# Monitor and maintain StorageGRID

StorageGRID

NetApp
April 10, 2024

This PDF was generated from https://docs.netapp.com/us-en/storagegrid-116/monitor/index.html on April 10, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

Monitor and maintain StorageGRID . . . 1
Monitor and troubleshoot . . . 1
Expand your grid . . . 335
Recover and maintain . . . 387
Review audit logs . . . 626

# Monitor and maintain StorageGRID

## Monitor and troubleshoot

### Monitor and troubleshoot: Overview

Use these instructions to monitor a StorageGRID system and to assess and resolve issues that might occur.

#### About these instructions

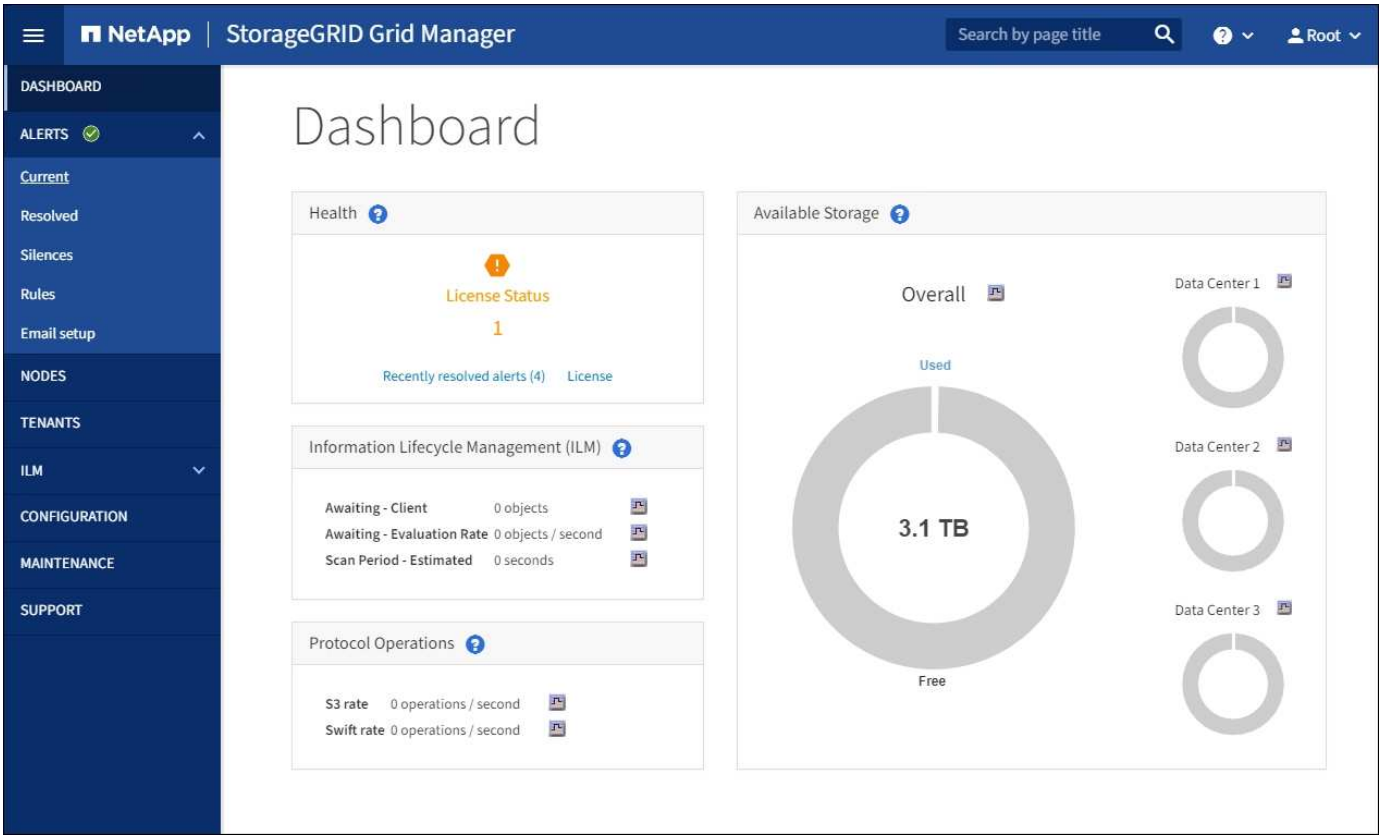
These instructions describe how to use the Grid Manager to monitor a StorageGRID system. You will learn which information you should monitor regularly, how to manage alerts and legacy alarms, how to use SNMP for monitoring, and how to obtain additional StorageGRID data, including metrics and diagnostics.

These instructions also describe how to troubleshoot a StorageGRID system and describe all system alerts, legacy alarms, and log files.

Use these instructions if you will be monitoring and supporting a StorageGRID system after it has been installed.

### View the Dashboard

When you first sign in to the Grid Manager, you can use the Dashboard to monitor system activities at a glance. The Dashboard includes information about system health, usage metrics, and operational trends and charts.



### Search field

The **Search** field in the header bar allows you to quickly navigate to a specific page or sidebar entry within the Grid Manager. For example, you can enter **key** to access the Key Management Server page.

### Health panel

| Description | View additional details | Learn more |
|---|---|---|
| Summarizes the system's health. A green checkmark means that there are no current alerts and all grid nodes are connected. Any other icon means that there is at least one current alert or disconnected node. | You might see one or more of the following links:<br>• **Grid details**: Appears if any nodes are disconnected (connection state Unknown or Administratively Down). Click the link, or click the blue or gray icon to determine which node or nodes are affected.<br>• **Current alerts**: Appears if any alerts are currently active. Click the link, or click **Critical**, **Major**, or **Minor** to see the details on the **ALERTS** > **Current** page.<br>• **Recently resolved alerts**: Appears if any alerts triggered in the past week are now resolved. Click the link to see the details on the **ALERTS** > **Resolved** page.<br>• **Legacy alarms**: Appears if any alarms (legacy system) are currently active. Click the link to see the details on the **SUPPORT** > **Alarms (Legacy)** > **Current alarms** page.<br>• **License**: Appears if there is an issue with the software license for this StorageGRID system. Click the link to see the details on the **MAINTENANCE** > **System** > **License** page. | • Monitor node connection states<br>• View current alerts<br>• View resolved alerts<br>• View legacy alarms<br>• Administer StorageGRID |

### Available Storage panel

| Description | View additional details | Learn more |
| --- | --- | --- |
| Displays the available and used storage capacity in the entire grid, not including archival media.<br><br>The Overall chart presents grid-wide totals. If this is a multi-site grid, additional charts appear for each data center site.<br><br>You can use this information to compare the used storage with the available storage. If you have a multi-site grid, you can determine which site is consuming more storage. | • To view the capacity, place your cursor over the chart's available and used capacity sections.<br>• To view capacity trends over a date range, click the chart icon for the overall grid, or for a data center site.<br>• To see details, select **NODES**. Then, view the Storage tab for the entire grid, an entire site, or a single Storage Node. | • View the Storage tab<br>• Monitor storage capacity |

### Information Lifecycle Management (ILM) panel

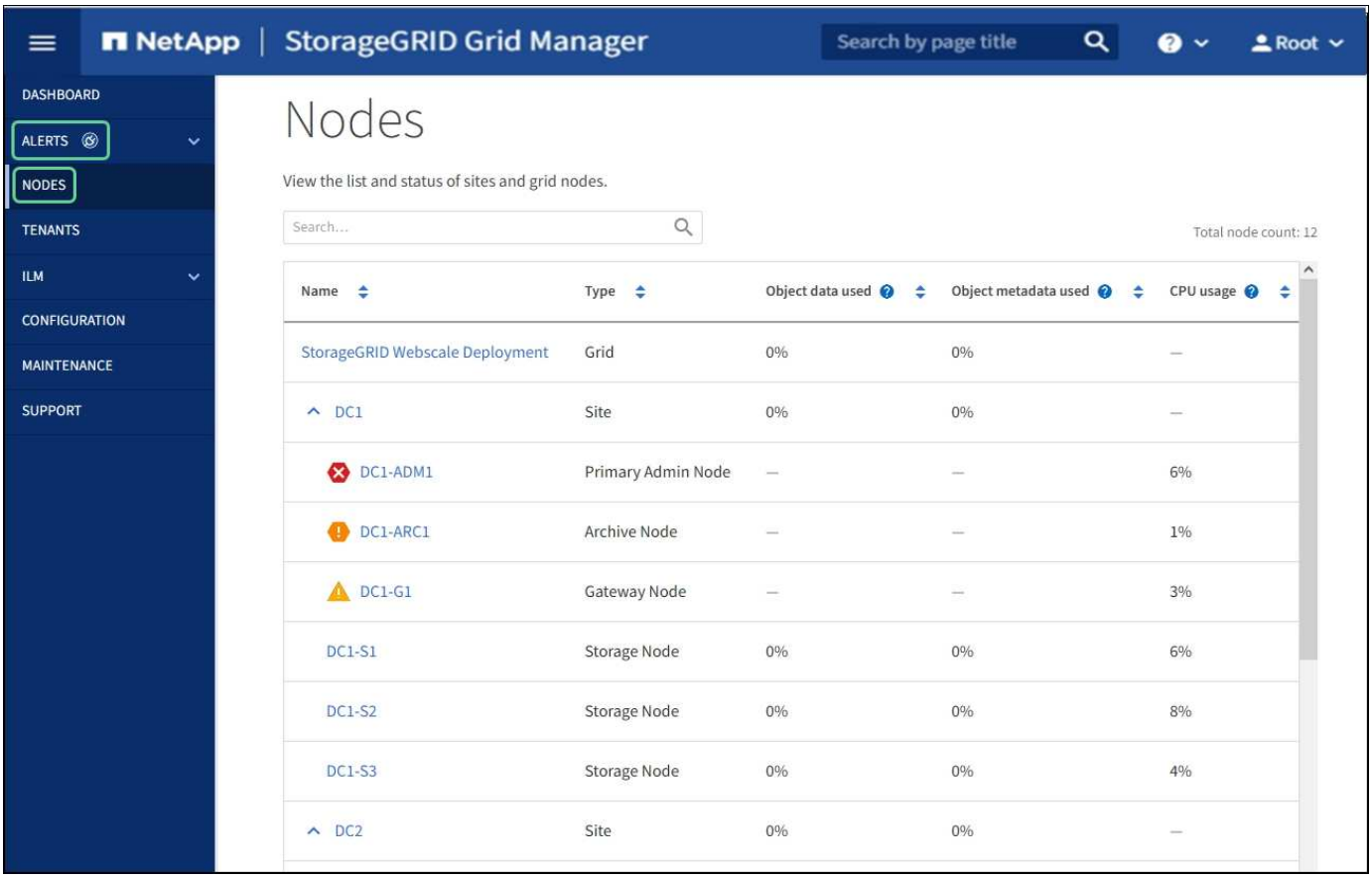
| Description | View additional details | Learn more |
| --- | --- | --- |
| Displays current ILM operations and ILM queues for your system. You can use this information to monitor your system's workload.<br><br>• **Awaiting - Client**: The total number of objects awaiting ILM evaluation from client operations (for example, ingest).<br>• **Awaiting - Evaluation Rate**: The current rate at which objects are evaluated against the ILM policy in the grid.<br>• **Scan Period - Estimated**: The estimated time to complete a full ILM scan of all objects. **Note:** A full scan does not guarantee that ILM has been applied to all objects. | • To see details, select **NODES**. Then, view the ILM tab for the entire grid, an entire site, or a single Storage Node.<br>• To see the existing ILM rules, select **ILM** > **Rules**.<br>• To see the existing ILM policies, select **ILM** > **Policies**. | • View the ILM tab<br>• Administer StorageGRID. |

### Protocol Operations panel

| Description | View additional details | Learn more |
|---|---|---|
| Displays the number of protocol-specific operations (S3 and Swift) performed by your system.<br><br>You can use this information to monitor your system's workloads and efficiencies. Protocol rates are averaged over the last two minutes. | • To see details, select **NODES**. Then, view the Objects tab for the entire grid, an entire site, or a single Storage Node.<br>• To view trends over a date range, click the chart icon to the right of the S3 or Swift protocol rate. | • View the Objects tab<br>• Use S3<br>• Use Swift |

## View the Nodes page

When you need more detailed information about your StorageGRID system than the Dashboard provides, you can use the Nodes page to view metrics for the entire grid, each site in the grid, and each node at a site.




The Nodes table lists all the sites and nodes in your StorageGRID system. Summary information is displayed for each node. If a node has an active alert, an icon appears next to the node name. If the node is connected and has no active alerts, no icon is shown.

