILM rules that make up the active ILM policy. For example, Figure 28 shows an ILM rule that dictates that at ingest one copy is stored at data center site one (DC1) on disk (Storage Nodes), one copy is stored at data center site two (DC2) on disk (Storage Nodes), and that one copy is stored at DC2 (Archive Node). At the end of one year, the copy on disk at DC2 is deleted.
Types of ILM rules

There are different types of ILM rules: Active, Active, Saved, and Built-in.

- **Active ILM rules**
  Active ILM rules are ILM rules currently used by the active ILM policy. You can view the list of active ILM rules at Grid Configuration > ILM Management > Overview > Active Policy.

- **Historical ILM rules**
  Historical ILM rules are ILM rules that were activated in the past. This includes ILM rules that are currently active and ILM rules that are no longer active. You can view the list of historical ILM rules with their most recent start and end times at Grid Configuration > ILM Management > Overview > Historical Rules.

- **Saved ILM rules**
  Saved ILM rules are ILM rules that have been defined, but not necessarily activated. You can view saved ILM rules at Grid Configuration > ILM Management > Configuration > Saved Rules.
• Built-in ILM rules
  The default active ILM policy contains the built-in ILM rules, Purge Deleted Objects v1.0 and Make 2 Copies v1.0. These ILM rules cannot be modified or deleted. However, you can choose to deactivate them if one or the other does not meet your object storage and protection requirements.

  The Purge Deleted Objects ILM rule specifies that all copies of an objected are purged when a client delete is issued. This built-in default ILM rule, ensures that object data does not remain in the system after a delete command is issued.
  The Make 2 Copies ILM rule specifies that two copies are stored indefinitely on any disk in the StorageGRID Webscale system (that is, in the All Storage Nodes storage pool). This built-in default ILM rule, ensures that all ingested objects are preserved.

**ILM rule version numbers**

Each ILM rule is automatically assigned a version number with the form major.minor (for example, 2.5). The first time an ILM rule is created, its version number is 1.0. A change to the ILM rule triggers a minor revision.

The version number is incremented each time the ILM rule is modified. When the minor revision number reaches ten, the major revision number increases by one. For example, the version number changes from 1.9 to 2.0.
Determining storage locations

You determine the locations where object data is stored through the configuration of storage pools, which requires the configuration of storage grades.

Storage grades

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 such as Flash, SAS, SATA, and tape, a label name 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 will reside.

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, SAS or SATA. Site is the location to which object data is stored.

Storage pools are configured based on how content placement instructions for an ILM rule are to be configured. How may copies will be made and of what type will they be? Will object data be replicated, erasure coded, or both? Will object data be archived? Where will objects be stored? 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 one copy on disc (Storage Node) when keeping one copy in the Archive Node.

The following figure shows examples of storage pools for a DC1 + DC2 + Archive topology that uses replication when making copies.

- DC1 SATA: All Storage Nodes (LDR services) at DC1 with SATA disks
- DC1 SAS: All Storage Nodes (LDR services) at DC1 with SAS disks
- DC2 SATA: All Storage Nodes (LDR services) at DC2 SATA disks
- DC1 + DC2 SATA: All Storage Nodes (LDR services) with SATA disks
- Archive: Archive media (tape) at DC2 site

An Erasure Coding profile allows you to associate 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 to create an erasure coded copy whose fragments are distributed amongst 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 erasure coding scheme selected for the Erasure Coding profile. These data and parity fragments are distributed amongst the associated storage pool's Storage Nodes. For example, an erasure coding scheme of 6+3 creates six data fragments and three parity fragments distributed across nine Storage Nodes.

An erasure coding scheme is defined by the erasure code's parameters and determines the maximum number of fragments that can be lost while maintaining the ability to retrieve the object. An erasure code's parameters are the number of data and parity fragments generated for each part of an erasure

Related concepts

What an Erasure Coding profile is on page 70

What an Erasure Coding profile is

An Erasure Coding profile allows you to associate 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 to create an erasure coded copy whose fragments are distributed amongst 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 erasure coding scheme selected for the Erasure Coding profile. These data and parity fragments are distributed amongst the associated storage pool's Storage Nodes. For example, an erasure coding scheme of 6+3 creates six data fragments and three parity fragments distributed across nine Storage Nodes.

An erasure coding scheme is defined by the erasure code's parameters and determines the maximum number of fragments that can be lost while maintaining the ability to retrieve the object. An erasure code's parameters are the number of data and parity fragments generated for each part of an erasure
coded object. For example, in a 6+3 erasure coding scheme, each part of object data is encoded into six data fragments and three parity fragments 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 the ability to recover an object depends on the erasure coding scheme used.

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 and cannot be retrieved.
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. At the same time, 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 may 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 one megabyte.

**Matching criteria and filter evaluation**

A filter is a set of criteria used to evaluate an object and determine which ILM rule should be applied to an ingested object's data. The main element used to filter objects to the correct ILM rule is metadata.

Filter logic: Because a filter includes multiple elements and an ILM rule can contain multiple filters, Boolean logic is used to determine matches. The “AND” operand is used for logic within a filter and the “OR” operand is used between filters. If logic is not matched within the first filter, the next filter is evaluated.

Metadata: Metadata criteria differs in S3, Swift, CDMI, and SGAPI. If metadata is selected for use as filtering criteria, determine the type of applications that will be ingesting objects into the StorageGRID Webscale system: S3, Swift, CDMI, or SGAPI.

**StorageGRID API metadata tags**

StorageGRID API (SGAPI) metadata tags can be either strings or integers. Strings are used for metadata such as object location. Strings are case-sensitive. Integers are used for metadata such as site ID.

The following figure lists the SGAPI metadata that you can use to create ILM rules. The client application must supply and confirm the existence of custom metadata for each object. When developing an ILM policy that uses custom metadata, you must work with the developer of the client application to ensure that the ILM policy performs as intended.

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Code</th>
<th>Definition</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDMI Protocol Handler Version</td>
<td>PCDM</td>
<td>If present, indicates that the object was ingested into the StorageGRID Webscale system using CDMI. Objects ingested using CDMI also contain PHTP metadata.</td>
<td>Used to create filters that match all objects ingested through CDMI. Set the CDMI Protocol Handler Version to Exists or to Greater Than 0.</td>
</tr>
<tr>
<td>Metadata</td>
<td>Code</td>
<td>Definition</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>External Application Identifier</td>
<td>XAID</td>
<td>The client application that created the object.</td>
<td>To create ILM rules for StorageGRID API applications where the client application specifies values for XAID, XTYP, and XVER.</td>
</tr>
<tr>
<td>External Object Type</td>
<td>XTYP</td>
<td>The type of object, as defined by the external application.</td>
<td></td>
</tr>
<tr>
<td>External Object Version</td>
<td>XVER</td>
<td>The version of the object, as defined by the external application.</td>
<td></td>
</tr>
</tbody>
</table>
| Ingest Time                    | CTME | The “Object Store Begin” timestamp. The time when the object starts to be-ingested into the StorageGRID Webscale system. | Used to specify object ingest time in microseconds elapsed since January 1, 1970.  
  Note: Ingest Time must be specified in microseconds, not seconds. |
| HTTP Protocol Handler Version  | PHTP | Indicates objects ingested through the SGAPI or CDMI interfaces. Objects ingested using CDMI will also contain PHTP metadata. | Used to create filters that match objects ingested through the SGAPI and CDMI interfaces. Set the HTTP Protocol Handler Version to Greater Than 0. |
| Last Access Time               | LATM | The last time that the object was retrieved from the StorageGRID Webscale system by an SGAPI client or CDMI client with Last Access Time enabled. | Specifies last access time in microseconds elapsed since January 1, 1970.  
  Note: Last Access Time must be specified in microseconds, not seconds. |
<p>| Object Size                    | CSIZ | Plain-text object size in bytes                                           | For instance, used to ensure that small objects are stored to disk and not tape, which avoids the poor retrieval performance of tape. |</p>
<table>
<thead>
<tr>
<th>Metadata</th>
<th>Code</th>
<th>Definition</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Security Partition | SPAR | The decimal identification number of a security partition. This value corresponds to the SPAR field reported in the audit messages HDEL, HGEE, HHEA, HPUE, and ORLM. For information about audit messages, see the *Audit Message Reference*. | For SGAPI or CDMI, to determine the SPAR value for a security partition, add the security partition number to the Partition Identifier for the security partition. Note: Security partitions are ignored for objects ingested through the S3 and Swift interfaces. The base security partition number is derived by converting the hexadecimal 0x4854545000000000 to a decimal (5211883371348623360) where 0x4854 corresponds to the four character code HTTP. Prerequisites • Base security partition number: 5211883371348623360 • Value for Partition Identifier (see **HTTP Management > Security Partitions > Overview > Main**) Steps 1. Add the Partition Identifier number to the base security partition number: 

```
security_partition_number + Partition_Identifier = SPAR
```

For example:

```
521188337134862360 + 1 = 521188337134862361
```

The Security Partition metadata value is:

```
521188337134862361
```

| Source Node ID  | INID | The node ID of the service which first processed the data and created the original object. | Normally not used for ILM rules. |
### Metadata

<table>
<thead>
<tr>
<th>User Number</th>
<th>NUM</th>
<th>Definition</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>User String</td>
<td>STR</td>
<td>String value set by the client application.</td>
<td>Used to filter objects based on a string value.</td>
</tr>
</tbody>
</table>

### Related tasks

*Specifying time values for metadata* on page 76

### Related information

*StorageGRID Webscale 10.2 Troubleshooting Guide*

### CDMI metadata tags

Filtering can be set against CDMI metadata criteria; however, only non-UTF8 metadata names and values can be used. Supplying and confirming the existence of CDMI metadata for each object is the responsibility of the client application.

For the CDMI metadata filter to be applied against an object, the object must include the CDMI metadata listed in the filter, or else the object is evaluated against the next filter. When developing an ILM policy that uses CDMI metadata, you must work with the developer of the client application to ensure that the ILM policy performs as intended.

Filtering can be set against the following CDMI metadata:

- Object Size
- Last Access Time
- User Metadata

### S3 metadata tags

Using a filter as criteria in a search involves the use of metadata. Use the metadata filter to evaluate an object and determine which ILM rule should be applied to an ingested object's data.

You can use the following S3 properties to filter data:

- Account ID
- Bucket name
- Key
- Last access time
- Object size
- User metadata

### Swift metadata tags

Using a filter as criteria in a search involves the use of metadata. Use the metadata filter to evaluate an object and determine which ILM rule should be applied to an ingested object's data.

You can use the following Swift properties to filter data:

- Account ID
- Container name
Specifying time values for metadata

When you configure an ILM rule’s matching criteria, you can specify time for the CTME and LATM metadata tags.

Steps

1. Determine the difference between local time and UTC time using a UTC Time conversion tool, such as one of the following:
   - The Time Now: www.thetimenow.com/utc/coordinated_universal_time

2. Calculate the UTC time in microseconds by using the Linux command:
   
   ```
   date -d 'YYYY-MM-DD HH:MM:SS UTC' +%s000000
   ```
   
   Example
   
   ```
   # date -d '2015-03-14 00:00:00 UTC' +%s000000
   14262912000000
   ```

Related concepts

StorageGRID API metadata tags on page 72

Reference time

Because each content placement instruction you configure for an ILM rule uses time to determine when to carry out its instructions, you must select a reference time from which time is calculated.

The following reference times are available for ILM rules:

- **Ingest Time**
  All placement instructions are specified relative to when the object was ingested. Time can be specified in days or years. Ingest Time is the default reference time for ILM rules.

- **Last Access Time**
  The time associated with the object when a client application with Last Access Time enabled retrieves the object. Last Access Time metadata updates when a client application with Last Access Time enabled in its profile retrieves the object. If selected, this system metadata tag applies to all objects regardless of the interface (S3, Swift, CDMI, or SGAPI) used.
**Note:** When you enable Last Access Time for an S3, Swift, CDMI, or SGAPI client, the StorageGRID Webscale system updates metadata each time the client retrieves an object. As a result, Last Access Time affects system performance. It is recommended that you only enable Last Access Time when ILM policies use Last Access Time metadata.

- **User Defined Creation Time**
  For objects ingest through the either the S3 or Swift interface, you can use the information contained in a user defined metadata tag as reference time. Time is evaluated as seconds since January 1, 1970. If the timestamp cannot be extracted from the metadata tag (for instance, the tag does not exist), ingest time will be used as reference time.
  User defined metadata tag:
  - S3: `x-amz-meta-creation-time`
  - Swift: `X-Object-Meta-creation-time`

**Enabling or disabling Last Access Time**

You can enable and disable Last Access Time for individual StorageGRID API clients and CDMI clients.

About this task

Use the HTTP profile to specify the Last Access Time setting. For more information about HTTP profiles, see the *StorageGRID API Reference* or the *Cloud Data Management Interface Integration Guide*.

Steps

1. Sign in to the NMS MI using an account that has Grid Management permissions.
2. Go to Grid Management > HTTP Management > Permissions > Configuration > Main > HTTP /CDMI and /UUID Namespaces.
3. Click Edit next to the HTTP profile that you want to modify.
4. Perform one of the following actions:
   - To enable Last Access Time, select the Read and the Last Access Time check boxes for each SGAPI or CDMI client.
   - To disable Last Access Time, clear the Last Access Time check box for each SGAPI or CDMI client.
5. Click Apply Changes.

With Last Access Time enabled, you can create an ILM rule that uses Last Access Time as the Reference Time.

**Content placement instructions**

Content placement instructions determine where, when and how object data is stored. Each row in the Content Placement section of an ILM rule represents one copy of object data at a specified location.
(storage pool) and at a specified time. As well, each row determines how that copy is made: whether object data is replicated or erasure coded.

**Note:** An ILM rule must include at least one content placement instruction and at least one instruction must start on day 0.

To create copies, at least two content placement instructions must be active at the same time. If only one content placement instruction is active, only one instance of an object is retained by the StorageGRID Webscale system — there are no copies. To protect against permanent loss, it is recommended that an ILM rule always have at least two active content placement instructions. If there is only one instance of an object and the object is lost, it cannot be recovered.

**Warning:** Although it is possible to create an ILM rule with only one content placement instruction, it is not recommended. If an object is lost, it cannot be recovered.

Time limits can be set for how long a copy is kept at a specified location. If more than one content 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.

### Storage pools

Where object data is stored is determined by selecting a storage pool. For erasure coded object data, the selected storage pool also indicates (in parentheses) the erasure coding profile that will be used.

For erasure coded copies, multiple content placement instructions cannot simultaneously use the same Erasure Coding profile.

### Temporary copies if storage pool unavailable

For replicated copies, in addition to the preferred storage pool, content placement instructions should specify an alternate storage pool for a temporary copy. This storage pool is used in case the preferred storage pool is unavailable. Temporary copies are not used for object data that is erasure coded.

One special case where an alternate storage pool is usually inappropriate is when the preferred storage pool is archival media. In addition, Archive Nodes should not be used to store temporary copies.

**Warning:** The use of temporary copies is strongly recommended for replicated copies. Failure to specify an alternate storage pool puts object data at risk if the preferred pool is unavailable.

If the preferred storage pool is unavailable at the time that the ILM evaluation occurs (for example, if the Storage Nodes in the storage pool are full), the following happens:

1. Object data is copied to each preferred storage pool if possible.
2. For each preferred storage pool that is unavailable, a copy is made in the alternate storage pool.
3. When a preferred storage pool becomes available, a copy is made in the preferred storage pool.
After copies are made for each preferred storage pool, temporary copies in all alternate storage pools are purged. No temporary copy is purged until copies are made in all preferred storage pools.

For example, if content placement instructions specify the following placement for all content at ingest:

- Store two copies at DC1 (alternate placement for a temporary copy is DC2)
- Store one copy at the local site (alternate placement for a temporary copy is DC2)

If the DC1 storage pool is unavailable when the object is ingested, two temporary copies are stored in the DC2 storage pool and one copy is stored at the local site. When the DC1 pool becomes available, two copies are made in the DC1 storage pool and the DC2 copies are deleted.

If neither the DC1 storage pool nor the local site storage pool is available when the object is ingested, three temporary copies are made in the DC2 storage pool. When the local site storage pool becomes available, a copy is made at the local site, but temporary copies at DC2 are not purged (all three are retained until the ILM rule is satisfied and copies are placed for all preferred storage pools). When the DC1 storage pool becomes available, two copies are made in the DC1 storage pool, and all three temporary copies are purged from DC2 site.

Copy age

The age of a copy (how long a copy has been stored in a location) can be used in a number of ways. For example, you might want to store three copies at ingest and delete one copy after a pre-defined period of time has elapsed.

Retention diagram

The Retention Diagram pictorially represents content placement instructions and displays what happens to a copy over time. Each line represents an instance of object data, the storage pool where it is to be stored, and the time when it is stored in that storage pool.

Note: Remember that 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.

The icon representing the copy indicates how that copy is made:

- Erasure coded copy
- Replicated copy

Each line of the Retention Diagram is derived from the equivalent content placement instruction and can be dynamically updated by clicking Refresh whenever you update content placement instructions. Use the Retention Diagram to help determine if content placement instructions are configured correctly for the ILM rule.
Because the Retention Diagram indicates the number of copies stored to a storage pool at a specified time, it is a useful tool to help determine how object data is protected from loss over time and if those protections are adequate. Are there always going to be adequate numbers of copies distributed throughout the system to protect data from loss?

**Dual Commit**

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 may be made in different locations and initial “Dual Commit” copies purged.

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.

For client applications that interface to the StorageGRID Webscale system through S3, Swift, or CDMI, Dual Commit is enabled by default. For client applications that interface to the StorageGRID Webscale system through SGAPI, Dual Commit is disabled by default.

If ILM rules are configured to only store one instance of replicated object data, disable Dual Commit to avoid unnecessarily making and purging the copy created by the dual commit operation.

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

**Related information**

- *StorageGRID Webscale 10.2 Simple Storage Service Implementation Guide*
- *StorageGRID Webscale 10.2 Swift Implementation Guide*
- *StorageGRID Webscale 10.2 Cloud Data Management Interface Implementation Guide*
- *StorageGRID Webscale 10.2 StorageGRID API Reference*

**Object deletions and purging**

The ILM policy can be used to dictate the actions taken by the StorageGRID Webscale system when an object is deleted by the client application: purge the object from the StorageGRID Webscale system or keep the object regardless of the client application’s actions. This latter case protects against accidental or malicious object deletions.

To configure an ILM policy to purge objects from the StorageGRID Webscale system when they are deleted by the client application, the ILM policy must contain an ILM rule with the filter option Object not referenced by API selected. In general this ILM rule is set as the highest priority ILM rule, but in some cases may not be depending on the requirements of the ILM policy’s logic. The default active ILM policy contains the built-in ILM rule, Purge Deleted Objects v1.0. The Purge Deleted Objects ILM rule specifies that all copies of an objected are purge when a client delete is issued. This built-in default ILM rule, ensures that object data does not remain in the system after a delete command is issued.

**How deletion protection works**

Deletion protection protects objects from accidental deletion.

The StorageGRID Webscale system offers the following levels of deletion protection:

- Preserved: based on object metadata
Table 1: Deletion Protection Levels

<table>
<thead>
<tr>
<th>Scope</th>
<th>Settings</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preserved</td>
<td>Content that meets specific ILM filtering criteria</td>
<td>The client application is allowed to delete the object; the object can no longer be referenced by the client; the object is kept in the StorageGRID Webscale system.</td>
</tr>
<tr>
<td>Protected System-wide</td>
<td>The ILM policy allows purging when the client application deletes the object (must be changed from default) Disable Client Delete disabled (default)</td>
<td>The client application is allowed to delete the object; the object can no longer be referenced by the client. The object is purged from the StorageGRID Webscale system.</td>
</tr>
</tbody>
</table>

How deletion protection settings work together

The following decision tree and table summarize what happens when a client application deletes an object. What happens is dependent on how deletion protection settings are configured.

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
</tr>
<tr>
<td>B</td>
</tr>
<tr>
<td>C</td>
</tr>
</tbody>
</table>
Deletion protection settings

You can choose to prevent object deletion for specific objects as they are evaluated against ILM rules or for all objects system wide.

ILM rules

The ILM policy can be configured to use ILM rules that dictate what to do when an object is deleted by the client: purge the object from the StorageGRID Webscale system or keep it.

System wide client delete protection

Enabling Disable Client Delete under Grid Management > Grid Configuration > Configuration > Main overrides the delete and last access time permissions defined for profiles on the Grid Management > HTTP Management > Permissions > Configuration > Main page. Disable Client Delete is a system wide setting.

The following actions occur depending on the API client:

- For S3 clients, all delete bucket and delete object requests are denied.
- For Swift clients, all delete container and delete object requests are denied.
- For a CDMI client, all delete, metadata update, and last access time updates are denied.
- For a StorageGRID API client, all HTTP DELETE operations are denied.
DELETE permission in HTTP profile

The DELETE permission under Grid Management > HTTP Management > Permissions > Configuration > Main indicates if clients assigned the HTTP profile can use the HTTP DELETE command to release a UUID handle. For more information, see either the StorageGRID API Reference or Cloud Data Management Interface Integration Guide.

Related concepts

Object deletions and purging on page 80

Related tasks

Enabling or disabling Last Access Time on page 77
Designing and implementing an ILM policy is a process that requires careful planning. You must define the logic for how objects will be filtered and how object data will be distributed, taking into account the topology of the StorageGRID Webscale system, object protection requirements, and available storage types, along with client interfaces and access patterns.

**Warning:** An ILM policy that has been incorrectly configured can result in unrecoverable data loss. Carefully review the ILM policy and its ILM rules before activating it. Always confirm that the policy will work as intended.

It is recommended that you first plan the logic of your ILM policy and its ILM rules on paper, carefully analyzing all possible scenarios to make sure that the ILM policy is sound and will protect objects from loss as intended.

Before creating an ILM policy, determine the following:

- The number and type of copies (replicated or erasure coded) required, 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

**Related concepts**

*What information lifecycle management is* on page 63

---

### Configuring information lifecycle management rules and policy

Configuring information lifecycle management rules and policy is restricted to user accounts with Grid Management permissions. All other accounts can only view ILM information.

#### Steps

1. Configure storage grades on page 84
2. Configuring storage pools on page 87
3. Configuring Erasure Coding profiles on page 89
4. Creating an ILM rule on page 91
5. Configure and activate an ILM policy on page 94

#### Configure storage grades

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 such as Flash, SAS, SATA, and tape, a label name 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 will reside.
Note: You cannot configure storage grades for Archive Nodes.

Configuring a storage grade is a two-step process:

1. Create a list of storage grades.
2. Assign a storage grade to LDR services.

If storage grade is not a concern (for example, your StorageGRID Webscale system includes only one type of disk storage), skip configuring storage grades and instead use the system-generated storage grade “All Disks” when configuring a storage pool.

Related tasks

Creating a list of storage grades on page 85
Assigning storage grade to LDR services on page 86

Creating a list of storage grades

Do not create more storage grades than necessary. For example, there is no need to create one storage grade for each Storage Node. Doing so can create backlog problems if LDR services become unavailable.

Steps

1. Sign in to the NMS MI using an account with Grid Management permissions.
2. In the NMS MI, go to Grid Management > Grid Configuration > Storage Grades > Configuration > Main.
3. For each storage grade you need to define, click Insert to add a row and enter a label for the storage grade.
4. To edit an existing storage grade, click **Edit** and modify the label as required. The Default storage grade cannot be modified. It is reserved for new LDR services added during a StorageGRID Webscale system expansion.

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

5. Click **Apply Changes**.

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

**Related tasks**

_Assigning storage grade to LDR services_ on page 86

**Assigning storage grade to LDR services**

After a storage grade has been configured, assign a storage grade to each LDR service. In general, this step is done only once to match storage grades to the StorageGRID Webscale system’s topology. You do not need to change this mapping again unless you add new storage.

**Before you begin**

A list of storage grades has been created.

**Steps**

1. Sign in to the NMS MI using an account that has Grid Management permissions.

2. In the NMS MI, go to **Grid Management > Grid Configuration > Storage Grades > Configuration > Main**.
3. For each LDR service, click Edit and select a storage grade from the list.

4. Click Apply Changes.

   Warning: Assigning a storage grade is only performed once unless you add or replace Storage Nodes. 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.

Related concepts

Configure storage grades on page 84

Configuring storage pools

Before you begin

Storage grades are configured.

About this task

When creating storage pools, follow these basic 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 that are as large as possible. Small storage pools can cause significant replication backlogs if resources become 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.
- For a storage pool that will be associated with an erasure code, it is recommended that you 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 the Archive Node's Target Type is Cloud Tiering - Simple Storage Service (S3), the Archive Node must be in its own storage pool.

