StorageGRID® Webscale 10.1

Troubleshooting Guide
## Contents

1 **Problem determination** ................................................. 7
   - Overview of problem determination ................................ 7
   - Define the problem .................................................. 8
   - Assess the risk and impact on the system ......................... 9
   - Collect data .......................................................... 10
     - Check connectivity status ....................................... 10
     - Check for alarms ............................................... 10
     - Monitor SSM events .............................................. 11
       - Review SSM events ........................................... 12
       - Create custom syslog events ................................ 12
       - Reset the count of custom events to zero ................. 14
     - Trigger an AutoSupport message .............................. 14
     - Plot trends ....................................................... 15
     - Establish baselines ............................................. 15
     - List recent changes ............................................ 16
     - Check the status of the services ............................ 17
   - Gather application log files and system data ..................... 18
     - Retrieve log files and system data with Lumberjack ......... 18
     - Manually retrieve log files .................................. 21
     - Perform ingest and retrieval tests ........................... 21
     - Look up objects .................................................. 22
     - Analyze data ...................................................... 22
   - Escalate if required ............................................... 22

2 **Troubleshooting queues** .............................................. 25
   - Introduction ......................................................... 25
   - Queues: define problem .......................................... 25
   - Queues: assess impact ............................................ 26
   - Queues: collect data .............................................. 26
   - Replication queues: analysis .................................... 27
     - Object ingest queue ........................................... 27
     - Object replication queue .................................... 28

3 **Troubleshooting Admin Nodes** .................................... 29
   - Connection to NMS unavailable .................................. 29
     - New installations ............................................... 29
     - Unexpectedly while the system is running .................... 30

4 **Troubleshooting Storage Nodes** .................................. 31
   - Object store (storage volume) failures ......................... 31
Troubleshooting Guide | 4

Troubleshoot SAVP Total Usable Space (Percent) alarm ................................. 32
SSTS Storage Status alarm ................................................................. 34
  Troubleshoot SSTS Alarms ............................................................. 34
Lost object data ............................................................... 37
  Determine the number of lost objects ............................................. 37
  Lost erasure coded object data ...................................................... 38
  Determine if lost object data can be recovered ............................... 39
  Check unavailable resources for lost objects .................................. 40
  Reset the values for lost objects data ......................................... 41
SVST (Services: Status - Cassandra) alarm ........................................ 42
  Troubleshoot SVST alarm ............................................................ 43
  Rebuild the distributed key value store ........................................... 45

5 Troubleshooting tips ................................................................. 47
  Time synchronization ................................................................. 47
  NTP vs SNTP protocol ............................................................... 47
  Running GNU screen in multi-display mode .................................... 47
  Corrupt ISO message when using load_cds.py script ..................... 48
  Error using load_cds.py ............................................................ 48
  Provisioning ................................................................. 48
    Provisioning log files ........................................................... 48
    Errors in the grid specification file ......................................... 49
      Initial installation ............................................................... 49
      Expansion and maintenance procedures ................................ 50
  Mounting a USB flash drive ...................................................... 51
    Script to mount USB flash drives .......................................... 51
  Change IP addresses .............................................................. 51
    Update IP configuration GDU task fails ................................... 51
    Grid node fails to connect .................................................... 52

A Alarms reference ................................................................. 53
  Alarms and recommended actions ............................................... 53
    A ..................................................................................... 53
    BCDE .................................................................................. 59
    F ...................................................................................... 62
    HI .................................................................................... 63
    LM ................................................................................... 63
    NO ................................................................................... 65
    PR .................................................................................... 68
    ST .................................................................................... 71
    UV .................................................................................... 74
    X .................................................................................... 75

B Log files ................................................................. 77
  Application log files ................................................................. 77
Problem determination

A methodology for troubleshooting a problem

Overview of problem determination

This chapter provides an overview of the recommended problem determination methodology for the StorageGRID Webscale system. Follow the process outlined in Figure 1 to determine the problem with the StorageGRID Webscale system.

For an example of how to use this problem determination methodology, see Chapter 2: “Troubleshooting queues”.

![Diagram of problem determination methodology]
Define the problem

The first step to solving a problem is to define the problem clearly. Use the worksheet in Table 1 to describe the problem and establish its history.

Table 1: Problem Definition Worksheet

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the problem? What is the StorageGRID Webscale system doing or not doing? What are its symptoms?</td>
<td></td>
</tr>
<tr>
<td>When did the problem start?</td>
<td></td>
</tr>
<tr>
<td>How did you first notice the problem?</td>
<td></td>
</tr>
<tr>
<td>Is the problem repeatable?</td>
<td></td>
</tr>
<tr>
<td>What is the frequency of the problem?</td>
<td></td>
</tr>
<tr>
<td>What seems to trigger the problem?</td>
<td></td>
</tr>
</tbody>
</table>
Assess the risk and impact on the system

After you have defined the problem, assess its risk and impact the StorageGRID Webscale system. For example, the presence of critical alarms does not necessarily mean that the system is not delivering core services. Assess the impact of the problem by answering the questions listed in Table 2.

Table 2: Risk and Impact Assessment Worksheet

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can the system ingest content?</td>
<td></td>
</tr>
<tr>
<td>Can client applications retrieve content?</td>
<td></td>
</tr>
<tr>
<td>Is data at risk?</td>
<td></td>
</tr>
<tr>
<td>Is the ability to conduct business severely affected?</td>
<td></td>
</tr>
<tr>
<td>Is the StorageGRID Webscale system still functioning even if operations are disrupted?</td>
<td></td>
</tr>
</tbody>
</table>
Collect data

After the problem has been defined and its impact assessed, collect data for analysis. This section describes procedures that you can use to collect data, depending on the nature of the problem:

- Check connectivity status
- Review alarms
- Monitor SSM events
- Trigger an AutoSupport message
- Check hardware monitoring
- Plot trends
- Establish baselines
- List recent changes
- Check the status of services
- Gather application log files and system data
- Perform ingest and retrieval tests
- Look up objects
- Perform an LDR verification

Check connectivity status

Confirm that servers are online and connected to each other. In the Grid Topology tree, look for grid nodes whose state is unknown (blue) or are administratively down, that is, that have been purposely stopped (gray). If all grid nodes are green, the primary Admin Node is connected to all other grid nodes. If grid nodes are blue, there is likely a connectivity issue.

Check for alarms

An alarm is triggered when the value of an attribute reaches a set alarm threshold value. Check the Grid Topology tree for any icons that are not green, indicating that an alarm has been triggered. For information about alarms, see the Grid Primer and the Administrator Guide.

For information on how to check and review alarms, see Table 3. For more information as to what might trigger an alarm and possible solutions, see Appendix A: “Alarms reference”.
### Table 3: Checking for Alarms

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get a list of all current alarms for the StorageGRID Webscale system</td>
<td>Click <strong>System Status</strong> in the header to display the alarms sorted by severity.</td>
</tr>
</tbody>
</table>

**NOTE** Review the System Status indicator in the NMS Management Interface (MI) is the System Status indicator. It immediately tells you the most serious status (state or alarm) of the system.

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get a list of all alarms triggered over a period of time</td>
<td>1. Click <strong>System Status</strong> in the header.  &lt;br&gt; 2. Click <strong>History</strong>.  &lt;br&gt; 3. Do one of the following:  &lt;br&gt; • Click one of the time periods.  &lt;br&gt; • Enter a custom range and click <strong>Custom Query</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find out how often alarms have been triggered for a particular attribute</td>
<td>1. Go to the service or component that has the attribute that triggered the alarm.  &lt;br&gt; 2. Click <strong>Alarms</strong> and then <strong>History</strong>.  &lt;br&gt; 3. Select the attribute from the list.  &lt;br&gt; 4. Do one of the following:  &lt;br&gt; • Click one of the time periods.  &lt;br&gt; • Enter a custom range and click <strong>Custom Query</strong>.  &lt;br&gt; The alarms are listed in reverse chronological order.  &lt;br&gt; 5. To return to the alarms history request form, click <strong>History</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine whether an alarm has been disabled globally</td>
<td>If a default alarm is disabled globally, an asterisk appears beside the alarm on <strong>Configuration ▶ Alarms</strong> of the component associated with the attribute.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default Alarms (1 Result(s))</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabled</strong></td>
<td><strong>Attribute</strong></td>
</tr>
<tr>
<td>*</td>
<td>SVST (Status)</td>
</tr>
</tbody>
</table>

### Monitor SSM events

The SSM ▶ Events component relays logged events from hardware drivers. Interpretation of these numbers depends on the hardware and drivers used for the server. Treat this data as a general indicator of server problems.
**Review SSM events**

The Last Event attribute in SSM > Events captures the last event detected by the grid node. You can perform a custom query to generate a list of the event messages generated by the server over time. These messages can contain useful troubleshooting information and can be used to help determine the source of a problem.

**View last SSM event**

To view the last SSM event, go to `<grid_node> > SSM > Events > Overview > Main`.

The Last Event attribute reports the log message.

**Review multiple SSM events**

1. Go to `<grid_node> > SSM > Events > Reports > Text`.
2. Change Attribute to Last Event.
3. Optionally, select a time period for Quick Query.
4. Click Update.

![Events Report](image)

**Create custom syslog events**

Consider creating custom events to monitor recurring problems.

Custom events allow you to track all kernel, daemon, error and critical level user events logged to the syslog. A custom event can be useful for monitoring the occurrence of system log messages (and thus network security events and hardware faults) not captured by default by the SSM > Events component.
After a custom event is created, every occurrence of it is monitored. The result is an increase to the Count value of Custom Events on the SSM ➤ Events ➤ Overview page of the server being monitored.

**Steps**

1. Sign in to the NMS MI using the Admin or Vendor Account.
2. Go to Grid Management ➤ Grid Configuration ➤ Events ➤ Configuration ➤ Main.
3. Click **Edit** (or **Insert** if this is not the first event).
4. Enter a custom event string, for example, `shutdown`

![Custom Events](image)

*Figure 3: Custom Events*

5. Click **Apply Changes**.
6. Go to `<grid_node> ➤ SSM ➤ Events ➤ Overview ➤ Main`.
7. Under System Events, monitor the Count of Custom Events.

![Custom Events Count](image)

*Figure 4: Custom Events Count*
If the count increases, a custom event you are monitoring is being triggered on that server.

**Reset the count of custom events to zero**

1. Go to `<grid_node> ▶ SSM ▶ Events ▶ Configuration ▶ Main.
2. Select the **Reset** check box for Custom Events.
3. Click **Apply Changes**.

**Trigger an AutoSupport message**

Manually trigger the sending of an AutoSupport message to NetApp Support. Included in this message are system and site level attribute information, all alarms raised in the last seven days, the current status of all grid tasks (including historical data), events information as listed on the SSM ▶ Events ▶ Overview page, Admin Node database usage, the number of lost objects (zero or more), and the system’s ILM policy. This information can assist NetApp Support in troubleshooting problems with the StorageGRID Webscale system. For more information about AutoSupport, see the Administrator Guide.

**Steps**

1. Sign in to the NMS MI using the Admin or Vendor Account.
2. Go to Grid Management ▶ NMS Management ▶ AutoSupport ▶ User-Triggered.

![Figure 5: AutoSupport Page](image)

3. Click **Send**.

**NOTE**  To send an AutoSupport message, the StorageGRID Webscale system’s e-mail server must be correctly configured. For more information, see the Administrator Guide.
Plot trends

Reports (both chart and text) are an invaluable tool when troubleshooting. The fastest way to create a chart is to click the Chart button on the Overview tab of a component or service. This is known as an immediate report. You can also create charts from the Reports tab. For detailed information on how to create charts, see the Grid Primer.

Establish baselines

Baseline information is operational data during normal system operations that provides clues that can help you solve problems. Table 4 below gives examples of useful data to gather using the NMS MI.

Table 4: Collecting Baseline Information

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
<th>How to Obtain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average size of ingested objects</td>
<td>________ MB</td>
<td>Divide the average number of bytes stored daily by the average number of objects stored daily.</td>
</tr>
<tr>
<td>Average size of retrieved objects</td>
<td>________ MB</td>
<td>Divide the average number of bytes retrieved daily by the average number of objects retrieved daily.</td>
</tr>
<tr>
<td>Average storage consumption</td>
<td>________ GB consumed/day</td>
<td>Go to the StorageGRID Webscale system’s Overview page, and click next to Used Storage Capacity and Percentage Usable Storage Capacity to create charts. Find a period where the operation is fairly stable and estimate the daily storage consumption rate in bytes and in percentage. You can collect this information for the entire system or a subset of it.</td>
</tr>
<tr>
<td></td>
<td>________ % consumed/day</td>
<td></td>
</tr>
</tbody>
</table>
List recent changes

Make a list of any recent changes made to the StorageGRID Webscale system or its environment. See Table 5 for examples of what to consider.

Table 5: Recent Changes Checklist

<table>
<thead>
<tr>
<th>Item</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Was the StorageGRID Webscale system recently installed or expanded?</td>
<td></td>
</tr>
<tr>
<td>Has any hardware been repaired or refreshed recently?</td>
<td></td>
</tr>
<tr>
<td>Have any third-party applications been added or removed?</td>
<td></td>
</tr>
<tr>
<td>Have there been any changes to the network infrastructure? For example, VLANS, routers, or DNS.</td>
<td></td>
</tr>
<tr>
<td>Have any long term grid tasks been recently triggered?</td>
<td></td>
</tr>
<tr>
<td>Is data migration taking place?</td>
<td></td>
</tr>
<tr>
<td>Have any changes been made to client application interfaces?</td>
<td></td>
</tr>
<tr>
<td>Have any changes been made to the ILM policy?</td>
<td></td>
</tr>
<tr>
<td>Have any changes been made to delete protection options?</td>
<td></td>
</tr>
<tr>
<td>Have any changes been made to dual content commit or dual metadata commit?</td>
<td></td>
</tr>
<tr>
<td>Have any changes been made to storage compression?</td>
<td></td>
</tr>
</tbody>
</table>
Check the status of the services

Check the status of all services to make sure they are running.

• In the NMS MI, go to `<grid_node> ▶ SSM ▶ Services ▶ Overview ▶ Main` and check the status of all services on that grid node.

<table>
<thead>
<tr>
<th>Item</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have any changes been made to storage encryption?</td>
<td></td>
</tr>
<tr>
<td>Have any changes been made to security partitions?</td>
<td></td>
</tr>
<tr>
<td>Have any changes been made to NTP sources?</td>
<td></td>
</tr>
<tr>
<td>Have any changes been made to hardware monitoring agents?</td>
<td></td>
</tr>
<tr>
<td>Have any changes been made to the archiving middleware configuration?</td>
<td></td>
</tr>
<tr>
<td>Have any other changes been made to the StorageGRID Webscale system or its environment?</td>
<td></td>
</tr>
</tbody>
</table>

Table 5: Recent Changes Checklist (cont.)
Gather application log files and system data

To help troubleshoot a problem, you can retrieve log files and system data for your StorageGRID Webscale system. This information can be retrieved manually or with Lumberjack, which is installed on every grid node as part of a standard StorageGRID Webscale deployment.

Support might ask you to forward relevant sections of log files; for example, bycast.log or servermanager.log. Because application log files can be quite large, it is recommended that you send only the relevant portions of log files in a compressed format.

Retrieve log files and system data with Lumberjack

Lumberjack is a collection tool that gathers and organizes log files and system data on a per grid node basis. Retrievals must be set with a specific start time and are archived in a .tar file to a directory of your choice or by default to /var/local/tmp.

Log files retrieved

When you run Lumberjack, it always retrieves the following log files:

- boot.msg
- bycast-err.log
- bycast.log
- cassandra-env.sh
- cassandra.yaml
- gdu-console.log
- install.log
- messages
- servermanager.log
- system.log
Optionally, the following log files can also be retrieved:

**Audit logs**
- audit.log

**CMS logs**
- cms.errlog

**mysql logs**
- my.cnf
- mysql.err
- mysql-slow.log

**NMS logs**
- nms.log
- nms.errlog

**Samba logs**
- log.nmbd
- log.smbd
- log.winbindd

**Other logs**
- adc.errlog
- ams.errlog
- arc.errlog
- clb.errlog
- cmn.errlog
- compaq (directory)
- dds.errlog
- dsierro.log
- gridstat.errlog
- GridstatBackend.errlog
- ldr.errlog
- loopstats. <date>
- net-snmpd.log
- ntp
- peerstats. <date>
- provision-crash-<grid_info>.log
- provision-fail.log
- raid-mon-cciss.errlog
- raid-mon-cciss.log
- ssm.errlog

For more information about log files, see Appendix B: “Log files”.

**System data**

While Lumberjack’s main function is to retrieve log files, Lumberjack also gathers configuration and system data, which can be used to troubleshoot the StorageGRID Webscale system. This configuration and system data is also saved to files within Lumberjack’s outputted .tar file. System data is saved to the system_command file and configuration data in the form of various bundles files.

**Steps**

**NOTE** The destination directory must have at least 1 GB of free space.

1. Determine the log files you need to gather and the time range within which to gather those files.
2. At the grid node hosting the log files, access a command shell and log in as root using the password listed in the password.txt file.