### Connection state icons

- **Not connected - Unknown** : The node is not connected to the grid for an unknown reason. For example, the network connection between nodes has been lost or the power is down. The **Unable to**

**communicate with node** alert might also be triggered. Other alerts might be active as well. This situation requires immediate attention.

> A node might appear as Unknown during managed shutdown operations. You can ignore the Unknown state in these cases.

- **Not connected - Administratively down** : The node is not connected to the grid for an expected reason. For example, the node, or services on the node, has been gracefully shut down, the node is rebooting, or the software is being upgraded. One or more alerts might also be active.

If a node is disconnected from the grid, it might have an underlying alert, but only the “Not connected” icon appears. To see the active alerts for a node, select the node.

### Alert icons

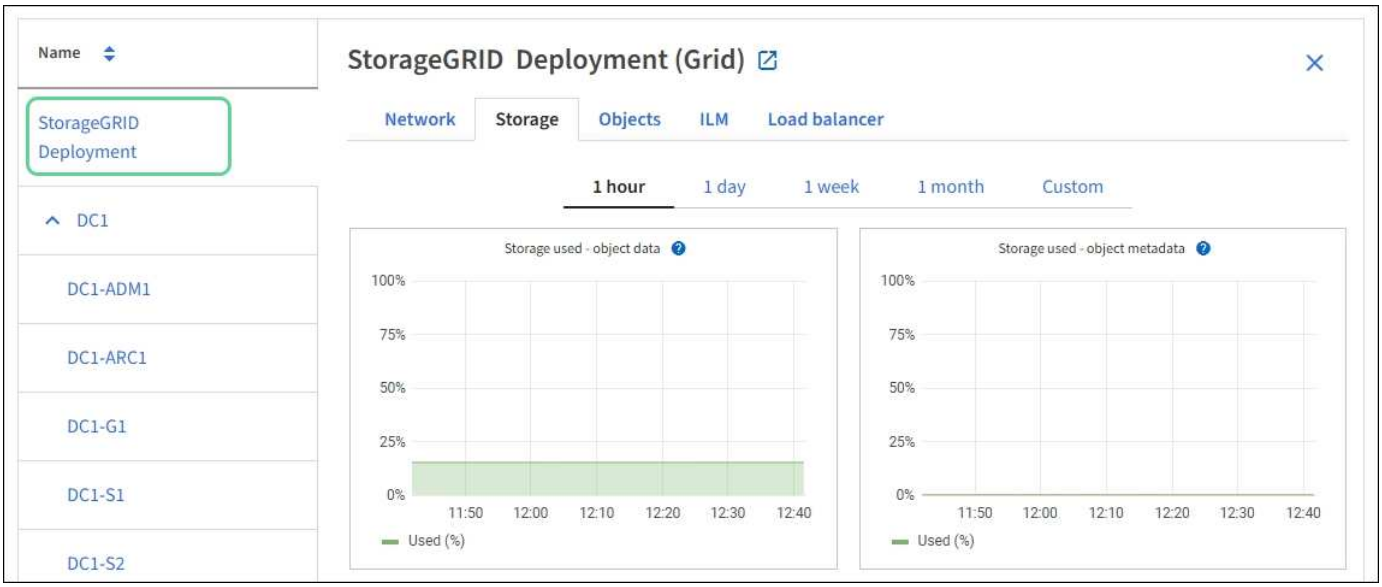
If there is an active alert for a node, one of the following icons appears next to the node name:

- **Critical** : An abnormal condition exists that has stopped the normal operations of a StorageGRID node or service. You must address the underlying issue immediately. Service disruption and loss of data might result if the issue is not resolved.
- **Major** : An abnormal condition exists that is either affecting current operations or approaching the threshold for a critical alert. You should investigate major alerts and address any underlying issues to ensure that the abnormal condition does not stop the normal operation of a StorageGRID node or service.
- **Minor** : The system is operating normally, but an abnormal condition exists that could affect the system’s ability to operate if it continues. You should monitor and resolve minor alerts that do not clear on their own to ensure they do not result in a more serious problem.

### Viewing details for a system, site, or node

To view the available information, select the name of the grid, site, or node as follows:

- Select the grid name to see an aggregate summary of the statistics for your entire StorageGRID system.
- Select a specific data center site to see an aggregate summary of the statistics for all nodes at that site.
- Select a specific node to view detailed information for that node.



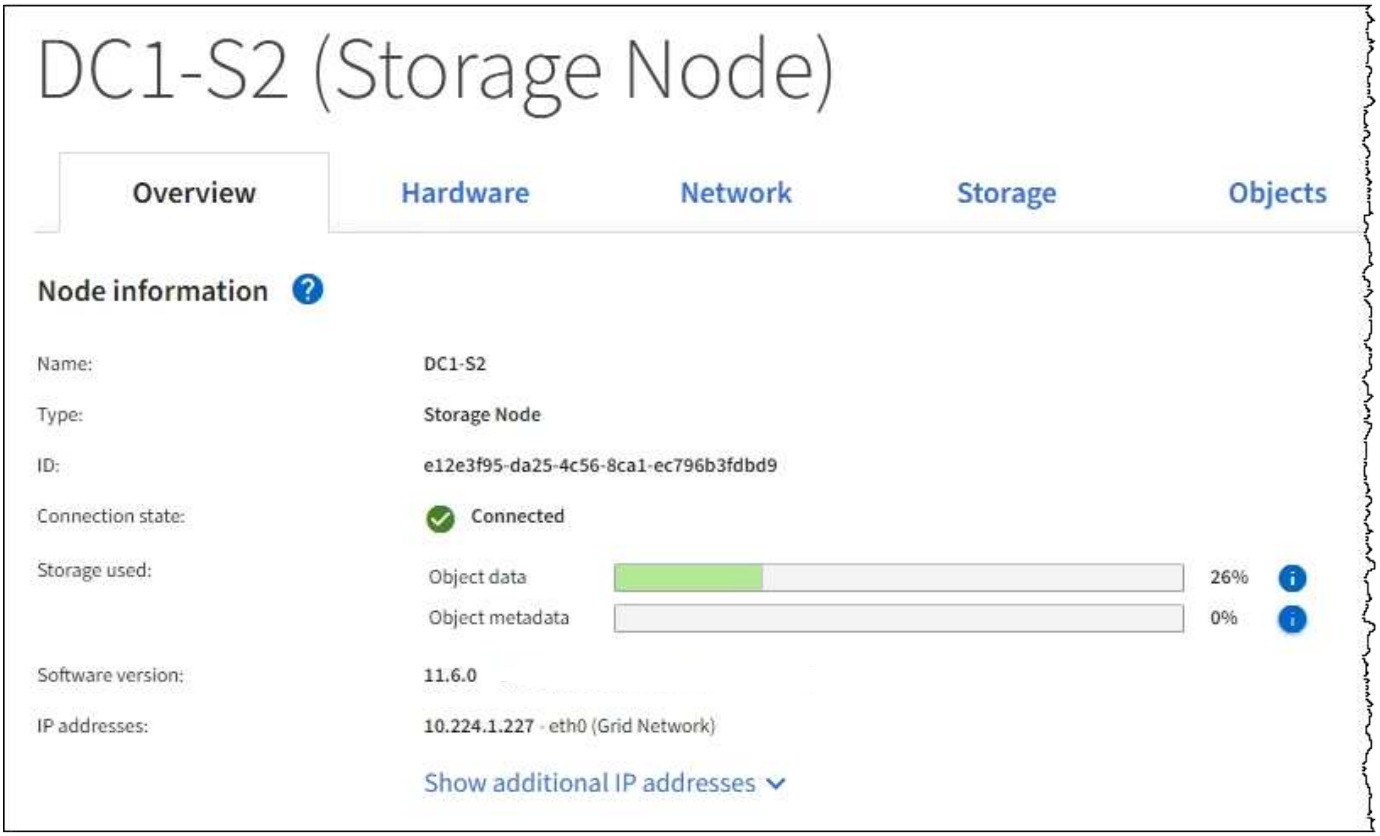

### View the Overview tab

The Overview tab provides basic information about each node. It also shows any alerts currently affecting the node.

The Overview tab is shown for all nodes.

#### Node Information

The Node Information section of the Overview tab lists basic information about the grid node.



The overview information for a node includes the following:

- **Name**: The hostname assigned to the node and displayed in the Grid Manager.
- **Type**: The type of node — Admin Node, primary Admin Node, Storage Node, Gateway Node, or Archive Node.
- **ID**: The unique identifier for the node, which is also referred to as the UUID.
- **Connection state**: One of three states. The icon for the most severe state is shown.
  - **Unknown** : The node is not connected to the grid for an unknown reason. For example, the network connection between nodes has been lost or the power is down. The **Unable to communicate with node** alert might also be triggered. Other alerts might be active as well. This situation requires immediate attention.

    > A node might appear as Unknown during managed shutdown operations. You can ignore the Unknown state in these cases.

  - **Administratively down** : The node is not connected to the grid for an expected reason. For example, the node, or services on the node, has been gracefully shut down, the node is rebooting, or the software is being upgraded. One or more alerts might also be active.
  - **Connected** : The node is connected to the grid.
- **Storage used**: For Storage Nodes only.
  - **Object data**: The percentage of the total usable space for object data that has been used on the Storage Node.
  - **Object metadata**: The percentage of the total allowed space for object metadata that has been used on the Storage Node.
- **Software version**: The version of StorageGRID that is installed on the node.
- **HA groups**: For Admin Node and Gateway Nodes only. Shown if a network interface on the node is included in a high availability group and whether that interface is the Primary interface.
- **IP addresses**: The node's IP addresses. Click **Show additional IP addresses** to view the node's IPv4 and IPv6 addresses and interface mappings.

#### Alerts

The Alerts section of the Overview tab lists any alerts currently affecting this node that have not been silenced. Click the alert name to view additional details and recommended actions.