The default ILM policy contains the built-in ILM rule Make 2 Copies, which uses the built-in storage pool All Storage Nodes. The All Storage Nodes pool is automatically set up and contains all disks in the StorageGRID Webscale deployment. You cannot delete or modify this pool; however, it is not mandatory to include this storage pool in your ILM policy.

Steps

1. Sign in to the NMS MI using an account that has Grid Management permissions.

2. In the NMS MI, go to Grid Management > ILM Management > Configuration > Storage Pools.

3. To add a storage pool:
   a. Click Insert at the end of the row for the last storage pool.
b. Enter a representative name for the storage pool. Create a name that makes for easy identification when configuring Erasure Coding profiles and ILM rules.

c. 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.

d. 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 the of 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.

e. 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.

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

4. To change the storage pool name, enter a new name beside Pool Name.

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

6. Click Apply Changes.

   Warning: Before making changes to storage pool definitions, carefully consider the impact on the ILM policy to make sure the policy will work as intended.

   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 concepts

Configure storage grades on page 84
Related tasks

Activating the ILM policy on page 95

Viewing current storage pools

Steps

1. In the NMS MI, go to Grid Management > ILM Management > Configuration > 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.

   ![Storage Pool Table](image)

   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

An Erasure Coding profile associates a storage pool with an erasure coding scheme, determining how many fragments are created and where those fragments are distributed. This Erasure Coding profile is then used to configure an ILM rule’s Content Placement instructions to create an erasure coded copy of object data.

Before you begin

Storage pools are configured.

About this task

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

Note: You must modify the default Erasure Coding profile listed on the page before adding a new profile.
Steps

1. Sign in to the NMS MI using an account that has Grid Management permissions.

2. In the NMS MI, go to Grid Management > ILM Management > Erasure Coding > Configuration > Main.

3. If this not the first profile, click Insert to add a new profile.

4. Enter a representative name for the Erasure Coding profile. Create a name that makes for easy identification when configuring ILM rules.

5. 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.

6. Select an available erasure coding scheme.
   
   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 the following:
   
   - **Storage Overhead**: Additional storage that is required to manage parity fragments for each erasure coded object. Value is calculated as a percentage of each object’s data size. Storage Overhead = Total number of parity fragments / Total number of data fragments.
   
   - **Storage Node Redundancy**: The number of Storage Nodes that can be lost while still maintaining the ability to retrieve erasure coded object data.

   - **Site Redundancy**: Lists whether or not the selected erasure code can support the loss of a site and still maintain the ability to retrieve erasure coded object data. To support site redundancy,
the selected storage pool must include multiple sites, each with enough Storage Nodes to support the loss of a site and still maintain the minimum fault loss tolerance of the selected erasure code. For example, to support site redundancy using a 6+3 erasure coding scheme, the selected storage pool must include three sites with three Storage Nodes at each site.

7. To add another profile, click Insert 
Once added an Erasure Coding profile cannot be deleted.

8. Click Apply Changes.

Related tasks
* Configuring storage pools on page 87

Creating an ILM rule

When creating ILM rules, pay particular attention to the type of copy required (erasure coded or replicated) and whether archiving is planned. 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 content placement instructions.

Before you begin

- You are logged in with an account that has Grid Management permissions.
- Storage pools are configured.
- To use last access time metadata, Last Access Time must be enabled for S3, Swift, CDMI, or StorageGRID API clients.

Steps

1. Sign in to the NMS MI using an account that has Grid Management permissions.
2. Go to Grid Management > ILM Management > Configuration > Rules.
4. Under Rule Name, enter a representative and unique name for the ILM rule.
5. Set up the first filter.
   a. Under Filter 1, enter a representative name for the filter.
   b. Specify whether the ILM rule applies to objects referenced by an API (S3, Swift, CDMI, or SGAPI).
   c. Specify whether the ILM rule applies to all objects ingested into the StorageGRID Webscale system or only to a subset defined by metadata.
      If you choose metadata, select a metadata type: S3, Swift, CDMI, or SGAPI. If the metadata criteria is an integer, the valid characters are digits (0-9). If the criteria is a string, any character is allowed. Strings are case-sensitive.
      Note: If an object does not have the metadata tag specified in the filtering criteria, the object does not match the filter.
   d. To add more metadata criteria for each API, click Insert next to the last criteria.
   e. To add more filters, click Insert next to the last filter name.
In order to match an ILM rule, an object must match one filter specified in the ILM rule (an OR operation). In order to match a filter, an object must meet all filter criteria (an AND operation).

6. Specify a reference time:
   a. Ingest Time
      Content placement instructions are specified relative to when the object was ingested. Time can be specified in days or years.
   b. Last Access Time
      The time associated with the object when a client application with Last Access Time enabled retrieves the object. This system metadata tag applies to all objects regardless of the interface (S3, Swift, CDMI, or SGAPI) used. For an ingested object that has never been retrieved, any ILM rule using Last Access Time will default to using the object’s create time.
   c. User Defined Creation Time
      For objects ingest through the either the S3 or Swift interfaces, you can use the information contained in custom metadata tags as reference time. Time is evaluated as seconds since January 1, 1970.

7. Configure content placement instructions to determine the number of copies made, the type of copy made, when the copy is made, and where each copy is stored. Each row represents one copy. To create more than one instance of an object’s data, multiple content placement instructions must be active at the same time.

   a. Specify the time (in days or years) when the content placement instruction becomes active. An ILM rule must contain at least one content placement instruction at Day 0 (ingest).
   b. Select the type of copy to be made: replicated or erasure coded.
      Note: 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 one megabyte.
   c. Select a storage pool to set the location where the copy will be stored. Available storage pools are dependent on the type of copy selected: replicated or erasure coded.
      For erasure coded copies:
      • The selected storage pool also indicates (in parentheses) the erasure coding profile that will be used.
      • Multiple content placement instructions cannot simultaneously use the same Erasure Coding profile.
      • With erasure coded object data, you cannot select a storage pool that includes an Archive Node. To archive data, add a second content placement instruction, select Replicated and then a storage pool that includes an Archive Node.
   d. Select the time period for which the copy will be stored in the selected storage pool.
      If Forever is not selected, after the selected time period expires, the content placement instructions for the next time period are applied at the next ILM evaluation time. When a time period ends, that instance of an object is purged from the StorageGRID Webscale system. Purging removes both object data and metadata.
e. If the type of copy is replicated, select a storage pool to temporarily place copies if the preferred storage pool is unavailable.
Erasure coded copies cannot be stored in a temporary storage pool.

f. Click **Insert** to add a new row. Each row represents one copy at a specified location and specified time.

**Warning:** Avoid creating ILM rules that reduce the number of copies to zero (except as part of an ILM rule to purge objects deleted by a client application). If objects have not been deleted by the client application, links from the client application to the objects are broken.

When placing copies in more than one storage pool, use distinct, non-overlapping storage pools. For example, do not use a storage pool that contains all Storage Nodes in the StorageGRID Webscale system and a second pool that contains all Storage Nodes at DC1.

**Warning:** Failure to specify distinct, non-overlapping storage pools can result in unexpected behavior and fewer copies than intended.

g. Click **Refresh** to update the Retention Diagram and display a visual representation of the configured content placement instructions. Each row represents one copy at a specific location and at a specific time.

**Note:** Click Refresh often as you edit an ILM rule to confirm that the ILM rule is defined as intended.

Verify that there are no gaps in the placement of copies. For instance, this example is not valid because no copies are maintained between day 12 and day 13:

8. Click **Apply Changes**.

A new ILM rule is created and appended with version number 1.0. You can view the new rule at **Grid Management > ILM Management > Configuration > Saved Rules**. The ILM rule is saved, but is not yet active.

**Related concepts**

- Matching criteria and filter evaluation on page 72
- Content placement instructions on page 77
- Configure and activate an ILM policy on page 94

**Related tasks**

- Configuring storage pools on page 87
- Enabling or disabling Last Access Time on page 77
Configure and activate an ILM policy

Activating an ILM policy is a two-step process.

1. Configure the proposed ILM policy.
2. Activate the proposed ILM policy.

Keep the ILM policy as simple as possible. This avoids potentially dangerous situations where object data is not protected as intended as changes are made to the StorageGRID Webscale system over time. You cannot configure an ILM policy that uses an ILM rule that creates erasure coded copies and an ILM rule that archives object data. To archive object data, you must only use ILM rules that create replicated copies.

Related tasks

Activating the ILM policy on page 95

Configuring the ILM policy

Steps

1. Sign in to the NMS MI using an account that has Grid Management permissions.
2. Go to Grid Management > ILM Management > Configuration > Proposed Policy.

The proposed ILM policy is displayed below the list of available ILM rules.

By default, the proposed ILM policy is the same as the active ILM policy when the proposed ILM policy is first displayed. The currently active ILM policy is displayed below the proposed ILM policy.

3. Optionally, change the name of the proposed ILM policy.
4. To add an ILM rule to the proposed policy, select the Add to Policy check box next to the ILM rule in the Saved Rules table. The ILM rule automatically appears in the Proposed Policy section.

5. To delete an ILM rule from the proposed policy, clear the Add to Policy check box in the Saved Rules list. You can also remove a rule from the proposed policy by clicking Delete.

6. To reorder the priority of ILM rules, drag them up or down.
   The order of ILM rules within an ILM policy is extremely important. ILM rules are evaluated as they are listed in the table: from top to bottom.
   
   **Warning:** The order of ILM rules within an ILM policy is extremely important. ILM rules are evaluated as they are listed in the table: from top to bottom.

7. Specify the default ILM rule for the proposed ILM policy by selecting Default. Every ILM policy must contain a default ILM rule.

8. Click Save.
   The proposed ILM policy configuration is saved.
   Review the filter criteria and the placement instructions carefully to ensure the proposed policy is correct.

9. Do one of the following:
   - If the proposed ILM policy is correct, click Activate.
     The ILM policy is now active.
   - If the proposed ILM policy is incorrect, click Revert to Active Policy.
     All changes are discarded.
     
     **Note:** It is not possible to revert to the active policy unless a proposed policy has first been saved.

**Related concepts**

*Matching criteria and filter evaluation* on page 72

**Related tasks**

*Activating the ILM policy* on page 95

**Activating the ILM policy**

Before activating the ILM policy, carefully analyze all possible scenarios to confirm that the ILM policy is sound and will protect object data as intended.

**About this task**

**Warning:** Errors in an ILM policy can cause unrecoverable data loss. Carefully review the policy before activating it to make sure it will work as intended.

**Steps**

1. Sign in to the NMS MI using an account that has Grid Management permissions.
2. Go to Grid Management > ILM Management > Configuration > Proposed Policy.
3. Carefully review the proposed ILM policy to make sure it is correct.
4. Click Activate.
5. Click OK to confirm you want to change the ILM policy.

The policy is now active and appears in Overview > Active Policies and Overview > Historical Policies. The name and version number of the active ILM policy is also displayed at CMS > Content > Overview > Main.

All new objects ingested into the StorageGRID Webscale system are stored according to the new ILM policy. Similarly, all objects marked for re-evaluation will be stored according to the new ILM policy.

6. Verify that the ILM policy is storing objects where you intended.

7. If required, apply the new ILM policy to previously evaluated objects.

If you choose to apply the new ILM policy to previously evaluated objects, the ILM Re-evaluation (User Triggered) grid task runs in the background and forces all CMS services to re-evaluate all objects. Copies are created and purged as necessary to meet the new ILM rules of the ILM policy.

Related tasks

Verifying ILM policy on page 96
Evaluating existing objects against new ILM policy on page 102

Verifying ILM policy

After you have activated a new ILM policy, ingest test objects into the StorageGRID Webscale system and confirm that copies are being made as intended and placed in the correct locations. Perform an “object lookup” for the ingested object. To confirm the location of an object’s data through an object lookup, you need the object’s identifier (CBID, UUID, S3 bucket/key, Swift container/object, or CDMI data object ID).

Before you begin

Object identifier, one of:

• CBID: An object’s CBID can be obtained from latest audit log, which is located on the Admin Node at /var/local/audit/export.

• UUID: When an object is ingested through the StorageGRID API (SGAPI) interface, the StorageGRID Webscale system returns a UUID to the client application.

• 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.

• 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.

• 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.

Before this task

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.

After you have obtained the object identifier, look up its location to confirm that it is correct.

**Steps**

1. In the NMS MI, go to **primary_Admin Node > CMN > Object Lookup > Configuration > Main**.

2. Enter the object’s identifier (CBID, UUID, S3 bucket/key, Swift container/object, or CDMI data object ID).

3. Click **Apply Changes**.

4. Click **Overview**.
The Object Lookup page displays the current location of the object and any metadata associated with the object.

Related concepts

*Configuring audit client access* on page 166

**Working with ILM rules and ILM polices**

**Modifying ILM rules**

You can modify existing ILM rules to change filters or content placement instructions.

**Steps**

1. Sign in to the NMS MI using an account that has Grid Management permissions.
2. Go to *Grid Management > ILM Management > Configuration > Rules*.
3. Select *Select Rule > ILM_rule_to_modify*.
4. Under *Matching Criteria* and *Reference Time*, modify filters as required.
5. Under **Content Placement**, modify content placement instructions as required.

6. Click **Apply Changes**.

   A new version of the ILM rule is created.

**Related concepts**

- *Matching criteria and filter evaluation* on page 72
- *Content placement instructions* on page 77
- *Configure and activate an ILM policy* on page 94

### Copying and creating a new ILM rule

You can copy an existing ILM rule and then use it as a starting point to create a new ILM rule.

**Steps**

1. Sign in to the NMS MI using an account that has Grid Management permissions.

2. Go to **Grid Management > ILM Management > Configuration > Saved Rules**.

3. Locate the ILM rule you want to copy and click **Copy**.

   The ILM rule opens in the **Grid Management > ILM Management > Configuration > Rules** page.

4. Change the name of the ILM rule.

5. Under **Matching Criteria** and **Reference Time**, modify filters as required.

6. Under **Content Placement**, modify content placement instructions as required.

7. Click **Apply Changes**.

   A new ILM rule is created.

**Related concepts**

- *Matching criteria and filter evaluation* on page 72
- *Content placement instructions* on page 77
- *Configure and activate an ILM policy* on page 94

### Deleting an ILM rule

To keep the list of saved ILM rules manageable, delete any saved ILM rules that you are not likely to use again such as test ILM rules. You cannot delete the default ILM rule or ILM rules that are included in the active and proposed ILM policies.

**Steps**

1. Sign in to the NMS MI using an account that has Grid Management permissions.

2. **Grid Management > ILM Management > Configuration > Saved Rules**.

3. Locate the ILM rule you want to delete and click **Delete**.

4. Click **OK** to confirm that you want to delete the ILM rule.

   **Note:** Before you delete an ILM rule, confirm that it is not used in a proposed ILM policy that you intend to activate.
5. Click **Apply Changes**.

The ILM rule is removed from the list of Saved Rules.

**Note:** If the ILM rule is removed from the list of Saved Rules.

**Related concepts**

*Configure and activate an ILM policy* on page 94

**Viewing historical ILM policies**

Historical ILM policies are never deleted and can be viewed at any time.

**Steps**

1. Go to **Grid Management > ILM Management > Overview > Historical Policies**.

2. To view the ILM rules and storage pools associated with an ILM policy, click the policy name. All policies are displayed with start and end dates.

3. Click the Expand All [ ] to display more information about the storage pools and the rules.

4. Click the Close All [ ] to hide the additional information, to display more information about the storage pools and the rules.

**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.

**Steps**

1. Go to **Grid Topology > deployment**.
2. To view the ILM processing queue, examine the following:

   • Current ILM Activity: Shows the number of objects to be processed by each of the listed CMS services.

   • Future ILM Activity: Shows the number of objects to be processed by all of the CMS services in the future, either the next day or anytime.

**Setting alarms on the ILM activity queue**

You can set an alarm on the ILM activity queue to monitor ILM processing and 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.

**About this task**

Default alarms generate a notice, minor, or major system alarm based on the following number of objects to be processed.

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Threshold Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>&gt;= 150,000 objects</td>
</tr>
<tr>
<td>Minor</td>
<td>&gt;= 1 million objects</td>
</tr>
<tr>
<td>Major</td>
<td>&gt;=10 million objects</td>
</tr>
</tbody>
</table>

If the threshold is met or exceeded, the system generates an alarm and sends notifications as set by your alarm configurations. The system then displays the visual alarm indicator at the deployment level of the grid topology tree and the System Status icon at the top of the page. If the queue is evaluated when the value is 499 or less, no alarm is triggered and no notification is sent.

You can also configure custom alarms on the current ILM evaluation queue.
Steps

1. Sign in to the NMS MI using an account that has Maintenance permissions.

2. Go to Grid Topology > deployment > Configuration > Alarms.

![Configuration (Alarms): Summary - StorageGRID Webscale Deployment](image)

3. To set the ILM processing queue alarm, click the Edit icon.

4. Enable the alarm attribute, select the attribute, severity, and other options.

5. Click Apply Changes.

6. To view the customized ILM alarm, go to Grid Topology > deployment > Configuration > Main.

Related concepts

* Alarms management on page 41

Related tasks

* Creating custom alarms on page 47

Evaluating existing objects against new ILM policy

After you change the ILM policy, all new objects ingested into the StorageGRID Webscale system are evaluated against the new ILM policy and object data is copied and stored according to ILM policy’s ILM rules. However, previously evaluated objects are not re-evaluated and object data remains “as is”. To re-evaluate previously evaluated objects against the new ILM policy, you must trigger an ILM Re-evaluation (User Triggered).

About this task

Evaluating previously ingested objects against the new ILM policy is not always required. Object data may be okay as it is in the system. For example, if you add a new site to the StorageGRID Webscale system and update the ILM policy to add ILM rules for objects ingested at that new site,
there might be no need to re-evaluate objects already in the StorageGRID Webscale system and protected from loss. In another instance, you might add a new storage grade and decide that it is not necessary that all previously stored object data be stored on the new grade of storage.

**Note:** Because an ILM re-evaluation places additional load on the StorageGRID Webscale system, confirm that it is a necessary action.

### Steps

1. Check whether an ILM re-evaluation has already been triggered:
   
   a. Go to *primary Admin Node > CMN > Grid Tasks*.

   b. If you see the grid task ILM Re-evaluation (User Triggered) in the table of Active tasks, you must cancel the active ILM evaluation before triggering a new one.

      • Under Actions, select **Pause**, then click **Apply Changes**.

      • When Status updates to Paused, under Actions, select **Abort**, and then click **Apply Changes**.

      The ILM Re-evaluation (User Trigger) grid task moves to the Historical table with a status of Aborted.

      If you start a new ILM Re-evaluation (User Triggered) grid task while an earlier one is still in progress, the second ILM Re-evaluation (User Triggered) grid task fails.

2. Go to *Grid Management > ILM Management > Configuration > Proposed Policy*.

3. Review the active policy to ensure that it is correct.

4. Click **Re-evaluate Content**.

5. Click **OK** to confirm that you want to apply the new ILM policy to existing content.

   This forces all objects to be re-evaluated against the new ILM policy. Copies will be created or purged as necessary to meet the ILM policy’s new ILM rules.

6. Review the progress of the ILM re-evaluation by checking the progress of the ILM Evaluation (User Triggered) grid task at the *primary Admin Node > CMN > Grid Tasks*.

   Charting the % Complete can provide an estimate on when the ILM re-evaluation will complete.

### Example ILM policies

ILM Management (see *Grid Management > ILM Management > Configuration*) allows you to design sophisticated and complex ILM policies.

However, in practice, most ILM policies are simple. A basic ILM policy:
• Keeps two copies of all object data forever
• Indicates what to do when a client application deletes an object: purge the object or keep it.

The following ILM policy examples can be used as a starting point to define an ILM policy that meets your object protection and retention requirements.

Warning: The following policies are only examples. There are many ways to specify an ILM policy. Before activating an ILM policy, carefully analyze all possible scenarios to make sure that your ILM policy is sound and safe and will protect content as intended.

Single data center site ILM policy

A typical ILM policy for a single Data Center (DC) site topology should include the following ILM rules:

• Purge content from the StorageGRID Webscale system when it is deleted by the client application (optional rule).
• At ingest, store at least two copies in two storage pools indefinitely (default rule).

To activate an ILM rule, add it to an ILM policy.

Related concepts
• ILM rule to make copies in two storage pools (DC only) on page 106
• Configure and activate an ILM policy on page 94

Data center + data center and archive ILM policy

A typical ILM policy for a multi-site topology that includes an Archive Node should include the following ILM rules:

• At ingest, store one copy at DC1, one copy at DC2, and one copy to tape or S3 (Archive Node). After a period of time, remove the copy at DC2 (default rule for this ILM policy).
• Purge content from the StorageGRID Webscale system when it is deleted by the client application.

To activate the ILM rule, add it to an ILM policy.

Related concepts
• Configure and activate an ILM policy on page 94
Example ILM rules

The following ILM rule examples can be used as starting points to define ILM rules that meet your object protection and retention requirements.

**Warning:** The following ILM rules 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 to delete objects based on age**

The sample ILM rule in the following table stores three replicated copies at ingest and deletes one copy after a predefined period of time has elapsed.

**Warning:** Avoid creating ILM rules that purge objects at ingest. If you activate an ILM policy that purges objects at ingest, objects are irretrievably lost.

**Table 2: ILM rule to delete objects based on age**

<table>
<thead>
<tr>
<th>Rule definition</th>
<th></th>
</tr>
</thead>
</table>
| Storage Pools   | Two storage pools that do not contain Archive Nodes.  
|                 | In this example, the storage pools are named Data Center 1 and Data Center 2. |
| Rule Name       | Make 3 Copies and Delete 1 Copy after 1 Year |
| Filter Name     | Match All Objects |
| Matching Criteria | If the policy includes a rule to purge deleted objects, select Object referenced by API.  
|                 | Otherwise, select Both.  
| Reference Time  | Ingest Time |
| Content Placement | On Day 0, keep a replicated copy in Data Center 1 forever; temp copies in Data Center 2  
|                 | On Day 0, keep a replicated copy in Data Center 2 forever; temp copies in Data Center 1  
|                 | On Day 0, keep a replicated copy in Data Center 2 for 1 Years; temp copies in Data Center 1 |
ILM rule to make copies in two storage pools (DC only)

The sample ILM rule in the following table places replicated copies indefinitely in two storage pools.

Note: This ILM rule is different than the built-in ILM rule Make 2 Copies. The built-in ILM rule places object data anywhere in the StorageGRID Webscale system and not at a specifically configured location.

<table>
<thead>
<tr>
<th>Rule definition</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Pools</td>
<td>Two storage pools on different Storage Nodes at the same site</td>
</tr>
<tr>
<td></td>
<td>In this example, the storage pools are named Data Center 1 Pool 1 and Data Center 1 Pool 2.</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Store One Copy in Two Storage Pools</td>
</tr>
<tr>
<td>Filter Name</td>
<td>Match All Objects</td>
</tr>
<tr>
<td>Matching Criteria</td>
<td>If the policy includes a rule to purge deleted objects, select Object referenced by API.</td>
</tr>
<tr>
<td></td>
<td>Otherwise, select Both.</td>
</tr>
<tr>
<td>Reference Time</td>
<td>Ingest Time</td>
</tr>
<tr>
<td>Content Placement</td>
<td>On Day 0, keep a replicated copy in Data Center 1 Pool 1 forever; temp copies in Data Center 1 Pool 2</td>
</tr>
<tr>
<td></td>
<td>On Day 0, keep a replicated copy in Data Center 1 Pool 2 forever; temp copies in Data Center 1 Pool 1</td>
</tr>
</tbody>
</table>
### ILM rule to archive erasure coded object data

The sample ILM rule in the following table stores erasure coded object data in one storage pool (on disk) forever. The storage pool is located at DC1. At the same time, a replicated copy of the erasure coded object data is archived forever to Amazon Web Services (AWS). Note that for this ILM rule example, it is assumed that the **Archive Node > ARC > Target** component’s value for Storage Class is Standard. Meaning that the Archive Node is configured for standard S3 redundancy, which protects object data from loss.