3. Run Lumberjack. Enter: `lumberjack.rb -s <start_time> <options>`

   where:

   • `<start_time>` is the start time within which to gather logs. Format is:
     `YEAR-MM-DDTHH:MM:SS`
     For example:
     `lumberjack.rb -s 2011-02-02T12:01:01`

   Options include the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s <code>&lt;start_time&gt;</code></td>
<td>Start time within which to gather logs (mandatory). Format is <code>YEAR-MM-DDTHH:MM:SS</code></td>
</tr>
<tr>
<td>-e <code>&lt;end_time&gt;</code></td>
<td>Ending time within which to gather logs. Format is <code>YEAR-MM-DDTHH:MM:SS</code></td>
</tr>
<tr>
<td>-v, --verbose</td>
<td>Displays details of the actions Lumberjack is performing as it performs them.</td>
</tr>
<tr>
<td>-o, --output <code>&lt;directory&gt;</code></td>
<td>Specify an output directory for logs other than the default. Default is <code>/var/local/tmp</code>.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Help menu.</td>
</tr>
<tr>
<td>-l, --logs <code>&lt;option&gt;</code></td>
<td>Specify logs to retrieve. Default is all mandatory logs. Options:</td>
</tr>
<tr>
<td></td>
<td>• s = samba logs</td>
</tr>
<tr>
<td></td>
<td>• n = nms logs</td>
</tr>
<tr>
<td></td>
<td>• c = cms logs</td>
</tr>
<tr>
<td></td>
<td>• a = audit logs</td>
</tr>
<tr>
<td></td>
<td>• o = Other log files</td>
</tr>
</tbody>
</table>

   By default, files are saved to `/var/local/tmp` and stored in a `.tar` file with the following naming convention:
   `<grid_id>-<hostname>-<yyyyymmddhhmssstarttime>-<yyyyymmddhhmssendtime>.tar.gz`
   For example:
   `400061-99-14-20120217090701-20120217100000.tar.gz`

4. If requested by Support, send the `.tar` file to Support.
Manually retrieve log files

1. Determine the log files you need to gather.
2. At the grid node hosting the log files, access a command shell and log in as root using the password listed in the Passwords.txt file.
3. Change directories to locate the file:
   - For the bycast.log file, enter: `cd /var/local/log`
   - For the audit.log file, enter: `cd /var/local/audit/export/`
   - For other files, consult the section “Application log files” on page 77 for the directory name.
4. Copy the file to `/var/local/tmp`
   You should display the output to screen first to confirm this is what you want and then repeat the zgrep command, directing the output to a text file.
5. Extract the messages in the time range where the error occurred using the zgrep command. Enter:
   ```
   zgrep <string> <filename> > <mylogfile>.txt
   ```
   **NOTE** Log files that are compressed due to log rotation should not be uncompressed as this can interfere with the log rotation scripts. Use zgrep tool to grep the contents of a compressed log file without uncompressed the file.
   where
   - `<string>` is the text you are looking for
   - `<filename>` is the compressed application log file
   - `<mylogfile>` is the name of the file where to direct the output
   For example, to extract messages from a compressed bycast.log file that was created on January 16, 2008, enter:
   ```
   zgrep 2008-01-16 bycast.log.2.gz
   ```
   Confirm that the expected results are returned and then repeat the command, but direct the output to a file. Enter:
   ```
   zgrep 2008-01-16 bycast.log.2.gz > logJan1608.txt
   ```
6. If requested by Support, compress the output file and send it to Support.

Perform ingest and retrieval tests

To troubleshoot retrieval performance issues, you can perform a simple test that uses a workstation in the place of the actual client application and analyze the store/retrieve performance during the test compared to the performance normally seen with the client application.
Look up objects

Depending on the problem, you might want to confirm where object data is being stored. For example, you might want to verify that the ILM policy is performing as expected and object data is being stored where intended. You can display object metadata and the location of object data using the object’s unique identifier (in the NMS MI, go to `<primary_Admin Node> ▶ CMN ▶ Object Lookup`). For the detailed procedure, see the Administrator Guide.

Analyze data

Use the information that you collect to determine the cause of the problem and potential solutions. The analysis is problem-dependent, but in general:

- Locate points of failure and bottlenecks using the alarms.
- Reconstruct the problem history using the alarm history and charts.
- Use charts to find anomalies and compare the problem situation with normal operation.

Escalate if required

If you cannot resolve the problem on your own, contact Support. Before contacting Support, gather the information listed in Table 6 below to facilitate problem resolution.

<table>
<thead>
<tr>
<th>Item</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Problem statement</strong></td>
<td>What are the problem symptoms? What is the history of the problem? See “Define the problem” on page 8.</td>
</tr>
<tr>
<td><strong>Impact Assessment</strong></td>
<td>What is the severity of the problem? See “Assess the risk and impact on the system” on page 9.</td>
</tr>
<tr>
<td><strong>Grid ID</strong></td>
<td>The Grid ID is displayed in the NMS MI, under Grid Configuration ▶ Overview.</td>
</tr>
<tr>
<td><strong>Software version</strong></td>
<td>Check the value of storage-grid-release in the NMS MI under SSM ▶ Services.</td>
</tr>
</tbody>
</table>
### Table 6: Escalation Information Checklist (cont.)

<table>
<thead>
<tr>
<th>✓ Item</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customization</strong></td>
<td>Summarize how the StorageGRID Webscale system is configured. For example, list whether it uses storage compression, storage encryption, content protection options, archiving middleware, metadata dual commit, content dual commit, and so on.</td>
</tr>
<tr>
<td><strong>Grid specification file copy</strong></td>
<td>Create a copy of the current version of the grid specification file by copying the latest version from the NMS MI. See Grid Management ➤ Grid Configuration ➤ Configuration. For more information, see the Administrator Guide.</td>
</tr>
<tr>
<td></td>
<td>Note that this is only a copy of the grid specification file and not the actually grid specification file. This copied version is only used for troubleshooting purposes. It cannot be used to provision the StorageGRID Webscale system.</td>
</tr>
<tr>
<td><strong>Baseline information</strong></td>
<td>Collect baseline information regarding ingest operations, retrieval operations, and storage consumption. See “Establish baselines” on page 15.</td>
</tr>
<tr>
<td><strong>Recent changes</strong></td>
<td>Summarize any recent changes made to the system or its environment. See “List recent changes” on page 16.</td>
</tr>
</tbody>
</table>
Troubleshooting queues

Example of how to define a problem

Introduction

The following sections describe how to apply the problem determination methodology to troubleshooting queues. For example, a growing queue of objects waiting to be evaluated against ILM rules.

Queues: define problem

Table 7 provides an example of the type of information that you would collect to define the problem.

Table 7: Queues Example: Problem Definition

<table>
<thead>
<tr>
<th>Question</th>
<th>Sample Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the problem? What is the StorageGRID Webscale system doing or not doing? What are the symptoms?</td>
<td>Client applications are reporting that they cannot store objects to the StorageGRID Webscale system. Many alarms have been triggered.</td>
</tr>
<tr>
<td>When did the problem start?</td>
<td>Object creation was denied at about 14:50 this afternoon.</td>
</tr>
<tr>
<td>How did you first notice the problem?</td>
<td>Notified by client application. Also received e-mail notifications.</td>
</tr>
<tr>
<td>Is the problem repeatable?</td>
<td>Problem is ongoing.</td>
</tr>
<tr>
<td>What is the frequency of the problem?</td>
<td>This is the first time this has happened.</td>
</tr>
</tbody>
</table>
Queues: assess impact

Table 8 below summarizes the impact the example problem is having on system operations.

Table 8: Queues Example: Impact Assessment

<table>
<thead>
<tr>
<th>Question</th>
<th>Sample Response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Can the StorageGRID Webscale system ingest content?</strong></td>
<td>No.</td>
</tr>
<tr>
<td><strong>Can applications retrieve content?</strong></td>
<td>Some objects can be retrieved and others cannot.</td>
</tr>
<tr>
<td><strong>Is data at risk?</strong></td>
<td>No.</td>
</tr>
<tr>
<td><strong>Is the ability to conduct business severely affected?</strong></td>
<td>Yes, because client applications cannot store objects to the StorageGRID Webscale system and data cannot be retrieved consistently.</td>
</tr>
</tbody>
</table>

Queues: collect data

To troubleshoot the example problem, you need to establish timelines and compare the current situation to baseline system operations. In order to do this, look at the alarm history and plot trends.

Figure 7 illustrates some of the alarms that have been triggered.

Table 7: Alarm History
Replication queues: analysis

As the ingest rate increased, the number of ingests pending and the number of ILM evaluations pending increased because the LDR and CMS services could not keep up with the increased ingest rate.

Trends suggest that something must have changed in the StorageGRID Webscale deployment’s environment to account for the increased number of objects being ingested into the system. Did new client applications start ingesting objects? Is legacy data being migrated to the StorageGRID Webscale system? Data migration can cause queues to build up to a point where operations are disrupted. For guidelines on how to manage data migration, see the Administrator Guide.

Queues should be resolved early by a prompt response to alarms with a severity of Notice. Figure 8 shows where ingest and replication queues are likely to build up and where alarms are likely to be triggered.

![Figure 8: Potential Alarms Due to Queues Building Up]

Object ingest queue

If an Insufficient Free Space alarm is triggered, the amount of available space available has dropped below the Swapout No Create Watermark.
Object replication queue

Following ingest, copies of object data are made according to the StorageGRID Webscale system’s ILM policy. During periods of high ingest, queues might form as it can become difficult for the CMS and LDR services to keep up with the required ILM activities.

For LDR services, content replication queues are likely to form on both the source and destination LDR services. The number of Inbound Replications – Queued (RIRQ) on the destination LDR service and of Output Replications – Queued (RORQ) on the source LDR service are likely to increase and failures can trigger alarms. The Outbound Replications – Failed (RIRF) and Outbound Replications – Failed (RORF) alarms should clear after system activity goes back down.
Troubleshooting Admin Nodes

How to determine the source of Admin Node related problems

Connection to NMS unavailable

You might see the Connection to NMS Unavailable screen:

- when attempting to sign in to the NMS MI on a new installation for the first time
- unexpectedly, while using the NMS MI

![Connection to NMS Unavailable](image)

*Figure 9: Connection to NMS Unavailable*

New installations

When StorageGRID Webscale software is first installed and the NMS MI is not yet ready to receive attribute data, the Connection to NMS Unavailable page is displayed. This is normal system behavior. When installation of the NMS MI completes and it begins to retrieve attribute data, you are redirected to the login window. If the screen persists for more than a few minutes, there can be connectivity issues with the Admin Node.
Unexpectedly while the system is running

If this error occurs unexpectedly while the StorageGRID Webscale system is running, there might be a connection problem with the NMS MI, or there might be an issue with services running on the Admin Node.

Check connectivity and restart the MI service

Check physical connections between the Admin Node and the rest of the StorageGRID Webscale system. If there are no physical connection problems, restart the MI service.

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. Enter: `/etc/init.d/mi restart`
3. Log out. Enter: `exit`

If the NMS login window does not reappear after the MI service has been restarted, contact Support.

Check other Admin Nodes

If the StorageGRID Webscale system is deployed with multiple Admin Nodes, you can use another Admin Node to check the status of the unavailable primary Admin Node.

Steps

1. Sign in to the NMS MI of an available Admin Node.
2. Go to `<unavailable Admin Node> ➤ SSM ➤ Services ➤ Overview ➤ Main`.

A service that is experiencing a problem has a status of Not Running and might also be displayed in blue. Determine if alarms have been triggered and take appropriate action.
Troubleshooting Storage Nodes

How to determine the source of storage related problems

Object store (storage volume) failures

Object stores are also known as storage volumes.

The underlying storage on a Storage Node is divided into object stores. These object stores (or storage volumes) are physical partitions that act as mount points for StorageGRID Webscale system’s storage. You can view object store information for each Storage Node at LDR ► Storage ► Overview ► Main.

![Figure 10: Object Stores on a Storage Node](image)

Depending on the nature of the failure, faults with a storage volume might be reflected in an alarm on the storage status or on the health of an object store. If a storage volume fails, you should repair the failed
storage volume to restore the Storage Node to full functionality as soon as possible. If necessary, you can place the Storage Node in a read-only state so that the StorageGRID Webscale system can use it for data retrieval while you prepare for a full recovery of the server. For recovery procedures, see the *Maintenance Guide*.

### Troubleshoot SAVP Total Usable Space (Percent) alarm

1. Click **System Status** to display alarms (Figure 11). Notice the SAVP alarm.

![Figure 11: SAVP Alarm](image)

2. Click the attribute name to display more information (Figure 12).

![Figure 12: SAVP Help](image)

3. Look up the troubleshooting information for the SAVP alarm. See, “SAVP” on page 71. The recommended actions are:
   - Add storage
   - Migrate data to archive media

4. Determine when this LDR service’s storage is likely to reach capacity:
   - In the NMS MI, go to the LDR service’s Storage component that triggered the alarm. Click the **Service** link in the System Status table. This takes you to LDR ➤ Storage ➤ Alarms ➤ Main.
b. Go to LDR ➤ Storage ➤ Alarms ➤ Main.

Figure 13: LDR ➤ Storage ➤ Overview Page with SAVP Alarm

Notice the alarm for Total Usable Space (Percent). Click to chart usable space available over the last hour (Figure 14). Total space available has been steadily decreasing.

Figure 14: Trend for LDR Total Usable Space (Percent) – Last Hour

c. Notice the alarm for Total Usable Space (Percent). Click to chart usable space available over the last hour (Figure 14). Total space available has been steadily decreasing.

d. Review the trend over the last day to estimate how fast storage capacity is decreasing (Figure 15). Total available space for this LDR service decreased about 15% in the last day.

Figure 15: Trend for LDR Total Usable Space – Last Day
If there is no available storage for the StorageGRID Webscale system's other Storage Nodes, add storage to the system by adding Storage Node's.

For more information about Storage Nodes, see the Administrator Guide.

**SSTS Storage Status alarm**

In the following example, the notice alarm SSTS (Storage Status) has been triggered.

**Troubleshoot SSTS Alarms**

1. Go to LDR ➤ Storage ➤ Alarms ➤ Main to display the alarms on the Storage Node.

   ![Figure 16: SSTS Alarm](image)

2. Go to LDR ➤ Storage ➤ Overview ➤ Main and review the Total Usable Space (STAS) attribute to determine the amount of storage available for the LDR service (see Figure 17). In this example, there is only 10 GB of usable storage remaining. For this StorageGRID Webscale deployment, 10 GB is the default value of the Storage Volume Read-Only Watermark (see Grid Management ➤ Grid Configuration ➤ Storage ➤ Overview ➤ Main).
3. Plot storage consumption over the last few hours (Figure 18). In this example, Total Usable Space dropped from roughly 55 GB at 14:00 to 10 GB at 18:00, which corresponds to the time at which the SSTS alarm was triggered.

4. Verify the storage watermarks for the StorageGRID Webscale system. Go to Grid Management ► Grid Configuration ► Storage ► Overview ► Main.
When the amount of usable disk space (Total Usable Space (STAS)) dropped below the Storage Volume Read-Only Watermark, Storage Status – Current (SSCR) changed to Read-only. As Storage State – Desired was set to Online, Storage Status (SSTS) changed to Insufficient Usable Space and a Notice alarm was triggered.

In most situations, an alarm for Total Usable Space (Percent) SAVP is also triggered; however, this depends on the relationship between the watermark setting in gigabytes (GB) and the alarm settings in percent. In this example, the Storage Volume Read-Only Watermark threshold (10 GB) was crossed before for the SAVP alarm threshold (10%).

Consult the troubleshooting information for the SSTS alarm (see page 73). This alarm is triggered because there is no more available...
storage for the Storage Node. Add storage capacity by expanding the StorageGRID Webscale system and adding Storage Nodes.

For procedures on how to manage a full Storage Node, see the Administrator Guide.

Lost object data

Retrieval attempts can be made for several different reasons, including read requests from a client application, background verification of replicated object data, ILM re-evaluation, or when restoring object data during a Storage Node recovery. The StorageGRID Webscale system uses object location information that is listed in each object’s metadata to determine the location of the requested object data. When the StorageGRID Webscale system cannot find object data at any of the locations listed in the metadata for the object, a LOST (Lost Objects) alarm is triggered and the Lost Objects attribute (found on the <Storage Node> ▶ DDS ▶ Data Store ▶ Overview ▶ Main page) increases by one.

All LOST (Lost Objects) alarms should be investigated immediately to determine whether these objects might still exist in an offline or otherwise currently unavailable grid node (Storage Node or Archive Node) and might be recoverable or are truly lost.

If the StorageGRID Webscale system’s ILM rules include only one content placement instruction for replicated object data and a replicated object is lost, the lost object data cannot be recovered. In the case of lost replicated object data without copies, there is no recovery solution. The only action to be taken is to reset the Lost Object attribute for the DDS service and clear the LOST (Lost Objects) alarm. For more information, see “Reset the values for lost objects data” on page 41.

Determine the number of lost objects

If a LOST (Lost Objects) alarm is triggered, the number of lost objects is tracked by the Lost Objects attribute on the <Storage Node> ▶ DDS ▶ Data Store ▶ Overview ▶ Main page. Both replicated and erasure coded object data is counted.
Steps

1. From the NMS MI, go to `<Storage Node> ➤ DDS ➤ Data Store ➤ Overview ➤ Main.

2. Review the Lost Objects attribute.

![Figure 21: Lost Objects Detected](image)

Lost erasure coded object data

If the lost object data is erasure coded, as well as the LOST (Lost Objects) alarm, the ECOR (Copies Lost) alarm is triggered. The number of lost erasure coded copies of object data is tracked by the Copies Lost attribute found on the `<Storage Node> ➤ LDR ➤ Erasure Coding ➤ Overview ➤ Main` page. The first time a retrieval attempt fails, the Reads - Failed attribute goes up; however, it does not go up on subsequent retrieval retries against the same lost object.

Steps

1. From the NMS MI, go to `<Storage Node> ➤ LDR ➤ Erasure Coding ➤ Overview ➤ Main` for the Storage Node that has raised the (ECOR) Copies Lost alarm.