#### Related information

Monitor node connection states

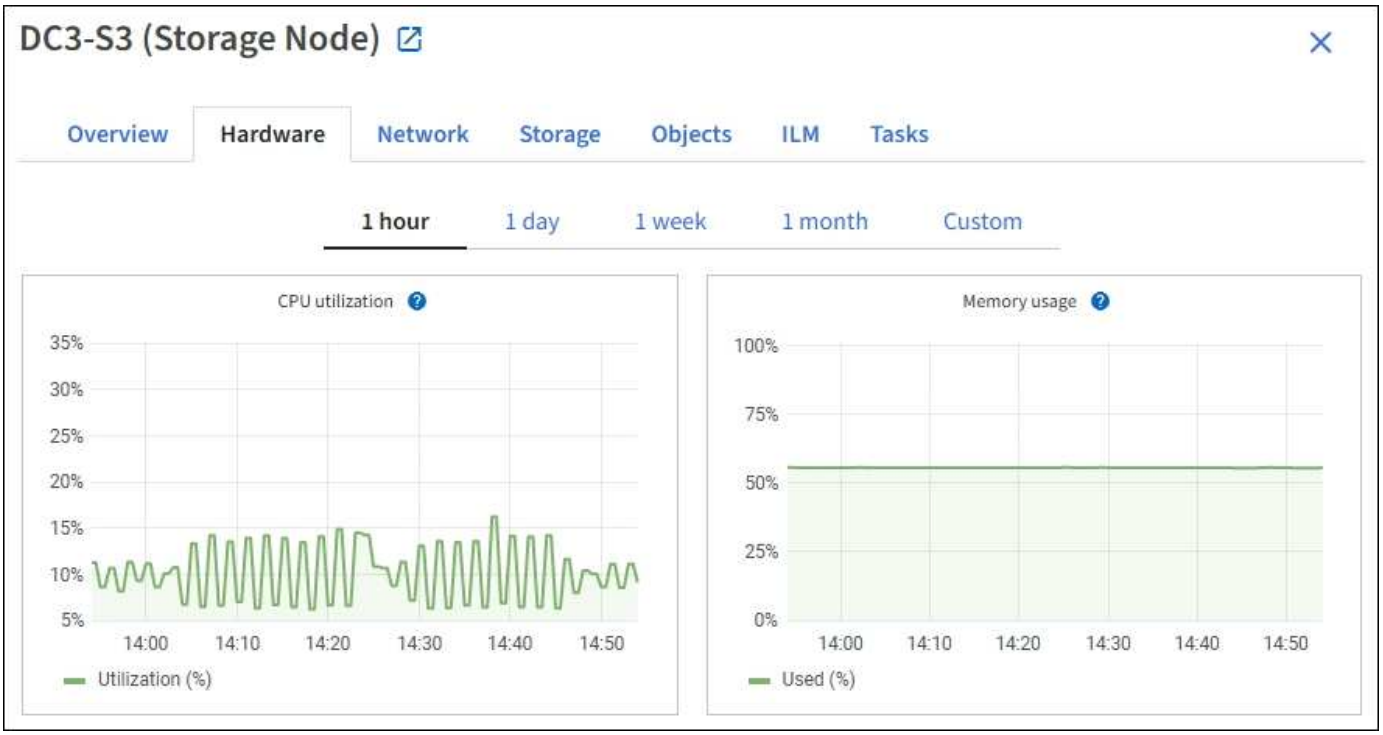
View current alerts

View a specific alert

**View the Hardware tab**

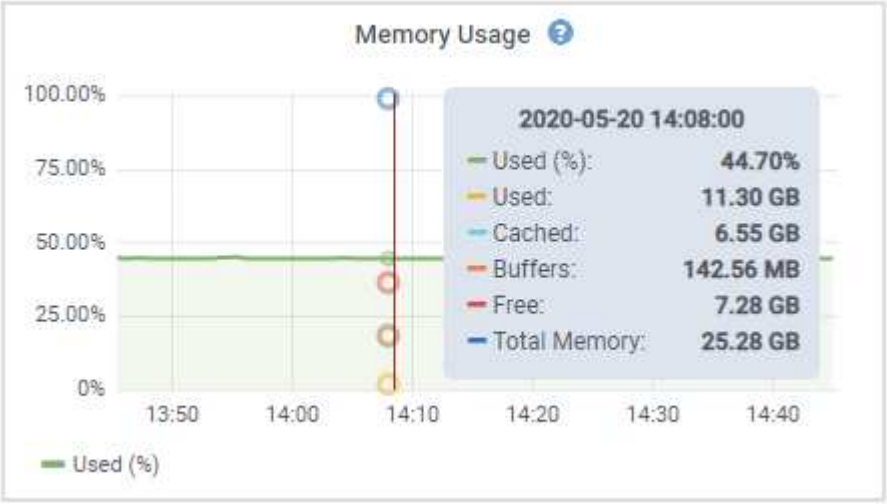
The Hardware tab displays CPU utilization and memory usage for each node, and additional hardware information about appliances.

The Hardware tab is shown for all nodes.




To display a different time interval, select one of the controls above the chart or graph. You can display the information available for intervals of 1 hour, 1 day, 1 week, or 1 month. You can also set a custom interval, which allows you to specify date and time ranges.

To see details for CPU utilization and memory usage, hover your cursor over each graph.



If the node is an appliance node, this tab also includes a section with more information about the appliance hardware.

#### View information about appliance Storage Nodes

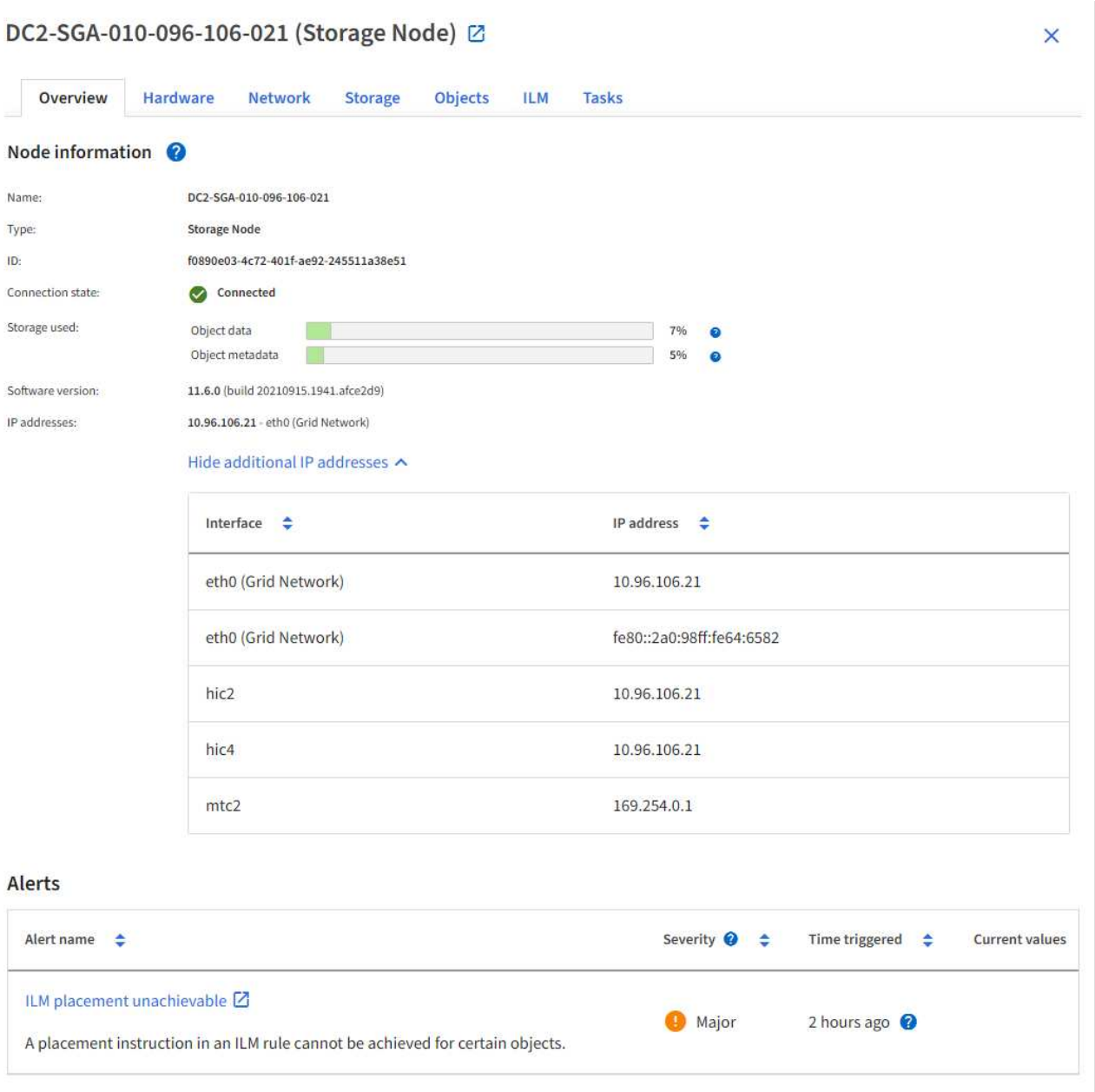
The Nodes page lists information about service health and all computational, disk device, and network resources for each appliance Storage Node. You can also see memory, storage hardware, controller firmware version, network resources, network interfaces, network addresses, and receive and transmit data.

**Steps**

1. From the Nodes page, select an appliance Storage Node.
2. Select **Overview**.

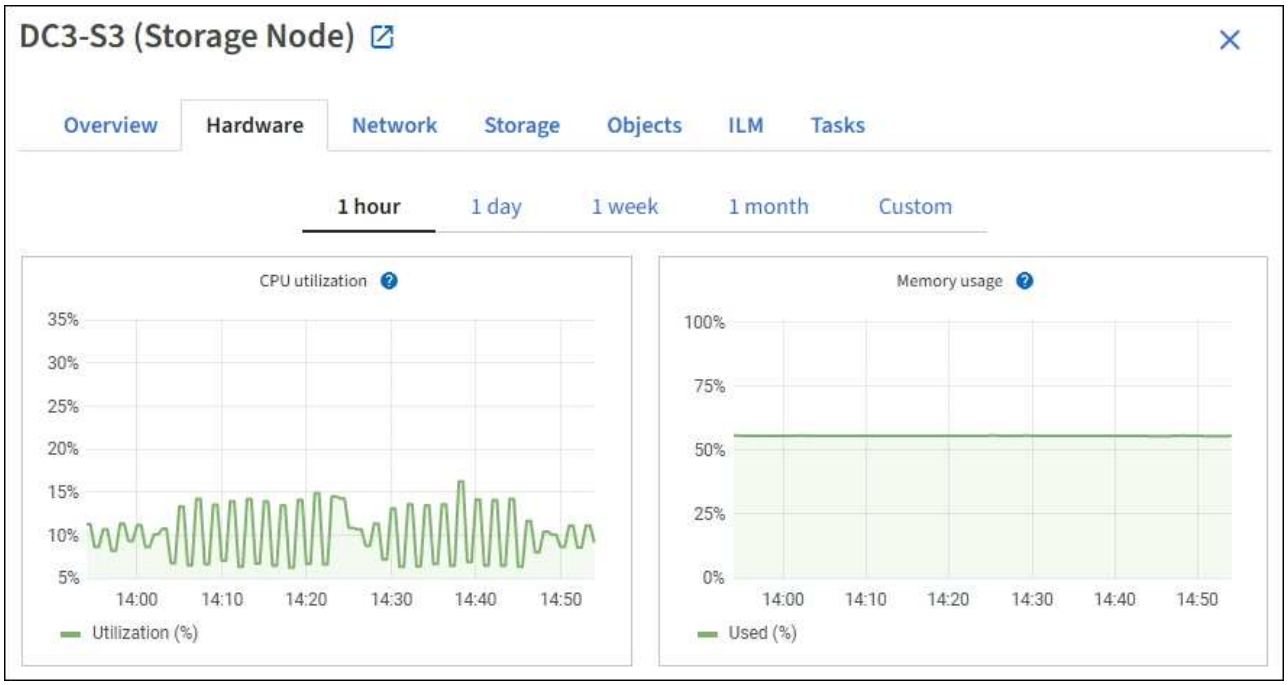
   The Node information section of the Overview tab displays summary information for the node, such as the node's name, type, ID, and connection state. The list of IP addresses includes the name of the interface for each address, as follows:

   - **eth**: The Grid Network, Admin Network, or Client Network.
   - **hic**: One of the physical 10, 25, or 100 GbE ports on the appliance. These ports can be bonded together and connected to the StorageGRID Grid Network (eth0) and Client Network (eth2).
   - **mtc**: One of the physical 1 GbE ports on the appliance. One or more mtc interfaces are bonded to form the StorageGRID Admin Network interface (eth1). You can leave other mtc interfaces available for temporary local connectivity for a technician in the data center.




The Alerts section of the Overview tab displays any active alerts for the node.

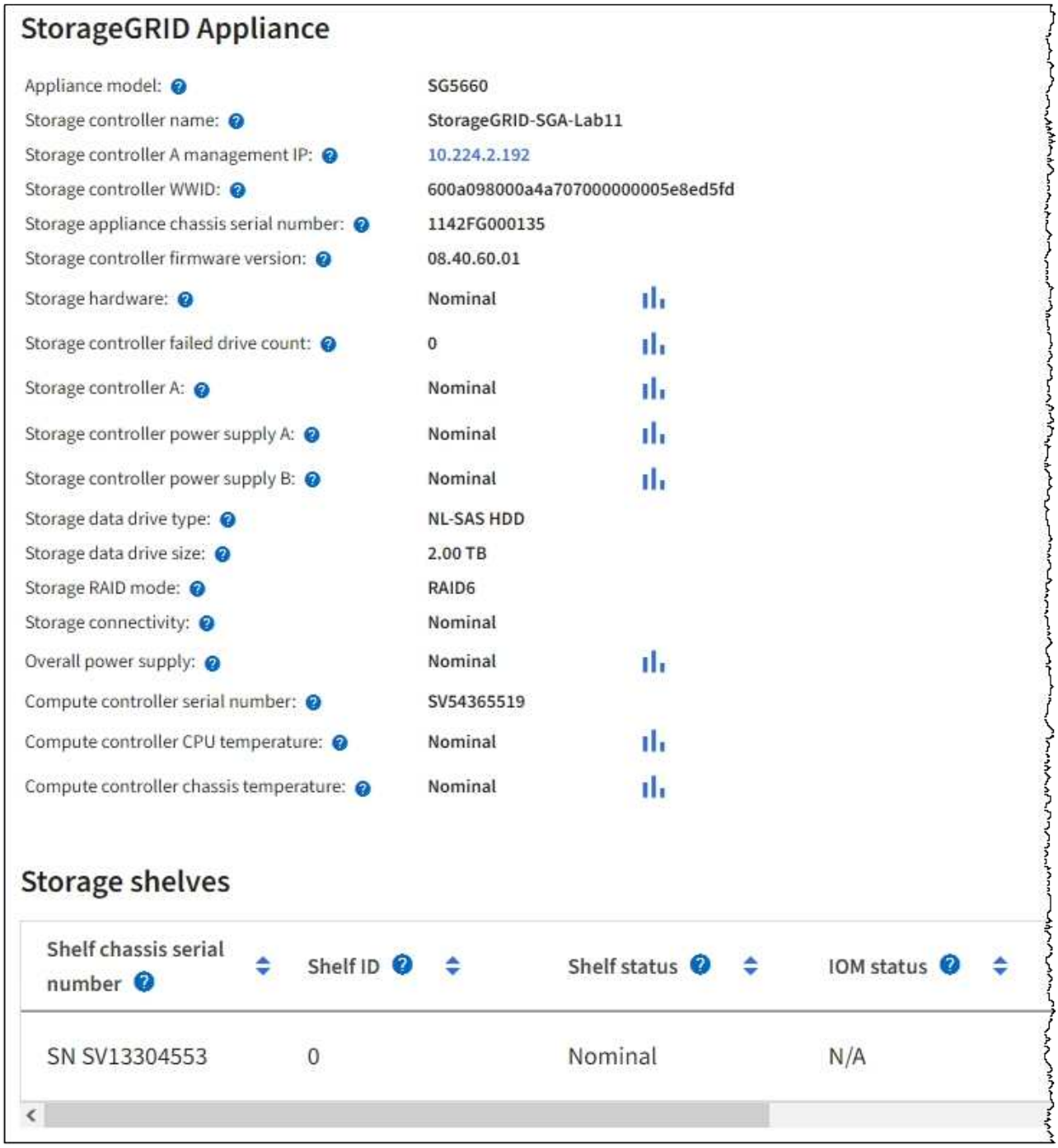
3. Select **Hardware** to see more information about the appliance.
   a. View the CPU Utilization and Memory graphs to determine the percentages of CPU and memory usage over time. To display a different time interval, select one of the controls above the chart or graph. You can display the information available for intervals of 1 hour, 1 day, 1 week, or 1 month. You can also set a custom interval, which allows you to specify date and time ranges.