**Table 3: ILM rule to archive erasure coded object data**

<table>
<thead>
<tr>
<th>Rule definition</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Storage Pools</strong></td>
<td>One storage pool at one site that is associated with Erasure Coding profile EC Storage. One storage pool only includes an Archive Node with a Target Type of Cloud Tiering - Simple Storage Service (S3). In this example, the storage pools are named EC Storage DC1 and S3 Archive.</td>
</tr>
<tr>
<td><strong>Rule Name</strong></td>
<td>Archive EC Object Data</td>
</tr>
<tr>
<td><strong>Filter Name</strong></td>
<td>Match all Objects</td>
</tr>
<tr>
<td><strong>Matching Criteria</strong></td>
<td>If the policy includes a rule to purge deleted objects, select Object referenced by API. Otherwise, select Both. All Objects</td>
</tr>
<tr>
<td><strong>Reference Time</strong></td>
<td>Ingest Time</td>
</tr>
<tr>
<td>Rule definition</td>
<td>Content Placement</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>On Day 0, keep an erasure coded copy in EC Storage Pool (EC Storage DC 1) for 365 days.</td>
</tr>
<tr>
<td></td>
<td>On Day 365, keep a replicated copy in S3 Archive forever; temp copies in Data Center 1.</td>
</tr>
</tbody>
</table>

**Rule Name:** Archive EC Object Data

**Matching Criteria**

- All objects
- Objects with the following special metadata:
  - Object Life
  - User Metadata

**Reference Time**

- Last Access Time
- User Created Creation Time

**Content Placement**

- Keep an erasure coded copy in EC Storage Pool (EC Storage DC 1) for 365 days.
- Keep a replicated copy in S3 Archive forever; temp copies in Data Center 1.
Managing disk storage

Storage Nodes provide the StorageGRID Webscale system with its disc storage capacity, providing the StorageGRID Webscale system with services to store, move, verify, and retrieve object data and metadata stored to disk.

What a Storage Node is

A Storage Node provides the StorageGRID Webscale system with its disc storage capacity. It includes services and process to store, move, verify, and retrieve object data and metadata stored to 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:

- Object data storage
- Object data transfers from another LDR service (Storage Node)
- Data storage management
- Protocol interfaces (HTTP, S3, Swift, CDMI)

For general information about the LDR service's role in the management of objects, see the StorageGRID Webscale 10.2 Grid Primer.
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 CDMI container objects, CDMI named objects, S3 buckets, S3 objects, Swift containers, 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, CDMI, and SGAPI).

Because the synchronization of distributed key value stores 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.

The Total Objects value includes all objects and object segments. The S3 Objects value includes all S3 objects and uncompleted S3 multipart uploads.

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.

**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.

**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, copied, and purged, see the *Grid Primer*.

**Related tasks**

.getConfiguring information lifecycle management rules and policy on page 84

**Related information**

*StorageGRID Webscale 10.2 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.
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.

Managing Storage Nodes

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.

The LDR service maps objects to a volume ID and automatically balances content across a Storage Node’s object stores.

Object stores are identified by their unique volume ID. When objects are saved to a Storage Node, the LDR service randomly (based on available storage space) assigns the object’s data to a volume ID and is mapped to the object store with that volume ID. (Object metadata is always mapped to object store 0.) Note that the object is also assigned a unique content block identifier (CBID), but only to map the object’s path within the directory structure of the object store.

Because volume IDs are randomly assigned and take into consideration available usable space on each object store, object data is placed evenly across the Storage Node’s object stores. When an object store fills to capacity, the Storage Node continues to accept objects until all object stores have filled to capacity and there is no more room on the Storage Node.
Storage capacity

To track 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 1 + Useable Space 2 + Useable Space 3
Watermarks

Watermarks are global settings used to manage a Storage Node’s usable storage space. Watermarks are used to 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 through the NMS MI. Go to Grid Management > Grid Configuration > Storage > Overview > Main.

### Object Segmentation

<table>
<thead>
<tr>
<th>Description</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segmentation</td>
<td>Enabled</td>
</tr>
<tr>
<td>Maximum Segment Size</td>
<td>1 GB</td>
</tr>
</tbody>
</table>

### Storage Watermarks

<table>
<thead>
<tr>
<th>Description</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Volume Soft Read-Only Watermark</td>
<td>10 GB</td>
</tr>
<tr>
<td>Storage Volume Hard Read-Only Watermark</td>
<td>5 GB</td>
</tr>
<tr>
<td>Metadata Reserved Free Space</td>
<td>2.000 GB</td>
</tr>
</tbody>
</table>

### Ports

<table>
<thead>
<tr>
<th>Description</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLB HTTP Port</td>
<td>8080</td>
</tr>
<tr>
<td>Code</td>
<td>Name</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------------</td>
</tr>
</tbody>
</table>
| VHWM  | Storage Volume Soft Read-Only Watermark   | 10 GB   | 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. |
| VROM  | Storage Volume Hard Read-Only Watermark   | 5 GB    | 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. |
| CAWM  | Metadata Reserved Space Watermark         | 2 TB    | 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**

*Manage full Storage Nodes* on page 118

**Storage Node configuration settings**

This table summarizes Storage Node configuration settings.
<table>
<thead>
<tr>
<th>Service/Component</th>
<th>Name</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDR</td>
<td>HTTP/CDMI State</td>
<td>HSTE</td>
<td>Set the LDR service to one of:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Online: Operation continues normally</td>
</tr>
<tr>
<td>Auto-Start HTTP</td>
<td>HTAS</td>
<td></td>
<td>Enable the HTTP component when the LDR service is restarted. If not selected, the HTTP interface remains Offline until explicitly enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If Auto-Start HTTP is selected, the state of the system on restart depends on the state of the LDR &gt; Storage component. If the LDR &gt; Storage component is Read-only on restart, the HTTP interface is also Read-only. If the LDR &gt; Storage component is Online, then HTTP is also Online. Otherwise, the HTTP interface remains in the Offline state.</td>
</tr>
<tr>
<td>LDR &gt; Storage</td>
<td>Storage State – Desired</td>
<td>SSDS</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Offline: When the desired state is Offline, the LDR service takes the LDR &gt; Storage component offline.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Health Check</td>
<td>SHCT</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Service/Component</td>
<td>Name</td>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------</td>
<td>------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>LDR &gt; Verification</strong></td>
<td>Reset Missing Objects Count</td>
<td>VCMI</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 <a href="#">Configuring the background verification rate</a> on page 127.</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 <em>StorageGRID Webscale 10.2 Troubleshooting Guide</em>.</td>
</tr>
<tr>
<td><strong>LDR &gt; Erasure Coding</strong></td>
<td>Reset Writes Failure Count</td>
<td>RSWF</td>
<td>Reset 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 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 the counter for delete failures of erasure coded object data from the Storage Node.</td>
</tr>
<tr>
<td></td>
<td>Reset Copies Lost Count</td>
<td>RCCC</td>
<td>Reset the counter for the number of lost 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 the counter for corrupt fragments of erasure coded object data on the Storage Node.</td>
</tr>
<tr>
<td>Service/Component</td>
<td>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 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 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 the counter for all CDMI transactions.</td>
</tr>
<tr>
<td>LDR &gt; HTTP</td>
<td>Reset HTTP Counts</td>
<td>LHAC</td>
<td>Reset the counter for all HTTP transactions.</td>
</tr>
</tbody>
</table>

**Related information**

*StorageGRID Webscale 10.2 Troubleshooting Guide*

**Manage full Storage Nodes**

**Add storage**

As Storage Nodes reach capacity, the StorageGRID Webscale system must be expanded and additional storage added. There are two options available when considering how to increase storage capacity: adding storage volumes and adding Storage Nodes.

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

As well as adding storage volumes, 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*. 
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.

Steps
1. Go to Grid Topology > deployment.
2. 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.

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

1. Go to Storage Node > LDR > Storage > Overview > Main.
2. Note the current value for the attribute Total Usable Space (STAS).

Related concepts

Watermarks on page 114

Configure settings for stored objects

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.

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, CDMI, or SGAPI. 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.
Steps

1. Sign in to the NMS MI using the Vendor account or an account with Grid Management permissions.

2. Go to Grid Management > Grid Configuration > Configuration > Main.

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.

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. Sign in to the NMS MI using the Vendor account or an account with Grid Management permissions.

2. Go to Grid Management > Grid Configuration > Configuration > Main.

3. Change Stored Object Hashing to one of 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. Stored Object Compression is disabled by default.

**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.

**Steps**

1. Sign in to the NMS MI using the Vendor account or an account with Grid Management permissions.
2. Go to **Grid Management > Grid Configuration > Configuration > Main**.
3. Change Stored Object Encryption to **Enabled**.
4. Click Apply Changes.

**Stored object compression SGAPI settings**

For applications that use the StorageGRID API, object compression is accomplished through a header in the HTTP PUT request. For more information, see the StorageGRID API Reference.

For more information on configuring clients for object compression, see the applicable API reference.

**Mount 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 in the NMS MI under **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-81cf1809faba in the /etc/fstab file.
Security partitions

Security partitions is a system-wide setting that restricts access to objects, preventing applications from retrieving objects ingested through another client application. 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.

For more information about enabling security partitions, see the StorageGRID API Reference.

Tuning for object size

To improve throughput and object retrieval times, as well as maximizing storage and resource usage, optimize the StorageGRID Webscale system for the expected average size of object data after compression.

The Object Segmentation setting (see Grid Management > Grid Configuration > Storage > Configuration > Main) splits an object into a collection of smaller fixed-size objects in order to optimize storage and resources usage for large objects. Do not disable object segmentation unless advised by support. Object Segmentation is enabled by default.

Related tasks

*Configuring object segmentation on page 125*

Recommended optimization settings

The following recommendations and optimizations are for systems integrated with applications that regularly store large objects.

When optimizing for large objects consider the following:

- Objects should be stored to the StorageGRID Webscale system through a dedicated customer network interface.
- All network connections within the StorageGRID Webscale system should be capable of sustained operation at 10 Gbps.
• All network connections between the StorageGRID Webscale system and client applications should be capable of sustained operation at 10 Gbps.

• The StorageGRID Webscale system should be configured with a minimum of four LDR services so that when Storage Nodes are I/O bound during ingest of a large object, there are other Storage Nodes available to handle regular system operations.

• Client applications can also simultaneously ingests smaller objects into the StorageGRID Webscale system.

• Smaller objects are not routinely purged from the StorageGRID Webscale system.

Configuring object segmentation

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.

About this task

When Object Segmentation is enabled, the LDR service splits the object into segments as it is ingested into the StorageGRID Webscale system and creates a segment container which lists the header information of all segments as content. For StorageGRID API clients, the UUID of the segment container is returned as the ingest result. For CDMI clients, the OID is returned.

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 GB (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. One for the segment container plus two for the object segments:

segment container + segment + segment = three stored objects
Object segmentation is enabled by default. It is recommended that object segmentation always be enabled.

**Note:** Do not change this setting unless advised to do so by Support.

**Steps**

1. Sign in to the NMS MI using the Vendor account or an account with Grid Management permissions.
2. Go to Grid Management > Grid Configuration > Storage > Configuration > Main.
3. Change **Segmentation** to **Disabled**.

The default of **Maximum Segment Size** is 1000000000 bytes (1 GB).

**Note:** Do not change this setting unless advised to do so by Support.

4. Click **Apply Changes**.

**Verifying object integrity**

The StorageGRID Webscale system proactively verifies the integrity of object data on Storage Nodes.

There are two different verification processes: background verification and foreground verification. Background verification is run automatically and continuously by the StorageGRID Webscale system, while you must manually trigger the foreground verification process.

**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 automatically attempts to replace the missing or corrupt object data from copies stored elsewhere in the system.

There are two instances of background verification that continuously run in parallel on every Storage Node. One instance checks for missing or corrupt copies of replicated object data while the other instance checks for corrupt fragments of erasure coded object data. 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 created 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 purged 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.

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.

**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. Sign in to the NMS MI using the Vendor or Admin account or an account with Maintenance
permissions.
2. Go to **LDR > Verification > Configuration > Main**.
3. Under Background Verification, select **Verification Priority > High** or **Verification Priority >
Adaptive**.
Setting the Verification Priority to High triggers a Notice level alarm for VPRI (Verification Priority).

4. Click Apply Changes.

5. 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.

6. 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.

If a copy of replicated object data is found to be missing, the StorageGRID Webscale 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 created 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.

Foreground verification does not check for missing fragments of erasure coded object data.
Running foreground verification

Foreground verification enables you to manually 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 storage.

Before you begin

- 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

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 attribute (see Storage Node > LDR > Verification > Overview > Main) goes up by one, and 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 Object alarm is 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 all complete. 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 on-line status. When the Storage Node's state returns to online, the LDR Foreground Verification grid task continues until it completes.

Foreground verification does not check for missing fragments of erasure coded object data.

Steps

1. Sign into NMS MI using the Vendor or Admin account or an account with Maintenance permissions.

2. Go to Storage Node > LDR > Verification > Configuration > Main.

3. Under Foreground Verification, select ID for the storage volume or volumes to verify.
4. 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 **Admin Node > CMN > Grid Task > Overview > Main**. If object data is found to be missing, the missing object data is automatically replicated.

5. Go to **Storage Node > LDR > Verification > Overview > Main** and under **Verification Results** note the value of **Missing Objects Detected**.

If the count for the attribute **Missing Objects Detected** is large (if there are a 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.

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 10.2 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.

*Note:* TSM middleware is not supported for OpenStack deployments of the StorageGRID Webscale system.

**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.

*Note:* TSM middleware is not supported for OpenStack deployments of the StorageGRID Webscale 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

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

Before you begin

• 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 GB (4,831,838,208 bytes). S3 API requests that exceed this value will fail if connection to Amazon Web Services (AWS).

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. Sign in to the NMS MI using the Vendor or Admin account or an account with Maintenance permissions.

2. Go to Archive Node > ARC > Target > Configuration > Main.

3. Select Cloud Tiering - Simple Storage Service (S3) from the Target Type drop-down list.
4. 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 the StorageGRID Webscale system is the target archival storage system, do not clear if the target system is configured with publicly-signed certificates.

- **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 targeted archival storage systems is another instance of the StorageGRID Webscale system, Storage Class controls the target system's dual-commit behaviour

5. Click **Apply Changes**.

The specified configuration settings are validated and applied to your StorageGRID Webscale system. Once configured, the target cannot be changed.

**Related tasks**

*Configuring object segmentation* on page 125

**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.

**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. Sign in to the NMS MI using the Vendor or Admin account or an account with Maintenance permissions.

2. Go to **Archive Node > ARC > Target > Configuration > Main**.
3. Modify the following account information, as necessary:
   - Access Key
   - Secret Access Key
   - Endpoint Authentication
   - Storage Class
   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 cannot be changed.

4. 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.

**About this task**

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

**Steps**

1. Go to **Archive Node > ARC > Configuration > Main**.
2. Select one of the following options from the **Cloud Tiering Service State** drop-down list:
   - Read-Write Enabled
   - Read-Only Enabled
   - Read-Write Disabled

3. 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 through the NMS MI.

**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. Sign in to the NMS MI using the Vendor or Admin account or an account with Maintenance permissions.

2. Go to **Archive Node > ARC > Target > Configuration > Main**.
3. Select Tivoli Storage Manager (TSM) from the **Target Type** drop-down list.

4. 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.

5. 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.

6. Click Apply Changes.

Managing Archive Nodes

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.

Steps

1. Go to Archive Node > ARC > Target > Configuration > Main.

2. Change Maximum Retrieve Sessions to be the same as Number of Sessions.
3. 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.

**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. Go to **Archive Node > ARC > Store > Configuration > Main**.

![Configuration: ARC (DC1-ARC1-98-165) - Target](image1)

2. Change **Archive Store State** to **Offline**.

![Configuration: ARC (DC1-ARC1-98-165) - Store](image2)
3. Select **Archive Store Disabled** on Startup.

4. 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.

**Steps**

1. Go to **Archive Node** > ARC > Target > Configuration > Main.

2. Change Maximum Retrieve Sessions to be the same as the number of concurrent sessions listed in Number of Sessions.

3. 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.

4. 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.

**Steps**

1. Sign in to the NMS MI using the Vendor or Admin account or an account with Maintenance permissions.

2. Go to **Archive Node** > ARC > Replication > Configuration > Main.

3. 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.

4. 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.

Steps

1. Sign in to the NMS MI using the Vendor or Admin account or an account with Maintenance permissions.

2. Go to Archive Node > ARC > Retrieve > Configuration > Main.

3. 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.
4. 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 140

**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.

**Steps**

1. Sign in to the NMS MI using the Vendor or Admin account or an account with Maintenance permissions.

2. Go to Archive Node > ARC > Store > Main.

3. 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 archival storage system. Useful when the targeted 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 (Stores Failure) alarm.

4. 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.

**Steps**

1. Sign in to the NMS MI using the Vendor or Admin account or an account with Maintenance permissions.

2. Go to Archive Node > ARC > Store > Main.

   ![Configuration: ARC (98-127) - Store](image)

3. Select **Reset Store Failure Count**.

4. Click **Apply Changes**.

   The Store Failures attribute resets to zero.

**Set 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 (go to ARC > Retrieve > Overview > Main) depend on how the archival storage system is configured and used. 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 alarms* on page 47
What an Admin Node is

The Admin Node provides services for the web interface, system configuration, and audit logs. Each site in a StorageGRID Webscale deployment may include one Admin Node.

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 provided by the NMS MI. The NMS service itself can be monitored through the NMS MI.

Related concepts

Monitoring grid tasks on page 188

Related tasks

Verifying ILM policy on page 96
Admin Node redundancy

A StorageGRID Webscale system can include multiple Admin Nodes; however, only one Admin Node is allowed per site. This provides you with the redundancy multiple IP address from which you can to sign in to NMS MI 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 through the NMS MI. Meanwhile, attribute processing continues, alarms are still triggered, and related notifications sent. However, multiple Admin Nodes does 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 146

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 to the NMS MI. 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.

**E-mail 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.

**The preferred vs. standby sender**

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 e-mail, all NMS services send a test e-mail.

**Related concepts**

- About alarms and e-mail notifications on page 32
- What AutoSupport is on page 54

**Related tasks**

- Selecting a preferred sender on page 40
- Sending test e-mails on page 38
Changing the name of an Admin Node

You can change the name of an Admin Node as it appears on pages in the NMS MI. Creating a unique name for each Admin Node can be useful in differentiating Admin Nodes. This is particularly useful in identifying a preferred sender of e-mail notifications and AutoSupport messages.

About this task

When you change the name of an Admin Node using the following procedure, the name is only changed as it appears in the NMS MI. The name of an Admin Node is not changed in the Grid Topology tree.

Note: When the name of an Admin Node is changed using the following procedure, changes are lost whenever the provision command is run. For example, during expansion.

Steps

1. Sign in to the NMS MI using the Admin or Vendor account.

2. Go to Grid Management > NMS Management > General > NMS Names.

3. In the NMS Names table, click Edit next to the name you want to change.

   The value under Name becomes editable.

4. Under Name, type a new name for the Admin Node.

5. Click Apply Changes.

Related concepts

NMS entities on page 148

Related tasks

Selecting a preferred sender on page 40

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 NMS MSI 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.

**Note:** Do not change these setting unless advised by technical support.

### Table 4: Grid Management > Grid Configuration > NMS Entities Settings

<table>
<thead>
<tr>
<th>Scope</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>Text</td>
</tr>
<tr>
<td>Device Model ID</td>
<td>Text</td>
</tr>
<tr>
<td>Device Model Version</td>
<td>Text</td>
</tr>
<tr>
<td>Name</td>
<td>Text</td>
</tr>
<tr>
<td>Language</td>
<td>Drop-down menu</td>
</tr>
</tbody>
</table>

To export these settings for future reference, use the Export button 📝.

**Changing an NMS entity name**

When changing the name of an NMS entity, changes are lost whenever the provision command is run (for example, during expansion).

**Steps**

1. Sign in to the NMS MI using the Vendor account or an account with Grid Management permissions.
2. Go to **Grid Management > Grid Configuration > NMS Entities > Configuration > Main**.
3. Click **Edit** next to the item you want to rename and type a new name.
4. Click **Apply Changes**.

   Because changes are lost whenever you run the provision command, you should export and save these changes for future reference. To export these settings for future reference, click **Export**.
Managing StorageGRID Webscale 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 grid network, supplementary network, and external NTP sources IP addresses at any time.

**Note:** You cannot add a new network to a grid node.

Procedures differ depending on whether your StorageGRID Webscale system includes a StorageGRID Webscale system appliance. For the procedure to change the IP addresses of a system that includes a StorageGRID Webscale system appliance, see the *StorageGRID Webscale Appliance Installation and Maintenance Guide*.

**Grid network IP address**

The grid network is the communication link between grid nodes.

**Supplementary network IP address**

The supplementary network is an optional configuration that allows for networking between servers that must integrated on a network other than the grid network.

**Related tasks**

*Changing IP addresses* on page 152

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.

**Step**

1. Go to `grid node > SSM > Resources`.

   IP addresses are listed in the Network Addresses table.

**Example**

<table>
<thead>
<tr>
<th>Network Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>eth0</td>
</tr>
<tr>
<td>eth0</td>
</tr>
</tbody>
</table>

The IP address assigned to eth0 is always the grid node’s grid network IP address. If the interface is bonded, the IP address is assigned to eth0 and eth1.

Regardless of whether IPv6 is used for external interfaces, the Network Addresses table always displays link-local IPv6 addresses beginning with fe80::; these are automatically assigned by Linux. A grid node configured with IPv6 shows an additional IPv6 address as well as any link-local addresses.
Changing IP addresses

You can change the IP address of the grid network that provides communication between grid nodes. You can also change the IP address of a supplementary network, which is an optional configuration that enables networking between servers that must be integrated on a network other than a grid network.

Before you begin

- You must have obtained the following information:
  - Current IP address
  - New IP address (including netmask)
  - Provisioned grid specification file.
  - Provisioning passphrase
  - Passwords.txt file
- USB flash drives
- Grid Designer User Guide
- Service laptop with Grid Designer
- CMN service is available (initially unavailable if all grid IP addresses are changed)
- All grid nodes must be connected to the StorageGRID Webscale system such that they can connect to the Admin Node

About this task

Because changing IP addresses can result in service disruptions to the StorageGRID Webscale system, it is recommended that you schedule a time when you can perform this procedure that lessens the impact to the StorageGRID Webscale system.

The IP address assigned to eth0 is always the grid node’s grid network IP address. For a StorageGRID Webscale appliance, if the interface is bonded, the IP address is assigned to hic2 and hic4.

The following table lists the grid nodes that must be selected and updated in the Grid Deployment Utility by running the Update IP Configuration task when performing IP addresses changes to the StorageGRID Webscale system.

<table>
<thead>
<tr>
<th>Update to</th>
<th>IP address changed</th>
<th>Grid nodes to select in GDU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Node</td>
<td>grid network</td>
<td>all (system-wide)</td>
</tr>
<tr>
<td>Storage Node (with ADC service)</td>
<td>grid network</td>
<td>all at site primary Admin Node</td>
</tr>
<tr>
<td>Storage Node (without ADC service)</td>
<td>grid network</td>
<td>Storage Nodes updated primary Admin Node</td>
</tr>
<tr>
<td>Archive Node</td>
<td>grid network</td>
<td>Archive Node at site primary Admin Node</td>
</tr>
<tr>
<td>Update to</td>
<td>IP address changed</td>
<td>Grid nodes to select in GDU</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>new grid node</td>
<td>N/A</td>
<td>all</td>
</tr>
<tr>
<td>(NTP primary)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>network gateway</td>
<td>grid network</td>
<td>all (system-wide)</td>
</tr>
<tr>
<td>routing changed</td>
<td>supplementary</td>
<td>all grid nodes using updated profile</td>
</tr>
<tr>
<td></td>
<td>network</td>
<td>primary Admin Node</td>
</tr>
<tr>
<td>external NTP</td>
<td>NTP</td>
<td>primary NTP grid nodes</td>
</tr>
<tr>
<td>source</td>
<td></td>
<td>primary Admin Node</td>
</tr>
</tbody>
</table>

**Steps**

1. Update the latest version of the provisioned grid specification file with Grid Designer to change the IP address.
   
   For more information, see the *Grid Designer User Guide*.

2. Provision the StorageGRID Webscale system.
   
   Always back up the provisioning data in two safe and secure locations. These copies can be used to restore the StorageGRID Webscale system in the case of an emergency or during an expansion or maintenance procedure.

3. If not already done, unzip the SAID package file:
   
   a. Change to the `/var/local/provision` directory.
   
   b. Unzip the SAID zip file.

4. Identify the SSH Access Password in the *Passwords.txt* file:
   
   a. Open the *Passwords.txt* file.

   ```
   Using username “root”
   Server refused by Key
   Using keyboard-interactive authentication
   Password:Last login: Fri Jan 9 15:34;40 2015 from 10.99.99.1
   ---------------------------------
   This private computer is for authorized use only and contains software that is provided under license. Please consult the End User Agreement for terms and conditions.
   ---------------------------------
   ---
   DCl-ADM1-159:/~ # cd /var/local/provision/
   DCl-ADM1-159:/var/local/provision/ # cd GID000001_Rev2/
   DCl-ADM1-159:/var/local/provision/GID000001_Rev2/ # vi Passwords.txt
   ```
   
   b. Identify the password in the SSH Access Password column for the primary Admin Node.