2. Review the Copies Lost attribute.
Determine if lost object data can be recovered

Use the following procedure when the LOST (Lost Objects) alarm is triggered to determine if object data can be recovered:

1. Use the audit log to determine the identifier (CBID) of the object that triggered the LOST (Lost Objects) alarm:
   a. At the Admin Node, access a command shell and log in as root using the password listed in the Passwords.txt file.
   b. Change to the directory where the audit logs are located. Enter:
      ```
      cd /var/local/audit/export/
      ```
   c. Use `grep` to extract the Object Lost (OLST) audit messages. Enter:
      ```
      grep OLST <audit_file_name>
      ```
   d. Note the CBID value included in the message. For example:

```
Admin: # grep OLST audit.log
2012-01-14T11:03:27.362483
[AUDT:] [CBID(UI64):0x498D8A1F681F05B3] [UUID(CSTR):"6213A021-91FC-49C0-4F44-EC6BF377D264"] [NOID(UI32):12088241] [VOLI(UI64):2] [RSLT(FC32):NONE] [AVER(UI32):10] [ATYP(FC32):OLST] [ATIM(UI64):1350613602969243] [ATID(UI64):16956755694216746320] [ANID(UI32):139599984] [AMID(FC32):BCMS] [ASQN(UI64):62] [ASES(UI64):1350580983645305]
```

2. Use the `ObjectByCBID` command to find the object by its identifier (CBID) and then determine if data is at risk.
   a. Telnet to localhost 1411 to access the DDS console.
   b. Enter: `/proc/OBRP/ObjectByCBID -h <hexadecimal_CBID_value>`
Check unavailable resources for lost objects

Check Storage Nodes and Archive Nodes for services that might be offline or otherwise unavailable. It may be that an object is not lost, but rather that the system could not query a location because it is currently unavailable.

**NOTE** Erasure coded copies of object data cannot be archived.

1. Check if any LDR or ARC services are offline or otherwise unavailable. Go to LDR ▶ Overview ▶ Main and check the LDR State, or ARC ▶ Overview ▶ Main and check the ARC State.

2. If an LDR or ARC service is offline, disconnected, or otherwise unavailable:
   a. Restore the LDR or ARC service’s state to Online.
   b. When the state of the LDR or ARC service is restored to Online, run the manual recovery procedure to determine if the object has a location on the previously unavailable resource, and, if possible, recover the object. See “Reset the values for lost objects data” on page 41.

Table 9: Output to Examine

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>No UUID metadata</td>
<td>If there is no UUID metadata and the ILM policy is configured to purge objects when objects are deleted, no manual intervention is required. It is safe to ignore the alarm. If the UUID is not present, it indicates that the object was intentionally purged. If the ILM policy is configured to keep deleted objects, contact Support.</td>
</tr>
</tbody>
</table>
| UUID is present   | If there is a UUID and the number of locations is zero, the object is potentially missing. Check if the object is available on an offline or unavailable resource. See “Check unavailable resources for lost objects” on page 40. If you do not find a copy of the object on an offline or unavailable storage resource and the ILM policy does not include an ILM rule with only one active content placement instruction, contact Support. Be ready to provide answers to the following questions:
   - Is the ILM policy configured to purge content from the StorageGRID Webscale system when it is deleted by the client application?
   - For replicated object data, is there a storage recovery in progress? That is, has a Volume_Lost command been issued on any Storage Node and is the recovery still in progress? |
| Locations = 0     |                                                                                                                                              |

Check unavailable resources for lost objects
3. If you cannot restore the LDR service’s state, but its storage file system is intact, perform a manual search for the CBID in the /var/local/rangedb directory. Enter:

```
find /var/local/rangedb/?/p -type f -name <CBID>p
```

where p indicates that this is persistent content.

If the object is not found in persistent storage, contact Support.

4. If you cannot restore the ARC service’s state:
   a. If your Archive Node uses Tivoli Storage Manager (TSM) as the middleware, query the TSM database on the TSM server for the object. Enter: `/usr/local/arc/tsmtool q -L <CBID>`

**WARNING** Use the tsmtool utility carefully as it permits low-level operations that can place content at risk. Use only the commands and options described below.

For example:

```
DC-ARC1: # /usr/local/arc/tsmtool q -L 296894BCC6984C770
DC-ARC1: # 1,66548445,//19069718,/20100122,/296894BCC6984C770,F,66103,1264195285000000,184467
```

In this example, the object data is stored on the TSM tape library and the command returns information about it, including the count (the count is the first parameter in the output) and the CBID. If the object data is not found, contact Support.

b. If your Archive Node uses Cloud Tiering - Simple Storage Service (S3) as the middleware, check the S3 bucket configured for the object.

**Reset the values for lost objects data**

After investigating the StorageGRID Webscale system and verifying that all recorded lost objects are permanently lost or that it is a false alarm, you can reset the value of the Lost Objects attribute to zero. For erasure coded object data, you can also reset the values of Copies Lost and Reads - Failed to zero.

**Steps**

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

2. Go to `<Storage Node> ▶ DDS ▶ Data Store ▶ Configuration ▶ Main` for the Storage Node that has raised the (LOST) Lost Objects alarm.

3. Select **Reset Lost Objects Count**.
4. Click **Apply Changes**.

   The Lost Objects attribute is reset to 0 and the LOST (Lost Objects) alarm clears. It can take a few moments for the Lost Objects attribute to reset and the alarm to clear after you click Apply Changes.

5. For erasure coded object data, go to `<Storage Node> ➤ LDR ➤ Erasure Coding ➤ Configuration ➤ Main` for the Storage Node that has raised the (ECOR) Copies Lost alarm.

6. Select **Reset Read Failure Count** and **Reset Copies Lost Count**.

7. Click **Apply Changes**.

   The Reads - Failed and Copies Lost attributes reset to 0 and the ECOR (Copies Lost) alarm clears. It can take a few moments for the attributes to reset and the alarm to clear after you click Apply Changes.

---

**SVST (Services: Status - Cassandra) alarm**

A SVST alarm may be an indication that you need to rebuild the DDS service’s distributed key value store (Cassandra database) for a Storage Node.
If Cassandra is stopped for more than 15 days (for example, the Storage Nodes is powered off), when it is brought back on-line, Cassandra will not start. You must rebuild the Cassandra database for the affected DDS service.

**Troubleshoot SVST alarm**

1. Go to `<Storage_Node>` ➤ SSM ➤ Services ➤ Alarms ➤ Main to display alarms. The SVST alarm was triggered.

   ![Figure 25: SVST Alarm](image)

   Cassandra is not running, which is indicated on the `<Storage_Node>` ➤ SSM ➤ Services ➤ Overview ➤ Main page.

   ![Figure 26: Cassandra Not Running](image)

2. Try restarting Cassandra:
   a. At the Storage Node, access a command shell and log in as root using the password listed in the password.txt file.
   b. Enter: `/etc/init.d/cassandra status`
   c. If Cassandra is not running, restart it: `/etc/init.d/cassandra restart`
3. If Cassandra does not restart, determine how long Cassandra has been down. If Cassandra has been down for longer than 15 days, you must rebuild the Cassandra database.

You can determine how long Cassandra has been down by charting it or by reviewing the servermanager log file.

To chart Cassandra:

a. Go to <Storage_Node> ➤ SSM ➤ Services ➤ Reports ➤ Charts.
b. Select Attribute ➤ Service: Status - Cassandra
c. Enter a Start Data that is at least 16 days before today’s date and for End Date, today’s date.
d. Click Update.

If the chart shows Cassandra as being down for more than 15 days, rebuild the Cassandra database. The following chart example shows that Cassandra has been down for at least 17 days.

![Chart showing Cassandra not running](image)

To review the servermanager log file:

a. At the Storage Node, access a command shell and log in as root using the password listed in the password.txt file.
b. Enter: `cat /var/local/log/servermanager.log`

The contents of the servermanager log file are displayed.
c. In the servermanager log file, if Cassandra has been down for longer than 15 days, the following message is displayed:

```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not started because it has been offline for longer than its 15 day grace period - rebuild cassandra
```

Make sure the time-stamp of this message is the time when you attempted restarting Cassandra. See step 2.

There can be more than one entry for Cassandra; thus, you must locate the most recent entry.

If Cassandra is down for longer than 15 days, you must rebuild the Cassandra database. See “Rebuild the distributed key value store” on page 45.

After Cassandra is rebuilt, alarms should clear. If alarms do not clear, contact support.

---

**Rebuild the distributed key value store**

If a DDS service’s distributed key value store (Cassandra database) for a Storage Node is off-line for more than 15 days, you must rebuild the DDS service’s distributed key value store. Choosing to rebuild the database means that the database is deleted from the grid node and rebuilt from other grid nodes.

**WARNING** This procedure should never be performed on multiple grid nodes concurrently as it may result in data loss.

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

2. Rebuild the Cassandra database. Enter: `rebuild-cassandra-data`

   When prompted, enter: `y`

   ```
   DC1-S1 #: rebuild-cassandra-data
   This will delete nonsystem Cassandra SSTables and commit logs. Do you want to proceed? [y/N]? y
   Removing Cassandra commit logs
   Removing Cassandra SSTables
   starting service cassandra
   Running nodetool rebuild command
   Rebuilding Cassandra is done.
   ```

   After the Cassandra is rebuilt, alarms should clear. If alarms do not clear, contact Support.

3. Monitor the status of `nodetool rebuild`.
Troubleshooting tips

Some common problems that might occur over time

Time synchronization

NTP vs SNTP protocol

If you encounter time synchronization problems, verify that the external time sources for the StorageGRID Webscale system 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.

Running GNU screen in multi-display mode

The GNU screen program is a useful troubleshooting tool since you can use it to let two or more users interact with a shell session simultaneously. Below is an example of two users connecting to the same Grid Deployment Utility (GDU) session:

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. Both users are now viewing GDU and inputs can come from either user.

```
# screen -ls
There is a screen on:
5361.GDU      (Attached)
1 Socket in /var/run/uscreens/S-root.
# screen -r -x GDU
```
The screen command-line options used in the example are:

- **-S <name>** To name the session
- **-ls** To list the existing sessions
- **-r** To resume a detached screen session. This brings the program back to your terminal.
- **-x <name>** To attach to a screen session that is already attached by another user (multi display mode). Either user can interact with the screen session or detach from it.

For more information, display the man page for `screen` and consult the GNU official web site [http://www.gnu.org/software/screen/](http://www.gnu.org/software/screen/).

---

**Corrupt ISO message when using load_cds.py script**

If you get an error message that a corrupt ISO has been detected (for instance, a failed md5sum check), check the integrity of the CD and copy the ISO image again.

---

**Error using load_cds.py**

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 log files**

If provisioning fails because the grid specification file is incorrect, the file `provision-fail.log` is created on the Provisioning USB flash drive. 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 Provisioning USB flash drive:

- provision-fail.log
- provision-crash-<grid_info>.log

  `<grid_info>` includes the grid ID, the grid revision being created, and a timestamp.

If `provision-fail.log` is the only file created, fix the grid specification file and run provisioning again.

If the file `provision-crash-<grid_info>.log` is also created, contact Support.

**NOTE** If an error occurs during provisioning, no information is saved. Therefore, you do not need to run the remove-revision command.

### Errors in the grid specification file

A common cause of provisioning errors is data entry errors in the grid specification file. If this is the case, fix the grid specification file and run provisioning again.

Look for data entry errors such as typos or duplicate IP addresses. Fix any such errors and provision the StorageGRID Webscale system again. If you cannot find any errors, contact Support.

If the provision command completes normally, but you discover an error in the provisioning data after examining the configuration pages in the SAID package, fix the grid specification file by updating it with Grid Designer and then provision the StorageGRID Webscale system.

### Initial installation

**NOTE** Follow this procedure if the revision number of the grid specification file is 1. For example, GID234567_REV1_SAIID.zip.

If during the initial installation you discover errors in the SAID package, you must fix the grid specification file and reinstall the primary Admin Node from the beginning, that is, you must reinstall SLES, load provisioning software, and provision the StorageGRID Webscale system.
Expansion and maintenance procedures

NOTE Follow this procedure if the revision number of the grid specification file is greater than 1. For example, GID234567_REV3_SAID.zip. This procedure cannot be used for a new installation.

Prerequisites and required materials

• Passwords.txt file
• Current provisioning passphrase
• Service laptop
• No scripts or grid tasks generated by provisioning are running.

Steps

1. Confirm that no scripts or grid tasks generated by provisioning have been started.
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. Remove the provisioning data from the StorageGRID Webscale system. Enter: remove-revision
   The remove-revision command does not remove grid tasks generated by provisioning, or roll back grid tasks that have already been run.

WARNING Do not use the remove-revision command if you have started any scripts or grid tasks that were generated by provisioning. Contact Support for assistance.

4. When prompted, enter the provisioning passphrase.
5. Cancel any pending grid tasks created by the provisioning.
6. Fix the grid specification file with Grid Designer and save it to the root directory of the /var/local/provision directory. Do not change the REV<revision_number> value.

NOTE The /var/local/provision directory must contain only one grid specification file at the root level. Otherwise, provisioning will fail.

7. Run provisioning again and generate a new SAID package. The old SAID package is overwritten and a new one is generated that uses the same naming convention.
8. Review the contents of the SAID package to confirm that the provisioning information is correct.

### Mounting a USB flash drive

#### Script to mount USB flash drives

To access files on a USB flash drive, use the following procedure to mount the USB flash drive. This procedure uses a script that automatically determines the device name of the USB flash drive.

1. At the grid node, access a command shell and log in as root using the password listed in the *Passwords.txt* file.
2. At the server hosting the grid node, insert the USB flash drive.
3. Enter: `mount_usb_flash_drive.py`
   
   The script reports that the USB flash drive is mounted to `/mnt/usb`.
5. Unmount the flash drive. Enter: `umount /mnt/usb`
6. Log out. Enter `exit`

### Change IP addresses

#### Update IP configuration GDU task fails

When performing procedures to change IP addresses, if the Update IP Configuration GDU task fails, the status of the affected grid node is listed as `Error` in the Servers panel of GDU.

It might be possible to determine the point of failure by reviewing the contents of the *gdu_console* log. Determine the point of failure, resolve the problem, and then run the Update IP Configuration GDU task again. If the problem persists, contact Support.

For more information about the *gdu_console* log, see “Deployment logs” on page 80.
Grid node fails to connect

When performing procedures to change IP addresses, if the Update IP Configuration GDU task completes successfully and the grid node is listed as Available in the Servers panel of GDU, but the affected grid node fails to connect to the StorageGRID Webscale (grid node icon is NOT green in the NMS MI's Grid Topology tree), it might be an indication that the server hosting the affected grid node failed to reboot. If this occurs, reboot the server manually. If this does not resolve the problem, contact Support.

It might be possible to determine the point of failure when running the Update IP Configuration GDU task by reviewing the contents of the gdu_console log. See “Deployment logs” on page 80.
Alarms reference

Alarms and recommended actions

The following tables lists all pre-configured StorageGRID Webscale system alarms. Responses are assigned according to the severity of the alarm. This can vary if you customize the alarm settings to fit your system management approach.

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABRL</td>
<td>Available Attribute Relays</td>
<td>Restore connectivity to a service (an ADC service) running an Attribute Relay Service as soon as possible. If there are no connected attribute relays, the grid node cannot report attribute values to the NMS service. Thus, the NMS service can no longer monitor the status of the service, or update attributes for the service. If the problem persists, contact Support.</td>
</tr>
<tr>
<td>ACMS</td>
<td>Available Metadata Services</td>
<td>An alarm is triggered when an LDR or ARC service loses connection to a DDS service. If this occurs, ingest or retrieve transactions cannot be processed. If the unavailability of DDS services is only a brief transient issue, transactions can be delayed. Check and restore connections to a DDS service to clear this alarm and return the service to full functionality.</td>
</tr>
<tr>
<td>Code</td>
<td>Name</td>
<td>Recommended Action</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| ACTS | Archive Node State        | If this alarm is triggered, you will need to complete the appropriate action to resolve the error:  
If the ACTE attribute for the Archive Node is set to Read-Only Enabled or Read-Write Disabled, you must set the attribute to Read-Write Enabled.  
If a major alarm is triggered due to an authentication failure, you must verify the Amazon Web Services credentials associated with bucket and update the values, if necessary.  
If a major alarm is triggered due to any other reason, contact Support. |
| ADCA | ADC Status                | If an alarm is triggered, check ADC ► Overview ► Main and ADC ► Alarms ► Main to determine the cause of the alarm.  
If the problem persists, contact Support. |
| ADCE | ADC State                 | If the value of ADC State is Standby, continue monitoring the service and if the problem persists, contact Support.  
If the value of ADC State is Offline, restart the service. If the problem persists, contact Support. |
| AITE | Archive Retrieve State    | If the value of Archive Retrieve State is Waiting for Middleware, check the middleware and ensure that it is operating correctly. If the ARC service has just been added to the StorageGRID Webscale system, ensure that the middleware is configured correctly.  
If the value of Archive Retrieve State is Offline, attempt to update the state to Online. Go to ARC ► Retrieve ► Configuration ► Main, select Archive Retrieve State ► Online, and click Apply Changes.  
If the problem persists, contact Support.  
This alarm is only present if Tivoli Storage Manager is configured as the middleware type. |
| AITU | Archive Retrieve Status   | If the value of Archive Retrieve Status is Middleware Error, check the middleware for errors.  
If the value of Archive Retrieve Status is Session Lost, check the middleware to ensure it is online and operating correctly. Check the network connection with the middleware.  
If the value of Archive Retrieve Status is Unknown Error, contact Support. |
<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALIS</td>
<td>Inbound Attribute Sessions</td>
<td>If the number of inbound attribute sessions on an attribute relay grows too large, it can be an indication that the StorageGRID Webscale system has become unbalanced. Under normal conditions, attribute sessions should be evenly distributed amongst ADC services. An imbalance can lead to performance issues. If the problem persists, contact Support.</td>
</tr>
<tr>
<td>ALOS</td>
<td>Outbound Attribute Sessions</td>
<td>The ADC service has a high number of attribute sessions, and is becoming overloaded. If this alarm is triggered, contact Support.</td>
</tr>
<tr>
<td>ALUR</td>
<td>Unreachable Attribute Repositories</td>
<td>Check network connectivity with the NMS service to ensure that the service can contact the attribute repository. If this alarm is triggered and network connectivity is good, contact Support.</td>
</tr>
<tr>
<td>AMQS</td>
<td>Audit Messages Queued</td>
<td>If audit messages cannot be immediately forwarded to an audit relay or repository, the messages are stored in a disk queue. During heavy loads this queue can exceed 100,000 messages. If this occurs, monitor the queue to determine if messages are being forwarded. If the alarm is triggered, check the load on the system—if there have been a significant number of transactions this can be normal and will resolve itself over time. In this case, the alarm can be ignored and will clear itself. If the alarm persists, view a chart of the queue size. If the number continues increasing without occasional decreases, contact Support. In rare instances, the disk queue can be large enough to cause a thread deadlock when the AMS service starts. If a thread deadlock occurs, contact Support.</td>
</tr>
<tr>
<td>AOTE</td>
<td>Archive Store State</td>
<td>If the value of Archive Store State is Waiting for Middleware, check the middleware and ensure that it is operating correctly. If the service has just been added to the StorageGRID Webscale system, ensure that the middleware is correctly configured. If the value of Archive Store State is Offline, check the value of Archive Store Status. Correct any problems before moving the Archive Store State back to Online. This alarm is only present if Tivoli Storage Manager is configured as the middleware type.</td>
</tr>
</tbody>
</table>
### AOTU Archive Store Status
If the value of Archive Store Status is Session Lost check that the middleware is online.
If the value of Middleware Error, check the middleware for errors.
If the value of Archive Store Status is Unknown Error, contact Support.