b. Scroll down to view the table of components for the appliance. This table contains information such as the model name of the appliance; controller names, serial numbers, and IP addresses; and the status of each component.

> Some fields, such as Compute controller BMC IP and Compute hardware, appear only for appliances with that feature.

Components for the storage shelves, and expansion shelves if they are part of the installation, appear in a separate table below the appliance table.




| Field in the Appliance table | Description |
|---|---|
| Appliance model | The model number for this StorageGRID appliance shown in SANtricity software. |
| Storage controller name | The name for this StorageGRID appliance shown in SANtricity software. |
| Storage controller A management IP | IP address for management port 1 on storage controller A. You use this IP to access SANtricity software to troubleshoot storage issues. |

| Field in the Appliance table | Description |
| --- | --- |
| Storage controller B management IP | IP address for management port 1 on storage controller B. You use this IP to access SANtricity software to troubleshoot storage issues.<br><br>Some appliance models do not have a storage controller B. |
| Storage controller WWID | The worldwide identifier of the storage controller shown in SANtricity software. |
| Storage appliance chassis serial number | The chassis serial number of the appliance. |
| Storage controller firmware version | The version of the firmware on the storage controller for this appliance. |
| Storage hardware | The overall status of the storage controller hardware. If SANtricity System Manager reports a status of Needs Attention for the storage hardware, the StorageGRID system also reports this value.<br><br>If the status is “needs attention,” first check the storage controller using SANtricity software. Then, ensure that no other alarms exist that apply to the compute controller. |
| Storage controller failed drive count | The number of drives that are not optimal. |
| Storage controller A | The status of storage controller A. |
| Storage controller B | The status of storage controller B. Some appliance models do not have a storage controller B. |
| Storage controller power supply A | The status of power supply A for the storage controller. |
| Storage controller power supply B | The status of power supply B for the storage controller. |
| Storage data drive type | The type of drives in the appliance, such as HDD (hard disk drive) or SSD (solid state drive). |
| Storage data drive size | The effective size of one data drive.<br><br>**Note**: For nodes with expansion shelves, use the Data drive size for each shelf instead. Effective drive size might differ by shelf. |
| Storage RAID mode | The RAID mode configured for the appliance. |

| Field in the Appliance table | Description |
| --- | --- |
| Storage connectivity | The storage connectivity state. |
| Overall power supply | The status of all power supplies for the appliance. |
| Compute controller BMC IP | The IP address of the baseboard management controller (BMC) port in the compute controller. You use this IP to connect to the BMC interface to monitor and diagnose the appliance hardware.<br><br>This field is not displayed for appliance models that do not contain a BMC. |
| Compute controller serial number | The serial number of the compute controller. |
| Compute hardware | The status of the compute controller hardware. This field is not displayed for appliance models that do not have separate compute hardware and storage hardware. |
| Compute controller CPU temperature | The temperature status of the compute controller's CPU. |
| Compute controller chassis temperature | The temperature status of the compute controller. |

| Column in the Storage shelves table | Description |
| --- | --- |
| Shelf chassis serial number | The serial number for the storage shelf chassis. |
| Shelf ID | The numeric identifier for the storage shelf.<br><br>• 99: Storage controller shelf<br>• 0: First expansion shelf<br>• 1: Second expansion shelf<br><br>**Note:** Expansion shelves apply to the SG6060 and SG6060X only. |
| Shelf status | The overall status of the storage shelf. |
| IOM status | The status of the input/output modules (IOMs) in any expansion shelves. N/A if this is not an expansion shelf. |
| Power supply status | The overall status of the power supplies for the storage shelf. |

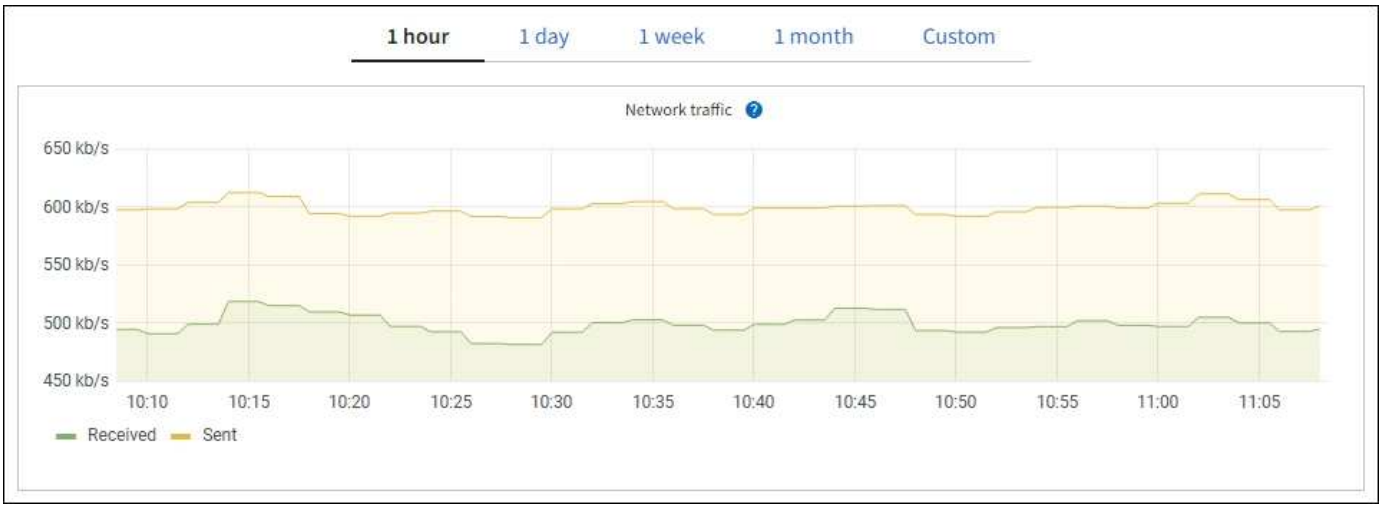
| Column in the Storage shelves table | Description |
|---|---|
| Drawer status | The status of the drawers in the storage shelf. N/A if the shelf does not contain drawers. |
| Fan status | The overall status of the cooling fans in the storage shelf. |
| Drive slots | The total number of drive slots in the storage shelf. |
| Data drives | The number of drives in the storage shelf that are used for data storage. |
| Data drive size | The effective size of one data drive in the storage shelf. |
| Cache drives | The number of drives in the storage shelf that are used as cache. |
| Cache drive size | The size of the smallest cache drive in the storage shelf. Normally, cache drives are all the same size. |
| Configuration status | The configuration status of the storage shelf. |

c. Confirm that all statuses are “Nominal.”

   If a status is not “Nominal,” review any current alerts. You can also use SANtricity System Manager to learn more about some of these hardware values. See the instructions for installing and maintaining your appliance.

4. Select **Network** to view information for each network.

The Network Traffic graph provides a summary of overall network traffic.




a. Review the Network Interfaces section.

**Network interfaces**

| Name | Hardware address | Speed | Duplex | Auto-negotiation | Link status |
|---|---|---|---|---|---|
| eth0 | 00:50:56:A7:66:75 | 10 Gigabit | Full | Off | Up |

Use the following table with the values in the **Speed** column in the Network Interfaces table to determine whether the 10/25-GbE network ports on the appliance were configured to use active/backup mode or LACP mode.

> The values shown in the table assume all four links are used.

| Link mode | Bond mode | Individual HIC link speed (hic1, hic2, hic3, hic4) | Expected Grid/Client Network speed (eth0,eth2) |
|---|---|---|---|
| Aggregate | LACP | 25 | 100 |
| Fixed | LACP | 25 | 50 |
| Fixed | Active/Backup | 25 | 25 |
| Aggregate | LACP | 10 | 40 |
| Fixed | LACP | 10 | 20 |
| Fixed | Active/Backup | 10 | 10 |

See the installation and maintenance instructions for your appliance for more information about configuring the 10/25-GbE ports.

b. Review the Network Communication section.

   The Receive and Transmit tables show how many bytes and packets have been received and sent across each network as well as other receive and transmit metrics.

**Network communication**

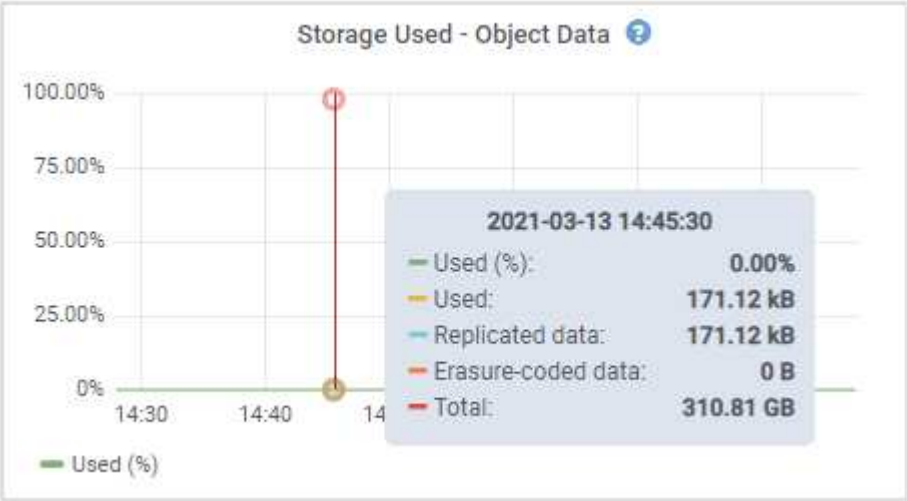
Receive

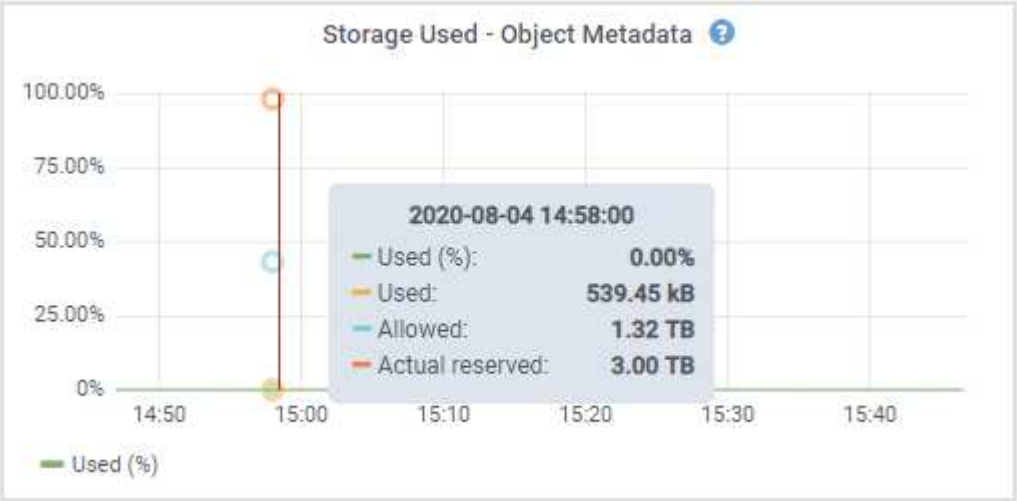
| Interface | Data | Packets | Errors | Dropped | Frame overruns | Frames |
|---|---|---|---|---|---|---|
| eth0 | 2.89 GB | 19,421,503 | 0 | 24,032 | 0 | 0 |

Transmit

| Interface | Data | Packets | Errors | Dropped | Collisions | Carrier |
|---|---|---|---|---|---|---|
| eth0 | 3.64 GB | 18,494,381 | 0 | 0 | 0 | 0 |

5. Select **Storage** to view graphs that show the percentages of storage used over time for object data and object metadata, as well as information about disk devices, volumes, and object stores.




a. Scroll down to view the amounts of available storage for each volume and object store.