   ```
   Password Data for Grid ID: 000001, Revision 2
   Revision Prepared on: 2015-01-09 +0000
   
   NMS Interface
   
   Assigned password for the NMS “Vendor” account: PASSWORD
   Server Consoles
   
   Server ‘root’ Account Passwords
   ```
5. If the grid network IP address is changing:
   a. Use Server Manager and select Shutdown to gracefully stop all services, halt the operating
      system, and power down the server.
   b. Perform any necessary physical networking changes.
   c. Power the server back up.
   d. Access a command shell and log in as root using the password listed in the Passwords.txt
      file.
   e. Change the grid IP address. Enter (on one line):
      ```bash
      change-grid-ip.rb -i new_grid_IP_address -n netmask -g gateway
      ```
      where `gateway` is the network gateway.
   f. Repeat all of step 5 for each grid node that is changing.

6. Starting with the primary Admin Node, use GDU to update IP configuration settings:
   a. Access a command shell and log in as root using the password listed in the Passwords.txt
      file.
      **Note:** The primary Admin Node must be updated first.
   b. Start GDU if it is not already running. Enter:
      ```bash
      ssh-add
      ```
   c. Enter the SSH access password listed in the Passwords.txt file.
   d. Enter: `gdu-console`
   e. In GDU, select the grid node to be updated and confirm that the Server Info panel lists its
      Current State as Available.
   f. Select **Update IP Configuration** in the Tasks panel, and then select **Start Task** in the Actions
      panel and press **Enter**.
   g. Repeat substeps 6e and 6f for each server being changed.
      Wait for the Update IP Configuration GDU task to complete on the primary Admin Node
      before updating other grid nodes. All other grid nodes can be updated concurrently.
      **Note:** Wait for the Update IP Configuration GDU task to complete on the primary Admin
      Node before updating other grid nodes. All other grid nodes can be updated concurrently.
   h. Quit GDU.

7. After all Storage Nodes running an ADC service have been updated:
   a. At the server hosting the Admin Node, access a command shell and log in as root using the
      password listed in the Passwords.txt file.
b. Enter: `import-bundles`

c. Log out of the server.

8. If you are changing the grid network IP address of an Admin Node, advise administrators that the web browser address for access to the NMS MI has changed.

If, after completing this procedure, there are IP address errors, you must run the procedure again starting at step 1. Do not run the `remove-revision` command.

### Enabling Domain Name Service globally

You can enable Domain Name Service (DNS) for all grid nodes. When DNS is enabled, you can use Fully Qualified Domain Name (FQDN) hostnames rather than IP addresses. This affects email notifications, AutoSupport, and server connectivity.

#### About this task

After installation completes, a DNST alarm is triggered on the grid node’s SSM service. After the DNS is configured and the new server information reaches all grid nodes, the alarm clears.

#### Steps

1. Sign in to the NMS MI using the Vendor or Admin account or an account with Maintenance permissions.

2. Go to Grid Management > Grid Configuration > Network > Configuration > Main.

3. Click Edit (if this is the first entry) or Insert and add a DNS server hostname.

4. Click Apply Changes.

   The DNST alarm is triggered.

5. To monitor the progress of the DNS configuration, go to Grid Topology > data_center > grid_node > SSM > Resources > Overview and look at the Network Resources section.

   Until the DNS information is configured on all grid nodes, the DNS Status field displays “Not configured” and the DNST alarm remains. After the information reaches all grid nodes, the DNS Status field displays “Running” and the DNST alarm clears.

#### Related tasks

- [Modifying the DNS configuration for a single grid node](#) on page 155

### Modifying the DNS configuration for a single grid node

Rather than configure Domain Name Service (DNS) globally for the entire deployment, you can configure DNS differently for each Admin Node or Archive Node. When DNS is enabled, you can use Fully Qualified Domain Name (FQDN) hostnames rather than IP addresses. This affects email notifications, AutoSupport, and server connectivity.

#### Steps

1. At the Admin Node or Archive Node, access a command shell and log in as root using the password listed in the `Passwords.txt` file.

2. Run the DNS setup script by entering: `setup_resolv.rb`.

   The script responds with the list of supported commands.
Tool to modify external name servers

available commands:
  add search <domain>
    add a specified domain to search list
    e.g.> add search netapp.com
  remove search <domain>
    remove a specified domain from list
    e.g.> remove search netapp.com
  add nameserver <ip>
    add a specified IP address to the name server list
    e.g.> add nameserver 192.0.2.65
  remove nameserver <ip>
    remove a specified IP address from list
    e.g.> remove nameserver 192.0.2.65
  remove nameserver all
    remove all nameservers from list
  save
    write configuration to disk and quit
  abort
    quit without saving changes
  help
    display this help message

Current list of name servers:
  192.0.2.64
Name servers inherited from global DNS configuration:
  192.0.2.126
  192.0.2.127
Current list of search entries:
  netapp.com

Enter command [add search <domain>|remove search <domain>|add
  nameserver <ip>]
  [remove nameserver <ip>|remove nameserver all|save]
  abort|help]

3. Add the IP address of a server that provides domain name service for your network. Enter: **add nameserver IP_address**

4. Repeat the command to add name servers.

5. Follow instructions as prompted for other commands.

6. Save your changes and exit the application. Enter: **save**

7. Close the command shell on the server. Enter: **exit**

8. Repeat from step 1 for each grid node.

Configure 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 Software CD at: /mibs/BYCAST-STORAGEGRID-MIB.mib

Detailed registry

The following OID is displayed on third-party monitor servers. This OID reports the overall system status of the StorageGRID Webscale system.

<table>
<thead>
<tr>
<th>Table 5: System status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element</td>
</tr>
<tr>
<td>OID</td>
</tr>
<tr>
<td>Hierarchy</td>
</tr>
<tr>
<td>Values</td>
</tr>
<tr>
<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>

<table>
<thead>
<tr>
<th>Table 6: System label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element</td>
</tr>
<tr>
<td>OID</td>
</tr>
<tr>
<td>Hierarchy</td>
</tr>
<tr>
<td>Values</td>
</tr>
</tbody>
</table>

Network Time Protocol configurations

The StorageGRID Webscale system uses the network time protocol (NTP) to synchronize time within the system. At least two servers in the StorageGRID Webscale system are specified as primary NTP servers.

They synchronize to at least three external time sources and with each other. Every server in the StorageGRID Webscale system that is not an NTP server acts as an NTP client and synchronizes with these primary NTP servers.
External time sources must use the NTP protocol and not the SNTP protocol. In particular, the Windows Time Service does not provide enough synchronization accuracy because it uses SNTP.

**Updating the Network Time Protocol external sources list**

If you encounter problems with the stability or availability of the NTP servers originally specified, update the list of external NTP sources that the StorageGRID Webscale system uses.

**Before you begin**

- IP address of the new external NTP source
- Provisioned grid specification file.
- Provisioning passphrase
- **Passwords.txt** file
- Service laptop with Grid Designer
- *Grid Designer User Guide*
- USB flash drives

**Steps**

1. Update the latest version of the provisioned grid specification file with Grid Designer to change the NTP servers. For more information, see the *Grid Designer User Guide*.
2. Provision the StorageGRID Webscale system.
   
   Always back up the provisioning data in the `/var/local/provision` directory to two safe and secure locations. These copies can be used to restore the StorageGRID Webscale system in the case of an emergency or during an expansion or maintenance procedure.
3. Identify which grid nodes act as primary NTP servers.
   
   This information is listed on the NTP tab of the `index.html` file, which is found in the Doc directory of the SAID package.
4. Start GDU on the primary Admin Node if it is not already running.
5. In GDU, select the grid node (as determined in step 3) in the **Servers** panel and confirm that its Current State is Available.
6. Select **Update IP Configuration** in the **Tasks** panel, and then select **Start Task** in the **Actions** panel and press Enter.
7. Repeat steps 5 and 6 for each primary NTP server in the StorageGRID Webscale system.

**Adding, removing, or updating Network Time Protocol sources**

If you change the IP address of a primary NTP source, or add or remove a grid node that acted as a primary NTP source (for example, through an expansion), use the following procedure to update the list of primary NTP sources used by NTP clients.

**Before you begin**

Prerequisites and required materials

- The grid specification file has been updated with changed IP addresses and the StorageGRID Webscale system provisioned.
• Servers acting as primary NTP servers have been identified. This information is listed on the NTP tab of the index.html file, which is found in the Doc directory of the SAID package.

Steps
1. At the primary Admin Node, access a command shell and log in as root using the password listed in the Passwords.txt file.
2. Start the Grid Deployment Utility (GDU) on the primary Admin Node if it is not already running.
3. In the GDU, select a grid node acting as an NTP client in the Servers panel and confirm that its Current State is Available.
4. Select Update IP Configuration in the Tasks panel, and then select Start Task in the Actions panel and press Enter.
5. Repeat steps 3 and 4 for each NTP client.

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).

![Diagram showing link costs between DC1, DC2, and DC3](image)

<table>
<thead>
<tr>
<th>Link</th>
<th>Link cost</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Between data center sites</td>
<td>0</td>
<td>Usually a high speed link exists between sites.</td>
</tr>
</tbody>
</table>
### Updating link costs

**Steps**

1. Sign in to the NMS MI using the Vendor account or an account that has Grid Management permissions.

2. Go to **Grid Management > Grid Configuration > Link Cost > Configuration > Main.**

3. 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 the changes, click **Revert.**

4. Click **Apply Changes.**

### Changing network transfer encryption

The StorageGRID Webscale system only accepts HTTP commands submitted over a network connection that uses Transport Layer Security (TLS) to provide transport protection for control traffic between grid nodes. The Network Transfer Encryption option provides a method to set the algorithm used to encrypt all control traffic between grid nodes.

**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. Sign in to the NMS MI using the Vendor account or an account with Grid Management permissions.

2. Go to Grid Management > Grid Configuration > Configuration > Main.

3. Change Network Transfer Encryption to one of AES256-SHA, or AES128-SHA.

4. Click Apply Changes.

Customize the SSH access point

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.

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.

**Related tasks**

*Configuring passwordless SSH access* on page 162

**Configuring passwordless SSH access**

**Steps**

1. At the primary Admin Node, access a command shell and log in as root using the password listed in the Passwords.txt file.

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`

**Adding or changing the SSH private key password**

The SSH access point can be installed with or without a password on the SSH key. By default the ssh access point is installed with a password. Check Passwords.txt to see if a password has been configured.

**About this task**

If there is a password, all other grid nodes can be accessed from the primary Admin Node using a single password (the SSH Access Password listed in the Passwords.txt file).

**Steps**

1. At the primary Admin Node, access a command shell and log in as root using the password listed in the Passwords.txt file.

2. Enter: `ssh-keygen -p -f /root/.ssh/id_rsa`

3. When prompted for a new password, select a password of more than four characters. It can include a series of words, punctuation, numbers, whitespace, or a string of characters.
Select a password that you can easily remember, but is not easily guessed. There is no way to recover a lost password.

4. Log out of the primary Admin Node. Enter: `exit`

### Removing the SSH private key

To prevent the primary Admin Node from acting as an SSH access point for the StorageGRID Webscale system, remove the SSH private key from the primary Admin Node. If you remove the SSH key from the primary Admin Node, users must enter the password of each grid node to gain access to its command shell.

**About this task**

*Note:* The Grid Deployment Utility (GDU), which you use for most installation, expansion, and maintenance procedures, requires passwordless access from the primary Admin Node to other servers. If you remove the ssh private key, you must re-add it before using GDU.

Always back up the private key before removing the file from the server. The private key file might be required when performing maintenance procedures.

**Steps**

1. At the primary Admin Node, access a command shell and log in as root using the password listed in the `Passwords.txt` file.
2. Copy the SSH private key from the primary Admin Node to a secure location: Enter: `scp /root/.ssh/id_rsa destination`
   
   where `destination` is a secure location to store the ssh private key
3. Remove the SSH private key from the primary Admin Node. Enter: `rm/root/.ssh/id_rsa`
   
   The primary Admin Node can no longer be used as an SSH access point to other grid nodes.
4. Log out of the primary Admin Node. Enter: `exit`

### Support for IPv6 and IPv4

The following table summarizes IPv6 and IPv4 support. IPv6 is supported for all external interfaces.

*Note:* Due to poor browser support for self-signed HTTPS certificates when using IPv6, IPv6 is restricted to Internet Explorer.

<table>
<thead>
<tr>
<th>IP address</th>
<th>IPv6</th>
<th>IPv4</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>External server I/P</td>
<td>✓</td>
<td>✓</td>
<td>The StorageGRID Webscale system does not support the use of both IPv6 and IPv4 for external interfaces. The StorageGRID Webscale system must use one or the other for all interface connections.</td>
</tr>
<tr>
<td>IP address</td>
<td>IPv6</td>
<td>IPv4</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------</td>
<td>------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Internal server I/P addresses</td>
<td>✗</td>
<td>✓</td>
<td>IPv6 support does not include internal system communications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The following procedures must use IPv4:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Remote access through ssh, for example, ssh <code>ssh Storage_Node_IP_address</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Entries in the <code>etc/hosts</code> file</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Maintenance scripts</td>
</tr>
<tr>
<td>NTP sources</td>
<td>✓</td>
<td>✓</td>
<td>Related procedures include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• For IPv4, specify the IP address of the NTP servers in Grid Designer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• For IPv6, contact Support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Run the script <code>setup_ntp.rb</code> to add or remove external NTP servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Edit the tags <code>ntp &gt; sources &gt; ip</code> in the grid specification file</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Excludes servers acting as time sources internal to the StorageGRID Webscale system.</td>
</tr>
<tr>
<td>DNS server</td>
<td>✓</td>
<td>✓</td>
<td>Add or remove DNS server using <code>setup_resolv.rb</code></td>
</tr>
<tr>
<td>E-mail server</td>
<td>✓</td>
<td>✓</td>
<td>This is specified in the NMS MI:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>configure the IP address of the SMTP mail server in <code>Grid Management &gt; NMS Management &gt; E-mail &gt; Server</code></td>
</tr>
<tr>
<td>Tivoli Storage Manager middleware server used by the ARC service</td>
<td>✗</td>
<td>✓</td>
<td>This is specified in the NMS MI.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configure IP Range at <code>Grid Management &gt; HTTP Management &gt; Clients and at Grid Management &gt; Grid Configuration &gt; Link Cost</code></td>
</tr>
<tr>
<td>Client IP Range</td>
<td>✓</td>
<td>✓</td>
<td>This is specified in the NMS MI.</td>
</tr>
<tr>
<td>SNMP Agent</td>
<td>✓</td>
<td>✓</td>
<td>This is specified in the NMS MI.</td>
</tr>
<tr>
<td>IP address</td>
<td>IPv6</td>
<td>IPv4</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------</td>
<td>------</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>NMS MI Web Interface</td>
<td>✅</td>
<td>✅</td>
<td>Related procedures include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• For IPv4, specify the IP address of the NMS web interface in Grid Designer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• For IPv6, contact Support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Run the GDU task Update IP Configuration to change the IP address. See <em>Changing IP addresses</em> on page 152.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Edit the tags network &gt; ip and grid network &gt; ip in the grid specification file</td>
</tr>
</tbody>
</table>
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 145

Related information

StorageGRID Webscale 10.2 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

Required materials

- Passwords.txt file with the root account passwords (available in the SAID package)
- Configuration.txt file (available in the SAID package)

Steps

1. At the Admin Node, access a command shell and log in as root using the password listed in the Passwords.txt file.

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.


4. Start the CIFS configuration utility. Enter: 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>
</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. Enter: `workgroup_name`
   
   d. When prompted, create a NetBIOS name:
      
      • Enter a new NetBIOS name. Creating a meaningful NetBIOS name can help identify audit shares when browsing the network.
      —or—
      
      • Press Enter to use the Admin Node’s hostname as the NetBIOS name.
      
      By default, the Admin Node’s hostname is used.
      
      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 to add a user or group, enter: `user`
   
   c. When prompted for a user, enter the audit user name.
   
   d. When prompted, enter a password for the audit user.
   
   e. When prompted, re-enter the same password to confirm the entry.
   
   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. Enter: `share_number`
   
   c. When prompted to add a user or group. Enter:
      
      • `user`
      — or —
• group
d. When prompted for the audit user or group name, enter the name of the audit user or 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. Enter: 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)

Note: The setting ‘security=ads’ should NOT be combined 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.

9. Close the CIFS configuration utility. Enter: 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. Enter: ssh Admin_Node_IP_address
      IP addresses are listed in the Configuration.txt file. If prompted for a password, find the
      required password 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. Enter: exit

11. Log out of the command shell. Enter: exit

Configuring audit clients for Active Directory

Before you begin
Required materials
• Passwords.txt file with the root account passwords (available in the SAID package)
• CIFS Active Directory username and password
• 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. At the Admin Node, access a command shell and log in as root using the password listed in the Passwords.txt file.

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.


4. Start the CIFS configuration utility. Enter: `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></td>
<td></td>
</tr>
<tr>
<td>add-user-to-share</td>
<td>set-netbios-name</td>
<td></td>
</tr>
<tr>
<td>remove-user-from-share</td>
<td>join-domain</td>
<td></td>
</tr>
<tr>
<td>modify-group</td>
<td>add-password-server</td>
<td></td>
</tr>
<tr>
<td></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:

   In most deployments, you must set the authentication before adding the audit client.
   
   a. Enter: `set-authentication`
      If authentication has already been set, an advisory message appears. If authentication has already been set, go to step 6.
   
   b. When prompted for Workgroup or Active Directory installation, enter: `ad`
   
   c. When prompted, enter the name of the AD domain (short domain name).
   
   d. When prompted, enter the domain controller’s IP address or DNS hostname.
   
   e. When prompted, enter the full domain realm name.
      Use uppercase letters.
   
   f. When prompted to enable winbind support, enter: `y`
      Winbind is used to resolve user and group information from AD servers.
   
   g. When prompted, enter the NetBIOS name.
   
   h. When prompted, press Enter.
      The CIFS configuration utility is displayed.

6. Join the domain:

   a. If not already started, start the CIFS configuration utility. Enter: `config_cifs.rb`
   
   b. Enter: `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. You are prompted for the Administrator’s username. Enter: \textit{administrator\_username} where \textit{administrator\_username} is the CIFS Active Directory username, not the StorageGRID Webscale username.

e. You are prompted for the Administrator’s password. Enter: \textit{administrator\_password} where \textit{administrator\_password} is the CIFS Active Directory username, not the StorageGRID Webscale password.

f. When prompted, press \textbf{Enter}.
The CIFS configuration utility is displayed.

7. Verify that you have correctly joined the domain:

a. Enter: \texttt{join-domain}

b. When prompted to test if the server is currently a valid member of the domain, enter: \texttt{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 \textbf{Enter}.
The CIFS configuration utility is displayed.

8. Add an audit client:

a. Enter: \texttt{add-audit-share}

b. When prompted to add a user or group, enter: \texttt{user}

c. When prompted to enter the audit user name, enter the audit user name.

d. When prompted, press \textbf{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:

a. Enter: \texttt{add-user-to-share}
   A numbered list of enabled shares is displayed.

b. Enter the number of the audit-export share.

c. When prompted to add a user or group, enter: \texttt{group}
   You are prompted for the audit group name.

d. When prompted for the audit group name, enter the name of the audit user group.

e. When prompted, press \textbf{Enter}.
The CIFS configuration utility is displayed.

f. Repeat step 9 for each additional user or group that has access to the audit share.

10. Optionally, verify your configuration.

a. Enter: \texttt{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: The setting 'security=ads' should NOT be combined with the 'password server' parameter. (by default Samba will discover the correct DC to contact automatically).

b. When prompted, press Enter to display the audit client configuration.

c. When prompted, press Enter.
The CIFS configuration utility is displayed.

11. Close the CIFS configuration utility. Enter: 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. Enter: ssh Admin_Node_IP_address
      IP addresses are listed in the Configuration.txt file. If prompted for a password, passwords are 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 remote Admin Node. Enter: exit

13. Log out of the command shell. Enter: exit

Adding a user or group to a CIFS audit share

Before you begin

Required materials

• Passwords.txt file with the root account passwords (available in the SAID package)
• 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. At the Admin Node, access a command shell and log in as root using the password listed in the Passwords.txt file.

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. Quit Server Manager. Enter: press Ctrl+C.

4. Start the CIFS configuration utility. Enter: 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>
</tbody>
</table>
5. Enter: \texttt{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). Enter:
   \texttt{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 to add a user or group:
   
   Enter: \texttt{user}
   
   — or —
   
   Enter: \texttt{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.

9. When prompted, press \texttt{Enter}.
   
   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:

   a. Enter: \texttt{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

   b. When prompted, press \texttt{Enter} to display the audit client configuration.

   c. When prompted, press \texttt{Enter}.

12. Close the CIFS configuration utility. Enter: \texttt{exit}

13. If the StorageGRID Webscale deployment is a single site, go to step 14.
   
   — 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. Enter: \texttt{ssh Admin\_Node\_IP\_address}
      
      IP addresses are listed in the Configuration.txt file. If prompted for a password,
      passwords are 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. Enter: **exit**

14. Log out of the command shell. Enter: **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**

Required materials

- **Passwords.txt** file with the root account passwords (available in the SAID package)
- **Configuration.txt** file (available in the SAID package)

**Steps**

1. At the Admin Node, access a command shell and log in as root using the password listed in the **Passwords.txt** file.

2. Start the CIFS configuration utility. Enter: **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. Enter: **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. Enter: **audit_share_number**

5. When prompted to remove a user or a group:

   - Enter: **user**
     ```
     user
     --- or ---
     ```

   - Enter: **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. Enter: **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. Enter: 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. Enter: 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 171
Removing a user or group from a CIFS audit share on page 173

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

Required materials

- Passwords.txt file with the root account passwords (available in the SAID package)
- 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. At the Admin Node, access a command shell and log in as root using the password listed in the Passwords.txt file.
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.

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:
   a. Enter: `add-audit-share`
   b. When prompted, enter the audit client’s IP address or IP Address range for the audit share. Enter: `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.

6. If more than one audit client is permitted to access the audit share, add the IP address of the additional user:
   a. Enter: `add-ip-to-share`
      A numbered list of the audit shares configured on the Admin Node is displayed. The audit share is named `/var/local/audit/export`.
   b. Enter the number of the audit share. Enter: `audit_share_number`
   c. When prompted, enter the audit client’s IP address or IP Address range for the audit share. Enter: `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).
   d. When prompted, press Enter.
      The NFS configuration utility is displayed.
   e. Repeat step 6 for each additional audit client that has access to the audit share.

7. Optionally, verify your configuration.
   a. Enter: `validate-config`
      The services are checked and displayed.
   b. When prompted, press Enter.
      The NFS configuration utility is displayed.

8. Close the NFS configuration utility. Enter: `exit`

9. If the StorageGRID Webscale deployment is a single site, go to step 10.
    — or —

   Optionally, if the StorageGRID Webscale deployment includes Admin Nodes at other sites, enables these audit shares as required:
   a. Remotely log in to a site’s Admin Node. Enter: `ssh Admin_Node_IP_address`
      IP addresses are listed in the `Configuration.txt` file. If prompted for a password, passwords are listed in the `Passwords.txt` file.
b. Repeat steps 4 through 8 to configure the audit shares for each additional Admin Node.

c. Close the remote secure shell login to the remote Admin Node. Enter: \texttt{exit}

10. Log out of the command shell. Enter: \texttt{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.

\section*{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.

\subsection*{Before you begin}

Required materials

- \texttt{Passwords.txt} file with the root account passwords (available in the SAID package)
- \texttt{Configuration.txt} file (available in the SAID package)

\subsection*{Steps}

1. At the Admin Node, access a command shell and log in as root using the password listed in the \texttt{Passwords.txt} file.

2. Start the NFS configuration utility. Enter: \texttt{config_nfs.rb}

\begin{tabular}{|c|c|c|}
\hline
Shares & Clients & Config \\
\hline
add-audit-share & add-ip-to-share & validate-config \\
enable-disable-share & remove-ip-from-share & refresh-config \\
\hline
help & exit & validate-config \\
\hline
\end{tabular}

3. Enter: \texttt{add-ip-to-share}

A list of NFS audit shares enabled on the Admin Node is displayed. The audit share is listed as: \texttt{/var/local/audit/export}

4. Enter the number of the audit share. Enter: \texttt{audit_share_number}

5. When prompted, enter the audit client’s IP address or IP Address range for the audit share. Enter: \texttt{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.

6. When prompted, press \texttt{Enter}.

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.

a. Enter: \texttt{validate-config}

The services are checked and displayed.
b. When prompted, press **Enter**.
   The NFS configuration utility is displayed.