### ARCE ARC State
The ARC service has a state of Standby until all ARC components (Replication, Store, Retrieve, Middleware) have started. It then transitions to Online.
If the value of ARC State does not transition from Standby to Online, check the status of the ARC components.
If the value of ARC State is Offline, restart the service. If the problem persists, contact Support.

### AROQ Objects Queued
This alarm can be triggered if the removable storage device is running slowly due to problems on the middleware server, or if the middleware server encounters multiple read errors. Check the middleware server for errors, and ensure that it is operating correctly.
In some cases, this error can occur as a result of a high rate of data requests. Monitor the number of objects queued as system activity declines.

### ARRC Remaining Capacity
If the remaining capacity of the attribute repository drops too low, the StorageGRID Webscale system can require expansion. To determine if expansion is required, contact Support.

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOTU</td>
<td>Archive Store Status</td>
<td>If the value of Archive Store Status is Session Lost check that the middleware is online. If the value of Middleware Error, check the middleware for errors. If the value of Archive Store Status is Unknown Error, contact Support.</td>
</tr>
<tr>
<td>ARCE</td>
<td>ARC State</td>
<td>The ARC service has a state of Standby until all ARC components (Replication, Store, Retrieve, Middleware) have started. It then transitions to Online. If the value of ARC State does not transition from Standby to Online, check the status of the ARC components. If the value of ARC State is Offline, restart the service. If the problem persists, contact Support.</td>
</tr>
<tr>
<td>AROQ</td>
<td>Objects Queued</td>
<td>This alarm can be triggered if the removable storage device is running slowly due to problems on the middleware server, or if the middleware server encounters multiple read errors. Check the middleware server for errors, and ensure that it is operating correctly. In some cases, this error can occur as a result of a high rate of data requests. Monitor the number of objects queued as system activity declines.</td>
</tr>
<tr>
<td>ARRC</td>
<td>Remaining Capacity</td>
<td>If the remaining capacity of the attribute repository drops too low, the StorageGRID Webscale system can require expansion. To determine if expansion is required, contact Support.</td>
</tr>
</tbody>
</table>
### ARRF  Request Failures
If an object data retrieval from archive media fails, the Archive Node retries the retrieval as the failure can be due to a transient issue. However, if the object data is corrupted on tape or the tape has been marked as being permanently unavailable by the Tivoli Storage Manager administrator, the retrieval does not fail. Instead, the Archive Node continuously retries the retrieval and the value for Request Failures continues to increase.

This alarm can indicate that the storage media holding the requested data is corrupt. Check the middleware server to further diagnose the problem.

If you determine that the object data is no longer in the archive, the object will have to be removed from the StorageGRID Webscale system. For more information, contact Support.

Once the problem that triggered this alarm is addressed, reset the failures count. Go to ARC ▶ Retrieve ▶ Configuration ▶ Main, select Reset Request Failure Count and click Apply Changes.

### ARRS  Repository Status
The NMS service is unexpectedly not gathering attribute information from the StorageGRID Webscale system.

If the problem persists, contact Support.

### ARRV  Verification Failures
To diagnose and correct this problem, contact Support.

Once the problem that triggered this alarm is addressed, reset the failures count. Go to ARC ▶ Retrieve ▶ Configuration ▶ Main, select Reset Verification Failure Count and click Apply Changes.

### ARVF  Store Failures
This alarm can occur as a result of middleware errors or media errors. Check the middleware server for errors, and ensure that it is operating correctly.

Once the problem that triggered this alarm is addressed, reset the failures count. Go to ARC ▶ Store ▶ Configuration ▶ Main, select Reset Store Failure Count and click Apply Changes.

### ASXP  Audit Shares
An alarm is triggered if the value of Audit Shares is Unknown. This alarm can indicate a problem with the installation or configuration of the Admin Node.

If the problem persists, contact Support.

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARRF</td>
<td>Request Failures</td>
<td>If an object data retrieval from archive media fails, the Archive Node retries...</td>
</tr>
<tr>
<td>ARRS</td>
<td>Repository Status</td>
<td>The NMS service is unexpectedly not gathering attribute information from the...</td>
</tr>
<tr>
<td>ARRV</td>
<td>Verification Failures</td>
<td>To diagnose and correct this problem, contact Support.</td>
</tr>
<tr>
<td>ARVF</td>
<td>Store Failures</td>
<td>This alarm can occur as a result of middleware errors or media errors. Check...</td>
</tr>
<tr>
<td>ASXP</td>
<td>Audit Shares</td>
<td>An alarm is triggered if the value of Audit Shares is Unknown. This alarm can...</td>
</tr>
</tbody>
</table>
### Troubleshooting Guide

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUMA</td>
<td>AMS Status</td>
<td>If the value of AMS Status is DB Connectivity Error, restart the grid node.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the problem persists, contact Support.</td>
</tr>
<tr>
<td>AUME</td>
<td>AMS State</td>
<td>If the value of AMS State is Standby, continue monitoring the StorageGRID Webscale system. If the problem persists, contact Support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the value of AMS State is Offline, restart the service. If the problem persists, contact Support.</td>
</tr>
<tr>
<td>AUXS</td>
<td>Audit Export Status</td>
<td>If an alarm is triggered, correct the underlying problem and then restart the AMS service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the problem persists, contact Support.</td>
</tr>
<tr>
<td>Code</td>
<td>Name</td>
<td>Recommended Action</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>--------------------</td>
</tr>
</tbody>
</table>
| BASF | Available Object Identifiers | When a StorageGRID Webscale system is provisioned, the CMN service is allocated a fixed number of object identifiers. This alarm is triggered when the StorageGRID Webscale system begins to exhaust its supply of object identifiers.  
To allocated more identifiers, contact Support. |
| BASS | Identifier Block Allocation Status | By default, an alarm is triggered when object identifiers cannot be allocated because ADC quorum cannot be reached.  
Identifier block allocation on the CMN service requires a quorum (50% + 1) of the ADC services to be online and connected. If quorum is unavailable, the CMN service is unable to allocate new identifier blocks until ADC quorum is re-established. If ADC quorum is lost, there is generally no immediate impact on the StorageGRID Webscale system (clients can still ingest and retrieve content), as the CMS services maintain a store (approximately one month’s worth) of cached identifiers; however, if the condition continues, the StorageGRID Webscale system will lose the ability to ingest new content.  
If an alarm is triggered, investigate the reason for the loss of ADC quorum (for example, it can be a network or Storage Node failure) and take corrective action.  
If the problem persists, contact Support. |
| BRDT | Module temperature | An alarm is triggered if the temperature of a StorageGRID Webscale appliance E5600SG controller exceeds a nominal threshold.  
If the Storage Node is a StorageGRID Webscale appliance, StorageGRID Webscale indicates that the storage controller needs attention.  
Check hardware components and environmental issues for overheated condition. If necessary, replace the component. |
| BTOF | Offset | An alarm is triggered if the service time (seconds) differs significantly from the operating system time. Under normal conditions, the service should resynchronize itself. If the service time drifts too far from the operating system time, system operations can be affected. Confirm that the StorageGRID Webscale system’s time source is correct.  
If the problem persists, contact Support. |
<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>BTSE</td>
<td>Clock State</td>
<td>An alarm is triggered if the service’s time is not synchronized with the time tracked by the operating system. Under normal conditions, the service should resynchronize itself. If the time drifts too far from operating system time, system operations can be affected. Confirm that the StorageGRID Webscale system’s time source is correct. If the problem persists, contact Support.</td>
</tr>
<tr>
<td>CAHP</td>
<td>Java Heap Usage Percent</td>
<td>An alarm may indicate an issue with ingest rates. Check the ILM Activity at Grid Topology ► Deployment ► Overview ► Main If the problem persists, contact Support.</td>
</tr>
<tr>
<td>CAIH</td>
<td>Number Available Ingest Destinations</td>
<td>This alarm clears when underlying issues of available LDR services are corrected. Ensure that the HTTP component of LDR services are online and running normally. If the problem persists, contact Support.</td>
</tr>
<tr>
<td>CAQH</td>
<td>Number Available Q/R Destinations</td>
<td>This alarm clears when underlying issues of available LDR services are corrected. Ensure that the HTTP component of LDR services are online and running normally. If the problem persists, contact Support.</td>
</tr>
</tbody>
</table>
| CASA | Data Store Status                         | An alarm is raised if the Cassandra data store becomes unavailable. Check the status of Cassandra:  
1. At the Storage Node, access a command shell and log in as root using the password listed in the password.txt file.  
2. Enter: `/etc/init.d/ cassandra status`  
3. If Cassandra is not running, restart it: `/etc/init.d/cassandra restart`  
This alarm may also be an indication that the DDS service’s distributed key value store (Cassandra database) for a Storage Node requires rebuilding. See “SVST” on page 74 and “SVST (Services: Status - Cassandra) alarm” on page 42. If the problem persists, contact Support. |
A table is presented that outlines various alarm cases, their descriptions, and recommended actions.

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Recommended Action</th>
</tr>
</thead>
</table>
| CASE | Data Store State   | An alarm is raised when the Data Store State attribute (Storage Node ➤ DDS ➤ Data Store ➤ Overview ➤ Main) has a state of Joining. This occurs during the Storage Node installation and expansion processes. This alarm will clear when the state of the Data Store State attribute changes from Joining to Normal.  
If the alarm does not clear or is triggered outside of the process of installing or adding a Storage Node, contact Support. |
| CDLP | Data Load (Percent)| If an alarm is triggered, it is an indication that the data store for this Storage Node is nearing capacity. Expand the StorageGRID Webscale system by adding Storage Nodes. Once storage is added, the system automatically rebalanced data and the alarm clears. |
| CLBA | CLB Status         | If an alarm is triggered, check CLB ➤ Overview ➤ Main and CLB ➤ Alarms ➤ Main to determine the cause of the alarm and to troubleshoot the problem.  
If the problem persists, contact Support. |
| CLBE | CLB State          | If the value of CLB State is Standby, continue monitoring the situation and if the problem persists, contact Support.  
If the state is Offline and there are no known server hardware issues (for example, the server is unplugged) or scheduled downtime, restart the service. If the problem persists, contact Support. |
| CMNA | CMN Status         | If an alarm is triggered, contact Support.  
An alarm is triggered and the value of CMN Status is No Online CMN during a hardware refresh of the primary Admin Node when the CMNs are switched (the value of the old CMN State is Standby and the new is Online).  
If the problem persists, contact Support. |
| CMNE | CMN State          | If the value of CMN State is Standby, continue monitoring the CMN service and if the problem persists, contact Support.  
If the value of CMN State is Offline, restart the service. If the problem persists, contact Support. |
| CMSS | CMS State          | If an alarm is triggered, contact Support. |
## Code | Name | Recommended Action
--- | --- | ---
CMST | CMS Status | If an alarm is triggered, contact Support.
CPRC | Remaining Capacity | An alarm is triggered if the remaining capacity (number of available connections that can be opened to the NMS database) falls below the configured alarm severity. If this alarm is triggered, contact Support.
CPUT | CPU Temperature | An alarm is triggered if the temperature of a StorageGRID Webscale appliance E5600SG CPU exceeds a nominal threshold. If the Storage Node is a StorageGRID Webscale appliance, StorageGRID Webscale indicates that the storage controller needs attention. Check hardware components and environment issues for overheated condition. If necessary, replace the component.
DNST | DNS Status | After installation completes, a DNST alarm is triggered in the SSM service. After the DNS is configured and the new server information reaches all grid nodes, the alarm is canceled.
ECOR | Copies Lost | An alarm is triggered whenever an erasure coded object cannot be retrieved because the erasure code’s fault loss tolerance has been breached — too many fragments have been lost. For more information, see “Lost object data” on page 37. If the problem persists, contact Support.

## F

## Code | Name | Recommended Action
--- | --- | ---
FOPN | Open File Descriptors | FOPN can become large during peak activity. If it does not diminish during periods of slow activity, contact Support.
### HI

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSTE</td>
<td>HTTP/CDMI State</td>
<td>It is critical that the HTTP protocol be online and running without errors. Check the state of the LDR service and the related Storage component. Ensure all are online. Check that the HTTP component is configured to autostart when the service is restarted.</td>
</tr>
<tr>
<td>HSTU</td>
<td>HTTP/CDMI Status</td>
<td></td>
</tr>
<tr>
<td>HTAS</td>
<td>Auto-Start HTTP</td>
<td>Specifies whether to start HTTP services automatically on start-up. This is a user-specified configuration option.</td>
</tr>
<tr>
<td>IQSZ</td>
<td>Number of Objects</td>
<td>Either objects are arriving for ingest faster than the ILM policy can evaluate them, or a large number of objects that require an ILM re-evaluation are being processed. Plot the value of IQSZ over the course of a day or week, and check that at times of low system activity the number of objects drops, and tends towards zero. If the problem persists, contact Support.</td>
</tr>
<tr>
<td>IRSU</td>
<td>Inbound Replication Status</td>
<td>An alarm indicates that inbound replication has been disabled. Confirm configuration settings at LDR Replication Configuration Main.</td>
</tr>
</tbody>
</table>