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

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

**Disk devices**

| Name | World Wide Name | I/O load | Read rate | Write rate |
|---|---|---|---|---|
| croot(8:1,sda1) | N/A | 0.04% | 0 bytes/s | 3 KB/s |
| cvloc(8:2,sda2) | N/A | 0.67% | 0 bytes/s | 50 KB/s |
| sdc(8:16,sdb) | N/A | 0.03% | 0 bytes/s | 4 KB/s |
| sdd(8:32,sdc) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |
| sde(8:48,sdd) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |

**Volumes**

| Mount point | Device | Status | Size | Available | Write cache status |
|---|---|---|---|---|---|
| / | croot | Online | 21.00 GB | 14.75 GB | Unknown |
| /var/local | cvloc | Online | 85.86 GB | 84.05 GB | Unknown |
| /var/local/rangedb/0 | sdc | Online | 107.32 GB | 107.17 GB | Enabled |
| /var/local/rangedb/1 | sdd | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/2 | sde | Online | 107.32 GB | 107.18 GB | Enabled |

**Object stores**

| ID | Size | Available | Replicated data | EC data | Object data (%) | Health |
|---|---|---|---|---|---|---|
| 0000 | 107.32 GB | 96.44 GB | 124.60 KB | 0 bytes | 0.00% | No Errors |
| 0001 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0002 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |

**Related information**

SG6000 storage appliances

SG5700 storage appliances

SG5600 storage appliances

#### View information about appliance Admin Nodes and Gateway Nodes

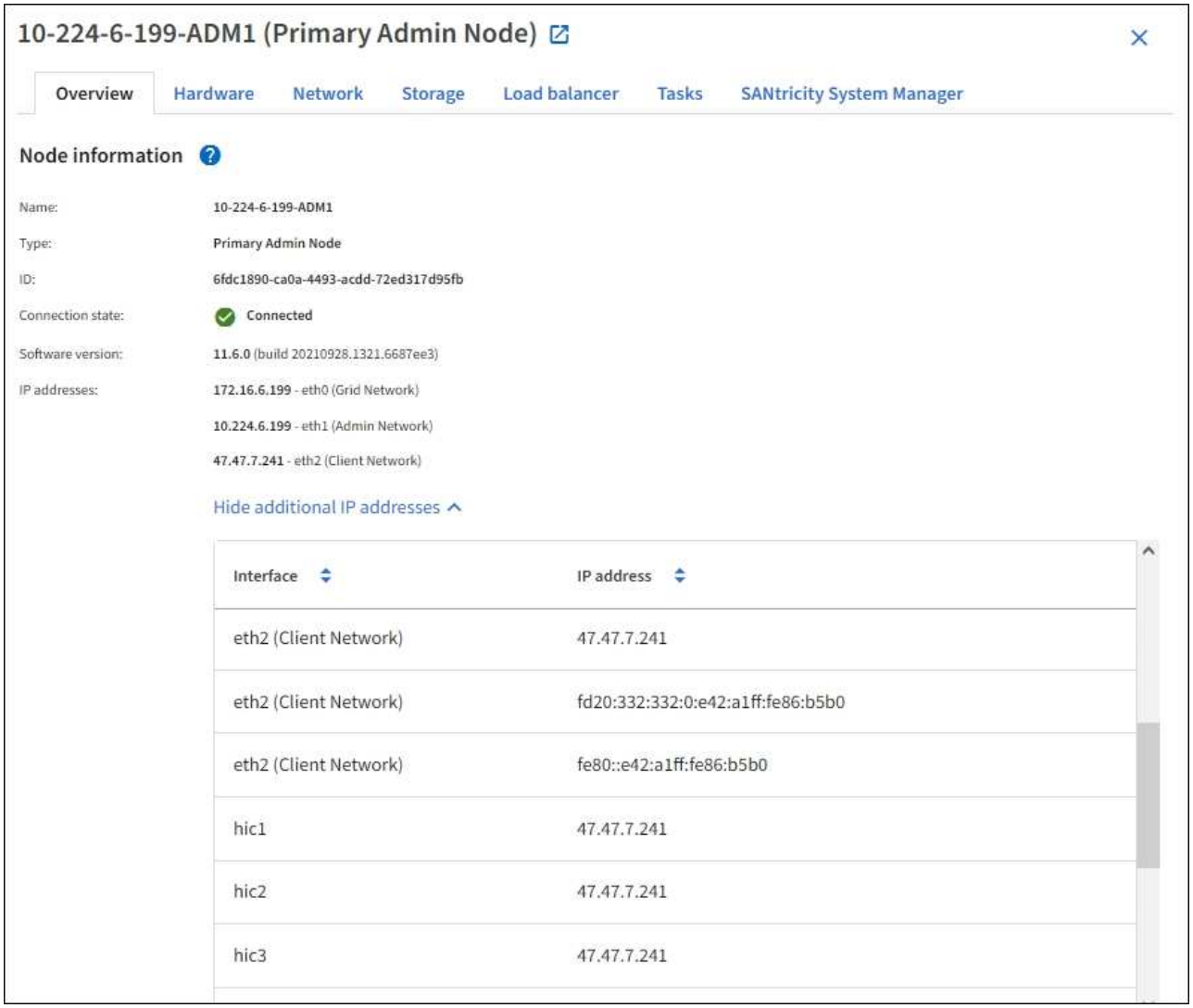
The Nodes page lists information about service health and all computational, disk device, and network resources for each services appliance that is used as an Admin Node or a Gateway Node. You can also see memory, storage hardware, network resources, network interfaces, network addresses, and receive and transmit data.

**Steps**

1. From the Nodes page, select an appliance Admin Node or an appliance Gateway Node.
2. Select **Overview**.

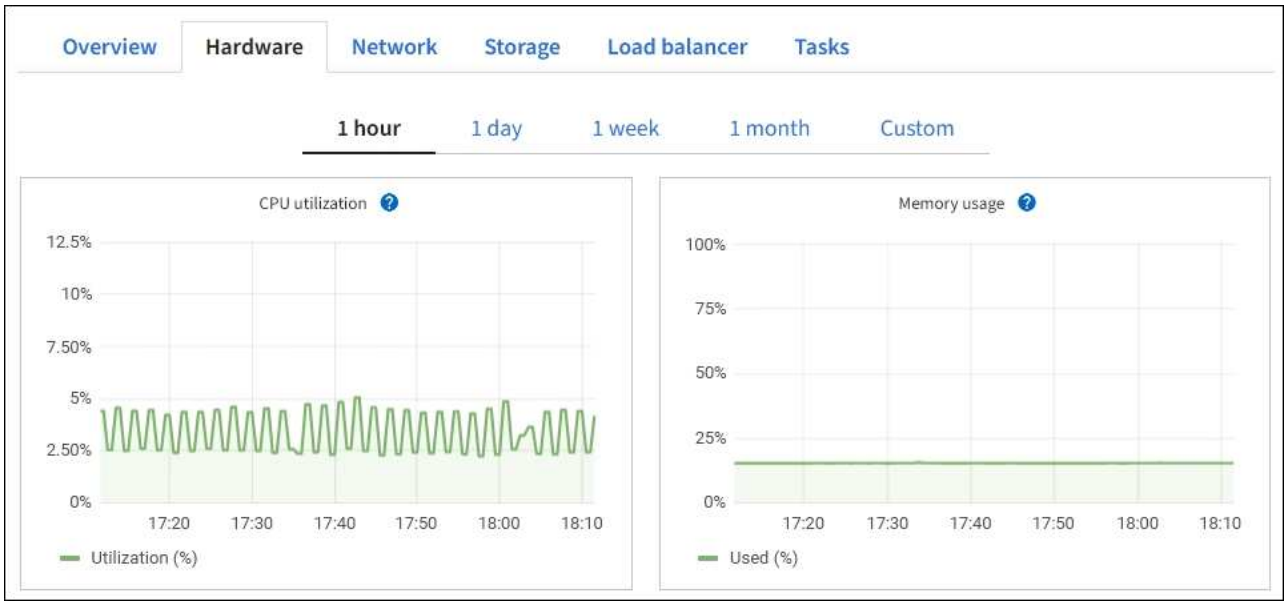
   The Node information section of the Overview tab displays summary information for the node, such as the node's name, type, ID, and connection state. The list of IP addresses includes the name of the interface for each address, as follows:

   - **adllb** and **adlli**: Shown if active/backup bonding is used for the Admin Network interface
   - **eth**: The Grid Network, Admin Network, or Client Network.
   - **hic**: One of the physical 10, 25, or 100 GbE ports on the appliance. These ports can be bonded together and connected to the StorageGRID Grid Network (eth0) and Client Network (eth2).
   - **mtc**: One of the physical 1-GbE ports on the appliance. One or more mtc interfaces are bonded to form the Admin Network interface (eth1). You can leave other mtc interfaces available for temporary local connectivity for a technician in the data center.

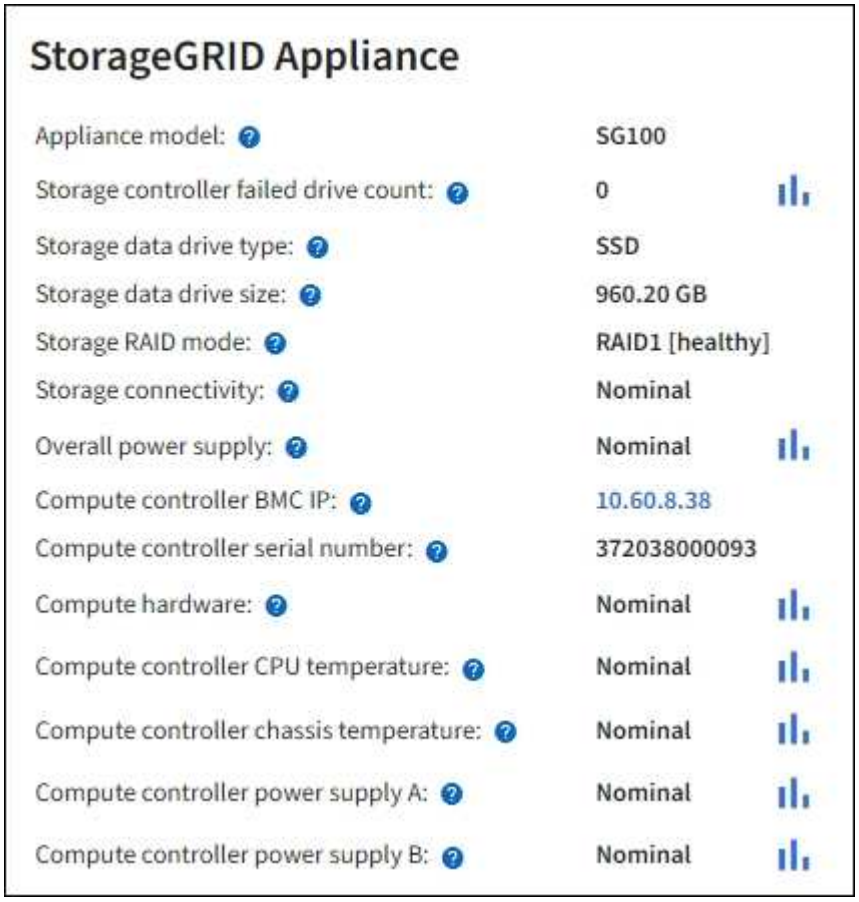



The Alerts section of the Overview tab displays any active alerts for the node.