9. Close the NFS configuration utility. Enter: **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. Enter: `ssh Admin_Node_IP_address`
      IP addresses are listed in the `Configuration.txt` file. If prompted for a password, find the required password 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. Enter: **exit**

11. Log out of the command shell. Enter: **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):
   ```
   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**

- `Passwords.txt` file with the root account passwords (available in the SAID package)
- `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 as root using the password listed in the Passwords.txt file.

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. 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:

   ```bash
   ssh Admin_Node_IP_address
   ```

   IP addresses are listed in the Configuration.txt file. If prompted for a password, find the required password 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 176
Removing an NFS audit client from the audit share on page 177
Managing user and group accounts

Various settings for user and group accounts allow you to configure permissions for the StorageGRID Webscale system. This allows you to manage access to the StorageGRID Webscale and its options.

About user accounts

The StorageGRID Webscale system has two built-in user accounts, Admin and Vendor.

- **Admin**: Responsible for system maintenance. The Admin account can configure services and components, but cannot make system-wide changes.
- **Vendor**: Responsible for system configuration. The Vendor account has full permissions.

Depending on your level of access, you can add new accounts, edit existing accounts, and delete accounts.

About group accounts

Three built-in group accounts (user groups) have been configured for the StorageGRID Webscale system, Vendor, Admin, and User.

The following table summarizes the permissions associated with each Group Account.
<table>
<thead>
<tr>
<th>Activity</th>
<th>Permission</th>
<th>User</th>
<th>Admin</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Management</td>
<td>Edit accounts</td>
<td>Own account only</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Except Vendor account</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Add accounts</td>
<td></td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Except grant Grid</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management permissions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>and add users in Vendor</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP Management</td>
<td>View</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Configure and activate</td>
<td></td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>ILM Management</td>
<td>View</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Configure and activate</td>
<td></td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>NMS Management</td>
<td>Configure E-mail</td>
<td></td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>notifications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Customize alarms at</td>
<td></td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>system-wide level</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set NMS GUI (NMS MI)</td>
<td></td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>timeout period</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity</td>
<td>Permission</td>
<td>User</td>
<td>Admin</td>
<td>Vendor</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------</td>
<td>------</td>
<td>-------</td>
<td>--------</td>
</tr>
<tr>
<td>Grid Options</td>
<td>View</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Configure</td>
<td>❌</td>
<td>❌</td>
<td>✓</td>
</tr>
<tr>
<td>Grid Tasks</td>
<td>Monitor</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Run</td>
<td>❌</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Node/Service/Component</td>
<td>View attributes</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Configure options</td>
<td>❌</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Create reports</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>View and acknowledge alarms</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Customize alarms</td>
<td>❌</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Permissions**

Built-in groups are granted a collection of permissions. There are four types of permissions:

- Grid Management
- Maintenance
- Accounts
- Alarm Acknowledgment

The following table describes the allowable tasks for each set of user group permissions.

<table>
<thead>
<tr>
<th>Permission set</th>
<th>Allowable tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts</td>
<td>• Create new accounts, configure existing accounts, and delete accounts&lt;br&gt;• Create new user groups, configure existing user groups, and delete user groups</td>
</tr>
</tbody>
</table>
### Permission set

<table>
<thead>
<tr>
<th>Permission set</th>
<th>Allowable tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Acknowledgment</td>
<td>• Acknowledge alarms</td>
</tr>
<tr>
<td>Grid Management</td>
<td>• Configure system-wide options</td>
</tr>
<tr>
<td></td>
<td>• Configure ILM</td>
</tr>
<tr>
<td></td>
<td>• HTTP Management</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>To allow a user to make system-wide configuration changes, the user group must</td>
</tr>
<tr>
<td></td>
<td>have both Maintenance and Grid Management permissions. A user with only Grid</td>
</tr>
<tr>
<td></td>
<td>Management permissions does not have system configuration privileges.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>• Configure the NMS MI (customize alarms, configure e-mail notifications, and</td>
</tr>
<tr>
<td></td>
<td>configure GUI timeout)</td>
</tr>
<tr>
<td></td>
<td>• Configure services and components</td>
</tr>
<tr>
<td></td>
<td>• Change Admin Node names</td>
</tr>
<tr>
<td></td>
<td>• Software Upgrade</td>
</tr>
</tbody>
</table>

### Creating user accounts

When you create a new user, that user is added to a defined group account profile with applicable permission settings. If a group with the necessary permission settings does not exist, you must create a group account.

**Steps**

1. Sign in to the NMS MI using an account that has Accounts permissions: for instance, Admin or Vendor.

2. Go to Grid Management > Account Management > Accounts > Main.

3. Under User Accounts, click the insert icon (➕) next to any current account and update entries as needed.

   Note that the list of group names is generated comes from the Group Accounts table; only members of the Vendor group can select the Vendor group.

4. Click Apply Changes.

   New settings are applied the next time you log out and then log back in to the NMS MI.

**Related tasks**

*Creating group accounts* on page 185
Modifying user accounts

You can modify a user account to update the password, name, default language and time zone, or group permissions.

Steps

1. Sign in to the NMS MI using an account that has Accounts permissions: for instance, Admin or Vendor.

   **Note:** Users who do not have Accounts permissions can edit only their passwords, first names, and last names.
   
   Admin users can edit all accounts except the Vendor account.

2. Go to Grid Management > Account Management > Accounts > Main.

3. Click the edit icon (-pencil) next to the name of the account you want to modify and update entries as needed:

   ![Account Management](image)

   **User Accounts**

<table>
<thead>
<tr>
<th>User Name</th>
<th>Password</th>
<th>First Name</th>
<th>Last Name</th>
<th>Language</th>
<th>Time Zone</th>
<th>DST Status</th>
<th>Group Name</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor</td>
<td>*********</td>
<td>Vendor</td>
<td>Maintenance</td>
<td>United States - English</td>
<td>Browser Default</td>
<td>Active</td>
<td>Vendor</td>
<td><img src="edit" alt="edit" /></td>
</tr>
<tr>
<td>Admin</td>
<td>*********</td>
<td>Network Administrator</td>
<td>United States - English</td>
<td>Browser Default</td>
<td>Active</td>
<td>Admin</td>
<td><img src="edit" alt="edit" /></td>
<td></td>
</tr>
<tr>
<td>Tech</td>
<td>*********</td>
<td>Field</td>
<td>Technician</td>
<td>United States - English</td>
<td>Browser Default</td>
<td>Active</td>
<td>Vendor</td>
<td><img src="edit" alt="edit" /></td>
</tr>
</tbody>
</table>

   **Group Accounts**

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Group Description</th>
<th>Guest</th>
<th>Maintenance</th>
<th>Alarm</th>
<th>Acknowledgement</th>
<th>Accounts</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor</td>
<td>Vendor Maintenance</td>
<td>Guest</td>
<td>Guest</td>
<td>Guest</td>
<td>Guest</td>
<td>Guest</td>
<td><img src="edit" alt="edit" /></td>
</tr>
<tr>
<td>Admin</td>
<td>Administrator</td>
<td>Guest</td>
<td>Guest</td>
<td>Guest</td>
<td>Guest</td>
<td>Guest</td>
<td><img src="edit" alt="edit" /></td>
</tr>
<tr>
<td>User</td>
<td>User</td>
<td>Guest</td>
<td>Guest</td>
<td>Guest</td>
<td>Guest</td>
<td>Guest</td>
<td><img src="edit" alt="edit" /></td>
</tr>
</tbody>
</table>

4. Click **Apply Changes**.

   The new settings are applied the next time the user signs out and then signs back in to the NMS MI.

Deleting user accounts

You can delete user accounts for users that no longer require access to the NMS MI.

Steps

1. Sign in to the NMS MI using an account that has Accounts permissions: for instance, Admin or Vendor.

   Any account with Accounts permission can delete any account except for the StorageGRID Webscale system’s built-in user accounts Vendor, Admin or User.
2. Go to Grid Management > Account Management > Accounts > Main.

3. Click the delete icon (X) next to the name of the account you want to delete.

4. Click Apply Changes.

Creating group accounts

You can create group accounts to manage the security permissions for a group of user accounts.

Steps

1. Sign in to the NMS MI using an account that has Accounts permissions: for instance, Admin or Vendor.

2. Go to Grid Management > Account Management > Accounts > Main.

3. Click the insert icon (+) in any line in the Group Accounts table to add a row.

4. Enter a name for the user group.

5. Enter a description for the user group.

6. Select a set of permissions.

   If you assign Maintenance or Grid Management permissions to a group, you should also assign Alarm Acknowledgment permissions.

   **Note:** To allow a user to make system-wide configuration changes, the user group must have both Maintenance and Grid Management permissions. A user with only Grid Management permissions does not have any configuration privileges.

   Only the Vendor account can select Grid Management permissions.

7. Click Apply Changes.

   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 tasks

- Creating user accounts on page 183
- Modifying user accounts on page 184

Modifying a group account

You can modify a group account to update the name or permissions associated with the group.

About this task

The StorageGRID Webscale system’s built-in group accounts (Vendor, Admin, and User) cannot be modified except for the group description.

Steps

1. Sign in to the NMS MI using an account that has Accounts permissions.

2. Go to Grid Management > Account Management > Accounts > Main.
3. Click the edit icon (edit) next to the name of the group account you want to modify and update entries as needed.

If you give Maintenance or Grid Management permissions to a group, you should also assign Alarm Acknowledgment permissions.

Only the Vendor account can select Grid Management permissions.

**Note:** To allow a user to make system-wide configuration changes, the user group must have both Maintenance and Grid Management permissions. A user with only Grid Management permissions does not have any configuration privileges.

4. Click **Apply Changes**.

## Deleting group accounts

You can delete a group account when you want to remove the groups from the system, and remove all permissions associated with the group account from user accounts that belong to the group.

**About this task**

When you delete a group account, users assigned to that group will lose all access privileges to the StorageGRID Webscale system, unless they are granted privileges by a different group. The StorageGRID Webscale system’s built-in group accounts (Vendor, Admin, and User) cannot be deleted.

**Steps**

1. Sign in to the NMS MI using an account that has Accounts permissions: for instance, Admin or Vendor.

2. Go to **Grid Management > Account Management > Accounts > Main**.

3. Click the delete icon (delete) next to the name of the group account you want to delete.

4. Click **Apply Changes**.
What grid tasks are

Grid tasks are scripts that implement specific changes to the StorageGRID Webscale system. For example, most maintenance and expansion procedures involve running grid tasks.

Most grid tasks are automatically generated when the provisioning process is run as part of maintenance and expansion procedures. They are then manually started and monitored. For example, decommissioning a Storage Node involves editing the provisioned grid specification file and then provisioning the StorageGRID Webscale system to generate the Storage Node Decommissioning grid task.

Running grid tasks

When performing procedures that generate grid tasks, you must ensure that you run the grid tasks in the correct order.

Each grid task’s description includes a revision number. No grid task should be run before all grid tasks from previous revisions have completed or been aborted.

Along with running grid tasks in the correct order, plan the execution of grid tasks based on the fact that most grid tasks cannot be run concurrently. This restriction occurs because most grid tasks require exclusive access to the same system resources. There are, however, a number of grid tasks that can be run concurrently. Information about which grid tasks can be run concurrently is listed with each procedure.

- System performance
  System-wide tasks are prioritized lower than normal system operations (such as processing retrieval requests from client applications). However, because running system-wide tasks puts additional load on the StorageGRID Webscale system, they can impact overall system performance during peak load. Moreover, if several system-wide tasks are in progress, they compete for resources, delaying the completion of individual tasks.
  If either of these situations occur, go to the primary Admin Node > CMN > Grid Tasks > Overview > Main page to identify which grid tasks are in progress, and which are closest to completion. You can pause grid tasks to reduce the overall load on the StorageGRID Webscale system or to allow other grid task to complete sooner.

- Resource locking
  When a grid task is started, it might require temporary sole access to specific system resources to complete successfully. When this occurs, the grid task locks the resources that it requires, which might block other grid tasks from using the same resource. This might result in the temporary blocking of other grid tasks that are running concurrently. When the grid task finishes with the system resource, it unlocks it, allowing other grid tasks to access the system resource and run to completion.

Related concepts

Monitoring grid tasks on page 188

Frequently used grid tasks

There are several grid tasks that are most frequently generated that you will encounter as you work through maintenance or expansion procedures.

The following table lists the most frequently used grid tasks:
<table>
<thead>
<tr>
<th>Code</th>
<th>Grid task name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BDLI</td>
<td>Bundle Import</td>
<td>Used when a configuration bundle needs to be updated, usually as one step of a larger maintenance procedure.</td>
</tr>
<tr>
<td>CCLE</td>
<td>Clean Up Unused Cassandra Keys</td>
<td>Used during the expansion procedure when adding Storage Nodes.</td>
</tr>
<tr>
<td>GDCM</td>
<td>Gateway Node Decommissioning</td>
<td>Used during the decommissioning of an API Gateway Node.</td>
</tr>
<tr>
<td>GEXP</td>
<td>Grid Expansion: Initial — or — Grid Expansion: Add Server</td>
<td>Used during the expansion procedure when adding grid nodes.</td>
</tr>
<tr>
<td>ILME</td>
<td>ILM Evaluation (Volume Lost) — or — ILM Re-evaluation (User Triggered)</td>
<td>Used to reapply the ILM policy to content.</td>
</tr>
<tr>
<td>LDCM</td>
<td>Storage Node Decommissioning</td>
<td>Moves all content off the specified Storage Node to other Storage Nodes and then permanently removes the selected Storage Node from the StorageGRID Webscale system.</td>
</tr>
<tr>
<td>VFGV</td>
<td>LDR Foreground Verification</td>
<td>Verifies the existence of replicated object data on a Storage Node.</td>
</tr>
</tbody>
</table>

**Monitoring grid tasks**

You can monitor the progress of grid tasks to verify that a system configuration step is complete; for example, as part of a maintenance or expansion procedure.

You can view the status of grid tasks on the `primary Admin Node > CMN > Grid Tasks > Overview > Main` page. Running grid tasks is restricted to accounts with Maintenance permissions such as the Admin and Vendor accounts.
Grid tasks go through three distinct phases:

- **Pending**: The grid task has been submitted, but not started yet.
- **Active**: The grid task has been started. It can be either actively running or temporarily paused. If a grid task’s status changes to Error, it will continuously retry until it is able to complete successfully or is aborted.
  A common reason for a grid task to enter an error state is if a grid node becomes unavailable (lost connection or crash) or another grid task is running. For grid tasks stuck with a Status of Error, when the issue is resolved, the grid task automatically starts running again.
- **Historical**: A grid task that has been submitted, but is no longer active.
  This includes grid tasks that completed successfully, were canceled, aborted, or that have failed.

### Attribute Description

<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. You should always run the earliest generated grid task first.</td>
</tr>
<tr>
<td>Valid From</td>
<td>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>Valid To</td>
<td>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>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Status</td>
<td>Current status of the active or historical grid task. For active grid tasks, one of:</td>
</tr>
<tr>
<td></td>
<td>• Starting</td>
</tr>
<tr>
<td></td>
<td>• Running</td>
</tr>
<tr>
<td></td>
<td>• Pausing</td>
</tr>
<tr>
<td></td>
<td>• Paused (either paused by the user or automatically paused by the grid task)</td>
</tr>
<tr>
<td></td>
<td>• Error: An error has been encountered. User action might be required. Grid task retries until successful or aborted.</td>
</tr>
<tr>
<td></td>
<td>• Aborting</td>
</tr>
<tr>
<td></td>
<td>• Abort Paused: Grid task failed to be aborted and is paused in error.</td>
</tr>
<tr>
<td></td>
<td>• Retrying</td>
</tr>
<tr>
<td></td>
<td>For historical grid tasks, one of:</td>
</tr>
<tr>
<td></td>
<td>• Successful</td>
</tr>
<tr>
<td></td>
<td>• Rollback Failed</td>
</tr>
<tr>
<td></td>
<td>• Expired</td>
</tr>
<tr>
<td></td>
<td>• Aborted</td>
</tr>
<tr>
<td></td>
<td>• Canceled</td>
</tr>
<tr>
<td></td>
<td>• Unauthorized</td>
</tr>
<tr>
<td></td>
<td>• Duplicate</td>
</tr>
<tr>
<td></td>
<td>• Invalid</td>
</tr>
<tr>
<td>Message</td>
<td>Information about the last stage of the active grid task.</td>
</tr>
<tr>
<td>Completion time</td>
<td>The date and time on which the grid task completed (or was canceled, expired, or was aborted).</td>
</tr>
</tbody>
</table>

**Charting a grid task**

You can chart the progress of an active grid task—particularly a grid task that takes a long time to complete—at primary Admin Node > CMN > Grid Tasks > Reports > Charts. This enables you to track a grid task’s progress and determine if the grid task is stalled.
**Note:** A grid task is only available for charting while it is active.

**Related tasks**

*Troubleshooting grid task retries* on page 194
You might observe that a grid task does not complete successfully, but that the StorageGRID Webscale system retries running the grid task multiple times. You should identify and solve this issue to conserve system resources.

## Running a grid task

You must run grid tasks to update the StorageGRID Webscale system as part of maintenance and expansion procedures.

### Before you begin

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.

### About this task

Under normal circumstances, grid tasks required for expansion or maintenance procedures appear automatically in the Pending table as part of the provisioning process.

### Steps

1. Go to **primary Admin Node > CMN > Grid Tasks > Configuration > Main**.

2. 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.

3. Click **Apply Changes**.

   The grid task moves from the Pending table to the Active table. You must wait for the NMS MI page to refresh before the change is visible. Do not submit the change again. The grid task continues to execute until it completes, is paused, or is aborted. When the grid task completes successfully, it moves to the Historical table with a Status of Successful. If the grid task fails, it might be for one of several reasons.

   **Note:** Configuration does not update automatically. To monitor the progress of a grid task, go to the Overview page and then, if necessary, back to the Configuration page to make changes.

### Related concepts

*Troubleshooting grid tasks* on page 193

### Related tasks

*Pausing an active grid task* on page 192
Pausing an active grid task

You can pause an active grid task before it finishes, to improve system performance. 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.

About this task

Steps

1. Go to \textit{primary Admin Node} > CMN > Grid Tasks > Configuration > Main.
2. Under Actions, select \textit{Pause} for the Active grid task you want to suspend temporarily.
3. Click \textit{Apply Changes}.

   The grid task remains on the Active table with its Status changed to Paused. This can be seen by returning to \textit{primary Admin Node} > CMN > Grid Tasks > Overview > Main.

Related concepts

\textit{Running grid tasks} on page 187

Resuming a paused grid task

You can resume a paused grid task when conditions permit.

Steps

1. Go to \textit{primary Admin Node} > CMN > Grid Tasks > Configuration > Main.
2. Under Actions, select \textit{Run} for the Active grid task you want to resume.
3. Click \textit{Apply Changes}.

   The grid task remains on the Active table, with its status changed to Active. You can confirm this by returning to \textit{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 for execution.

Steps

1. Go to \textit{primary Admin Node} > CMN > Grid Tasks > Configuration.
2. Under Actions, select \textit{Cancel} for the Pending grid task that you want to cancel.
3. Click \textit{Apply Changes}.

   The grid task remains on the Active table with its status changed to Active. You can confirm this by returning to \textit{primary Admin Node} > CMN > Grid Tasks > Overview > Main.
Aborting a grid task

You can abort a grid task from the Active table so that it is no longer available for execution.

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.

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. Go to primary Admin Node > CMN > Grid Tasks > Configuration > Main.
2. Under Actions, select Pause for the Active grid task you want to abort.
3. Click Apply Changes.
   When the page refreshes, the status of the grid task changes to Paused.
4. Under Actions, select Abort.
5. Click Apply Changes.
   The grid task remains on the Active table with its status changed to Active. You can confirm this by returning to primary Admin Node > CMN > Grid Tasks > Overview > Main.

After you finish

You can run a grid task you aborted again by resubmitting it with a Task Signed Text Block.

Related tasks

Submitting a Task Signed Text Block on page 195

If the grid task you need to run is not in the Pending table (for example, it has been aborted), you can manually load the grid task by submitting the Task Signed Text Block.

Removing grid tasks from the Historical table

You can manually remove grid tasks listed in the Historical table.

Steps

1. Go to primary Admin Node > CMN > Grid Tasks > Configuration > Main.
2. Select the Remove check box for the grid task.
3. Click Apply Changes.
   The grid task remains on the Active table with its status changed to Active. You can confirm this by returning to primary Admin Node > CMN > Grid Tasks > Overview > Main.

Troubleshooting grid tasks
Choices

- **Grid task fails to complete and moves to Historical table** on page 194
  In some cases, you might observe that a grid task moves to the Historical table without completing successfully.

- **Troubleshooting grid task retries** on page 194
  You might observe that a grid task does not complete successfully, but that the StorageGRID Webscale system retries running the grid task multiple times. You should identify and solve this issue to conserve system resources.

- **Grid task error management** on page 195
  If a grid task status changes to Error, the grid task retries until it is successful or aborted. Do not run any other grid tasks until the grid task with a status of Error completes successfully or is aborted.

- **Aborting grid tasks** on page 195
  If a grid task you are aborting enters an Internal Error state, you should attempt to abort the grid task again. If the grid task is still unable to complete the abort sequence, you should contact technical support.

- **Submitting a Task Signed Text Block** on page 195
  If the grid task you need to run is not in the Pending table (for example, it has been aborted), you can manually load the grid task by submitting the Task Signed Text Block.

**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 was aborted.
- Canceled: The grid task was canceled.
- Duplicate: The grid task has been previously loaded into the CMN service.
- Expired: The “task valid before” time has already passed.
- Invalid: The grid task was not valid.
- Rollback Failed: The grid task did not complete normally and failed to be aborted.
- Unauthorized: The grid task signature did not pass verification.

The most common reason for a grid task failure is that it has expired. If a grid task expires, it can never be run. A new grid task must be created and run. If there are multiple versions of the same grid task, you should always run the earliest generated (lowest revision number) grid task first.

Note that a grid task failure is not the same as a grid task error. The status of a grid task that encounters an error updates to Error and then Retrying as it attempts to finish. In this case, the grid task does not fail and move to the Historical table unless it is aborted.

**Troubleshooting grid task retries**

You might observe that a grid task does not complete successfully, but that the StorageGRID Webscale system retries running the grid task multiple times. You should identify and solve this issue to conserve system resources.

**Steps**

1. Pause and then restart the grid task.
2. Check the StorageGRID Webscale system for connectivity issues.
3. Restart the CMN service.
4. Abort the grid task, remove it from the Historical table, and then resubmit it.
5. Contact technical support.

Grid task error management

If a grid task status changes to Error, the grid task retries until it is successful or aborted. Do not run any other grid tasks until the grid task with a status of Error completes successfully or is aborted.

At the same time that the grid task enters the error state, a Grid Task Status alarm (SCAS) is triggered.

For information about the error, go to 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, if the grid task has not been aborted, it moves out of the error state and continues to a successful completion. If the grid task is aborted, it must be resubmitted.

Related tasks

Submitting a Task Signed Text Block on page 195
  If the grid task you need to run is not in the Pending table (for example, it has been aborted), you can manually load the grid task by submitting the Task Signed Text Block.

Aborting grid tasks

If a grid task you are aborting enters an Internal Error state, you should attempt to abort the grid task again. If the grid task is still unable to complete the abort sequence, you should contact technical support.

Steps

1. Go to primary Admin Node > CMN > Grid Tasks > Configuration.
2. Under Actions, select Abort.

Submitting a Task Signed Text Block

If the grid task you need to run is not in the Pending table (for example, it has been aborted), you can manually load the grid task by submitting the Task Signed Text Block.

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 NMS MI.
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:
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. Sign in to the NMS MI.

6. Go to primary Admin Node > CMN > Grid Tasks > Configuration > Main.

7. Under Submit New Task, select the prompt text so that you can replace it with the Task Signed Text Block.


9. 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.
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 such a data migration into the StorageGRID Webscale system. It is not a general guide to data migration, nor is it a detailed step by step procedure for executing such a migration. Instead, it provides you with the information required to plan and carry-out your data migration. Following the guidelines and instructions in this section ensures that data is migrated efficiently into the StorageGRID Webscale system without interfering with its day to day operations, and that once ingested, migrated data is handled appropriately by the StorageGRID Webscale system.

Confirm 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 are 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, assess the data profile of the objects that 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.

Determine 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, 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.

Related concepts

Matching criteria and filter evaluation on page 72
What information lifecycle management is on page 63
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. You must use either batch ingest or throttled continuous ingest, and continuously monitor the StorageGRID Webscale system during data migration 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 software 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.

Key attributes to monitor

Data migration must be monitored and adjusted to keep these attributes in an acceptable range to ensure a good balance between reliable and responsive daily operations and the best possible data migration rate.

This table lists information about the attributes that you must monitor during data migration, and the issues that they represent:
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Summary Page</td>
<td>If an alarm is triggered, a dangerous queue of objects that have yet to be evaluated against the active ILM policy has formed. Objects in this queue are in danger of loss as they have yet to be copied and stored according to the ILM policy’s ILM rules. Control this object queue by throttle the ingest rate of objects.</td>
</tr>
<tr>
<td>Current ILM Activity Deployment&gt; &gt; Overview &gt; Main &gt; Number of Objects (IQSZ)</td>
<td>If an alarm for this attribute is triggered, the targeted archival storage system might have reached capacity. Check the targeted archival storage system and resolve any issues that triggered an alarm.</td>
</tr>
<tr>
<td>Archive Node</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 the targeted archival storage system to ensure that there is sufficient capacity for the migrated data.</td>
</tr>
</tbody>
</table>

**Related tasks**

*Performing a batch ingest* on page 199
*Performing throttled continuous ingest* on page 200

## Performing a batch ingest

Batch ingest is when you periodically save a large batch of data to the StorageGRID Webscale system through a client application (S3, Swift, CDMI or SGAPI). The StorageGRID Webscale system does not throttle data ingest or otherwise control how data arrives, but processes each batch at its maximum possible rate.

### About this task

Because of the load batch ingests put on the StorageGRID Webscale system, perform this procedure outside of core operational hours and, if performing multiple batch ingests, wait until each batch ingest completes before starting the next. Because of the large queues of data that need to be processed before an operational request can be satisfied, performing a batch ingest during operational hours will interfere with the normal ingest and retrieval of data after each batch.

**Warning:** Do not perform a batch ingest simultaneously with day to day operations of the StorageGRID Webscale system.

### Steps

1. Ingest multiple objects through a supported interface (S3, Swift, CDMI, or SGAPI).
2. Monitor key attributes:
   
   - Configure custom notifications for migration alarms, so that you are alerted if any of the attributes exceed their acceptable levels.
   - Ensure attributes remain at acceptable values and alarm levels do not exceed the maximum levels.

   Attributes with a maximum acceptable alarm level of Minor have an acceptable attribute level chosen to provide an operational “window” for migration. For these attributes, if a Minor level
alarm is triggered, migration can continue as long as the attribute stays below the maximum value.

3. If an attribute value or alarm level exceeds minimum acceptable levels:
   • Suspend migration.