### LM

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>LATA</td>
<td>Average Latency</td>
<td>Check for connectivity issues. Check system activity to confirm that there is an increase in system activity. An increase in system activity will result in an increase to attribute data activity. This increased activity will result in a delay to the processing of attribute data. This can be normal system activity and will subside. Check for multiple alarms. An increase in average latency times can indicate an excessive number of triggered alarms. If the problem persists, contact Support.</td>
</tr>
</tbody>
</table>
## Code | Name | Recommended Action
--- | --- | ---
LATW | Worst-Case Latency | Check for connectivity issues.
 |  | Check system activity to confirm that there is an increase in activity. An increase in system activity will result in an increase to attribute data activity. This increased activity will result in a delay to the processing of attribute data. This can be normal system activity and will subside.
 |  | Check for multiple alarms. An increase in average latency times can indicate an excessive number of triggered alarms.
 |  | If the problem persists, contact Support.
LDRE | LDR State | If the value of LDR State is Standby, continue monitoring the situation and if the problem persists, contact Support.
 |  | If the value of LDR State is Offline, restart the service. If the problem persists, contact Support.
LOST | Lost Objects | Lost objects represent a loss of data. The Lost Objects attribute is incremented whenever the number of locations for an object drops to zero without the CMS service purposely purging the content to satisfy the ILM policy. For more information, see “Lost object data” on page 37.
 |  | If the problem persists, contact Support.
MINQ | E-mail Notifications Queued | Check the network connections of the servers hosting the NMS service and the external mail server. Also confirm that the NMS e-mail server configuration is correct.
MINS | E-mail Notifications Status | A minor alarm is triggered if the NMS service is unable to connect to the mail server. Check the network connections of the servers hosting the NMS service and the external mail server. Also confirm that the NMS e-mail server configuration is correct.
MISS | NMS Interface Engine Status | An alarm is triggered if the NMS interface engine on the Admin Node that gathers and generates interface content is disconnected from the system. Check Server Manager to determine if the server individual application is down.
MMQS | Peak Message Queue Size | An alarm indicates that the grid node is overloaded, and can not be able to process operations at a high enough rate to support normal system operation. Client requests can timeout when nodes are in this condition.
 |  | If the problem persists, contact Support.
<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>NANG</td>
<td>Network Auto Negotiate Setting</td>
<td>Check the network adapter configuration. The setting must match preferences of your network routers and switches. An incorrect setting can have a severe impact on system performance.</td>
</tr>
<tr>
<td>NDUP</td>
<td>Network Duplex Setting</td>
<td>Check the network adapter configuration. The setting must match preferences of your network routers and switches. An incorrect setting can have a severe impact on system performance.</td>
</tr>
<tr>
<td>NLNK</td>
<td>Network Link Detect</td>
<td>Check the network cable connections on the port and at the switch. Check the network router, switch, and adapter configurations. Restart the server. If the problem persists, contact Support.</td>
</tr>
<tr>
<td>NRER</td>
<td>Receive Errors</td>
<td>These errors can clear without being manually reset. If errors do not clear, check the network hardware. Check that the adapter hardware and driver are correctly installed and configured to work with your network routers and switches. When the underlying problem is resolved, reset the counter. Go to SSM ▶ Resources ▶ Configuration ▶ Main, select Reset Receive Error Count, and click Apply Changes. On servers that use the bnx2 driver for the Broadcom Corporation NetXtreme II BCM5708 Gigabit Ethernet controller, spurious Receive Errors or Transmit Errors can be reported. These errors can clear without being manually reset. Disable the default alarm on these two attributes to eliminate these “nuisance” alarms.</td>
</tr>
<tr>
<td>NRLY</td>
<td>Available Audit Relays</td>
<td>If audit relays are not connected to ADC services, audit events cannot be reported. They are queued and unavailable to users until the connection is restored. Restore connectivity to an ADC service as soon as possible. If the problem persists, contact Support.</td>
</tr>
<tr>
<td>NSCA</td>
<td>NMS Status</td>
<td>If the value of NMS Status is DB Connectivity Error, restart the service. If the problem persists, contact Support.</td>
</tr>
<tr>
<td>Code</td>
<td>Name</td>
<td>Recommended Action</td>
</tr>
<tr>
<td>------</td>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NSCE</td>
<td>NMS State</td>
<td>If the value of NMS State is Standby, continue monitoring and if the problem persists, contact Support. If the value of NMS State is Offline, restart the service. If the problem persists, contact Support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSPD</td>
<td>Speed</td>
<td>This can be caused by network connectivity or driver compatibility issues. If the problem persists, contact Support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTBR</td>
<td>Free Tablespace</td>
<td>If an alarm is triggered, check how fast database usage has been changing. A sudden drop (as opposed to a gradual change over time) indicates an error condition. If the problem persists, contact Support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adjusting the alarm threshold allows you to proactively manage when additional storage needs to be allocated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the available space reaches a low threshold (see alarm threshold), contact Support to change the database allocation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTER</td>
<td>Transmit Errors</td>
<td>These errors can clear without being manually reset. If they do not clear, check network hardware. Check that the adapter hardware and driver are correctly installed and configured to work with your network routers and switches.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When the underlying problem is resolved, reset the counter. Go to SSM ▶ Resources ▶ Configuration ▶ Main, select Reset Transmit Error Count, and click Apply Changes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On servers that use the bnx2 driver for the Broadcom Corporation NetXtreme II BCM5708 Gigabit Ethernet controller, spurious Receive Errors or Transmit Errors can be reported. These errors can clear without being manually reset. Disable the default alarm on these two attributes to eliminate these “nuisance” alarms.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTFQ</td>
<td>NTP Frequency Offset</td>
<td>If the frequency offset exceeds the configured threshold, there is likely a hardware problem with the local clock. If the problem persists, contact Support to arrange a replacement.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTLK</td>
<td>NTP Lock</td>
<td>If the NTP daemon is not locked to an external time source, check network connectivity to the designated external time sources, their availability, and their stability.</td>
</tr>
</tbody>
</table>
If the time offset exceeds the configured threshold, there is likely a hardware problem with the oscillator of the local clock. If the problem persists, contact Support to arrange a replacement.

If this server is configured to act as a primary NTP server for the StorageGRID Webscaler system, this attribute tracks the number of external NTP time sources available. It is normal for this number to fluctuate if there are a large number of external time sources available.

If the server is configured to act as a secondary NTP time server or an NTP client, the server uses other servers as its NTP time sources. For more information about the StorageGRID Webscale system’s NTP configuration, see the Solution Design document for your deployment.

If the number of NTP time sources available falls below the configured minimum, the accuracy and consistency of local time on the server can suffer. If the number of NTP time sources falls to zero, local server time will drift out of synchronization with the time recorded by other services. In extreme cases, this can disrupt system operations. Correct the issue as quickly as possible.

These values give an indication of the reliability and stability of the time source that NTP on the local server is using as its reference.

If an alarm is triggered, it can be an indication that the time source’s oscillator is defective, or that there is a problem with the WAN link to the time source.

If the value of NTP Status is Not Running, contact Support.

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTOF</td>
<td>NTP Time Offset</td>
<td>If the time offset exceeds the configured threshold, there is likely a hardware problem with the oscillator of the local clock. If the problem persists, contact Support to arrange a replacement.</td>
</tr>
<tr>
<td>NTSA</td>
<td>NTP Sources Available</td>
<td>If this server is configured to act as a primary NTP server for the StorageGRID Webscaler system, this attribute tracks the number of external NTP time sources available. It is normal for this number to fluctuate if there are a large number of external time sources available. If the server is configured to act as a secondary NTP time server or an NTP client, the server uses other servers as its NTP time sources. For more information about the StorageGRID Webscale system’s NTP configuration, see the Solution Design document for your deployment. If the number of NTP time sources available falls below the configured minimum, the accuracy and consistency of local time on the server can suffer. If the number of NTP time sources falls to zero, local server time will drift out of synchronization with the time recorded by other services. In extreme cases, this can disrupt system operations. Correct the issue as quickly as possible.</td>
</tr>
<tr>
<td>NTSD</td>
<td>Chosen Time Source Delay</td>
<td>These values give an indication of the reliability and stability of the time source that NTP on the local server is using as its reference.</td>
</tr>
<tr>
<td>NTSJ</td>
<td>Chosen Time Source Jitter</td>
<td>If an alarm is triggered, it can be an indication that the time source’s oscillator is defective, or that there is a problem with the WAN link to the time source.</td>
</tr>
<tr>
<td>NTSO</td>
<td>Chosen Time Source Offset</td>
<td>If the value of NTP Status is Not Running, contact Support.</td>
</tr>
<tr>
<td>NTSU</td>
<td>NTP Status</td>
<td>If the value of NTP Status is Not Running, contact Support.</td>
</tr>
</tbody>
</table>
Corrupt Objects Detected

Any corrupt objects are worthy of investigation. More than 10 indicates a major problem.

Note that this value is persistent: it is not updated once the corrupt objects have been restored.

If corrupt objects are detected, change the Verification Priority to High. This speeds up verification and assess the magnitude of the problem. Go to LDR ➤ Verification ➤ Configuration ➤ Main, select Verification Priority ➤ High and click Apply Changes.

After the underlying problem is resolved, reset the counter to clear the alarm. Go to LDR ➤ Verification ➤ Configuration ➤ Main, select Reset Corrupt Objects Count, and click Apply Changes.

Overall Power Status

An alarm is triggered if the power of a StorageGRID Webscale appliance enclosure deviates from the recommended operating voltage.

Check Power Supply A or B status to determine which power supply is operating abnormally.

If necessary, replace the power supply.

Objects Quarantined

After the objects are automatically restored by the StorageGRID Webscale system, the quarantined objects must be manually removed from the quarantine directory. Contact Support.

After the quarantined objects are removed, the value of OQRT is updated and the alarm clears.

Outbound Replication Status

An alarm indicates that outbound replication is not possible: storage is in a state where objects cannot be retrieved. An alarm is triggered if outbound replication is disabled manually. Check LDR ➤ Replication ➤ Configuration.

An alarm is triggered if the LDR service is unavailable for replication: LDR ➤ Storage.

Backup Result

If the value of Backup Result is Failed, ensure there are no HTTP alarms on LDR services and that capacity remains on some Storage Nodes. Backups are run automatically each day, and retained for two weeks.
### Code | Name | Recommended Action
---|---|---
PGFT | Page Fault Rate | If the page fault rate is too high, the StorageGRID Webscale system is spending too much time swapping information in and out of physical memory. The server can need more physical memory. If the problem persists, contact Support.

PMEM | Service Memory Usage (Percent) | Can have a value of Over Y% RAM where Y represents the percentage of memory being used by the server. Figures under 80% are normal. Over 90% is considered a problem. If memory usage is high for a single service, monitor the situation and investigate. If the problem persists, contact Support.

PSAS | Power Supply A Status | An alarm is triggered if the power supply A of a StorageGRID Webscale appliance deviates from the recommended operating voltage. If necessary, replace the power supply A.

PSBS | Power Supply B Status | An alarm is triggered if the power supply B of a StorageGRID Webscale appliance deviates from the recommended operating voltage. If necessary, replace the power supply B.

RDTE | Archive Middleware State | If the value of Archive Middleware State is Offline, check Archive Middleware Status and resolve any problems. Bring the component back online. Go to ARC Middleware Configuration Main, select Archive Middleware State Online, and click Apply Changes.
**RDTU**

**Archive Middleware Status**

If the value of Archive Middleware Status is Configuration Error and the ARC service (Archive Node expansion) has just been added to the StorageGRID Webscale system, ensure that the middleware server is correctly configured.

If the value of Archive Middleware Status is Connection Failure, or Connection Failure, Retrying, check the network configuration on the middleware server, and the network connection between the server and the StorageGRID Webscale system.

If the value of Archive Middleware Status is Authentication Failure, or Authentication Failure, Reconnecting, the StorageGRID Webscale system can connect to the middleware server, but cannot authenticate the connection. Check that the middleware server is configured with the correct user, password, and permissions, and restart the service.

If the value of Archive Middleware Status is Session Failure, an established session has been lost unexpectedly. Check the network connection between the middleware server and the StorageGRID Webscale system. Check the middleware server for errors.

If the value of Archive Middleware Status is Unknown Error, contact Support.

**RIRF**

**Inbound Replications – Failed**

Replication alarms (Inbound Replications – Failed RIRF and Outbound Replications – Failed RORF) can occur during periods of high load or temporary network disruptions. After system activity reduces, these alarms should clear. If the count of failed replications continues to increase, look for network problems and verify that the source and destination LDR and ARC services are online and available.

To reset the count, go to **ARC or LDR ➤ Replication ➤ Configuration ➤ Main**, select Reset Inbound Replication Failure Count, and click **Apply Changes**.

**RIRQ**

**Inbound Replications – Queued**

Alarms can occur during periods of high load or temporary network disruption. After system activity reduces, this alarm should clear. If the count for queued replications continues to increase, look for network problems and verify that the source and destination LDR and ARC services are online and available.
Replication alarms (Inbound Replications – Failed (RIRF) and Outbound Replications – Failed (RORF)) can occur during periods of high load or due to temporary network disruptions. After system activity reduces, these alarms should clear. If the count of failed replications continues to increase, look for network problems and verify that the source and destination LDR and the ARC services are online and available.

To reset the count, go to **ARC** or **LDR** ➤ **Replication** ➤ **Configuration** ➤ **Main**, select Reset Outbound Replication Failure Count, and click **Apply Changes**.

### Outbound Replications – Queued

The outbound replication queue contains object data being copied to satisfy ILM rules and objects requested by clients.

An alarm can occur as a result of a system overload. Wait to see if the alarm clears when system activity declines. If the alarm recurs, add capacity by adding Storage Nodes.

### Code | Name | Recommended Action
---|---|---
RORF | Outbound Replications – Failed | The threshold for a notice alarm is 10 objects, while greater than 50 objects triggers a minor alarm. Replication alarms (Inbound Replications – Failed (RIRF) and Outbound Replications – Failed (RORF)) can occur during periods of high load or due to temporary network disruptions. After system activity reduces, these alarms should clear. If the count of failed replications continues to increase, look for network problems and verify that the source and destination LDR and the ARC services are online and available. To reset the count, go to **ARC** or **LDR** ➤ **Replication** ➤ **Configuration** ➤ **Main**, select Reset Outbound Replication Failure Count, and click **Apply Changes**.
RORQ | Outbound Replications – Queued | The outbound replication queue contains object data being copied to satisfy ILM rules and objects requested by clients. An alarm can occur as a result of a system overload. Wait to see if the alarm clears when system activity declines. If the alarm recurs, add capacity by adding Storage Nodes.

### Code | Name | Recommended Action
---|---|---
SAVP | Total Usable Space (Percent) | If usable space reaches a low threshold, options include expanding the StorageGRID Webscale system or move object data to archive through an Archive Node.
SCAS | Status | If the value of Status for the active grid task is **Error**, look up the grid task message at **CMN** ➤ **Grid Tasks** ➤ **Overview** ➤ **Main**. The grid task message displays information about the error (for example, “check failed on node 12130011”). Once you have investigated and corrected the problem, restart the grid task. Go to **CMN** ➤ **Grid Tasks** ➤ **Configuration** ➤ **Main** and select **Actions** ➤ **Run**.
If the value of Status for a grid task being aborted is **Error**, retry aborting the grid task.
If the problem persists, contact Support.
<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCHR</td>
<td>Status</td>
<td>If the value of Status for the historical grid task is Aborted, investigate the reason and run the task again if required. If the problem persists, contact Support.</td>
</tr>
<tr>
<td>SHLH</td>
<td>Health</td>
<td>If the value of Health for an object store is Error, check and correct: • problems with the volume being mounted • file system errors</td>
</tr>
<tr>
<td>SLSA</td>
<td>CPU Load Average</td>
<td>The higher the value the busier the system. If the CPU Load Average persists at a high value, the number of transactions in the system should be investigated to determine whether this is due to heavy load at the time. View a chart of the CPU load average (CMS ▶ Resources ▶ Reports ▶ Charts). If the load on the system is not heavy and the problem persists, contact Support.</td>
</tr>
<tr>
<td>SMTT</td>
<td>Total Events</td>
<td>If the value of Total Events is greater than zero, check if there are known events (such as network failures) that can be the cause. Unless these errors have been cleared (that is, the count has been reset to 0), Total Events alarms can be triggered. When an issue is resolved, reset the counter to clear the alarm. Go to SSM ▶ Events ▶ Configuration ▶ Main, select the event and click Apply Changes. If the value of Total Events is zero, or the number increases and the problem persists, contact Support.</td>
</tr>
<tr>
<td>SMST</td>
<td>Log Monitor State</td>
<td>If the value of Log Monitor State is not Connected for a persistent period of time, contact Support.</td>
</tr>
<tr>
<td>SNST</td>
<td>Status</td>
<td>An alarm indicates that there is a problem storing the grid task bundles. If the value of Status is Checkpoint Error or Quorum Not Reached, confirm that a majority of ADC services are connected to the StorageGRID Webscale system (50 percent plus one) and then wait a few minutes. If the problem persists, contact Support.</td>
</tr>
<tr>
<td>SOSS</td>
<td>Storage Operating System Status</td>
<td>An alarm is triggered if SANtricity software indicates that there is a &quot;Needs attention&quot; issue with an E2700 StorageGRID Webscale appliance component. In the NMS MI, SSM ▶ Resources ▶ Overview page, check the power supply statuses. In SANtricity, check other appliance components to isolate the issue.</td>
</tr>
</tbody>
</table>
### Alarms reference

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSMA</td>
<td>SSM Status</td>
<td>If the value of SSM Status is Error, check the SSM ➤ Overview ➤ Main and SSM ➤ Overview ➤ Alarms pages to determine the cause of the alarm. If the problem persists, contact Support.</td>
</tr>
<tr>
<td>SSME</td>
<td>SSM State</td>
<td>If the value of SSM State is Standby, continue monitoring and if the problem persists, contact Support. If the value of SSM State is Offline, restart the service. If the problem persists, contact Support.</td>
</tr>
<tr>
<td>SSTS</td>
<td>Storage Status</td>
<td>If the value of Storage Status is Insufficient Usable Space, there is no more available storage on the Storage Node and data ingests are redirected to other available Storage Node. Retrieval requests can continue to be delivered from this grid node. Additional storage should be added. It is not impacting end user functionality, but the alarm persists until additional storage is added. If the value of Storage Status is Volume(s) Unavailable, a part of the storage is unavailable. Storage and retrieval from these volumes is not possible. Check the volume’s Health for more information (see LDR ➤ Storage ➤ Overview ➤ Main under Object Stores). If the value of Storage Status is Error, contact Support.</td>
</tr>
<tr>
<td>SUOP</td>
<td>Operations Not Committed</td>
<td>If the problem persists, contact Support.</td>
</tr>
</tbody>
</table>
This alarm clears when other alarms related to a non-running service are resolved. Track the source service alarms to restore operation.

A service is listed at SSM ► Services ► Overview ► Main under Services with a Status of Not Running when its state is Administratively Down. The service’s Status can be listed as Not Running for the following reasons:

- The service has been manually stopped (/etc/init.d/<service> stop)
- There is an issue with the MySQL database and Server Manager shuts down the MI service
- A grid node has been added, but not started
- During installation, a grid node has not yet connected to the Admin Node

If a service is listed as Not Running, restart the service (/etc/init.d/<service> restart)

This alarm may also be an indication that the DDS service’s distributed key value store (Cassandra database) for a Storage Node requires rebuilding. See “SVST (Services: Status - Cassandra) alarm” on page 42.

If the problem persists, contact Support.

### Code | Name | Recommended Action
--- | --- | ---
SVST | Status | This alarm clears when other alarms related to a non-running service are resolved. Track the source service alarms to restore operation.

A service is listed at SSM ► Services ► Overview ► Main under Services with a Status of Not Running when its state is Administratively Down. The service’s Status can be listed as Not Running for the following reasons:

- The service has been manually stopped (/etc/init.d/<service> stop)
- There is an issue with the MySQL database and Server Manager shuts down the MI service
- A grid node has been added, but not started
- During installation, a grid node has not yet connected to the Admin Node

If a service is listed as Not Running, restart the service (/etc/init.d/<service> restart)

This alarm may also be an indication that the DDS service’s distributed key value store (Cassandra database) for a Storage Node requires rebuilding. See “SVST (Services: Status - Cassandra) alarm” on page 42.

If the problem persists, contact Support.

### Code | Name | Recommended Action
--- | --- | ---
SVST | Status | This alarm clears when other alarms related to a non-running service are resolved. Track the source service alarms to restore operation.