3. Select **Hardware** to see more information about the appliance.
   a. View the CPU Utilization and Memory graphs to determine the percentages of CPU and memory usage over time. To display a different time interval, select one of the controls above the chart or graph. You can display the information available for intervals of 1 hour, 1 day, 1 week, or 1 month. You can also set a custom interval, which allows you to specify date and time ranges.




b. Scroll down to view the table of components for the appliance. This table contains information such as the model name, serial number, controller firmware version, and the status of each component.




| Field in the Appliance table | Description |
|---|---|
| Appliance model | The model number for this StorageGRID appliance. |

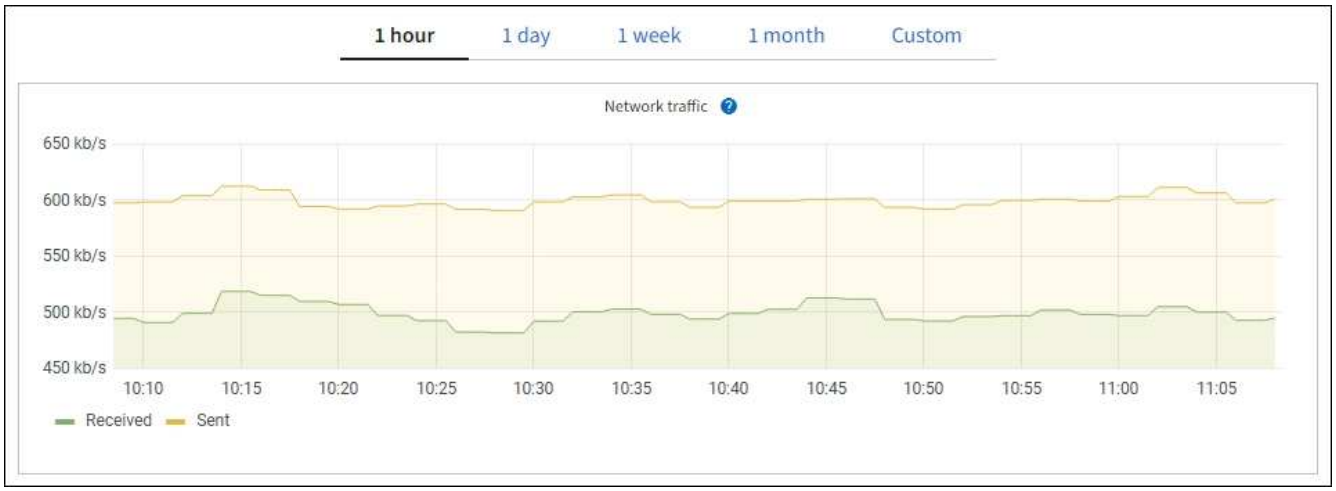
| Field in the Appliance table | Description |
| --- | --- |
| Storage controller failed drive count | The number of drives that are not optimal. |
| Storage data drive type | The type of drives in the appliance, such as HDD (hard disk drive) or SSD (solid state drive). |
| Storage data drive size | The effective size of one data drive. |
| Storage RAID mode | The RAID mode for the appliance. |
| Overall power supply | The status of all power supplies in the appliance. |
| Compute controller BMC IP | The IP address of the baseboard management controller (BMC) port in the compute controller. You can use this IP to connect to the BMC interface to monitor and diagnose the appliance hardware.<br><br>This field is not displayed for appliance models that do not contain a BMC. |
| Compute controller serial number | The serial number of the compute controller. |
| Compute hardware | The status of the compute controller hardware. |
| Compute controller CPU temperature | The temperature status of the compute controller's CPU. |
| Compute controller chassis temperature | The temperature status of the compute controller. |

c. Confirm that all statuses are "Nominal."

   If a status is not "Nominal," review any current alerts.

4. Select **Network** to view information for each network.

   The Network Traffic graph provides a summary of overall network traffic.




a. Review the Network Interfaces section.

**Network interfaces**

| Name | Hardware address | Speed | Duplex | Auto-negotiation | Link status |
|---|---|---|---|---|---|
| eth0 | 0C:42:A1:86:B5:B0 | 100 Gigabit | Full | Off | Up |
| eth1 | B4:A9:FC:71:68:36 | Gigabit | Full | Off | Up |
| eth2 | 0C:42:A1:86:B5:B0 | 100 Gigabit | Full | Off | Up |
| hic1 | 0C:42:A1:86:B5:B0 | 25 Gigabit | Full | On | Up |
| hic2 | 0C:42:A1:86:B5:B0 | 25 Gigabit | Full | On | Up |
| hic3 | 0C:42:A1:86:B5:B0 | 25 Gigabit | Full | On | Up |
| hic4 | 0C:42:A1:86:B5:B0 | 25 Gigabit | Full | On | Up |
| mtc1 | B4:A9:FC:71:68:36 | Gigabit | Full | On | Up |
| mtc2 | B4:A9:FC:71:68:35 | Gigabit | Full | On | Up |

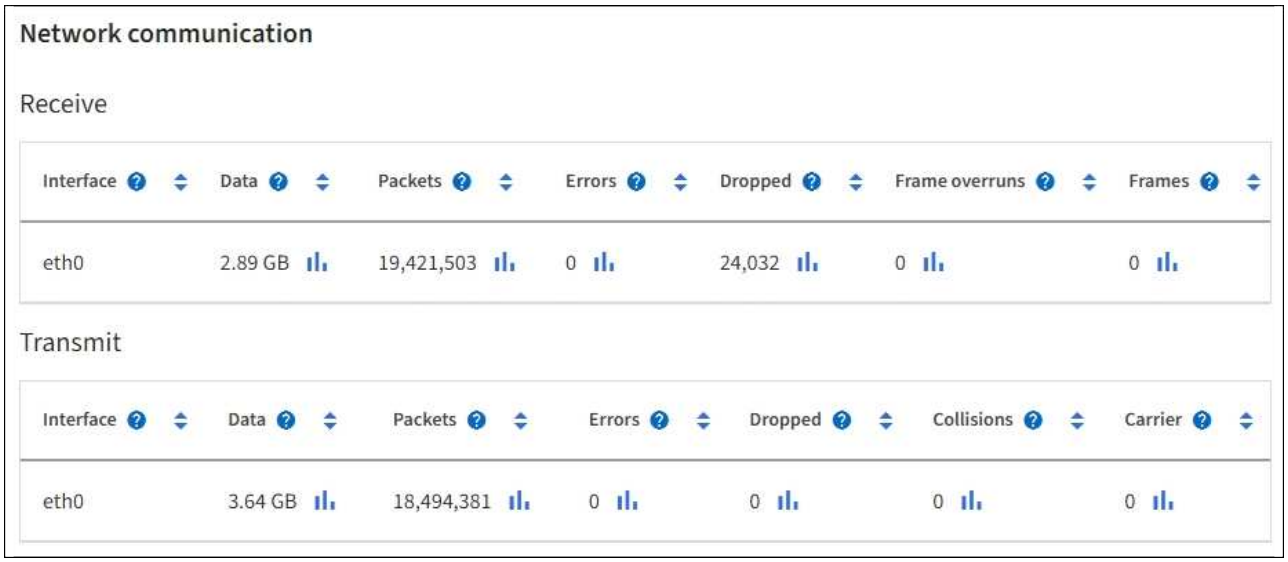
Use the following table with the values in the **Speed** column in the Network Interfaces table to determine whether the four 40/100-GbE network ports on the appliance were configured to use active/backup mode or LACP mode.

The values shown in the table assume all four links are used.

| Link mode | Bond mode | Individual HIC link speed (hic1, hic2, hic3, hic4) | Expected Grid/Client Network speed (eth0, eth2) |
|---|---|---|---|
| Aggregate | LACP | 100 | 400 |
| Fixed | LACP | 100 | 200 |
| Fixed | Active/Backup | 100 | 100 |
| Aggregate | LACP | 40 | 160 |
| Fixed | LACP | 40 | 80 |
| Fixed | Active/Backup | 40 | 40 |

b. Review the Network Communication section.

The Receive and Transmit tables show how many bytes and packets have been received and sent across each network as well as other receive and transmission metrics.



**Network communication**

Receive

| Interface | Data | Packets | Errors | Dropped | Frame overruns | Frames |
|---|---|---|---|---|---|---|
| eth0 | 2.89 GB | 19,421,503 | 0 | 24,032 | 0 | 0 |

Transmit

| Interface | Data | Packets | Errors | Dropped | Collisions | Carrier |
|---|---|---|---|---|---|---|
| eth0 | 3.64 GB | 18,494,381 | 0 | 0 | 0 | 0 |

5. Select **Storage** to view information about the disk devices and volumes on the services appliance.

DO-REF-DC1-GW1 (Gateway Node)

Overview | Hardware | Network | Storage | Load balancer | Tasks

**Disk devices**

| Name | World Wide Name | I/O load | Read rate | Write rate |
|---|---|---|---|---|
| croot(8:1,sda1) | N/A | 0.02% | 0 bytes/s | 3 KB/s |
| cvloc(8:2,sda2) | N/A | 0.03% | 0 bytes/s | 6 KB/s |

**Volumes**

| Mount point | Device | Status | Size | Available | Write cache status |
|---|---|---|---|---|---|
| / | croot | Online | 21.00 GB | 14.73 GB | Unknown |
| /var/local | cvloc | Online | 85.86 GB | 84.63 GB | Unknown |

**Related information**

SG100 and SG1000 services appliances

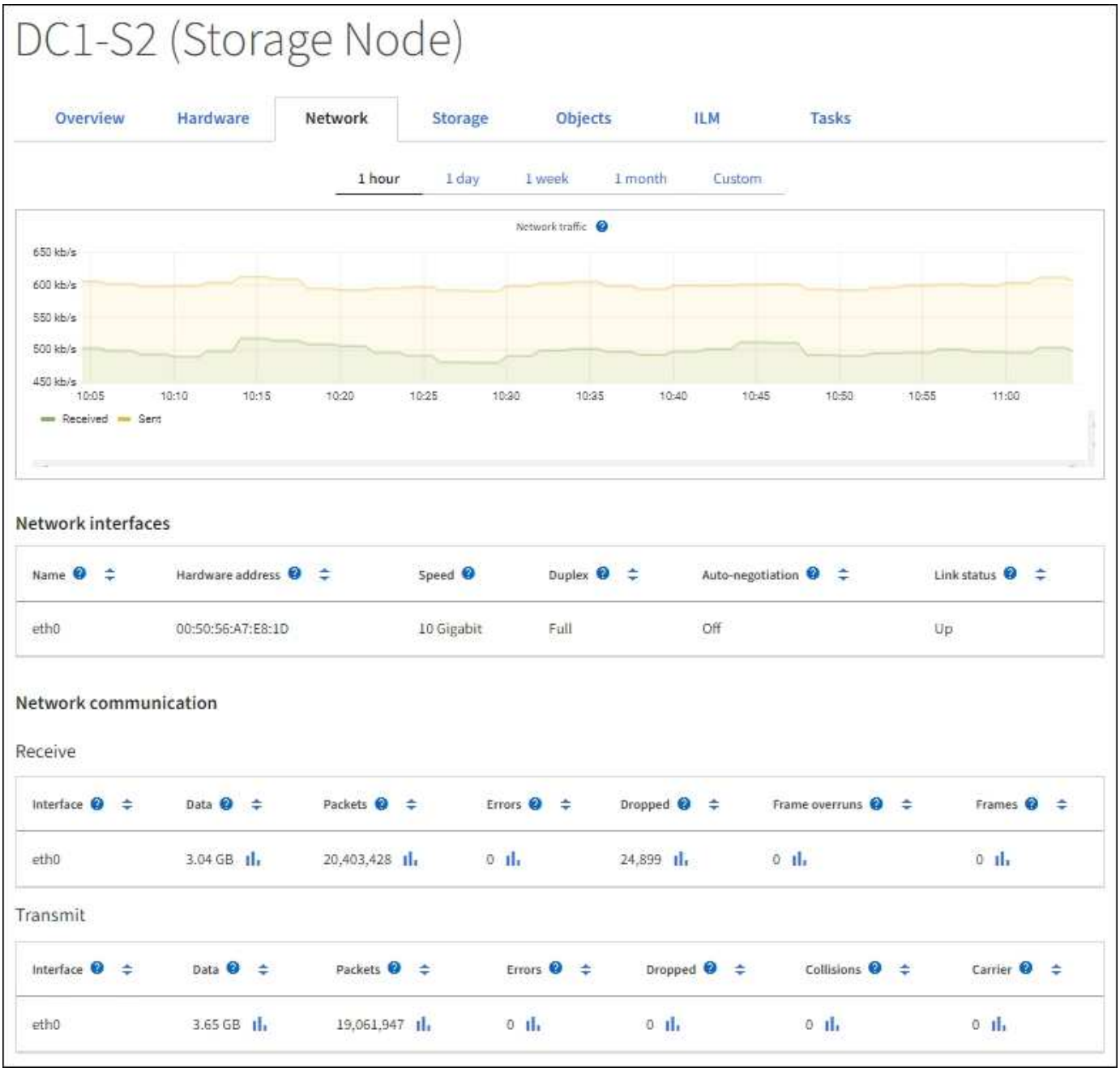
**View the Network tab**

The Network tab displays a graph showing the network traffic received and sent across all of the network interfaces on the node, site, or grid.