   • Wait until numerical attribute values decline to near zero (and other attributes return to an acceptable value), and all alarms are cleared.
   • Reduce the size of the next batch.

4. If attribute values remain in range and no alarms are triggered:
   • Wait until the StorageGRID Webscale system finishes ingesting a batch and returns to a “quiet” state. That is, numerical attribute values decrease to near zero, and all alarms are cleared.

5. Save the next batch of data.
   If necessary, adjust the size of the batch based on the StorageGRID Webscale system behavior when storing the previous batch.

6. After all migration data is transferred to the StorageGRID Webscale system, remember to:
   • Disable any custom notifications you created for the migration process in step 2.

Related tasks

Creating custom notifications for migration alarms on page 201

Performing throttled continuous ingest

If you have a way to throttle the rate at which data is saved to the StorageGRID Webscale system, you can migrate data through continuous ingest.

About this task

You can use continuous ingest, for example, if you:

• Have a data migration tool.
• Can configure the client application to throttle its copy rate.
• Have a method that permits you to limit the bandwidth consumed by migration data.

Throttling the rate that data is saved to the StorageGRID Webscale system is not a feature of StorageGRID Webscale software: to use throttled continuous ingest you must have an independent way to control the rate that data is sent to StorageGRID Webscale system.

Depending on the daily ingest load, it might also be possible to migrate data at a low rate during normal operational hours if it is possible to do so without exceeding the threshold levels that indicate that migration is consuming too many system resources.

Steps

1. Configure your data migration tool to save data continuously to the StorageGRID Webscale system at a low, controlled rate.

2. Monitor the value of the key attributes:
   • Configure custom notifications for migration alarms, so that you are alerted if any of the attributes exceed their acceptable levels.
• Ensure that attributes remain at acceptable values and alarm levels do not exceed the maximum levels.

Attributes with a maximum acceptable alarm level of Notice have an acceptable attribute value chosen to provide an operational “window” for migration. For these attributes, if a Notice level alarm is triggered migration can continue as long as the attribute stays below the maximum value.

• Ensure that attribute values remain relatively constant and do not gradually increase over time.

3. If the attribute values remain stable and well below the values, you can adjust the data migration rate up slightly.

Monitor the StorageGRID Webscale system closely to ensure that the new data migration rate is sustainable.

4. If the attribute values and alarm levels exceed minimal acceptable levels or numerical attribute values increase over time:
   • Suspend data migration until the values and alarm levels return to acceptable levels.
   • Lower the rate at which data is being saved to the StorageGRID Webscale system.
   • Resume migration.

5. After all migration data is transferred to the StorageGRID Webscale system, remember to:
   • Disable any custom notifications you created for the migration process in step 2.

Related tasks

Creating custom notifications for migration alarms on page 201

Creating custom notifications for migration alarms

You might want to configure the StorageGRID Webscale system to send a notification e-mail to the system administrator responsible for monitoring migration if the attribute values exceed their recommended maximum values.

About this task

You can accomplish this by configuring a global custom alarm to send notifications for each attribute:

Steps

1. If not already configured, specify the e-mail server the StorageGRID Webscale system should use for notifications.

2. If desired, create a template to customize the subject line, header, and footer of data migration notification e-mails.

3. Create an e-mail list that includes all administrators responsible for monitoring the data migration, and uses the template you created in step 2.

4. Create a Global Custom alarm for each attribute you need to monitor during data migration:
   a. Go to Grid Management > NMS Management > Alarms > Custom.
   b. Under Default Alarms, search for the default alarms for the first attribute. Under Filter by, select Attribute Code, then type the 4 letter code for the attribute. For example, ARVF.
   c. Click the submit arrow .
d. In the results list, click Copy next to the alarm you want to modify to move it to the Global Custom Alarms table.

e. Under Global Custom Alarms, in the Mailing List column for the copied attribute, add the mailing list you created in step f.

f. Repeat for each remaining attributes.

g. When finished creating Global Custom alarms, click Apply Changes.

After you finish

Administrators responsible for monitoring data migration now receive an e-mail 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 e-mail server settings** on page 34
  The E-Mail Server page allows you to configure SMTP mail server settings that enable the sending of e-mail for alarm notifications and AutoSupport messages. The StorageGRID Webscale system only sends e-mail; it cannot receive e-mail. Only the SMTP protocol is supported.

- **Creating mailing lists** on page 36
  The Lists page allows you to create mailing lists for notifications. A mailing list allows you to send one e-mail message to multiple e-mail 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 e-mail address.
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.

Using the Server Manager graphical or command-line interface

You can use Server Manager in the following ways, Graphical user interface (GUI) or Command-line interface (CLI).

If you are working with a StorageGRID Webscale appliance, you must use the Server Manager CLI. The Server Manager GUI is not available with an appliance.

Navigating the Server Manager graphical interface

Server Manager’s graphical interface on the local console of the server enables monitoring and coarse (whole server) control. The state of services is reported, along with server identity information such as IP addresses. You can stop services to reboot the server or shut the server down for hardware maintenance.

The display of service states is updated synchronously with changes in the services. However, there can be processing delays of up to 15 seconds before the GUI reflects the current state of all services.
The header line identifies the Server Manager application and its overall status. When running normally, the header has a blue background. If a service reports an error, the background immediately changes to red.

The status line is an aggregate representation of the state of the services under its control. If they are all stopped, the Status is Stopped; all running, Running, and so on. If any of the services are in an error state, the Status is Error. Similarly, if any of the services are in the Stopped state, the Status is Stopped.

### Service list

The body of the display lists the services monitored by Server Manager on this grid node.

- **Service Name:** The name of each service is shown. Some services can appear that are not identified through the NMS MI. These are services that can run independently and provide support capabilities to other services.

- **Version:** Where a version number is available from the service, it is displayed in the list. This provides a quick reference for administrators to verify the currency of services and identify if updates are required.

- **Status:** Normally these all report “Verified” (operating system services) or “Running.” As the services are being started or stopped, the status can report the transition stage, such as “Stopping” or “Starting.” Additionally, “Stopped” indicates a service that has been ordered stopped by the Server Manager and will not restart without a Server Manager command. Services that report a status of “Disabled” have the DoNotStart file in place that prevents them from being started when Server Manager restarts.

### Related concepts

*DoNotStart file* on page 211
Command buttons

Four command buttons are used to stop and start services and reboot or shut down the server. Use of these buttons ensures the services enter and leave the StorageGRID Webscale system gracefully.

- **Start All**
  Use the **Start All** button to start services that have been stopped for configuration changes. Server Manager executes a series of scripts to initiate dependent applications in a sequence that ensures prerequisite services are running before starting the services for grid nodes. All existing error states for all services are cleared. When all services are started, the grid node joins the StorageGRID Webscale system. Any services already running are not disrupted.

- **Stop All**
  Use the **Stop All** button to gracefully stop services on the grid node, effectively disconnecting it from the StorageGRID Webscale system. The operating system and Server Manager continue to run, allowing you to perform tasks such as configuration changes, software updates, and similar maintenance procedures that requires the operating system. Services and third-party applications are stopped.

  **Note:** Unlike the command `/etc/init.d/servermanager stop`, the **Stop All** button does not stop Server Manager and gridstat.

- **Restart**
  Use the **Restart** command to stop services and bring down the operating system to perform an automatic reboot. This is useful for resetting a grid node that has failed or when starting a new configuration.

  The Server Manager performs the same sequence as the **Stop All** command, then continues to bring down the operating system. The Server Manager and GUI are closed by the operating system as part of its shutdown. Settings in the operating system are used to trigger a reboot, which in turn restarts the Server Manager application. Server Manager then restarts the GUI and all services.

  **Note:** Unlike the command `/etc/init.d/servermanager restart`, the **Restart** button reboots the server from the BIOS up.

- **Shutdown**
  Use the **Shutdown** command to power down the server for hardware maintenance or reconfiguration. Similar to Restart, this command gracefully closes services and halts the operating system. Unlike Restart, this command does not trigger a reboot. The system is fully halted, and power is turned off. Power must be turned on to start the system.

  The Server Manager performs the same sequence as the **Stop All** command, then continues to bring down the operating system to a halted state. The Server Manager and GUI are closed by the operating system as part of the shutdown.

Related concepts

- **Command buttons** on page 205

Related tasks

- **Stopping Server Manager and all services** on page 209
- **Restarting Server Manager and all services** on page 209
Grid node identification

The bottom right area of the display provides information about the grid node itself.

- Host Name: This is the name of the grid node specified when the server is added to StorageGRID Webscale system at configuration time.
- Node Type: This is the type of grid node, for example Storage Node.
- IP Addresses: The grid nodes' operating system networking service is used to report the IP addresses assigned to the network interface(s). Most grid nodes have one address; however, if multiple adapters/addresses are available, all are reported.

Initiating an action

Steps

1. Use the mouse or the <Tab> and <Enter> keys to select the desired command button.
   A confirmation dialog opens allowing you to confirm or cancel the action.

2. Type the Server Manager password listed in the Passwords.txt file.

   ![Confirmation dialog]
   Are you sure you want to start all services?
   Password: ____________________________

3. Click OK to confirm the action.

Changing the Server Manager password

It is possible to change the server manager password for any server after installation.

About this task

Note: The new password is not saved. The Passwords.txt file does not get updated. Make sure to record the password in a safe place.

Steps

1. At the grid node, access a command shell and log in as root using the password listed in the Passwords.txt file.

2. Enter: `passwd mgr-pass`

3. When prompted, enter a new password.

4. Log out of the command shell. Enter: `exit`
5. Press Alt+F7 to return to the Server Manager GUI.

The password is reset to its original value if the operating system is reinstalled on the server as part of a maintenance procedure.

**Server Manager command shell procedures**

The command line scripts provide advanced users an additional level of control over the grid node and individual services needed to perform certain maintenance procedures.

The Server Manager GUI is available only at the local console of the server. The command line controls outlined in this section can be executed either at the local console or remotely through a secure shell login.

**Log in:** At the server, access a command shell and log in as root using the password listed in the Passwords.txt file.

**Log out:** When entering commands at the local console, always close the account login at the end of the procedure to avoid leaving a root-level command shell open.

1. Close the current command shell session. Enter: `exit`
2. Press Alt+F7 to return to the Server Manager GUI.

**Accessing a server remotely:** Using a remote secure shell login is particularly useful when monitoring or maintaining a remote site. There are two ways to access a grid node remotely using ssh:

- From the primary Admin Node using the ssh key password
- From any server using the remote server password

**Status information**

- Display current status
  Enter: `/etc/init.d/servermanager status`

The current status of the Server Manager control 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.

This status is the equivalent of the status shown in the header of the local console display.

- Continuously display service status
  1. Enter: `storagegrid-status`

<table>
<thead>
<tr>
<th>Host Name</th>
<th>DC1-ADM1-98-160</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Type</td>
<td>Admin Node</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.99.10.100</td>
</tr>
<tr>
<td>Operating System Kernel</td>
<td>3.0.76</td>
</tr>
<tr>
<td>Operating System Environment</td>
<td>SLES-11 SP3</td>
</tr>
<tr>
<td>StorageGRID Webscale Release</td>
<td>10.2.0</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>5.5.40</td>
</tr>
<tr>
<td>Time Synchronization</td>
<td>4.2.4p8</td>
</tr>
<tr>
<td>Network Monitoring</td>
<td>10.2.0</td>
</tr>
<tr>
<td>ams</td>
<td>10.2.0</td>
</tr>
<tr>
<td>cmn</td>
<td>10.2.0</td>
</tr>
<tr>
<td>nms</td>
<td>10.2.0</td>
</tr>
<tr>
<td>ssm</td>
<td>10.2.0</td>
</tr>
<tr>
<td>mi</td>
<td>10.2.0</td>
</tr>
<tr>
<td>tomcat</td>
<td>5.5.35.3</td>
</tr>
</tbody>
</table>
The same status information that is available from the Server Manager GUI is displayed.

2. To exit, press Ctrl+C.

- Displaying the version number
  Enter: /etc/init.d/servermanager version
  This command reports the current version of Server Manager. This information can be useful when updating the StorageGRID Webscale system.

- Displaying the current status of services
  Enter: /usr/local/servermanager/reader.rb
  The display of reader.rb does not update when the status of a service changes. Enter the command again to update the display.

- Displaying the status of individual services
  Enter: /etc/init.d/service status
  If the interlock DoNotStart file is in place, a status of disabled and the length of time the service has been disabled is returned. For example:

  ldr disabled for 1d, 14h, 13m, 40s

  indicates that the LDR service has been disabled for a total of 1 day, 14 hours, 13 minutes, and 40 seconds.

Related concepts

Navigating the Server Manager graphical interface on page 203

Starting Server Manager and all services manually

At installation, the Server Manager application and GUI start automatically whenever the operating system is started.

About this task

You might have to manually start Server Manager to initiate the core application if it has failed or the process has been killed by the operating system.

Step

1. Enter: /etc/init.d/servermanager start

   Note: This command executes a more fundamental start than the GUI Start All command button since it also starts servermanager and gridstat.

Related concepts

Command buttons on page 205
**Restarting Server Manager and all services**

**Step**

1. Enter: `/etc/init.d/servermanager restart`

   All services on the grid node are stopped and restarted, including the Server Manager core application and GUI.

   **Note:** This is not the same as the GUI command to Restart, which reboots the server from the BIOS up.

   Using the `restart` command is the same as using the `stop` command followed by the `start` command.

**Related concepts**

*Command buttons* on page 205

**Stopping Server Manager and all services**

Server Manager is intended to run at all times to automatically restore services if they go offline or the server is restarted. 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.

**About this task**

The only scenario that requires you to stop Server Manager itself while keeping the operating system running would be to integrate Server Manager to other services.

**Step**

1. Enter: `/etc/init.d/servermanager stop`

   Services are gracefully terminated and Server Manager core application is terminated.

**Stopping individual services**

Some maintenance procedures require a single service be stopped while keeping other services on the same grid node running. Only stop individual services when directed to do so by a maintenance procedure.

**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.

**Step**

1. Enter:

   `/etc/init.d/service stop`

   If the service fails to stop, perform a manual termination of the service.

**Related tasks**

*Forcing services to terminate* on page 210
Forcing services to terminate

Occasionally, a service will not stop after receiving the stop command (/etc/init.d/service stop). This failure of a service to stop can be the result of an unusual software state or other unexpected condition within the system.

Steps

1. Press Ctrl+C.

2. Enter: `sv -w time force-stop service`
   where time is the number of seconds to wait before executing the command.

   Example
   
   `sv -w 30 force-stop <service>` waits 30 seconds before forcefully terminating the service.

Restarting individual services

To restart a manually stopped service, enter: `/etc/init.d/service start`

To restart a running service, enter: `/etc/init.d/service restart`

Rebooting servers

With a reboot, all services are started automatically except for services that have a DoNotStart file. If services were previously in ErrorState, Server Manager removes the file and attempt to start the service again.

Steps

1. Stop services. This is an optional, but recommended step. Enter: `/etc/init.d/servermanager stop`

2. Reboot the server. Enter: `reboot`

   If a reboot command is directly issued to the system, you might not be able log in to the system remotely to monitor the shutdown process. Services can take some time to shut down.

Powering down servers

If you need to power down a server remotely, use the Linux shutdown command.

Steps

1. Stop services. This is an optional, but recommended step. Enter: `/etc/init.d/servermanager stop`

2. Shutdown the server. Enter: `shutdown -h now`
Service dependencies

Server Manager manages the dependencies between services, starting and stopping services as required to permit services and grid nodes to join the StorageGRID Webscale system.

Server Manager manages dependencies between services on start-up or shutdown. These dependencies are managed differently for a start-up and shutdown and are also managed differently depending on the service. The following figure illustrates these dependencies.

The following Server Manager dependencies should be noted:

- services: A DoNotStart file on any service (for example, ldr, ams, or cms) prevents that service from starting.
- ntp: All services are dependent upon the ntp service. The DoNotStart file on ntp will prevent all services from starting.
- mysql: The nms and mi services are dependent upon the mysql database service. The DoNotStart file on mysql will prevent mysql services from starting.

Although various services are dependent on each other, it is not always true that starting a service which was previously disabled will start dependent services. For example, if ntp is prevented from starting with the DoNotStart file, and then the DoNotStart file is removed and the ntp service manually started, services will not start. You must use Server Manager to start all services. In this case, dependent services are not started. However, if mi is prevented from starting with the DoNotStart file, and then the DoNotStart file is removed and the mi service started, attribute downsampling (attrDownSamp1, attrDownSamp2, attrDownPurge) and tomcat will be started. In this case dependent services are started.

DoNotStart file

The interlock file DoNotStart is used to prevent services from being started when Server Manager is started or restarted. This might be necessary when performing various maintenance or configuration procedures.

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 a service that they are all dependent upon from running. This is the ntp service.
To prevent an individual service from starting, or to prevent other services from starting that are not dependent upon ntp (such as the servermanager service or mi service), insert the DoNotStart file for the individual services.

**Inserting the ntp DoNotStart file**

**About this task**

*Note:* Inserting the DoNotStart file after the application has been started does not halt operation. The DoNotStart file is only checked when the service is started or restarted.

**Steps**

1. Stop all services and Server Manager: `/etc/init.d/servermanager stop`
2. Insert the DoNotStart file: `touch /etc/sv/ntp/DoNotStart`
   This creates the DoNotStart file. No file content is needed.
3. Restart Server Manager and all services: `/etc/init.d/servermanager start`

**Creating DoNotStart files for single services**

**Step**

1. At the operating system command line, enter:
   `touch /etc/sv/service/DoNotStart`
   where *service* is the name of the service.
   This creates the DoNotStart file. No file content is needed.

   When Server Manager or the grid node is restarted with the DoNotStart file present, Server Manager restarts without starting the service.

**Removing ntp DoNotStart files**

**Steps**

1. At the operating system command line, enter: `rm /etc/sv/ntp/DoNotStart`
2. To log out of the console, enter: `exit`
3. Restart the services.
   Press *Alt+F7* to return to the Server Manager GUI and click *Start All*.

**Removing DoNotStart files for single services**

**Steps**

1. At the operating system command line, enter: `rm /etc/sv/service/DoNotStart`
   where *service* is the name of the service.
2. Start the service. Enter: `/etc/init.d/service start`
   where *service* is the name of the service.
Troubleshooting Server Manager

Log files

Error messages related to Server Manager are captured in a log file 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 the log files to technical support to help with troubleshooting.

Service fails to start

While running normally, the Server Manager is constantly monitoring the services. If a service fails, Server Manager attempts to restart it. If there are three failed attempts to start services within five minutes, the service goes down and Server Manager does not attempt another restart.

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. Determine the status of a service. Enter: /etc/init.d/service status

2. The above step will inform you if a service is disabled. A status of “disabled” indicates the presence of a DoNotStart file.

3. Check for the presence of the DoNotStart file at: /etc/sv/service/DoNotStart

4. If the DoNotStart file is present:
   a. Delete the file. Enter: rm /etc/sv/service/DoNotStart; exit\n   b. Start the service. Enter: /etc/init.d/service start

Error state

Server Manager monitors services and restarts any that have terminated 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.

• Determine error state
  Display the service status. Enter: /etc/init.d/service status
  If the service is an error state, the following message is returned:
  service in error state

• Remove error state
  Restart the service. Enter: service


tomcat service

Before restarting the tomcat service from the command line, close any open NMS MI browser windows and ask users not to log in. While tomcat is restarting, the browser continues to present a cached login page that accepts input.

If you attempt to log in using this cached page, tomcat throws an error. After three such errors, tomcat cannot restart automatically and must be manually restarted from the command line.
The Grid Deployment Utility (GDU) is used to facilitate the installation of software on all grid nodes and is installed and available on the primary Admin Node.

Starting the Grid Deployment Utility

Steps

1. At the primary Admin Node, access a command shell and log in as root using the password listed in the Passwords.txt file.

   If you are using PuTTY as your Telnet/ssh client, in PuTTY, select Window > Translation > Remote character set > UTF-8.

2. Enter: `ssh-add`

   You need to run `ssh-add`, which adds the ssh private key to the ssh agent, each time you start a new shell session. For more information about ssh access points, see the Administrator Guide.

3. If prompted, enter the SSH Access Password listed in the Passwords.txt file.

4. If using PuTTY, start screen. For example, enter: `screen -S GDU`

   **Note:** Do not use screen if running GDU locally because the GDU console characters will not display properly.

   The name of the session (for example GDU in the command above) is optional, but recommended since it is useful for managing screen sessions.

   The screen program allows you to manage multiple shell instances concurrently, connect to the same session from different locations, detach from a session without stopping the program running within the session, and resume a session that was previously detached.

   To detach from a screen, press Ctrl+A and then Ctrl+D.

   To reattach to a screen, enter: `screen -r`
5. Start GDU. Enter: `gdu-console`

6. When prompted, enter the provisioning passphrase. Type the passphrase, press Tab to select OK, and then press Enter.

![Provisioning Repository Passphrase]

**Related concepts**

*Troubleshooting the Grid Deployment Utility* on page 218

**How to use the Grid Deployment Utility**

You use the Grid Designer Utility's (GDU) console to select grid nodes and the action to be performed on the grid node.

The GDU console consists of five panels:

- **Servers**: Displays the grid nodes for the StorageGRID Webscale system.
- **Tasks**: Displays the procedures that can be performed on the grid node selected in the Servers panel. Only the tasks applicable to the current situation are displayed. It is possible to run GDU tasks in parallel on different grid nodes. The list of tasks includes:

<table>
<thead>
<tr>
<th>Task</th>
<th>Select to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Services</td>
<td>Enable services for a grid node.</td>
</tr>
<tr>
<td>Install Software</td>
<td>Install StorageGRID Webscale software onto the virtual machine.</td>
</tr>
<tr>
<td>Load Configuration</td>
<td>Load NMS configuration settings.</td>
</tr>
</tbody>
</table>

- **Server Info**: Displays information about the selected grid node.
- **Log Messages**: Displays messages related to the selected task.
- **Actions**: Options for starting tasks, listing ISOs, and quitting the console.
<table>
<thead>
<tr>
<th>Task</th>
<th>Select to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot Server</td>
<td>Reboot the server and start the services.</td>
</tr>
<tr>
<td>Remount Storage</td>
<td>Check for preserved storage volumes and remount them. Used for maintenance procedures on Storage Nodes.</td>
</tr>
<tr>
<td>Start Services</td>
<td>Start Server Manager and all services.</td>
</tr>
<tr>
<td>Stop Services</td>
<td>Stop Server Manager and all services.</td>
</tr>
<tr>
<td>Update IP Configuration</td>
<td>Change IP addresses.</td>
</tr>
<tr>
<td>Update IP Configuration</td>
<td>Display the current server status.</td>
</tr>
</tbody>
</table>

These tasks are described in detail in the procedures where they are used.

- Server Info: Displays the state of the grid node selected in the Servers panel. The status can be one of:

<table>
<thead>
<tr>
<th>Current State</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>The grid node is available for the tasks listed in the Tasks panel.</td>
</tr>
<tr>
<td>Busy</td>
<td>A GDU task is running on this grid node.</td>
</tr>
<tr>
<td>Error</td>
<td>A GDU task has failed.</td>
</tr>
<tr>
<td>Pingable</td>
<td>The grid node is pingable, but cannot be reached because there is a problem with the hostname.</td>
</tr>
<tr>
<td>Reachable</td>
<td>The grid node can be reached, but is not available because the ssh host keys do not match.</td>
</tr>
</tbody>
</table>

- Log Messages: Displays the output of the GDU task executed for the grid node selected in the Servers panel. If you are running multiple GDU tasks in parallel, you can display the output of each task by selecting the appropriate grid node in the Servers panel.

- Actions: The actions are:

<table>
<thead>
<tr>
<th>Action</th>
<th>Select to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Task</td>
<td>Start the procedure selected in the Tasks panel.</td>
</tr>
<tr>
<td>ISO List</td>
<td>List the ISO images available in the /var/local/install directory of the primary Admin Node.</td>
</tr>
<tr>
<td>Quit</td>
<td>Quit GDU.</td>
</tr>
</tbody>
</table>

**Entering commands**

Use the keyboard to enter commands.

<table>
<thead>
<tr>
<th>To</th>
<th>Do</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go from panel to panel</td>
<td>Press Tab.</td>
</tr>
<tr>
<td>Go back from panel to panel</td>
<td>Press Shift Tab.</td>
</tr>
<tr>
<td>To</td>
<td>Do</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Go up and down within a panel</td>
<td>Press <strong>Up Arrow</strong> and <strong>Down Arrow</strong>&lt;br&gt;Press <strong>Page Up</strong> and <strong>Page Down</strong>&lt;br&gt;Press <strong>Home</strong> and <strong>End</strong></td>
</tr>
<tr>
<td>Go right and left within a panel</td>
<td>Press <strong>Left Arrow</strong> and <strong>Right Arrow</strong>.</td>
</tr>
<tr>
<td>Select a task</td>
<td>Press the space bar. X appears next to the selected task.</td>
</tr>
<tr>
<td>Activate a command</td>
<td>Press <strong>Enter</strong>.</td>
</tr>
</tbody>
</table>

**Quitting the Grid Deployment Utility**

If you quit GDU while a task is in progress, GDU pauses until the task completes, and then closes. Some tasks, such as formatting storage volumes on a new Storage Node, can take hours to complete.

**About this task**

Avoid quitting GDU while long-running tasks are in progress. Continue working in another terminal window.

**Steps**

1. Quit GDU. Select **Quit** in the **Actions** panel and then press **Enter**.<br>   When prompted, confirm that you want to quit GDU.
2. Remove the ability to access servers without a server password. Enter: `ssh-add -D`
3. Close the screen session. Enter: `exit`

**Troubleshooting the Grid Deployment Utility**

- **Display problems**
  Under certain circumstances, the GDU console might not display properly.
  
  - If using PuTTY, change the Window Translation setting to Use font encoding.
  - If running GDU locally, do not use screen.

- **Problems with server status**
  When starting GDU, the status update of all servers might hang, or take a long time to complete. After server status is updated, many appear as Unknown or Pingable when it is known that the servers are Available. This typically only occurs occasionally in large systems with many servers. To correct the problem, quit GDU, and restart with the `-k` option. Enter: `gdu-console -k`
Start GDU with the `-k` option bypasses its initial status update on startup. The state of all servers remains Unknown in GDU until you manually update them using the Update Status task.

- Log files
  The GDU logs are located on the primary Admin Node in `/var/local/log/gdu-console.log`.

- Missing tasks
  If you installed your StorageGRID Webscale system using the manual installation procedure, and a GDU task that you must execute is missing from the Tasks panel, check the GDU log to determine the reason. For instance, it is possible that a required ISO image is missing. To list the ISO images currently available in the `/var/local/install` directory, use the ISO List GDU action.

  ![ISO Repository Contents](image)

  The label Missing, required means that the ISO image of the CD required for the installation is not in the `/var/local/install` directory.

  The label Not present means that an ISO image that GDU expected to find is not in the `/var/local/install` directory, but GDU does not know whether this ISO image is actually required.

- Troubleshooting with screen in multi display mode
  The screen program is useful when two or more people need to interact with a shell session simultaneously for troubleshooting purposes. Below is an example of two users connecting to GDU at the same time.

  User 1 creates a named screen session and starts GDU.