A service is listed at SSM ► Services ► Overview ► Main under Services with a Status of Not Running when its state is Administratively Down. The service’s Status can be listed as Not Running for the following reasons:

- The service has been manually stopped (/etc/init.d/<service> stop)
- There is an issue with the MySQL database and Server Manager shuts down the MI service
- A grid node has been added, but not started
- During installation, a grid node has not yet connected to the Admin Node

If a service is listed as Not Running, restart the service (/etc/init.d/<service> restart)

This alarm may also be an indication that the DDS service’s distributed key value store (Cassandra database) for a Storage Node requires rebuilding. See “SVST (Services: Status - Cassandra) alarm” on page 42.

If the problem persists, contact Support.

### Code | Name | Recommended Action
--- | --- | ---
SVST | Status | This alarm clears when other alarms related to a non-running service are resolved. Track the source service alarms to restore operation.

A service is listed at SSM ► Services ► Overview ► Main under Services with a Status of Not Running when its state is Administratively Down. The service’s Status can be listed as Not Running for the following reasons:

- The service has been manually stopped (/etc/init.d/<service> stop)
- There is an issue with the MySQL database and Server Manager shuts down the MI service
- A grid node has been added, but not started
- During installation, a grid node has not yet connected to the Admin Node

If a service is listed as Not Running, restart the service (/etc/init.d/<service> restart)

This alarm may also be an indication that the DDS service’s distributed key value store (Cassandra database) for a Storage Node requires rebuilding. See “SVST (Services: Status - Cassandra) alarm” on page 42.

If the problem persists, contact Support.
VMFR  Space Available

If the value of Space Available gets too low (see alarm thresholds), it needs to be investigated as to whether there are log files growing out of proportion, or objects taking up too much disk space (see alarm thresholds) that need to be reduced or deleted.

If the problem persists, contact Support.

VMST  Status

An alarm is triggered if the value of Status for the mounted volume is Unknown. A value of Unknown or Offline can indicate that the volume cannot be mounted or accessed due to a problem with the underlying storage device.

VPRI  Verification Priority

By default, the value of Verification Priority is Adaptive. If Verification Priority is set to High, an alarm is triggered because storage verification can slow normal operations of the service.

VSTU  Object Verification Status

Look for other problems on LDR ► Verification ► Overview ► Main.

If the value of Object Verification Status is Verify Location Synchronize Failed, check that the LDR service is connected to at least one CMS service.

Also check the operating system for any signs of block-device or file system errors.

If the value of Object Verification Status is Maximum Number of Failures Reached, it usually indicates a low-level file system or hardware problem (I/O error) that prevents the Storage Verification task from accessing stored content. This alarm can also occur when there is a high number of content errors indicating that data was invalid.

If the value of Object Verification Status is Unknown Error, contact Support.

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>XAMS</td>
<td>Unreachable Audit Repositories</td>
<td>Check network connectivity to the server hosting the Admin Node.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the problem persists, contact Support.</td>
</tr>
</tbody>
</table>
Log files

A listing of the main application log files and an explanation of bycast.log

Application log files

The following sections list the logs used to capture events, diagnostic messages, and error conditions. You might be asked to forward these log files to Support to assist with troubleshooting.

The StorageGRID Webscale log files can be categorized as:
• StorageGRID Webscale software log files
• deployment log files
• third-party software log files

For a description of the audit log, see the Audit Message Reference.

Table 10 to Table 12 below list the logs in each category. These tables are for reference only. The logs are intended for advanced troubleshooting by Support. Advanced techniques that involve reconstructing the problem history using the audit logs and the application log files are beyond the scope of this guide. For more information about retrieving log files, see “Gather application log files and system data” on page 18.
# StorageGRID Webscale software logs

## Table 10: StorageGRID Webscale Software Logs

<table>
<thead>
<tr>
<th>Category</th>
<th>File Name</th>
<th>Notes</th>
<th>Found On</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td>/var/local/log/bycast.log</td>
<td>The file bycast.log is the primary StorageGRID Webscale troubleshooting file. The file bycast-err.log contains a subset of bycast.log (messages with severity ERROR and CRITICAL). CRITICAL messages are also displayed in the NMS MI under SSM ▶ Events. For more information, see “About the bycast.log” on page 81.</td>
<td>All grid nodes</td>
</tr>
<tr>
<td></td>
<td>/var/local/log/bycast-err.log</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>/var/local/core/</td>
<td>Contains any core dump files created if the program terminates abnormally. Possible causes include assertion failures, violations, or thread timeouts.</td>
<td></td>
</tr>
<tr>
<td><strong>Server Manager</strong></td>
<td>/var/local/log/servermanager.log</td>
<td>Log file for the Server Manager application running on the server.</td>
<td>All grid nodes</td>
</tr>
<tr>
<td></td>
<td>/var/local/log/GridstatBackend.errlog</td>
<td>Log file for the Server Manager GUI backend application.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>/var/local/log/gridstat.errlog</td>
<td>Log file for the Server Manager GUI.</td>
<td></td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td>/var/local/log/adc.errlog</td>
<td>Contains the Standard Error (stderr) stream of the corresponding services. There is one log file per service. These files are generally empty unless there are problems with the service.</td>
<td>Storage Node</td>
</tr>
<tr>
<td></td>
<td>/var/local/log/ams.errlog</td>
<td></td>
<td>Admin Node</td>
</tr>
<tr>
<td></td>
<td>/var/local/log/arc.errlog</td>
<td></td>
<td>Archive Node</td>
</tr>
<tr>
<td></td>
<td>/var/local/log/clb.errlog</td>
<td></td>
<td>API Gateway Node</td>
</tr>
<tr>
<td></td>
<td>/var/local/log/cmn.errlog</td>
<td></td>
<td>Admin Node</td>
</tr>
<tr>
<td></td>
<td>/var/local/log/cms.errlog</td>
<td></td>
<td>Storage Node</td>
</tr>
<tr>
<td></td>
<td>/var/local/log/cts.errlog</td>
<td></td>
<td>Archive Node</td>
</tr>
<tr>
<td></td>
<td>/var/local/log/dds.errlog</td>
<td></td>
<td>Storage Node</td>
</tr>
<tr>
<td></td>
<td>/var/local/log/ldr.errlog</td>
<td></td>
<td>Storage Node</td>
</tr>
<tr>
<td></td>
<td>/var/local/log/nms.errlog</td>
<td></td>
<td>Admin Node</td>
</tr>
<tr>
<td></td>
<td>/var/local/log/ssm.errlog</td>
<td></td>
<td>All grid nodes</td>
</tr>
<tr>
<td>Category</td>
<td>File Name</td>
<td>Notes</td>
<td>Found On</td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>NMS</td>
<td>/var/local/log/nms.log</td>
<td>Captures events related to the operation of the NMS service, for example, alarm processing, e-mail notifications, and configuration changes. Contains XML bundle updates resulting from configuration changes made in the NMS MI. Contains error messages related to the attribute downsampling done once a day. Contains Java web server error messages, for example, page generation errors and HTTP Status 500 errors.</td>
<td>Admin Node</td>
</tr>
<tr>
<td></td>
<td>/var/local/log/nms.errlog</td>
<td>Contains error messages related to MySQL database upgrades. Contains the Standard Error (stderr) stream of the corresponding services. There is one log file per service. These files are generally empty unless there are problems with the service.</td>
<td></td>
</tr>
</tbody>
</table>
Deployment logs

Table 11: Deployment Logs

<table>
<thead>
<tr>
<th>Category</th>
<th>File Name</th>
<th>Notes</th>
<th>Found On</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>StorageGRID Webscale Installer (SGI)</strong></td>
<td>/var/local/log/sgi.log</td>
<td>Log file created when the SGI is installed. Contains SGI error information.</td>
<td>SGI virtual machine</td>
</tr>
<tr>
<td><strong>Installation</strong></td>
<td>/var/local/log/install.log</td>
<td>Log file created during software installation. Contains a record of the installation events and software update events.</td>
<td>All grid nodes</td>
</tr>
<tr>
<td><strong>Grid Deployment Utility (GDU)</strong></td>
<td>/var/local/log/gdu-console.log</td>
<td>Log file created by the GDU program. Lists actions taken by the various GDU tasks; for example, all tasks performed by the Update IP Configuration task are listed.</td>
<td>Primary Admin Node</td>
</tr>
<tr>
<td><strong>Provisioning</strong></td>
<td>provision-fail.log</td>
<td>Log file created if the provisioning program detects an error in the grid specification file.</td>
<td>Provisioning media</td>
</tr>
<tr>
<td></td>
<td>provision-crash-&lt;grid_info&gt;.log</td>
<td>Log file created if the provisioning program terminates abnormally. &lt;grid_info&gt; includes the grid ID, the grid revision being created and a timestamp.</td>
<td></td>
</tr>
</tbody>
</table>

Third-party logs

Table 12: Logs for Third-Party Software

<table>
<thead>
<tr>
<th>Category</th>
<th>File Name</th>
<th>Notes</th>
<th>Found On</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Archiving</strong></td>
<td>/var/local/log/dsierror.log</td>
<td>Contains error information for TSM Client APIs.</td>
<td>Archive Node</td>
</tr>
<tr>
<td><strong>Cassandra</strong></td>
<td>/var/local/log/cassandra/system.log</td>
<td>Contains error information for Cassandra that can be used if problems occur when adding new Storage Nodes.</td>
<td>Storage Node</td>
</tr>
</tbody>
</table>
Table 12: Logs for Third-Party Software (cont.)

<table>
<thead>
<tr>
<th>Category</th>
<th>File Name</th>
<th>Notes</th>
<th>Found On</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>/var/local/log/mysql.err</td>
<td>Log files generated by MySQL.</td>
<td>Admin Node</td>
</tr>
<tr>
<td></td>
<td>/var/local/log/mysql-slow.log</td>
<td>The file mysql.err captures database errors and events such as startups and shutdowns. The file mysql-slow.log (the slow query log) captures the SQL statements that took more than 10 seconds to execute.</td>
<td></td>
</tr>
<tr>
<td>Operating system</td>
<td>/var/log/messages</td>
<td>This directory contains log files for the operating system. The errors contained in these logs are also displayed in the NMS MI under SSM Events.</td>
<td>All grid nodes</td>
</tr>
<tr>
<td>NTP</td>
<td>/var/log/ntp</td>
<td>Log file for NTP error messages.</td>
<td>All grid nodes</td>
</tr>
<tr>
<td></td>
<td>/var/lib/ntp/ntp/var/log/ntpstats/</td>
<td>The directory that contains NTP timing statistics. loopstats records loop filter statistics information. peerstats records peer statistics information.</td>
<td></td>
</tr>
<tr>
<td>SNMP Monitoring</td>
<td>/var/log/net-snmpd.log</td>
<td>Used by the NMS service for SNMP monitoring of system status as well as third party hardware monitoring tools using SNMP.</td>
<td>All grid nodes</td>
</tr>
<tr>
<td>Samba</td>
<td>/var/local/log/samba/</td>
<td>The Samba log directory includes a log file for each Samba process (smb, nmb, and winbind) and every client hostname/IP.</td>
<td>API Gateway Node Admin Node configured to export the audit share over CIFS</td>
</tr>
</tbody>
</table>

About the bycast.log

The file /var/local/log/bycast.log is the primary troubleshooting file for the StorageGRID Webscale software. There is a bycast.log file for every grid node. The file contains messages specific to that grid node.
The file `/var/local/log/bycast-err.log` is a subset of `bycast.log`. It contains messages of severity `ERROR` and `CRITICAL`.

**Log file rotation**

The `bycast.log` file is rotated when the file size reaches one GB. The archived log file is then compressed with a delay of one file.

For example, when `bycast.log` reaches one GB, the file is renamed `bycast.log.1` and a new `bycast.log` file is started. Once the new `bycast.log` reaches one GB, `bycast.log.1` is renamed and compressed to become `bycast.log.2.gz`, and `bycast.log` is renamed `bycast.log.1`.

**NOTE** Log files that are compressed due to log rotation should not be uncompressed on the server to which they are written as this can interfere with the log rotation scripts. To examine the contents of a compressed log file, see “Gather application log files and system data” on page 18.

**Message description**

Messages in `bycast.log` are written by the ADE (Asynchronous Distributed Environment) and by the CMS service. ADE is the runtime environment used by the each grid node’s services. This is an example of an ADE message:

Oct 7 14:07:11 um-sec-rg1-agn3 ADE: |12296889 29741 000055 SVMR EVHR 2008-09-27T17:10:29.784677| ERROR 0906 SVMR: Health check on volume 3 has failed with reason 'TOUT'

ADE messages contain the following:

- Node ID (12296889 in the example)
- Thread ID (29741 in the example)
- ADE process ID (000055 in the example)
- Module name (SVMR in the example)
- Message identifier (EVHR in the example)
- UTC system time (YYYY-MM-DDTHH:MM:SS.uuuuuu)
- Severity level (ERROR in the example)
- Message
Severity level

ADE log messages in bycast.log are assigned severity levels. For example:

- **NOTICE**: An event that should be recorded has occurred. Most log messages are at this level.
- **WARNING**: An unexpected condition has occurred.
- **ERROR**: A major error has occurred that will impact operations.
- **CRITICAL**: A service has stopped because of a critical error resulting from a software or hardware issue. Critical messages are also displayed in the NMS MI under SSM ▶ Events.

Error codes

Most ADE error messages contain error codes. Table 13 below lists common non-numerical codes and Table 14 lists the numerical error codes. The exact meaning of a non-numerical code depends on the context in which it is reported.

**Table 13: Common Error Codes in bycast.log**

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUCS</td>
<td>No error</td>
</tr>
<tr>
<td>GERR</td>
<td>Unknown</td>
</tr>
<tr>
<td>CANC</td>
<td>Canceled</td>
</tr>
<tr>
<td>ABRT</td>
<td>Aborted</td>
</tr>
<tr>
<td>TOUT</td>
<td>Timeout</td>
</tr>
<tr>
<td>INVL</td>
<td>Invalid</td>
</tr>
<tr>
<td>NFND</td>
<td>Not found</td>
</tr>
<tr>
<td>VERS</td>
<td>Version</td>
</tr>
<tr>
<td>CONF</td>
<td>Configuration</td>
</tr>
<tr>
<td>FAIL</td>
<td>Failed</td>
</tr>
<tr>
<td>ICPL</td>
<td>Incomplete</td>
</tr>
<tr>
<td>DONE</td>
<td>Done</td>
</tr>
<tr>
<td>SUNV</td>
<td>Service unavailable</td>
</tr>
<tr>
<td>Error Number</td>
<td>Error Code</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>001</td>
<td>EPERM</td>
</tr>
<tr>
<td>002</td>
<td>ENOENT</td>
</tr>
<tr>
<td>003</td>
<td>ESRCH</td>
</tr>
<tr>
<td>004</td>
<td>EINTR</td>
</tr>
<tr>
<td>005</td>
<td>EIO</td>
</tr>
<tr>
<td>006</td>
<td>ENXIO</td>
</tr>
<tr>
<td>007</td>
<td>E2BIG</td>
</tr>
<tr>
<td>008</td>
<td>ENOEXEC</td>
</tr>
<tr>
<td>009</td>
<td>EBADF</td>
</tr>
<tr>
<td>010</td>
<td>ECHILD</td>
</tr>
<tr>
<td>011</td>
<td>EAGAIN</td>
</tr>
<tr>
<td>012</td>
<td>ENOMEM</td>
</tr>
<tr>
<td>013</td>
<td>EACCES</td>
</tr>
<tr>
<td>014</td>
<td>EFAULT</td>
</tr>
<tr>
<td>015</td>
<td>ENOTBLK</td>
</tr>
<tr>
<td>016</td>
<td>EBUSY</td>
</tr>
<tr>
<td>017</td>
<td>EEXIST</td>
</tr>
<tr>
<td>018</td>
<td>EXDEV</td>
</tr>
<tr>
<td>019</td>
<td>ENODEV</td>
</tr>
<tr>
<td>020</td>
<td>ENOTDIR</td>
</tr>
<tr>
<td>021</td>
<td>EISDIR</td>
</tr>
<tr>
<td>022</td>
<td>EINVAL</td>
</tr>
<tr>
<td>023</td>
<td>ENFILE</td>
</tr>
<tr>
<td>024</td>
<td>EMFILE</td>
</tr>
<tr>
<td>025</td>
<td>ENOTTY</td>
</tr>
<tr>
<td>026</td>
<td>ETXTBSY</td>
</tr>
<tr>
<td>027</td>
<td>EFBIG</td>
</tr>
<tr>
<td>028</td>
<td>ENOSPC</td>
</tr>
</tbody>
</table>
Table 14: Numerical Error Codes in bycast.log (cont.)