The Network tab is shown for all nodes, each site, and the entire grid.

To display a different time interval, select one of the controls above the chart or graph. You can display the information available for intervals of 1 hour, 1 day, 1 week, or 1 month. You can also set a custom interval, which allows you to specify date and time ranges.

For nodes, the Network interfaces table provides information about each node's physical network ports. The Network communications table provides details about each node's receive and transmit operations and any driver reported fault counters.




**Related information**

Monitor network connections and performance

### View the Storage tab

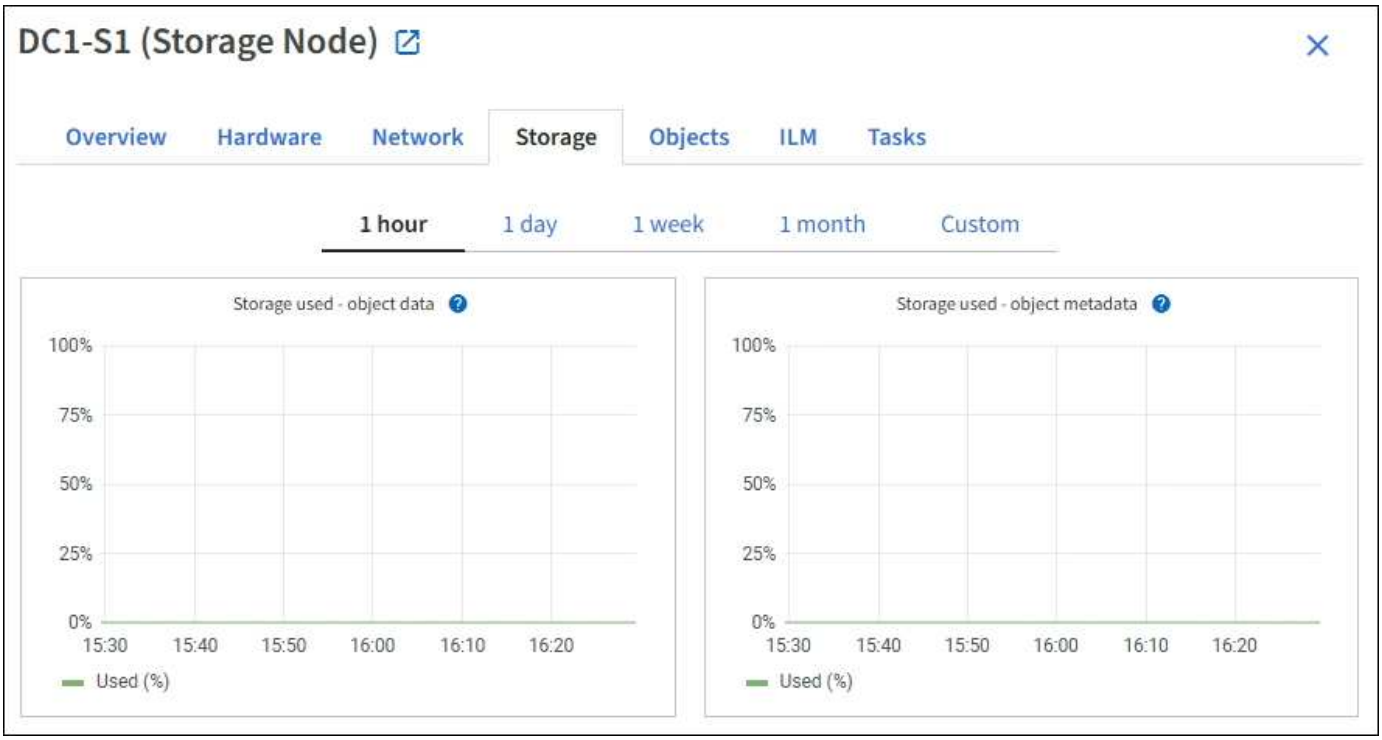
The Storage tab summarizes storage availability and other storage metrics.

The Storage tab is shown for all nodes, each site, and the entire grid.

#### Storage used graphs

For Storage Nodes, each site, and the entire grid, the Storage tab includes graphs showing how much storage has been used by object data and object metadata over time.

The total values for a site or the grid do not include nodes that not have reported metrics for at least five minutes, such as offline nodes.




**Disk devices, Volumes, and Object stores tables**

For all nodes, the Storage tab contains details for the disk devices and volumes on the node. For Storage Nodes, the Object Stores table provides information about each storage volume.

**Disk devices**

| Name | World Wide Name | I/O load | Read rate | Write rate |
|---|---|---|---|---|
| croot(8:1,sda1) | N/A | 0.04% | 0 bytes/s | 3 KB/s |
| cvloc(8:2,sda2) | N/A | 0.67% | 0 bytes/s | 50 KB/s |
| sdc(8:16,sdb) | N/A | 0.03% | 0 bytes/s | 4 KB/s |
| sdd(8:32,sdc) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |
| sde(8:48,sdd) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |

**Volumes**

| Mount point | Device | Status | Size | Available | Write cache status |
|---|---|---|---|---|---|
| / | croot | Online | 21.00 GB | 14.75 GB | Unknown |
| /var/local | cvloc | Online | 85.86 GB | 84.05 GB | Unknown |
| /var/local/rangedb/0 | sdc | Online | 107.32 GB | 107.17 GB | Enabled |
| /var/local/rangedb/1 | sdd | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/2 | sde | Online | 107.32 GB | 107.18 GB | Enabled |

**Object stores**

| ID | Size | Available | Replicated data | EC data | Object data (%) | Health |
|---|---|---|---|---|---|---|
| 0000 | 107.32 GB | 96.44 GB | 124.60 KB | 0 bytes | 0.00% | No Errors |
| 0001 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0002 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |

**Related information**

Monitor storage capacity

### Use the Task tab to reboot a grid node

The Task tab allows you to reboot the selected node. The Task tab is shown for all nodes.

**What you'll need**

- You are signed in to the Grid Manager using a supported web browser.
- You have the Maintenance or Root access permission.

- You have the provisioning passphrase.

**About this task**

You can use the Task tab to reboot a node. For appliance nodes, you can also use the Task tab to place the appliance into maintenance mode.

- Rebooting a grid node from the Task tab issues the reboot command on the target node. When you reboot a node, the node shuts down and restarts. All services are restarted automatically.

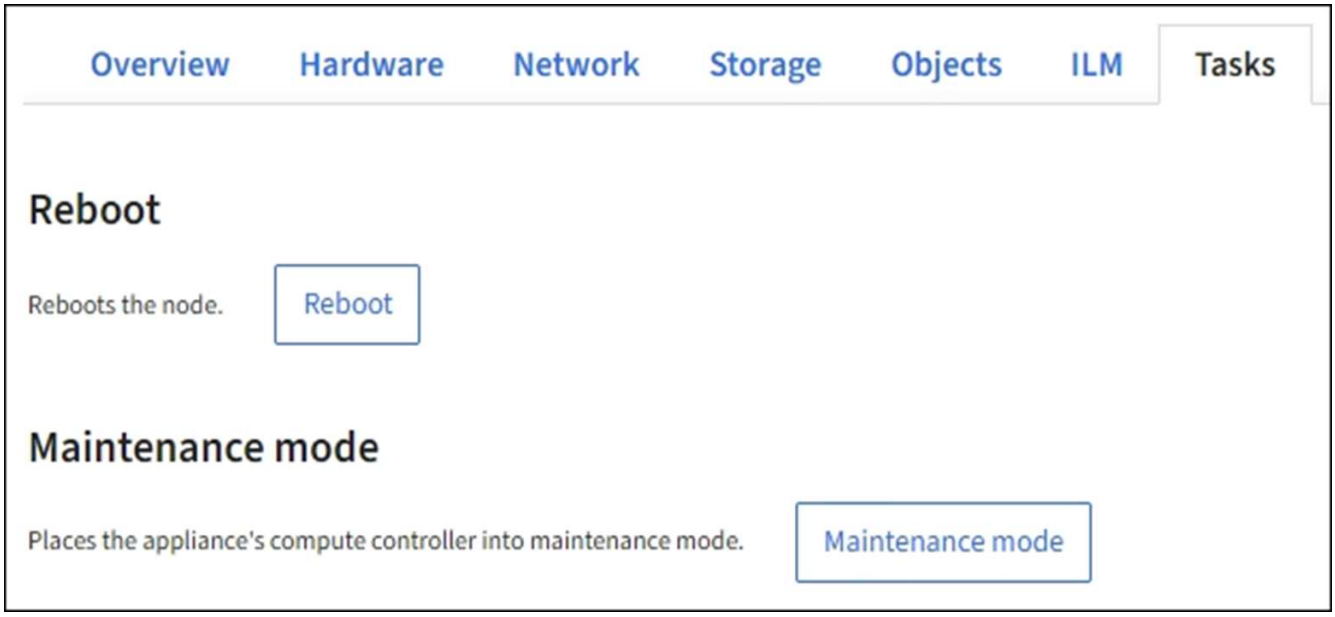
  If you plan to reboot a Storage Node, note the following:

  - If an ILM rule specifies an ingest behavior of Dual commit or the rule specifies Balanced and it is not possible to immediately create all required copies, StorageGRID immediately commits any newly ingested objects to two Storage Nodes on the same site and evaluates ILM later. If you want to reboot two or more Storage Nodes on a given site, you might not be able to access these objects for the duration of the reboot.
  - To ensure you can access all objects while a Storage Node is rebooting, stop ingesting objects at a site for approximately one hour before rebooting the node.
- You might need to put a StorageGRID appliance into maintenance mode to perform certain procedures, such as changing the link configuration or replacing a storage controller. For instructions, see the hardware installation and maintenance instructions for the appliance.

  In rare instances, placing a StorageGRID appliance into maintenance mode might make the appliance unavailable for remote access.

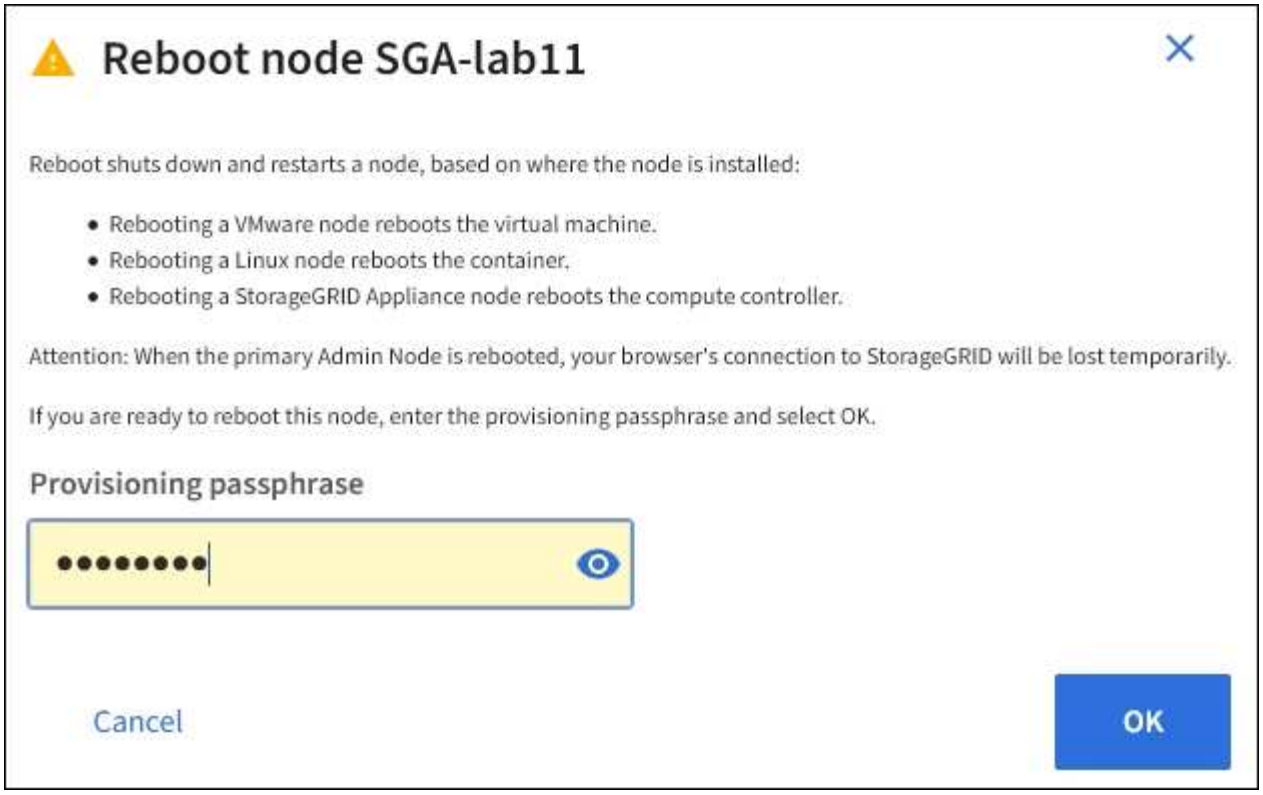
**Steps**

1. Select **NODES**.
2. Select the grid node you want to reboot.
3. Select the **Tasks** tab.




4. Select **Reboot**.

   A confirmation dialog box appears.