  ```
  # screen -S GDU
  # gdu-console
  ```

  User 2 lists the screen sessions and connects without detaching User 1.

  ```
  # screen -ls
  There is a screen on:
      5361.GDU       (Attached)
  1 Socket in /var/run/uscreens/S-root.
  # screen -r -x GDU
  ```

  Now both users are viewing GDU and inputs can come from either user.

### Copying ISO files in a multi-site environment

In a multi-site environment, copy ISO files to the servers in the remote location prior to installing or upgrading the software with GDU. This is an optional, but recommended, step to reduce the number of large files that would otherwise be transferred over a slow WAN link.

**Before you begin**

- ISO image of the StorageGRID Webscale Software Installation CD has been copied to the primary Admin Node using the `load_cds.py` command

- `ssh` access between the primary Admin Node and the servers at the remote location
Steps

1. At the primary Admin Node, access a command shell and log in as root using the password listed in the `Passwords.txt` file.

2. Copy the ISO image of the StorageGRID Webscale Software Installation CD to a server at the remote location. Enter (on one line):

   ```
   scp /var/local/install/StorageGRID_Webscale_iso destination:/var/local/tmp
   ```

   where:
   - `StorageGRID_Webscale_iso` is the name of the StorageGRID Webscale Software `.iso` file.
   - `destination` is the hostname or IP address of the first server at the remote location.

3. Log in to the server at the remote site where you copied the ISO files. Enter: `ssh destination` When prompted, enter the password for the remote server listed in the `Passwords.txt` file.

4. Change to the `/var/local/tmp` directory. Enter: `cd /var/local/tmp`

5. Load the ISOs using the `load_cds.py` script. Enter:

   ```
   load_cds.py StorageGRID_Webscale_iso
   ```

   where `StorageGRID_Webscale_iso` is the name of the StorageGRID Webscale Software `.iso` file.

6. Empty the temporary directory. Enter: `rm -r /var/local/tmp/*`

7. Copy ISOs from the first server at the remote location to the remaining servers at the remote location. For each remaining server:

   a. Copy the required ISO files to the server. Enter:

      ```
      scp /var/local/install/* next_server:/var/local/tmp
      ```

      where `next_server` is the hostname or IP address of the next server at the remote site.
b. Log in to the next server at the remote site where you copied the ISO files. Enter: `ssh next_server`
   When prompted, enter the password for the remote server listed in the `Passwords.txt` file.

c. Change to the `/var/local/tmp` directory. Enter: `cd /var/local/tmp`

d. Load the ISOs using the `load_cds.py` script. Enter:

   `load_cds.py StorageGRID_Webscale_iso`
   where `StorageGRID_Webscale_iso` is the name of the StorageGRID Webscale Software .iso file.

e. Empty the temporary directory. Enter: `rm -r /var/local/tmp/*`

f. End the ssh session. Enter: `exit`

g. Repeat from step a for each server at the remote site.

8. End the ssh session on the remote server. Enter: `exit`

9. Log out of the primary Admin Node. Enter: `exit`

About `load_cds.py`

The `load_cds.py` command accepts two different inputs: physical installation CDs or ISO images of the installation CDs stored in a directory on the primary Admin Node.

You can run the `load_cds.py` script as many times as you need. If you insert the same CD twice, no new ISO is created. The existing ISO will not be overwritten.

If the `load_cds.py` script fails because you inserted a CD unrecognized by the script, eject the CD and continue with the correct CD (you do not have to start over from the first CD you loaded).
Provisioning

Provisioning is the process of generating the set of configuration files required to install or expand your StorageGRID Webscale system. This collection of files is known as the GPT (Grid Provisioning Tool) repository, which includes the Software Activation and Integration Data (SAID) package.

Manually exporting a provisioned grid specification file

If you want to make changes to the StorageGRID Webscale system, you need to export the current grid specification file from the system.

**Before you begin**

- Passwords.txt file
- An SCP tool, such as WinSCP (available at [winscp.net/eng/download.php](http://winscp.net/eng/download.php)), to transfer files to and from the primary Admin Node
- Service laptop

**About this task**

*Note:* This procedure is included in event that you cannot download the provisioning backup from the NMS MI. You should use the NMS MI to access the current provisioned grid specification file whenever possible.

The following procedure steps you through the process of copying the current grid specification file locally on the primary Admin Node, and then transferring it to the service laptop where it can be opened and edited in the StorageGRID Webscale Grid Designer.

**Steps**

1. From the service laptop, log in to the primary Admin Nodes as root using the password listed in the Passwords.txt file.

2. Create a directory to hold the provisioned grid specification file. Enter: `mkdir -p /var/local/provision`

3. Copy the provisioned grid specification file to the directory. Enter: `copy-grid-spec /var/local/provision`

   You are asked for the password listed in the Passwords.txt file. Enter the password.

   The provisioned grid specification file is copied to the `/var/local/provision` directory created in step 2.

4. Use an SCP tool, such as WinSCP, to copy the `GIDGrid_ID_REVrevision_number_GSPEC.xml` file from the Admin Node to your service laptop.

5. Log out. Enter: `exit`

**Related tasks**

*Viewing the provisioned grid specification file in the NMS MI* on page 230
Manually provisioning the StorageGRID Webscale system

Use this procedure to manually implement the changes made to the provisioned grid specification file. The provisioning script imports the updated grid specification file into the StorageGRID Webscale system and generates any grid tasks required to complete the implementation of the changes.

Before you begin

- Grid specification file.
- `Passwords.txt` file
- Provisioning passphrase
- An SCP tool, such as WinSCP, on the service laptop to transfer files to and from the primary Admin Node.
- Service laptop

About this task

**Note:** This procedure is included in the event that your StorageGRID Webscale system cannot be provisioned automatically as part of an expansion or maintenance procedure run from the NMS MI. Provisioning is typically run automatically as part of the expansion and decommissioning procedures in the NMS MI.

Steps

1. Use an SCP tool, such as WinSCP, to transfer the grid specification file you want to provision from the service laptop to the `/var/local/provision` folder on the primary Admin Node.
2. At the primary Admin Node, access a command shell and log in as root using the password listed in the `Passwords.txt` file.
3. Verify that the grid specification file you want to provision is the only grid specification file located in the `/var/local/provision` directory. Delete any old grid specification files in the directory.
   **Note:** The `/var/local/provision` directory must only contain the grid specification file being provisioned. Otherwise, provisioning will fail.
4. Provision the StorageGRID Webscale system. Enter: `provision /var/local/provision`
5. When prompted, enter the provisioning passphrase.
   When the process completes successfully, a “Provisioning complete” is displayed. If provisioning ends with an error message, see *Troubleshooting provisioning* on page 226.
6. Back up the provisioning data in the `/var/local/provision` directory to two safe and secure locations. These copies can be used to restore the StorageGRID Webscale system in the case of an emergency or during an expansion or maintenance procedure.
   Copy the contents of the `/var/local/provision` directory to the service laptop (using an SCP tool, such as WinSCP) and then to two safe and secure locations for backup.
   **Warning:** Store copies of the `/var/local/provision` directory in at least two separate and secure locations. The `/var/local/provision` directory contains a copy of encryption keys.
and passwords that can be used to obtain data from your StorageGRID Webscale system. The Provisioning directory is also required to recover from a primary Admin Node failure.

After you finish
The contents of the Provisioning directory are used during expansion and maintenance of the StorageGRID Webscale system when a new SAID package must be generated.

Related concepts
- Preserving copies of the provisioning data on page 226

Related tasks
- Manually exporting a provisioned grid specification file on page 222

Changing the provisioning passphrase
Use this procedure to update the provisioning passphrase. The provisioning passphrase is used to encrypt the GPT repository. It is created when the StorageGRID Webscale system is first installed and is required for expansions and maintenance procedures.

Before you begin
- Passwords.txt file
- Current provisioning passphrase
- New provisioning passphrase
- An SCP tool, such as WinSCP, on the service laptop to transfer files to and from the primary Admin Node.
- Service laptop

About this task
Warning: The provisioning passphrase is required for many installation and maintenance procedures. The provisioning passphrase is not listed in the Passwords.txt file. Make sure that it is documented and kept in a safe and secure location.

Steps
1. From the service laptop, log in to the primary Admin Node as root using the password listed in the Passwords.txt file.
2. Change the passphrase and write the updated GPT repository to the specified directory. Enter: change-repository-password path
   where path is the path to the directory on the server where you want to store a copy of the updated GPT repository.
3. When prompted, enter the current passphrase.
4. When prompted, enter the new passphrase. It must be at least six characters.
5. When prompted, enter the new passphrase again.
   The passphrase of the GPT repository is changed to the new value, and an updated copy of the repository that uses this password is saved in the path directory.
**Warning:** Store the provisioning passphrase in a secure location. It is required for most installation, expansion, and maintenance procedures.

Back up the provisioning files to another directory on the primary Admin Node. Create the backup directory and then back up the provisioning files to the new directory. Enter:

```
mkdir -p /var/local/backup
backup-repository /var/local/backup
```

This backup copy can be used to restore the StorageGRID Webscale system in the event of a hardware failure, or to perform expansion and maintenance procedures. When prompted, enter the new provisioning passphrase.

6. Log out. Enter: `exit`

7. Use an SCP tool, such as WinSCP, to transfer the provisioning files from the `/var/local/backup` folder on the primary Admin Node to the service laptop.

8. Store the contents of the Provisioning directory (found at `/var/local/gpt-data/`) and the Backup Provisioning directories (`/var/local/backup`) separately in a safe place.

**Warning:** Store copies of the backup directory in two safe and secure locations. The directory contains encryption keys and passwords that can be used to obtain data from the system, and is required to recover from a primary Admin Node failure.

**Related concepts**

*Preserving copies of the provisioning data* on page 226

---

**Provisioning command reference**

The following commands are run using a Telnet/SSH application, such as PuTTY, to connect to the primary Admin Node to either update or copy grid provisioning data:

- `provision path`
- `change-repository-password path`
- `copy-grid-spec path`
- `backup-repository path`
- `restore-repository path`

The procedures in this appendix specify `/var/local/provisioning` as the `path` value. This is the recommended location, but you can specify a different path on the Admin Node and then transfer the generated files to the required location.

Be aware of the following when you run provisioning commands:

- The size of the GPT repository increases every time the provision command is run because a new revision is created and is added to the GPT repository.
- Preserving copies of the GPT repository is critical to the continued operation of the StorageGRID Webscale system.

**Related concepts**

*Preserving copies of the provisioning data* on page 226
Preserving copies of the provisioning data

Preserving the GPT repository is critical to the continued operation of StorageGRID Webscale software. The contents of the GPT repository are required when running expansion or maintenance procedures. The GPT repository is also required to restore the primary Admin Node, should it fail and require replacement.

Each time you run one of the commands that update or copy grid provisioning data, you must back up the provisioning data to two secure locations, preferably in two distinct physical locations. For example, upload the provisioning data to a network location that is secure and regularly backed up and to an external cloud data storage location. The provisioning data includes encryption keys and passwords that can be used to obtain data from the StorageGRID Webscale system.

**Warning:** Always store two copies of the GPT repository in two separate and secure locations. The GPT repository is essential to the continued operation of the StorageGRID Webscale system, and to recover from a failed primary Admin Node.

It is possible to back up provisioning data directly to the StorageGRID Webscale system. If you store a copy to the StorageGRID Webscale system, you must always store a second copy in another location outside of the StorageGRID Webscale system. The SAID package includes a two-part encryption key that permits you to recover data from grid nodes in the event of a catastrophic system failure. If the only copies of these keys are in the StorageGRID Webscale system, it is not possible to recover data after such a failure.

Troubleshooting provisioning

In case of provisioning errors, follow these guidelines.
**Provision command fails**

If provisioning fails because the grid specification file is incorrect, the file `provision-fail.log` is created in the `/var/local/provision` directory. This file contains the error message that the provisioning software displayed before terminating.

If the provisioning program terminates abnormally (crash), two identical log files are saved to the `/var/local/provision` directory on the primary Admin Node.

- `provision-fail.log`
- `provision-crash-grid_info.log`

where `grid_info` includes the grid ID, the grid revision being created and a timestamp.

If the `provision-fail.log` file is the only file created, fix the grid specification file by updating it with Grid Designer and then run provisioning again. If the `provision-crash-grid_info.log` file is created, contact Support.

If provisioning ends with an error, no information is saved and the `remove-revision` command does not need to be run.

**About the Software Activation and Integration Data package**

The Software Activation and Integration Data (SAID) package contains site-specific files for the StorageGRID Webscale system. It is generated during the provisioning process as a zip file and is named using the following naming convention: `GIDgrid_ID_REVrevision_number_SAID.zip`

The SAID package contains the following items:

**Table 8: SAID Package contents**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doc</td>
<td>Directory containing HTML files used to confirm provisioning.</td>
</tr>
<tr>
<td>Grid_Activation</td>
<td>Directory containing activation files, one for each server. Activation files are named <code>servername-autoinst.xml</code>. Activation files are keyed to work with the hardware used for the StorageGRID Webscale system and the version of StorageGRID Webscale software.</td>
</tr>
<tr>
<td>Grid_Tasks</td>
<td>Directory containing files created by some types of changes to the grid specification file, such as expansion. Grid tasks are used to trigger various actions that implement changes to the StorageGRID Webscale system.</td>
</tr>
<tr>
<td>Configuration.txt</td>
<td>File listing system-wide configuration and integration data generated during the provisioning process.</td>
</tr>
<tr>
<td>Grid specification file</td>
<td>XML file that encapsulates the topological design of the StorageGRID Webscale system. File name is <code>GIDgrid_ID_REVrevision_number_GSPEC.zip</code></td>
</tr>
<tr>
<td>Passwords.txt</td>
<td>File listing passwords used to access the StorageGRID Webscale system.</td>
</tr>
</tbody>
</table>
Viewing grid configuration files

You can confirm the configuration of your StorageGRID Webscale system by reviewing the SAID package's Doc/Index.html file.

Open the Doc/Index.html file in a supported browser and review its contents to confirm that the StorageGRID Webscale system is configured correctly.

<table>
<thead>
<tr>
<th>Grid Services</th>
<th>Network</th>
<th>Groups</th>
<th>Storage</th>
<th>NTP</th>
</tr>
</thead>
</table>

Grid Wide Settings

<table>
<thead>
<tr>
<th>Grid ID</th>
<th>401713</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grid Description</td>
<td>StorageGRID Webscale Deployment</td>
</tr>
<tr>
<td>Software Suite Version</td>
<td>10.0</td>
</tr>
<tr>
<td>Service Pack Required</td>
<td>none</td>
</tr>
<tr>
<td>Metadata Replication</td>
<td>enabled</td>
</tr>
</tbody>
</table>

Grid Options:

<table>
<thead>
<tr>
<th>Servers Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>DC1-A0M</td>
</tr>
<tr>
<td>DC1-S1</td>
</tr>
<tr>
<td>DC1-S2</td>
</tr>
<tr>
<td>DC1-S3</td>
</tr>
</tbody>
</table>

The following browsers are supported:

- Google Chrome 43
- Microsoft Internet Explorer 11.0
- Mozilla Firefox 38.0.5

Configuring Chrome to open the Doc/Index.html file

By default, the Chrome web browser is configured with security features, which render it incapable of opening the Doc/Index.html file. In order to open the Doc/Index.html file in Chrome, configuration changes must be made.

**Steps**

1. In Windows, go to **Start > All Programs > Accessories > Run**.
   
   The path to the Run dialog box may be different depending on the version of Windows used.
   
   The Run dialog box opens.

2. In the **Run** dialog box, click **Browse**.
   
   The Browse dialog box opens.
3. In the **Browse** dialog box, navigate to the Google directory, select the Chrome application and then click **Open**.

   The Run dialog box updates to include the path to Chrome.

   ![Run dialog box](image)

4. In the **Run** dialog box, add the following to the end of the path to Chrome (after the quotation mark):

   ```
   --allow-file-access-from-files
   or
   --disable-web-security
   ```

5. Click **OK**.

   Chrome starts and is now able to open the `Doc/Index.html` file. Changes are not saved when you close Chrome.

---

**Grid specification files**

The grid specification file is an XML file that encapsulates the configuration information needed to install, expand, and maintain a StorageGRID Webscale system. The file includes topology, servers, options, and networking details for the StorageGRID Webscale system.

Grid specification files are generated by Grid Designer and then used to provision the StorageGRID Webscale system. Provisioning the StorageGRID Webscale system changes the grid specification file such that any subsequent changes made to the StorageGRID Webscale system (maintenance procedure or expansion) require the use of the provisioned grid specification file.

For more information about Grid Designer, see the *Grid Designer User Guide*.

**Related tasks**

*Manually exporting a provisioned grid specification file* on page 222

---

**Naming convention**

Grid specification files use the naming convention

`GIDgrid_ID_REVrevision_number_GSPEC.xml`, where `grid_ID` refers to the StorageGRID Webscale system’s unique identifier and `revision_number` refers to the revision number of the grid specification file, for example, `GID1234_REV1_GSPEC.xml`.

The revision number is increased by 1 each time the grid specification file is modified; for example to add grid nodes or change IP addresses. For the initial installation of the StorageGRID Webscale system, the revision number must be 1 (REV1). Any other revision number will cause provisioning to fail.
Viewing the provisioned grid specification file in the NMS MI

You can view the contents of the provisioned grid specification file through the NMS MI. You cannot, however, open and update this version in Grid Designer.

About this task

To obtain a copy of the provisioned grid specification file that you can update with Grid Designer, you must export the provisioned grid specification file.

Steps

1. Go to Grid Management > Grid Configuration > Configuration.

2. In the Main page, click Export at the bottom of the page, to the right of the Grid Specification File label.

   A new browser window opens, showing the grid specification file in raw XML.

Related tasks

Manually exporting a provisioned grid specification file on page 222
Downloading the provisioned grid specification file

Before you edit the grid specification file, you should obtain a copy of the provisioned grid specification file from the StorageGRID Webscale system. Then, you can open the latest grid specification file in Grid Designer to edit it.

Before you begin
Provisioning passphrase

About this task
To expand a StorageGRID Webscale deployment or perform certain maintenance procedures, you must use the latest version of the provisioned grid specification file. Obtain this file by downloading the Provisioning Backup archive file (.zip) from the NMS MI.

Steps
1. Log in to the NMS MI using the Admin or Vendor account.
2. Select Grid Management > Grid Maintenance > Grid Provisioning Backup.
3. Enter the provisioning passphrase and click Start Download.
   The download starts immediately. Depending on your browser version, you may be prompted to select the location to save the file, or it may be saved automatically to the default download location.
4. Extract the saved grid specification file (GID<Grid_ID>_REV1_GSPEC.xml) from the gpt-repository.zip file.

Related tasks
Changing the name of an Admin Node on page 148
Changing IP addresses on page 152
Updating the Network Time Protocol external sources list on page 158
Manually exporting a provisioned grid specification file on page 222
Adding, removing, or updating Network Time Protocol sources on page 158
Manually provisioning the StorageGRID Webscale system on page 223
Glossary

ACL
Access control list. Specifies what users or groups of users are allowed to access an object and what operations are permitted, for example, read, write, and execute.

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
Application Programming Interface. A set of commands and functions, and their related syntax, that enable software to use the functions provided by another piece of software.

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. (Containers are sometimes used when interacting with the StorageGRID Webscale system through the StorageGRID API).

audit message
Information about an event occurring in the StorageGRID Webscale system that is captured and logged to a file.

AutoYaST
An automated version of the Linux installation and configuration tool YaST (Yet another Setup Tool), which is included as part of the SUSE Linux distribution.

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 only process basic (low order) ASCII text excluding control characters. See RFC 2045 for more details.

binding
The persistent assignment of a service (for example, an AMS service or SSM service) to the NMS service. This assignment is based on StorageGRID Webscale topology. See also, Admin Node.

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.

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
Within the StorageGRID Webscale system, there are several different uses (and technologies) for the term container:
• SGAPI: A container is a data structure used by the internals of StorageGRID Webscale software. In the StorageGRID API, an XML representation of a container is used to define queries or audit messages submitted using the POST command. Containers are used for information that has hierarchical relationships between components. The lowest-level component of a container is an atom. Containers can contain 0 to N atoms, and 0 to N other containers.

• CDMI and Swift: Analogous to a file system directory, a container object allows access to “child” data objects.

• Segmented objects: When an object is split into segments, a container is created that lists the header information for all segments of the split object. This is then 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.

**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 maximize the security of each grid node.

**fibre channel**
A networking technology primarily used for storage.

**GDU**
Grid Deployment Utility. A StorageGRID Webscale software utility used to facilitate the installation of software on all grid nodes. GDU is installed and available on the primary Admin Node.

**GPT**
Grid Provisioning Tool. A software tool included with StorageGRID Webscale software that permits you to provision a StorageGRID Webscale system for installation, maintenance, or expansion. GPT creates and maintains an encrypted repository of information about the system that is required to maintain the StorageGRID Webscale system and recover failed grid nodes.

**Grid ID signed text block**
A BASE64 encoded block of cryptographically signed data that contains the grid ID which must match the grid ID *(gid)* element in the grid specification file. 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 specification file
An XML file that provides a complete technical description of a specific StorageGRID Webscale deployment. It describes the system’s topology and specifies the hardware, options, grid nodes, network settings, and time synchronization for the deployment.

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.

HTTP

HTTPS
Hyper-Text Transfer Protocol, Secure. URIs that include HTTPS indicate that the transaction must use HTTP with an additional encryption/authentication layer and often, a different default port number. The encryption layer is usually provided by SSL or TLS. HTTPS is widely used on the internet for secure communications.

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 such factors. See also, Admin Node and storage pool.

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.

metadata
Information related to or describing an object stored in the StorageGRID Webscale system; for example, ingest time.

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” (implying that it is instantly available like spinning disk) nor “offline” (which could 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 necessarily 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, **NMS MI** and **Admin Node**.

**NMS MI**

NMS Management Interface. The web-based interface for managing and monitoring the StorageGRID Webscale system provided by the NMS software component. See also, **NMS service**.

**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 storage**

Object storage is an approach where stored data is accessed by unique identifiers rather than 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 typically act on entire objects as opposed to reading and writing bytes as is commonly done with files, and is typically 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.

**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**.

**OID**

Object Identifier. The unique identifier of an object.

**primary Admin Node**

Admin Node that hosts the CMN service. There is one per StorageGRID Webscale system. See also, **Admin Node**.

**provisioning**

The process of generating a new or updated SAID package and GPT repository. See also, **grid specification file** and **SAID**.
purge
The act of permanently removing an object from the StorageGRID Webscale system.

quorum
A simple majority: 50% + 1. Some system functionality requires a quorum of the total number of a particular service type.

SAID
Software Activation and Integration Data. Generated during provisioning, the SAID package contains site-specific files and software needed to install a StorageGRID Webscale system.

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. May also refer to a virtual machine.

Server Manager
Application that runs on all grid nodes, supervises the starting and stopping of services, and monitors all services on the grid node.

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.

SGAPI
StorageGRID Application Programming Interface. A set of commands and functions, and their related syntax, that provides client applications with the ability to connect directly to an Storage Node or Archive Node.

SLES
SUSE Linux Enterprise Server. A commercial distribution of the SUSE Linux operating system, used with the 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 execute commands over an authenticated and encrypted channel.

SSM
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.
SSL
Secure Socket Layer. The original cryptographic protocol used to enable secure communications over the internet. See also, TLS.

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.

StorageGRID Webscale
A registered trademark of NetApp Inc. for their object storage grid architecture and software system.

StorageGRID API
See SGAPI

storage volume
See object store

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.

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.

Tivoli Storage Manager
IBM storage middleware product that manages storage and retrieval of data from removable storage resources.

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 which 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 amongst several virtual servers.

**XFS**
A scalable, high performance journaled file system originally developed by Silicon Graphics.

**WAN**
Wide Area Network. A network of interconnected computers that covers a large geographic area such as a country.

**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 © 1994–2016 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

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, 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 at http://www.netapp.com/us/legal/netapptmlist.aspx.
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 to 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
/var/local/install directory 216, 218

A
aborting grid tasks
procedure for 193
access control policies
description of 19
overview of 19
supported 19
accounts permissions 180
accounts, group
changing 185
creating 185
deleting 185, 186
accounts, user
adding 183
creating 183
deleting 184
activation files 227
Active Directory
adding users or groups to audit share 171
audit clients 168
changing audit client share user or group name 174
configuring audit clients 168
removing users from audit share 173
active policy 63
ADC
link costs 159
ADC service 111
add-audit-share command, in config_cifs.rb 166, 168
add-ip-to-share command, in config_nfs.rb 176
add-user-to-share command 171
add-user-to-share command in config_cifs.rb 171
adding Storage Nodes 118
storage volumes 118
Admin Node
change name, in NMS MI 148
changing IP address 152
defined 145
primary
redundancy 146
primary Admin Node
change private key password 162
passwordless access 162
removing ssh private key 163
administration guide 10
Administrative Domain Controller
See ADC
AES-128 120
AES-256 120
alarm
acknowledgments 146
alarm triggering
elements 44
alarms
by code
SAVP Total Usable Space (Percent) 114
SSTS Storage Status 114
class overrides 46
clearing triggered alarms 53
creating custom alarms 47
creating global custom alarms 49
custom 43
custom notification migration 201
default 42
disable default alarm 51
disabling 51
disabling default alarms, grid wide 52
disabling global custom alarms, grid wide 53
disabling global custom alarms, service level 52
global custom 43
monitoring 43
new services 47
of same severity 45
overriding higher priority alarm 46
severity changes 46
table, displayed in 51
triggering evaluation order 43
triggering logic 43
types 42
All Storage Nodes storage pool 87
AMS
system events 32
API Gateway Node
decommissioning grid task 187
description of 131
appliance
viewing events 61
viewing Storage Nodes 58
ARC
archive read-only on startup 143
archive store state 143
configuration
Target component 137
optimizing for Tivoli Storage Manager 139
optimizing performance, TSM sessions 139
resetting store failure count 143, 144
retrieve component 142
Tivoli Storage Manager
unavailable 140
ARC service 132
archive
read-only on startup 143
retrieve state 142
store set 143, 144
Archive Node
configure replication settings 141
configure target 133
configuring cloud connections 134
configuring S3 connections 134
description 132
destination 133
optimizing for Tivoli Storage Manager middleware
setting custom alarms
target
Archive Nodes
capacity, full
optimizing for Tivoli Storage Manager middleware
attrDownPurge
attrDownSamp1
attrDownSamp2
attributes
by code
ROMK Hard Read-Only Watermark
SSCR Storage Status - Current
STAS Total Usable Space
VHWM Storage Volume Soft Read-Only Watermark
VROM Storage Volume Hard Read-Only Watermark
by name
Hard Read-Only Watermark
SSCR Storage Status - Current
Storage Volume Soft Read-Only Watermark
VHWM
STAS Total Usable Space
audit client configuration
CIFS, Active Directory
CIFS, Windows Workgroup
NFS
AutoSupport
described
disabling
preferred sender
sending
triggering
Available server state, in GDU
background verification
adaptive
configuring
high verification priority
LDR
priority
reset corrupt objects count
verification priority
Baseline 2 Copy Rule policy
bundle
import grid task
Busy state, in GDU

capacity
Archive Node
of storage
 cassandra
CCLE grid task
Clean Up Unused Cassandra Keys grid task
nodetool repair

CBID
defined
obtain
CDMI
certificates
change-grid-ip.rb
change-repository-password command
CIFS
audit directory, AD
configuring audit clients
CIFS audit share
changing group name
changing user name
removing users
NFS audit share
adding clients
changing client IP address
CMN service
defined
CMS
metadata
CMS service
command shell
accessing
logging in
logging out
commands
load_cds.py
comments
how to send feedback about documentation
compression
FSG profiles
lossless
Configuration.txt file
configuring
Archive Node
notifications
configuring LDAP
notifications
content block identifier
See CBID
content deletion
client application
scenarios, StorageGRID API
content placement instructions
content protection
configuration settings
delete permission in HTTP profile
Disable Client Delete
ILM rules
how to send comments about documentation 242
file system
  UUID 123
files
  files 218
force-stop 210
foreground verification
  missing replicated object data 129
FSG
  object segmentation 125
FSG profiles
  stored object compression 123

G
GDCM grid task 187
GDU
  Actions panel 216
  console 215
defined 215
  entering commands 217
  ISOs 218
  Log Messages panel 216
  missing task 218
  navigation 216
  PuTTY, with 215, 218
  quit, how to 218
  screen, with 215, 218
  Server Info panel 216
  Servers panel 216
  ssh access 162
  start command 215
  Tasks panel 216
troubleshooting 218
GDU tasks
  Enable Services 216
  Install Software 216
  Reboot Server 216
  Remount Storage 216
  Start Services 216
  Stop Services 216
  Update IP Configuration 216
  Update Status 216
gdu-console command 215
gdu-console.log 218
global custom alarms
  creating 49
  disabling 52, 53
  triggering logic 43
GPT repository 224
grid capacity
data migration 197
grid configuration
  network transfer encryption 160
tuning for object size 124
grid management permissions 180
Grid Management tree 11
grid network IP addresses 151
grid node
  IP address 151
grid specification file
downloading 231
  export 222, 230
  naming convention 229
  structure 229
  view 230
  view in NMS MI 230
grid tasks
  aborting 193, 195
  active 188
  API Gateway Node decommissioning 187
  BDLI 187
  bundle import 187
cancelling 192
  CCLE 187
  charting 190
description 187
  expansion 187
  GDCM 187
  GEXP 187
  Grid Expansion 187
  grid performance 187
  grid tasks
    VFGV 187
  historical 188
  ILM evaluation (Volume Lost) 187
  ILM evaluation grid tasks 187
  ILME 187
  LDR foreground verification 129
  LDR Foreground Verification 187
  managing errors 195
  monitoring 188
  operations 187
  pausing 192
  pending 188
  progress 188
  reasons for failure 194
  recovery 187
  removing from the Historical table 193
  resuming 192
  running 191
  status 188
  Storage Node decommissioning 187
task signed text block 195
troubleshooting 193
troubleshooting retries 194
Grid Topology tree 11
gridstat 211
group accounts
  Account Management 180
  changing 185
  creating 185
deleting 186
  Grid Options 180
  grid tasks 180
  HTTP Management 180
  ILM Management 180
  NMS Management 180
  node/service/component 180
  permissions 180
  updating 185
group policies
  editing for S3 tenant accounts 18
  editing for Swift tenant accounts 25
groups, in ILM policies 69
H hardware viewing events in the NMS MI 61
hashing, stored object 121
health check timeout LDR 115
historical ILM policies 100
Historical table status of failed grid tasks 194
HSTE HTTP/CDMI State 115
HTTP auto-start 115
profiles 82
HTTP DELETE operations 82
HTTP protocol handler version, in ILM rules 72
HTTP/CDMI State, set 115
I identity federation configuring OpenLDAP for 27
synchronization of LDAP server 28
ILM active rules 67
build policy 84
built-in rules 67
content age 79
content placement instructions 77
content protection 81, 82
default rule 63
define 66
dual commit 80
evaluation logic 63
filters 72, 91
groups 69
historical policies 100
historical rules 67
ILM re-evaluation 102
Last Access Time 76, 91
Make 2 Copies rule 67
metadata 72
object deletion 80
object identifier 96
Object not referenced by API 80
policies activate 95
apply, existing content 102
build 84
configure 94
historical policies 100
rules 80
sample policies 103
unavailable resources 78
version numbers 66
view historical 100
viewing activity queue 100
policy updates 65
reference time ingest time 76, 91
Last Access Time 91
retention diagram 79
rules active 67
alternate location 78
built-in 67
content placement instructions 77
copy 99
create 91
delete 99
examples 105
historical 67
Last Access Time 91
Last Access Time metadata 76
Make 2 Copies rule 87
modify 98, 99
ordering 94
reference time 76
saved 67
types 67
unavailable resources 78
sample policies data center 104
DC 104
DC + DC + archive 104
DC + DC and archive 104
sample rules archive erasure coded object data 107
delete based on content age 105
two copies in two locations 106
saved rules 67
storage 69, 84
storage grade assign to LDR 86
configuring 69, 84
storage locations 69
storage pools built-in 87
configure 87
guidelines 87
view existing 89
tags 72, 75
temporary location 78
time values 76
version numbers 68
ILM activity queue
setting alarms 101
ILM criteria evaluation 72
ILM policy viewing activity queue 100
ILM rules archival media 132
examples 105
filtering 75
last access time 91
Index.html file 228
information how to send feedback about improving
documentation 242
ingest time in ILM rules 72
INID, in ILM rules 72
Install Software GDU task 216
internal IP addresses
IPv6 support 163
IP address
change 152
grid network 151
supplementary network 151
view 151
IPv4 163
IPv6
external IP addresses 163
internal IP addresses 163
NTP 163
ISO List action, in GDU 216
ISOs
copy to another site 219
missing, in GDU 218
required, missing, in GDU 218

J
join-domain command, in config_cifs.rb 168

L
large object optimization
object segmentation 125
last access time
ILM rules 72, 91
Last Access Time 77, 91
Last Access Time, disable 77
Last Access Time, enable 77
LATM, in ILM rules 72
LDAP
configuring 26
disabling 28
LDAP server
forcing synchronization of 28
LDR
assign storage grade 86
background verification 115
configuration
Storage component 115
content balancing 112
corrupt objects 115
encryption 115, 120
full 127
health check timeout 115
HTTP/CDMI State 115
monitor available space 113
object mapping 112
object segmentation 125
object stores 112
replication 115
reset lost copies count, erasure coding 115
reset read failures, erasure coding 115
reset write failures, erasure coding 115
service 109
storage grade 86
storage state-desired 115
verification 127
volume ID 112
LDR service 109
LDRBackground verification 127
link costs
default values 159
update 160
lists, mailing
suppressing email notifications from 39
Load Configuration GDU task 216
load_cds.py command 221
Local Distribution Router service
See LDR service
log files
provisioning 227
servermanager.log 213
logging in
NMS MI 13
logging out
NMS MI 15

M
mail server 34
mailing lists
suppressing email notifications from 39
maintenance permissions 180
Make 2 Copies rule, ILM 63, 67, 87
management API
overview 29
management class, Tivoli Storage Manager 133
Management Interface
viewing appliance hardware events in 61
metadata
CDMI 75
in ILM rules 72
S3 75
SGAPI 72
Swift 75
tags 72, 75
MIB
OID values 157
SNMP 157
missing ISOs, in GDU 218
modifying DNS configuration
for single grid node 155
monitoring
storage 119
system capacity
system-wide 119
Monitoring
storage capacity
per Storage Node 119
mysql
Server Manager
dependencies 211

N
net monitor 211
NetBIOS name
file share configuration 168
network connections
viewing for appliance in the NMS MI 58
network transfer encryption
disable 160
enable 160
NFS audit share
  removing clients 177
  verifying integration 177

NFS share configuration
  add a client to an audit share 176
  changing client IP address 178
  configure the audit client 174
  remove a client from the audit share 177

NMS entities
  changing name 149
  device model ID 148
  device model version 148
  language 148
  name, in NMS MI 148
  OID 148
  settings 148

NMS management
  change Admin Node name 148
  customizing alarms 41
  e-mail notifications 32
  group accounts 180
  NMS MI timeout 15

NMS Management Interface
  viewing appliance Storage Node 58

NMS MI
  connecting to interface 13
  Grid Topology tree 11
  log in 13
  log out 15
  timeout period 15

NMS MI timeout period, change 15
NMS service
  defined 145

nodes
  viewing appliance in NMS Management Interface 58

nodetool repair 112

notifications
  configuring 33
  notifications, email suppress for mailing lists 39

NTP
  add NTP source 158
  IPv6 support 163
  remove NTP source 158

Server Manager
  dependencies 211
  SNTP, contrasted with 158
  update configuration 157
  update external time source 158
  update NTP source 158
  update primaries 158
  update secondaries 158

P
  passwordless access, ssh 162
  passwords
    Server Manager 206
  Passwords.txt 227
  permissions
    Account Management 180
    accounts 180
    alarm acknowledgment 180
    grid management 180
    Grid Options 180
    grid tasks 180
    HTTP Management 180
    ILM Management 180
    maintenance 180
    NMS Management 180
    Node/Service/Component 180
  PHTP, in ILM rules 72
  Pingable server state, in GDU 216
  policies
    activate 94
    active policy 63
    baseline 63
    configure 94
    migrated data 197
    verify 96
  power down server 210
  preferred sender, notifications 40
  preserved content 80

primary Admin Node
  change private key password 162
  passwordless access 162
  removing private key 163
  SSH access 161

private key password, change 162

O
  object count 110
  object data
    corrupt 126
    missing 126, 128
    verify 128
    verify integrity 126
  object deletion
    ILM 80

object lookup
  in the NMS MI 96

object metadata 111

Object not referenced by API 80

object segmentation
  disable 125
  FSG 125
  how it works 125
  retrieval 125
  StorageGRID API 125

object size
  FSG
    impact on 124
    recommended settings 124

object store
  volume ID 112

object stores 112

OID
  defined 148
  values 157

OpenLDAP
  configuration guidelines for 27
  optimizing performance, middleware sessions
    Tivoli Storage Manager 133
    ORLM 96
protected content 80
provision command 223
provision-crash-.log file 227
provision-fail.log file 227
provisioning
  command reference 225
defined 222
  GPT repository 224
  log files 227
  passphrase, change 223
  Preserving copies of the data 226
  procedure 223
  troubleshooting 226
purge
  ILM purge 80
PuTTY, with GDU 215, 218
Q
Quit action, in GDU 216
quit, how to 218
R
RAM usage 57
Reachable server state, in GDU 216
reader.rb 207
reboot
  server 210
  Server Manager 210
Reboot Server GDU task 216
reference time
  ILM 76
remote server
  access 161
  connect to 161
Remount Storage task, in GDU 216
remove-ip-from-share command, in config_nfs.rb 177
remove-user-from-share command, in config_cifs.rb 173
removing tenant accounts 26
required missing ISOS, in GDU 218
reset counters
  CDMI counts 115
  HTTP counts 115
  inbound replication failure count 115
  outbound replication failure count 115
  SSM events 57
resetting corrupt objects count 115
resetting lost copies count, erasure coding 115
resetting read failure count 115
resetting writes failure count 115
retention diagram 79
retries, grid task
  troubleshooting 194
rules
  default 63
  Make 2 Copies rule 63
  ordering 63
S
S3
metadata 75
modify Archive Node settings 135
modifying Cloud Tiering Service 136
modifying settings 135
S3 access keys
  and storage tenant accounts 28
S3 bucket/key
  obtain 96
S3 tenant accounts
  editing group policies 18
  managing 17
SAID package
  Configuration.txt file 227
  Doc directory 227, 228
  Escrow_Keys directory 227
  grid specification file 227
  Grid_Activation directory 227
  Grid_Tasks directory 227
  naming convention 227
  SAID package
    naming convention 227
sample policies 103
SAVP Total Usable Space (Percent)
  alarm 114
screen
  GDU, with 215
  multidisplay mode 218
scripts
  server manager status 207
  servermanager restart 209
  servermanager start 208
  servermanager status 207
  servermanager stop 209
  services monitored 207
  setup_ntp.rb 163
  setup_resolv.rb 163
  version number, display 207
security partition
  determine value 72
  in ILM rules 72
security partitions
  StorageGRID API 124
  segmentation 125
Server Connection Error 33
server identification
  host name 206
  IP address 206
  node type 206
Server Manager
  accessing remotely 207
  capabilities 203
  changing password 206
  command buttons 205
  control buttons 205
  current status 207
  dependencies
    mysql 211
    ntp 211
    services 211
  disabled service status 204
GUI 203
header, status in 204
overview 203
passwords 206
power down server 210
reader.rb 207
remote access 207
restart 205, 209
running time 207
scripts
servermanager restart 205
servermanager stop 205
service, terminate 210
services, restart individual 210
services, restart individual (running) 210
terminate service 210
server identification 206
service states 203
services listing 204
services status 204
services, restart all 209
services, start all 208
services, stop individual 209
shut down 205
start services 204, 208
start, manually 208
stop 205
stop services 205
troubleshooting
error state 213
tomcat 214
Server Status Monitor
See SSM
servermanager.log 213
servers
power down 210
reboot 210
shut down 205
service state notifications 32
services
creating alarms 47
disable global custom alarm 52
disabling default alarms 51
Server Manager
dependencies 211
status, Server Manager 204
stop 205, 209
terminate 210
set-authentication command, in config_cifs.rb 166, 168
setting alarms 101
setting custom Archive Node 144
setup_ntp.rb script 163
severity level notifications 32
SGAPI
metadata 72
share configuration
add-audit-share command 166, 168
add-ip-to-share command 176
add-user-to-share command 166
audit share (CIFS) 166
audit share (NFS) 174
join-domain command 168
NetBIOS name 168
remove-ip-from-share command 177
remove-user-from-share command 173
set-authentication command 166, 168
Simple Storage Service 133
SMTP mail server settings 34
SNMP
agent 156
configure 156
system status 156
SNMP monitoring
configure 156
MIB 156
OID 156
SNMPv2c 156
SNTP 158
source node ID, in ILM rules 72
SPAR
determine value 72
in ILM rules 72
SSCR Storage Status - Current 114
ssh
change password 162
GDU 162
passwordless access 162
private key 162
remove SSH private key 163
removing private key 163
ssh-keygen 162
SSH
add password to SSH private key 161
customize access point 161
passwordless access 161
ssh access password 161
ssh access point 161
SSH Access Password, with GDU 215
ssh private key, removing 163
ssh-add, with GDU 215
SSM
components
events 57
resources 58
timing 58
configuration
Resources component 58
reset event counters 57
services 57
SSTS Storage Status alarm 114
Start Services task, in GDU 216
Start Task action, in GDU 216
STAS Total Usable Space
attribute 113
status
grid tasks 188
of failed grid tasks 194
Stop Services task, in GDU 216
storage
background verification 127
calculate capacity 113
ILM 69, 84
storage capacity
monitoring per Storage Node 119
monitoring system-wide 119
watermarks 114
storage grade
assign to LDR 86
configuring 84
creating a list 85
Storage Node
  background verification 126
  foreground verification 126, 128, 129
  LDR 112
  object mapping 112
  watermarks 114
Storage Node rebuild, optimizing Tivoli Storage Manager 139
Storage Nodes
  viewing appliance in NMS Management Interface 58
storage object compression
  disable 122
storage pools
  configure 87
  erasure coding profiles 78
  ILM 69, 84
  unavailable resources 78
  view existing 89
Storage Status - Current SSCR 114
Storage Status SSTS alarm 114
storage tenant account
  managing federated user S3 credentials for 28
  S3 access keys and 28
StorageGRID API
  file delete 81
  object segmentation 125
  security partitions 124
StorageGRID Webscale system
  defined 10
  storagegrid-status 207
stored object compression
  FSG profiles 123
stored object encryption
  configure 120
stored object hashing
  configure 121
STRO - 9, in ILM rules 72
suggestions
  how to send feedback about documentation 242
  supplementary network IP addresses 151
Swift
  editing tenant account group policies 25
  editing tenant accounts 25
  metadata 75
Swift REST API
  creating tenant accounts 24
Swift tenant accounts
  managing 24
synchronization
  LDAP server and 28
system events 32
system status
  OID 156
  SNMP 156

T
  Telnet/ssh client, with GDU 215, 218
  template 35
tenant accounts
  authenticating with LDAP 26
  creating for S3 17
  creating for Swift 24
  deleting 26
  editing 18
  editing for Swift 25
  managing 17, 24
  removing 26
terminate services 210
test e-mail
  send 38
timeout, NMI MI 15
Tivoli Storage Manager
  ARC 133
  configure 137
  lifecycle and retention rules 133
  management class 133
  middleware 137
Tivoli Storage Manager ARC
  optimizing Archive Node 139, 141
  optimizing performance 139
tomcat
  restart 214
Total Usable Space (Percent) SAVP
  alarm 114
Total Usable Space STAS
  attribute 113
troubleshooting
  GDU 218
  grid task retries 194
  grid tasks 193
  log files 213
  provisioning 226
  Server Manager
    service does not start 213
    service does not start 213
twitter
  how to receive automatic notification of documentation changes 242

U
  unavailable resources, in ILM policies 78
Update IP Configuration task, in GDU 216
Update Status task, in GDU 216
Use font encoding setting in PuTTY, with GDU 218
user accounts
  adding 183
  creating 183
  deleting 184
  modifying 184
  permissions 180
user string, in ILM rules 72
UTF-8 setting in PuTTY, with GDU 215
UUID
  obtain 96

V
  verifying
    CIFS audit integration 174
  version
    reported by Server Manager 204
version information 57
version numbers
  ILM policies 66
  ILM rules 68
viewing
  default alarms 42
volume ID 112

W
watermarks
  view values 114

Windows Time Service 157
WinSCP 222
Workgroup share configuration
  adding users or groups to audit share 171
  audit clients 166
  changing audit client share user or group name 174
  removing user from audit share 173

X
XAID, in ILM rules 72