<table>
<thead>
<tr>
<th>Error Number</th>
<th>Error Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>029</td>
<td>ESPIPE</td>
<td>Illegal seek</td>
</tr>
<tr>
<td>030</td>
<td>EROFS</td>
<td>Read-only file system</td>
</tr>
<tr>
<td>031</td>
<td>EMLINK</td>
<td>Too many links</td>
</tr>
<tr>
<td>032</td>
<td>EPIPE</td>
<td>Broken pipe</td>
</tr>
<tr>
<td>033</td>
<td>EDOM</td>
<td>Math argument out of domain of func</td>
</tr>
<tr>
<td>034</td>
<td>ERANGE</td>
<td>Math result not representable</td>
</tr>
<tr>
<td>035</td>
<td>EDEADLK</td>
<td>Resource deadlock would occur</td>
</tr>
<tr>
<td>036</td>
<td>ENAMETOOLONG</td>
<td>File name too long</td>
</tr>
<tr>
<td>037</td>
<td>ENOLCK</td>
<td>No record locks available</td>
</tr>
<tr>
<td>038</td>
<td>ENOSYS</td>
<td>Function not implemented</td>
</tr>
<tr>
<td>039</td>
<td>ENOTEMPTY</td>
<td>Directory not empty</td>
</tr>
<tr>
<td>040</td>
<td>ELOOP</td>
<td>Too many symbolic links encountered</td>
</tr>
<tr>
<td>042</td>
<td>ENOMSG</td>
<td>No message of desired type</td>
</tr>
<tr>
<td>043</td>
<td>EIDRM</td>
<td>Identifier removed</td>
</tr>
<tr>
<td>044</td>
<td>ECHRNG</td>
<td>Channel number out of range</td>
</tr>
<tr>
<td>045</td>
<td>EL2NSYNC</td>
<td>Level 2 not synchronized</td>
</tr>
<tr>
<td>046</td>
<td>EL3HLT</td>
<td>Level 3 halted</td>
</tr>
<tr>
<td>047</td>
<td>EL3RST</td>
<td>Level 3 reset</td>
</tr>
<tr>
<td>048</td>
<td>ELNRNG</td>
<td>Link number out of range</td>
</tr>
<tr>
<td>049</td>
<td>EUNATCH</td>
<td>Protocol driver not attached</td>
</tr>
<tr>
<td>050</td>
<td>ENOCSI</td>
<td>No CSI structure available</td>
</tr>
<tr>
<td>051</td>
<td>EL2HLT</td>
<td>Level 2 halted</td>
</tr>
<tr>
<td>052</td>
<td>EBADE</td>
<td>Invalid exchange</td>
</tr>
<tr>
<td>053</td>
<td>EBADR</td>
<td>Invalid request descriptor</td>
</tr>
<tr>
<td>054</td>
<td>EXFULL</td>
<td>Exchange full</td>
</tr>
<tr>
<td>055</td>
<td>ENOANO</td>
<td>No anode</td>
</tr>
</tbody>
</table>
Table 14: Numerical Error Codes in bycast.log (cont.)

<table>
<thead>
<tr>
<th>Error Number</th>
<th>Error Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>056</td>
<td>EBADRQC</td>
<td>Invalid request code</td>
</tr>
<tr>
<td>057</td>
<td>EBADSLT</td>
<td>Invalid slot</td>
</tr>
<tr>
<td>059</td>
<td>EBFONT</td>
<td>Bad font file format</td>
</tr>
<tr>
<td>060</td>
<td>ENOSTR</td>
<td>Device not a stream</td>
</tr>
<tr>
<td>061</td>
<td>ENODATA</td>
<td>No data available</td>
</tr>
<tr>
<td>062</td>
<td>ETIME</td>
<td>Timer expired</td>
</tr>
<tr>
<td>063</td>
<td>ENOSR</td>
<td>Out of streams resources</td>
</tr>
<tr>
<td>064</td>
<td>ENONET</td>
<td>Machine is not on the network</td>
</tr>
<tr>
<td>065</td>
<td>ENOPKG</td>
<td>Package not installed</td>
</tr>
<tr>
<td>066</td>
<td>EREMOTE</td>
<td>Object is remote</td>
</tr>
<tr>
<td>067</td>
<td>ENOLINK</td>
<td>Link has been severed</td>
</tr>
<tr>
<td>068</td>
<td>EADV</td>
<td>Advertise error</td>
</tr>
<tr>
<td>069</td>
<td>ESRMNT</td>
<td>Srmount error</td>
</tr>
<tr>
<td>070</td>
<td>ECOMM</td>
<td>Communication error on send</td>
</tr>
<tr>
<td>071</td>
<td>EPROTO</td>
<td>Protocol error</td>
</tr>
<tr>
<td>072</td>
<td>EMULTIHOP</td>
<td>Multihop attempted</td>
</tr>
<tr>
<td>073</td>
<td>EDOTDOT</td>
<td>RFS specific error</td>
</tr>
<tr>
<td>074</td>
<td>EBADMSG</td>
<td>Not a data message</td>
</tr>
<tr>
<td>075</td>
<td>EOVERFLOW</td>
<td>Value too large for defined data type</td>
</tr>
<tr>
<td>076</td>
<td>ENOTUNIQ</td>
<td>Name not unique on network</td>
</tr>
<tr>
<td>077</td>
<td>EBADFD</td>
<td>File descriptor in bad state</td>
</tr>
<tr>
<td>078</td>
<td>EREMCHG</td>
<td>Remote address changed</td>
</tr>
<tr>
<td>079</td>
<td>ELIBBACC</td>
<td>Can not access a needed shared library</td>
</tr>
<tr>
<td>080</td>
<td>ELIBBAD</td>
<td>Accessing a corrupted shared library</td>
</tr>
<tr>
<td>081</td>
<td>ELIBSCN</td>
<td>.lib section in a.out corrupted</td>
</tr>
<tr>
<td>082</td>
<td>ELIBMAX</td>
<td>Attempting to link in too many shared libraries</td>
</tr>
</tbody>
</table>
Table 14: Numerical Error Codes in bycast.log (cont.)

<table>
<thead>
<tr>
<th>Error Number</th>
<th>Error Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>083</td>
<td>ELIBEXEC</td>
<td>Cannot exec a shared library directly</td>
</tr>
<tr>
<td>084</td>
<td>EILSEQ</td>
<td>Illegal byte sequence</td>
</tr>
<tr>
<td>085</td>
<td>ERESTART</td>
<td>Interrupted system call should be restarted</td>
</tr>
<tr>
<td>086</td>
<td>ESTRPIPE</td>
<td>Streams pipe error</td>
</tr>
<tr>
<td>087</td>
<td>EUSERS</td>
<td>Too many users</td>
</tr>
<tr>
<td>088</td>
<td>ENOTSOCK</td>
<td>Socket operation on non-socket</td>
</tr>
<tr>
<td>089</td>
<td>EDESTADDRREQ</td>
<td>Destination address required</td>
</tr>
<tr>
<td>090</td>
<td>EMSGSIZE</td>
<td>Message too long</td>
</tr>
<tr>
<td>091</td>
<td>EPROTOTYPE</td>
<td>Protocol wrong type for socket</td>
</tr>
<tr>
<td>092</td>
<td>ENOPROTOOPT</td>
<td>Protocol not available</td>
</tr>
<tr>
<td>093</td>
<td>EPROTONOSUP-PORT</td>
<td>Protocol not supported</td>
</tr>
<tr>
<td>094</td>
<td>ESOCKTNOSUP-PORT</td>
<td>Socket type not supported</td>
</tr>
<tr>
<td>095</td>
<td>EOPNOTSUPP</td>
<td>Operation not supported on transport endpoint</td>
</tr>
<tr>
<td>096</td>
<td>EPFNOSUPPORT</td>
<td>Protocol family not supported</td>
</tr>
<tr>
<td>097</td>
<td>EAFNOSUPPORT</td>
<td>Address family not supported by protocol</td>
</tr>
<tr>
<td>098</td>
<td>EADDRINUSE</td>
<td>Address already in use</td>
</tr>
<tr>
<td>099</td>
<td>EADDRNOTAVAIL</td>
<td>Cannot assign requested address</td>
</tr>
<tr>
<td>100</td>
<td>ENETDOWN</td>
<td>Network is down</td>
</tr>
<tr>
<td>101</td>
<td>ENETUNREACH</td>
<td>Network is unreachable</td>
</tr>
<tr>
<td>102</td>
<td>ENETRESET</td>
<td>Network dropped connection because of reset</td>
</tr>
<tr>
<td>103</td>
<td>ECONNABORTED</td>
<td>Software caused connection abort</td>
</tr>
<tr>
<td>104</td>
<td>ECONNRESET</td>
<td>Connection reset by peer</td>
</tr>
<tr>
<td>105</td>
<td>ENOBUFNS</td>
<td>No buffer space available</td>
</tr>
</tbody>
</table>
### Table 14: Numerical Error Codes in bycast.log (cont.)

<table>
<thead>
<tr>
<th>Error Number</th>
<th>Error Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>106</td>
<td>EISCONN</td>
<td>Transport endpoint is already connected</td>
</tr>
<tr>
<td>107</td>
<td>ENOTCONN</td>
<td>Transport endpoint is not connected</td>
</tr>
<tr>
<td>108</td>
<td>ESHUTDOWN</td>
<td>Cannot send after transport endpoint shutdown</td>
</tr>
<tr>
<td>109</td>
<td>ETOOMANYREFS</td>
<td>Too many references: cannot splice</td>
</tr>
<tr>
<td>110</td>
<td>ETIMEDOUT</td>
<td>Connection timed out</td>
</tr>
<tr>
<td>111</td>
<td>ECONNREFUSED</td>
<td>Connection refused</td>
</tr>
<tr>
<td>112</td>
<td>EHOSTDOWN</td>
<td>Host is down</td>
</tr>
<tr>
<td>113</td>
<td>EHOSTUNREACH</td>
<td>No route to host</td>
</tr>
<tr>
<td>114</td>
<td>EALREADY</td>
<td>Operation already in progress</td>
</tr>
<tr>
<td>115</td>
<td>EINPROGRESS</td>
<td>Operation now in progress</td>
</tr>
<tr>
<td>117</td>
<td>EUCLEAN</td>
<td>Structure needs cleaning</td>
</tr>
<tr>
<td>118</td>
<td>ENOTNAM</td>
<td>Not a XENIX named type file</td>
</tr>
<tr>
<td>119</td>
<td>ENAVAIL</td>
<td>No XENIX semaphores available</td>
</tr>
<tr>
<td>120</td>
<td>EISNAM</td>
<td>Is a named type file</td>
</tr>
<tr>
<td>121</td>
<td>EREMOTEIO</td>
<td>Remote I/O error</td>
</tr>
<tr>
<td>122</td>
<td>EDQUOT</td>
<td>Quota exceeded</td>
</tr>
<tr>
<td>123</td>
<td>ENOMEDIUM</td>
<td>No medium found</td>
</tr>
<tr>
<td>124</td>
<td>EEMEDIUMTYPE</td>
<td>Wrong medium type</td>
</tr>
<tr>
<td>125</td>
<td>ECANCELED</td>
<td>Operation Canceled</td>
</tr>
<tr>
<td>126</td>
<td>ENOKEY</td>
<td>Required key not available</td>
</tr>
<tr>
<td>127</td>
<td>EKEYEXPIRED</td>
<td>Key has expired</td>
</tr>
<tr>
<td>128</td>
<td>EKEYREVOKED</td>
<td>Key has been revoked</td>
</tr>
<tr>
<td>129</td>
<td>EKEYREJECTED</td>
<td>Key was rejected by service</td>
</tr>
<tr>
<td>130</td>
<td>EOWNERDEAD</td>
<td>For robust mutexes: Owner died</td>
</tr>
<tr>
<td>131</td>
<td>ENOTRECOVERABLE</td>
<td>For robust mutexes: State not recoverable</td>
</tr>
</tbody>
</table>
Copyright information

Copyright © 1994–2015 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, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, FAServer, FastStak, FilerView, FlexCache, FlexClone, FlexPod, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtrecity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, 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.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.
How to send comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. 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.

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
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 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 the “primary Admin Node” definition.

**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 “CLB service” service.

**ARC service**
Archive—Communicates with an external archive service to store objects in and retrieve objects from the archive. The ARC service is present on the Archive Node.

**Archive Node**
An Archive Node manages the storage of objects to, and retrieval of objects from, external archive services. Archive Nodes can be configured to work with Amazon Simple Storage Service (S3) or Tivoli Storage Manager (TSM).

**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 the “Admin Node” definition.

**bundle** A structured collection of configuration information used internally by various components of the StorageGRID Webscale system. Bundles are structured in container format.

**Cassandra** An open-source database that is scalable and distributed, provides high availability, and handles large amounts of data across multiple servers.

**CBID** Content Block Identifier — A unique internal identifier of a piece of content within the StorageGRID Webscale system.

**CDMI** Cloud Data Management Interface — An industry standard defined by SNIA that includes a RESTful interface for object storage. For more information, see [www.snia.org/cdmi](http://www.snia.org/cdmi).

**CIDR** Classless Inter-Domain Routing — A notation used to compactly describe a subnet mask used to define a range of IP addresses. In CIDR notation, the subnet mask is expressed as an IP address in dotted decimal notation, followed by a slash and the number of bits in the subnet. For example, 192.0.2.0/24.

**CLB service** Connection Load Balancer — The CLB service provides a gateway into the StorageGRID Webscale system for client applications connecting through HTTP. The CLB service is part of the API Gateway Node.

**Cloud Data Management Interface** See “CDMI” on page 96.
CMN service  
Configuration Management Node—The CMN service manages system-wide configuration 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 — 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 the “CBID” definition.

content handle  
See the “UUID” definition.

CSTR  
Null-terminated, variable length string.

data fragment  
An erasure coded chunk of object data. See the “erasure code” definition.

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** | The Enablement Layer is 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. |
| **erasure code** | A object data protection scheme that parses object data into data and parity fragments. See also the “data fragment” and “parity fragment” definitions. |
| **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 the “Task Signed Text Block” definition. |
HTTP  Hyper-Text Transfer Protocol—A simple, text based client/protocol for requesting hypertext documents from a server.

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 the “Admin Node” and “storage pool” definitions.

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. Contrast with WAN.

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 the “throughput” definition.

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 the “object store” definition.

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” definitions.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NMS MI</td>
<td>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” definition.</td>
</tr>
<tr>
<td>node ID</td>
<td>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.</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol—A protocol used to synchronize distributed clocks over a variable latency network such as the internet.</td>
</tr>
<tr>
<td>object</td>
<td>An artificial construct used to describe a system that divides content into data and metadata.</td>
</tr>
<tr>
<td>object storage</td>
<td>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).</td>
</tr>
<tr>
<td>object store</td>
<td>A configured file system on a disk volume. The configuration includes a specific directory structure and resources initialized at system installation.</td>
</tr>
</tbody>
</table>
| 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 the “segment container” definition. |
| OID           | Object Identifier—The unique identifier of an object.                                                                                        |
| parity fragment | An erasure coded chunk containing information that can be used to reconstruct object data if data fragments are lost. See the “erasure code” definition. |
| primary
  Admin Node  | Admin Node that hosts the CMN service. There is one per StorageGRID Webscale system. See also the “Admin Node” definition.                  |
provisioning  The process of generating a SAID package and GPT repository. This is done on the primary Admin Node using the provision command. The new or updated SAID package is saved to the Provisioning Media. See also the “grid specification file” and “SAID” definitions.

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 the “object segmentation” definitions.

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 LDR or CLB service.
<p>| <strong>SLES</strong> | SUSE Linux Enterprise Server — A commercial distribution of the SUSE Linux operating system, used with the StorageGRID Webscale system. |
| <strong>SQL</strong> | Structured Query Language — An industry standard interface language for managing relational databases. An SQL database is one that supports the SQL interface. |
| <strong>ssh</strong> | 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. |
| <strong>SSM</strong> | 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. |
| <strong>SSL</strong> | Secure Socket Layer — The original cryptographic protocol used to enable secure communications over the internet. See also the “TLS” definition. |
| <strong>Storage Node</strong> | The Storage Node provides storage capacity and services to store, move, verify, and retrieve objects stored on disks. |
| <strong>storage pool</strong> | The element of an ILM rule that determines the location where an object is stored. |
| <strong>StorageGRID Webscale</strong> | A registered trademark of NetApp Inc. for their object storage grid architecture and software system. |
| <strong>StorageGRID API</strong> | See the “SGAPI” definition. |
| <strong>storage volume</strong> | See the “object store” definition. |
| <strong>Task Signed Text Block</strong> | A BASE64 encoded block of cryptographically signed data that provides the set of instructions that define a grid task. |
| <strong>TCP/IP</strong> | Transmission Control Protocol / Internet Protocol — A process of encapsulating and transmitting packet data over a network. It includes positive acknowledgment of transmissions. |
| <strong>throughput</strong> | 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 the “latency” definition. |
| <strong>TLS</strong> | Transport Layer Security — A cryptographic protocol used to enable secure communications over the internet. See RFC 2246 for more details. |</p>
<table>
<thead>
<tr>
<th><strong>transfer syntax</strong></th>
<th>The parameters, such as the byte order and compression method, needed to exchange data between systems.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tivoli® Storage Manager</strong></td>
<td>IBM storage middleware product that manages storage and retrieval of data from removable storage resources.</td>
</tr>
<tr>
<td><strong>URI</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>UTC</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>UUID</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>VM</strong></td>
<td>Virtual Machine—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.”</td>
</tr>
<tr>
<td><strong>XFS</strong></td>
<td>A scalable, high performance journaled file system originally developed by Silicon Graphics.</td>
</tr>
<tr>
<td><strong>WAN</strong></td>
<td>Wide Area Network—A network of interconnected computers that covers a large geographic area such as a country. Contrast with the “LAN” definition.</td>
</tr>
<tr>
<td><strong>XML</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
Index

Symbols
/var/local/core 78
/var/log/ 78
/var/log/messages 81
/var/log/ntp 81

A
ABRL Available Attribute Relay alarm 53
ABRT error code 83
ACLs defined 95
ACMS Available Metadata Services alarm 53
ACTS Archive Node State alarm 54
ADC defined 95
ADC Device State ADCE alarm 54
ADC Device Status ADCA alarm 54
adc.errlog 78
ADCA ADC Device Status alarm 54
ADCE ADC Device State alarm 54
ADE 82 defined 95
ADE log messages. See bycast.log
Admin Node log files 79, 80, 81 troubleshooting 29–30 unavailable 30
Admin Nodes defined 95
AITE Archive Retrieve State alarm 54
AITU Archive Retrieve Status alarm 54
alarms by code
ABRL Available Attribute Relay 53
ACMS Available Metadata Services 53
ACTS 54
ADCA ADC Device Status 54
ADCE ADC Device State 54
AITE Archive Retrieve State 54
AITU Archive Retrieve Status 54
ALIS Inbound Attribute Sessions 55
ALOS Outbound Attribute Sessions 55
ALUR Unreachable Attribute Repositories 55
AMQS Audit Messages Queued 55
AOTE Archive Store State 55
AOTU Archive Store Status 56
ARCE ARC State 56
ARQ Objects Queued 56
ARR Remaining Capacity 56
ARRF Request Failures 57
ARRS Repository Status 57
ARRV Verification Failures 57
ARVF Store Failures 57
ASX Audit Share Exported 57
AUMA AMS Status 58
AUME AMS State 58
AUXS Audit Export Status 58
BASF Available Object Identifiers 59
BASS Status 59
BRDT Status 59
BTSE Clock State 60
CACES Connection Status 60
CAHP Java Heap Usage Percent 60
CAIH Available Ingest Destinations 60
CAQH Available Q/R Destinations 60
CDLP Data Load (Percent) 61
CLB Application/CDM State 61
CLBS CLB State 61
CMNA CMN Status 61
CMNE CMN State 61
CMSS CMS State 61
CMST CMS Status 62
CPRC Remaining Capacity 62
CPUT CPU Temperature 62
FOPN Open File Descriptors 62
HSTTE HTTP/CDMI State 63
HSTU HTTP/CDMI Status 63
HTAS Auto-Start HTTP 63
IJSZ Number of Objects 63
IRSU Inbound Replication Status 63
LAT Average Latency 63
LATW Worst Case Latency 64
LDRE LDR Device State 64
LOST Lost objects 64
MINQ E-mail Notifications Queued 64
MINS E-mail Notification Status 64
MISS NMS Interface Engine Status 64
MMQS Peak Message Queue Size 64
NANG Network Auto Negotiate Setting 65
NDUP Network Duplex setting 65
NLNK Network Link Detect 65
NRER Receive Errors 65
NRLY Available Audit Relays 65
NSCA NMS Status 65
NSCE NMS State 66
NSPD Speed 66
NTBR Free Tablespace 66
NTER Transmit Errors 66
NTFQ NTP Frequency Offset 66
NTLK NTP Lock 66
NTOF NTP Time Offset 67
NTSA NTP Sources Available 67
NTSD Chosen Time Source Delay 67
NTSJ Chosen Time Source Jitter 67
NTSO Chosen Time Source Offset 67
NTSU NTP Status 67
OCOR Corrupt Objects Detected 68
OPST Overall Power Status 68
OQRT Objects Quarantined 68
ORSU Outbound Replication Status 68
PBST Backup Status 68
PQFT Page Fault Rate 69
PMEM Service Memory Usage (%) 69
PSAS Power Supply A Status 69
PSAS Power Supply B Status 69
RDTE Archive Middleware State 69
RTU Archive Middleware Status 70

StorageGRID Webscale 10.1 215-09401_A0
RIRF Inbound Replication - Queued 27
RIRF Inbound Replications - Failed 27, 70
RIQR Inbound Replications - Queued 70
RORF Outbound Replications - Failed 27, 28, 71
RORQ Outbound Replication - Queued 27
RORQ Outbound Replications - Queued 71
SAVP Total Usable Space (Percent) 32, 37, 71
SCAS Status 71
SCHR Status 72
SHEL Health 72
SLSA CPU Load Average 72
SMRT Total Events 72
SMST Log Monitor Status 72
SNST Status 72
SOSM Storage Operating System Status 72
SSMA SSM Status 73
SSME SSM State 73
STS Storage Status 34, 73
SUOP Operations not committed 73
SVST Status 74
TPOP Pending operations 74
UMEM Available Memory 74
USWP Available Swap 74
VMFI Entries Available 74
VMFR Space Available 75
VMST Status 75
VPRI Verification Priority 75
VSTU Object Verification Status 75
XAMS Unreachable Audit Repositories 75
disabled 11
history 11
problem determination 10
reviewing 10
System Status button 11
tab 11
alarms reference 53–75
ALIS Inbound Attribute Sessions alarm 55
ALIS Outbound Attribute Sessions alarm 55
ALUR Unreachable Attribute Repositories alarm 55
AMQS Audit Messages Queued alarm 55
AMS defined 95
AMS State AUME alarm 58
AMS Status AUMA alarm 58
ams.errlog 78
AOTE Archive Store State alarm 55
AOTU Archive Store Status alarm 56
API defined 95
API Gateway Node defined 95
application log files 77
ARC defined 95
ARC State ARCE alarm 56
arc.errlog 78
ARCE ARC State alarm 56
Archive Middleware State RDTE alarm 69
Archive Middleware Status RDTU alarm 70
Archive Nodes defined 95
Archive Retrieve State AITE alarm 54
Archive Retrieve Status AITU alarm 54
Archive Store State AOTE alarm 55
Archive Store Status AOTU alarm 56
archiving log files 80
AROQ Objects Queued alarm 56
ARRC Remaining Capacity alarm 56
ARRF Request Failures alarm 57
ARRS Repository Status alarm 57
ARRV Verification Failures alarm 57
ARVF Store Failures alarm 57
ASXP Audit Share Exported alarm 57
Asynchronous Distributed Environment 82
atom defined 95
attributes by code
PSCA Percentage Storage Capacity Used 15
RIRF Inbound Replications - Queued 27, 28
RORQ Outbound Replications - Queued 27, 28
SAVP Total Usable Space (Percent) 32
SLE Last Event attribute 12
STAS Total Usable Space 34
XSC Used Storage Capacity 15
by name
Inbound Replications - Queued 27, 28
Last Event 12
Outbound Replications - Queued 27, 28
Percentage Usable Storage Capacity 15
Total Usable Space 34
Total Usable Space (Percent) 32
Used Storage Capacity 15
Audit Export Status AUSX alarm 58
audit message defined 96
audit messages defined 96
Audit Messages Queued AMQS alarm 55
Audit Share Exported ASXP alarm 57
audit.log 21
AUMA AMS State alarm 58
AUME AMS State alarm 58
Auto-Start HTTP HTAS alarm 63
AutoSupport 14
AutoYaST defined 96
AUXS Audit Export Status alarm 58
Available Attribute Relay ABRL alarm 53
Available Audit Relays NRLY alarm 65
Available Ingest Destinations CAIH alarm 60
Available Memory UMEM alarm 74
Available Metadata Services ACMS alarm 53
Available Object Identifiers BASF alarm 59
Available Q/R Destinations CAQH alarm 60
Available Swap USWP alarm 74
Average Latency LATA alarm 63
average size of ingested objects 15
average size of retrieved objects 15
average storage consumption 15

B
backlogs 27
Backup Status PBST alarm 68
BASE64 defined 96
baseline data 15
BASF Available Object Identifiers alarm 59
BASS Status alarm 59
binding defined 96
BRDT Status alarm 59
BTOP Offset alarm 59
specification files 98
tasks 98
gridstat.errlog 78
GridstatBackend.errlog 78

H
Health SHLH alarm 72
HSTE HTTP/CDMI State alarm 63
HSTU HTTP/CDMI Status alarm 63
HTAS Auto-Start HTTP alarm 63
HTTP defined 99
HTTP/CDMI State alarm 63
HTTP/CDMI Status alarm 63
HTTPS defined 99
Health SHLH alarm 72
HSTE HTTP/CDMI State alarm 63
HSTU HTTP/CDMI Status alarm 63
HTAS Auto-Start HTTP alarm 63
HTTP defined 99
HTTP/CDMI State alarm 63
HTTP/CDMI Status alarm 63
HTTPS defined 99

I
ICPL error code 83
ILM defined 99
impact assessment worksheet 9, 26
Inbound Attribute Sessions ALIS alarm 55
Inbound Replication Status IRSU alarm 63
Inbound Replications - Failed RIRF alarm 70
Inbound Replications - Queued RIRQ alarm 70
Inbound Replications - Queued RIRQ attribute 27, 28
ingest and retrieval test 21
install.log 80
installation log files 80
INVL error code 83
IQSZ Number of Objects alarm 63
IRSU Inbound Replication Status alarm 63

J
Java Heap Usage Percent alarm 60

L
LAN defined 99
Last Event SLLE attribute 12
LATA Average Latency alarm 63
latency defined 99
LAWT Worst Case Latency alarm 64
LDR defined 99
LDR Device State LDRE alarm 64
LDR watermarks 34, 36
ld.errlog 78
LDRE LDR Device State alarm 64
load_cds.py 48
load_cds.py script 48
log files 77–88
archiving 60
bycast.log 81
cassandra 80
gathering 18
GDU 80
general 78
installation 80
lumberjack.rb 18
MySQL 81
NMS 79
NTP 81
operating system 81
provision-crash-log 49
provision-fail.log 49
provisioning 48, 80
retrieve 18
rotation 82
Samba 81
See also
adc log files
Admin Node
AMS log files
API Gateway Node log files
ARC log files
archiving log files
CLB log files
CMN log files
files
GDU log files
heartbeat monitoring log files
installation log files
LDR log files
mysql log files
NMS log files
NTP log files
provisioning log files
Samba log files
Server Manager log files
SSM log files
server manager 78
services 78
SNMP 81
software update 80
log files Storage Node 80
Log Monitor State SMST alarm 72
LOST Lost objects alarm 64
lost objects 37–42
reset attribute 41
lumberjack 18
MINQ E-mail Notifications
Queued alarm 64
MINS E-mail Notification Status alarm 64
MISS NMS Interface Engine Status alarm 64
missing copies 38–42
MMQS Peak Message Queue Size alarm 64
mount_usb_flash_drive script 51
MySQL log files 81
mysql log files 81
mysql.err file 81
mysql-slow.log 81

N
namespace defined 99
NANG Network Auto Negotiate Setting alarm 65
NDUP Network Duplex setting alarm 65
nearline defined 99
Network Auto Negotiate Setting
NANG alarm 65
Network Duplex setting NDUP alarm 65
Network Link Detect NNLK alarm 65
new installation 29
NFND error code 83
NFS defined 99
NLNK Network Link Detect alarm 65
NMS defined 99
NMS Interface Engine Status alarm 64
NMS log files 79
NMS MI connectivity 29, 30 defined 100
unavailable connection 29
NMS State alarm 66
NMS Status alarm 65
nms.errlog 78
nms.errlog.log 79
node ID defined 100
NOTICE severity level, in
bycast.log ADE messages 83
NRER Receive Errors alarm 65
NRLY Available Audit Relays alarm 65
NSCA NMS Status alarm 65
NSCE NMS State alarm 66
NSPD Speed alarm 66
NTBR Free Tablespace alarm 66
NTER Transmit Errors alarm 66

md5sum check 48
metadata defined 99
migration 27
MINQ E-mail Notifications
Queued alarm 64
MINS E-mail Notification Status alarm 64
MISS NMS Interface Engine Status alarm 64
missing copies 38–42
MMQS Peak Message Queue Size alarm 64
mount_usb_flash_drive script 51
MySQL log files 81
mysql log files 81
mysql.err file 81
mysql-slow.log 81

N
namespace
defined 99
NANG Network Auto Negotiate Setting alarm 65
NDUP Network Duplex setting alarm 65
nearline
defined 99
Network Auto Negotiate Setting
NANG alarm 65
Network Duplex setting NDUP alarm 65
Network Link Detect NNLK alarm 65
new installation 29
NFND error code 83
NFS defined 99
NLNK Network Link Detect alarm 65
NMS defined 99
NMS Interface Engine Status alarm 64
NMS log files 79
NMS MI connectivity 29, 30
defined 100
unavailable connection 29
NMS State alarm 66
NMS Status alarm 65
nms.errlog 78
nms.errlog.log 79
node ID
defined 100
NOTICE severity level, in
bycast.log ADE messages 83
NRER Receive Errors alarm 65
NRLY Available Audit Relays alarm 65
NSCA NMS Status alarm 65
NSCE NMS State alarm 66
NSPD Speed alarm 66
NTBR Free Tablespace alarm 66
NTER Transmit Errors alarm 66

NOTICE severity level, in
bycast.log ADE messages 83
NRER Receive Errors alarm 65
NRLY Available Audit Relays alarm 65
NSCA NMS Status alarm 65
NSCE NMS State alarm 66
NSPD Speed alarm 66
NTBR Free Tablespace alarm 66
NTER Transmit Errors alarm 66
<table>
<thead>
<tr>
<th>Defined</th>
<th>Server Manager</th>
<th>101</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Server Manager log files</td>
<td>78</td>
</tr>
<tr>
<td></td>
<td>servermanager.log</td>
<td>78</td>
</tr>
<tr>
<td></td>
<td>Service Memory Usage (%) PMEM alarm</td>
<td>69</td>
</tr>
<tr>
<td>defined</td>
<td></td>
<td>101</td>
</tr>
<tr>
<td></td>
<td></td>
<td>101</td>
</tr>
<tr>
<td></td>
<td></td>
<td>101</td>
</tr>
<tr>
<td></td>
<td>Server Manager log files</td>
<td>78</td>
</tr>
<tr>
<td></td>
<td>status</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>SHLH Health alarm</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>SLES</td>
<td>78</td>
</tr>
<tr>
<td>defined</td>
<td></td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>SLLE Last Event attribute</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>SLSA CPU Load Average alarm</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>SMMT Total Events alarm</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>SMST Log Monitor State alarm</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>SNMP</td>
<td>81</td>
</tr>
<tr>
<td></td>
<td>SNMP log files</td>
<td>81</td>
</tr>
<tr>
<td></td>
<td>SNST Status alarm</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>SNTP</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>SOS Storage Operating System Status alarm</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>Space Available VMFR alarm</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>Speed NSFD alarm</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>SQL</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>ssh</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>SSL</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>SSM</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>SSM events</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>SSM State alarm</td>
<td>73</td>
</tr>
<tr>
<td></td>
<td>SSM Status alarm</td>
<td>73</td>
</tr>
<tr>
<td></td>
<td>ssm.errlog</td>
<td>78</td>
</tr>
<tr>
<td></td>
<td>SSMA SSM Status alarm</td>
<td>73</td>
</tr>
<tr>
<td></td>
<td>SSME SSM State alarm</td>
<td>73</td>
</tr>
<tr>
<td></td>
<td>SSTS Storage Status alarm</td>
<td>34, 73</td>
</tr>
<tr>
<td></td>
<td>STAS Total Usable Space attribute</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>Status BASS alarm</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>Status BRDT alarm</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>Status SCAS alarm</td>
<td>71</td>
</tr>
<tr>
<td></td>
<td>Status SCHR alarm</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>Status SNST alarm</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>Status SVST alarm</td>
<td>74</td>
</tr>
<tr>
<td></td>
<td>Status VMST alarm</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>storage consumption</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Storage Node object store failures</td>
<td>31–42</td>
</tr>
<tr>
<td></td>
<td>Storage Node Soft Read-Only Watermark</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Storage Nodes</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>storage pool</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>Storage Status SSTS alarm</td>
<td>34, 73</td>
</tr>
<tr>
<td></td>
<td>Storage Volume Read-Only Watermark</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>Storage Volume read-Only Watermark</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>StorageGRID Webscale system defined</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>Store Failures ARVF alarm</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>SUCS error code</td>
<td>83</td>
</tr>
<tr>
<td></td>
<td>SUNV error code</td>
<td>83</td>
</tr>
<tr>
<td></td>
<td>SUOP Operations not committed alarm</td>
<td>73</td>
</tr>
<tr>
<td></td>
<td>SVST Status alarm</td>
<td>74</td>
</tr>
<tr>
<td></td>
<td>Swapout No Create Watermark</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>syslog, create</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>system data, retrieve</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>System Status button</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>T</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>task signed text block defined</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>TCP/IP</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>test ingest</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>test retrieve</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>throughput defined</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>time synchronization</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>TLS</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>Total Events SMMT alarm</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>Total Usable Space (Percent) SAVP alarm</td>
<td>32, 71</td>
</tr>
<tr>
<td></td>
<td>Total Usable Space (Percent) SAVP attribute</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Total Usable Space STAS alarm</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Total Usable Space STAS attribute</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>TOUT error code</td>
<td>83</td>
</tr>
<tr>
<td></td>
<td>TPOPs Pending operations alarm</td>
<td>74</td>
</tr>
<tr>
<td></td>
<td>transfer syntax defined</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>Transmit Errors NTER alarm</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>trends, plot</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>troubleshooting new installation</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>NMS MI</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>troubleshooting provisioning</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>TSM</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>U</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>UMEM Available Memory alarm</td>
<td>74</td>
</tr>
<tr>
<td></td>
<td>Unreachable Attribute Repositories ALUR alarm</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>Unreachable Audit Repositories XAMS alarm</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>update log files</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td>URI</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>USB flash drives</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>mounting</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>Used Storage Capacity XUSC attribute</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>USWP Available Swap alarm</td>
<td>74</td>
</tr>
<tr>
<td></td>
<td>UTC</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>UUIDs defined</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>V</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>Verification Failures ARRV alarm</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>Verification Priority VPRI alarm</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>VERS error code</td>
<td>83</td>
</tr>
<tr>
<td></td>
<td>virtual machine definition</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>VMFI Entries Available alarm</td>
<td>74</td>
</tr>
<tr>
<td></td>
<td>VMFR Space Available alarm</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>VMST Status alarm</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>VPRI Verification Priority alarm</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>VSTU Object Verification Status alarm</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>W</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>WAN</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>WARNING severity level, in bycast.log ADE messages</td>
<td>83</td>
</tr>
<tr>
<td></td>
<td>Windows Time Service</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Worst Cast Latency LATW alarm</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>XAMS Unreachable Audit Repositories alarm</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>XFS</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>XML</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>XUSC Used Storage Capacity attribute</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Z</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>zcat command</td>
<td>21</td>
</tr>
</tbody>
</table>