> If you are rebooting the primary Admin Node, the confirmation dialog box reminds you that your browser's connection to the Grid Manager will be lost temporarily when services are stopped.

5. Enter the provisioning passphrase, and click **OK**.
6. Wait for the node to reboot.

   It might take some time for services to shut down.

   When the node is rebooting, the gray icon (Administratively Down) appears on the left side of the **Nodes** page. When all services have started again and the node is successfully connected to the grid, the **Nodes** page should display a normal status (no icons to the left of the node name), indicating that no alerts are active and the node is connected to the grid.

**Related information**

SG6000 storage appliances

SG5700 storage appliances

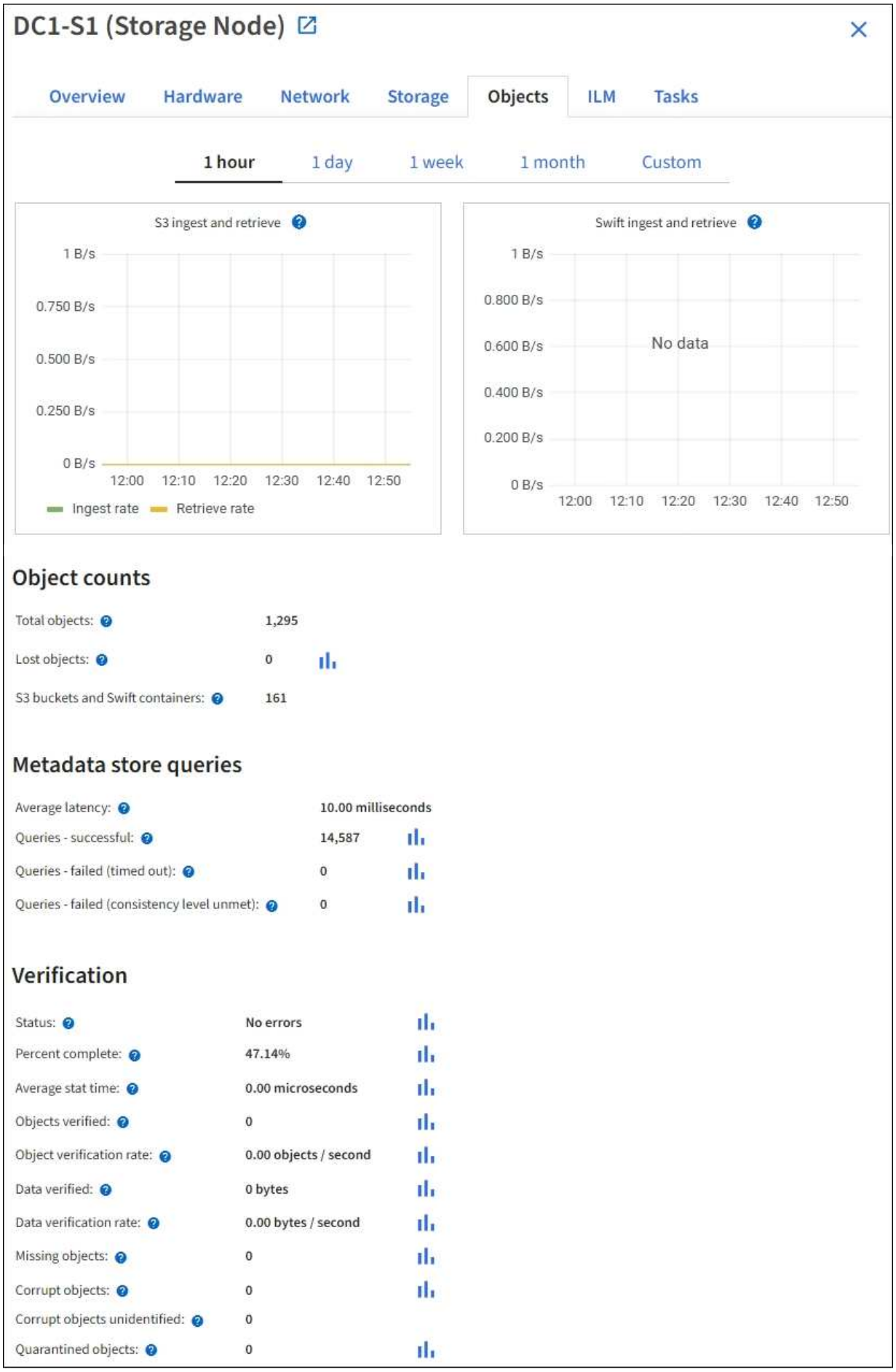
SG5600 storage appliances

SG100 and SG1000 services appliances

**View the Objects tab**

The Objects tab provides information about S3 and Swift ingest and retrieve rates.

The Objects tab is shown for each Storage Node, each site, and the entire grid. For Storage Nodes, the Objects tab also provides object counts and information about metadata queries and background verification.

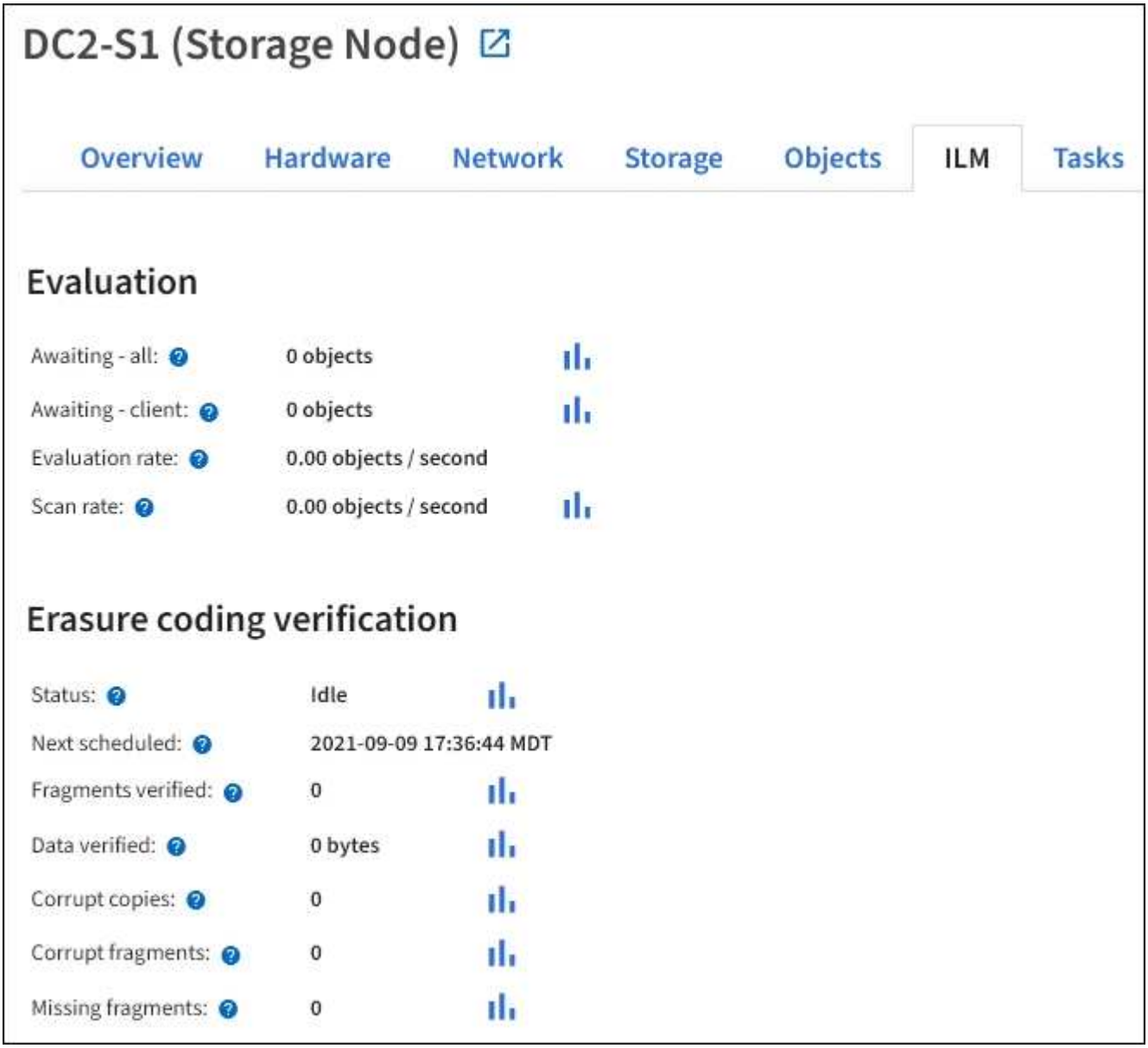

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 B/s
0 B/s
No data
12:00
12:10
12:20
12:30
12:40
12:50
Object counts
Total objects: 1,295
Lost objects: 0
S3 buckets and Swift containers: 161
Metadata store queries
Average latency: 10.00 milliseconds
Queries - successful: 14,587
Queries - failed (timed out): 0
Queries - failed (consistency level unmet): 0
Verification
Status: No errors
Percent complete: 47.14%
Average stat time: 0.00 microseconds
Objects verified: 0
Object verification rate: 0.00 objects / second
Data verified: 0 bytes
Data verification rate: 0.00 bytes / second
Missing objects: 0
Corrupt objects: 0
Corrupt objects unidentified: 0
Quarantined objects: 0

### View the ILM tab

## The ILM tab provides information about Information Lifecycle Management (ILM) operations.

The ILM tab is shown for each Storage Node, each site, and the entire grid. For each site and the grid, the ILM tab shows a graph of the ILM queue over time. For the grid, this tab also provides the estimated time to complete a full ILM scan of all objects.

For Storage Nodes, the ILM tab provides details about ILM evaluation and background verification for erasure coded objects.




**Related information**

Monitor information lifecycle management

Administer StorageGRID

### View the Load Balancer tab

## The Load Balancer tab includes performance and diagnostic graphs related to the operation of the Load Balancer service.

The Load Balancer tab is shown for Admin Nodes and Gateway Nodes, each site, and the entire grid. For each site, the Load Balancer tab provides an aggregate summary of the statistics for all nodes at that site. For the entire grid, the Load Balancer tab provides an aggregate summary of the statistics for all sites.

If there is no I/O being run through the Load Balancer service, or there is no load balancer configured, the graphs display “No data.”

#### Request traffic

This graph provides a 3-minute moving average of the throughput of data transmitted between load balancer endpoints and the clients making the requests, in bits per second.

> This value is updated at the completion of each request. As a result, this value might differ from the real-time throughput at low request rates or for very long-lived requests. You can look at the Network tab to get a more realistic view of the current network behavior.

#### Incoming request rate

This graph provides a 3-minute moving average of the number of new requests per second, broken down by request type (GET, PUT, HEAD, and DELETE). This value is updated when the headers of a new request have been validated.

#### Average request duration (non-error)

This graph provides a 3-minute moving average of request durations, broken down by request type (GET, PUT, HEAD, and DELETE). Each request duration starts when a request header is parsed by the Load Balancer service and ends when the complete response body is returned to the client.

#### Error response rate

This graph provides a 3-minute moving average of the number of error responses returned to clients per second, broken down by the error response code.

### Related information

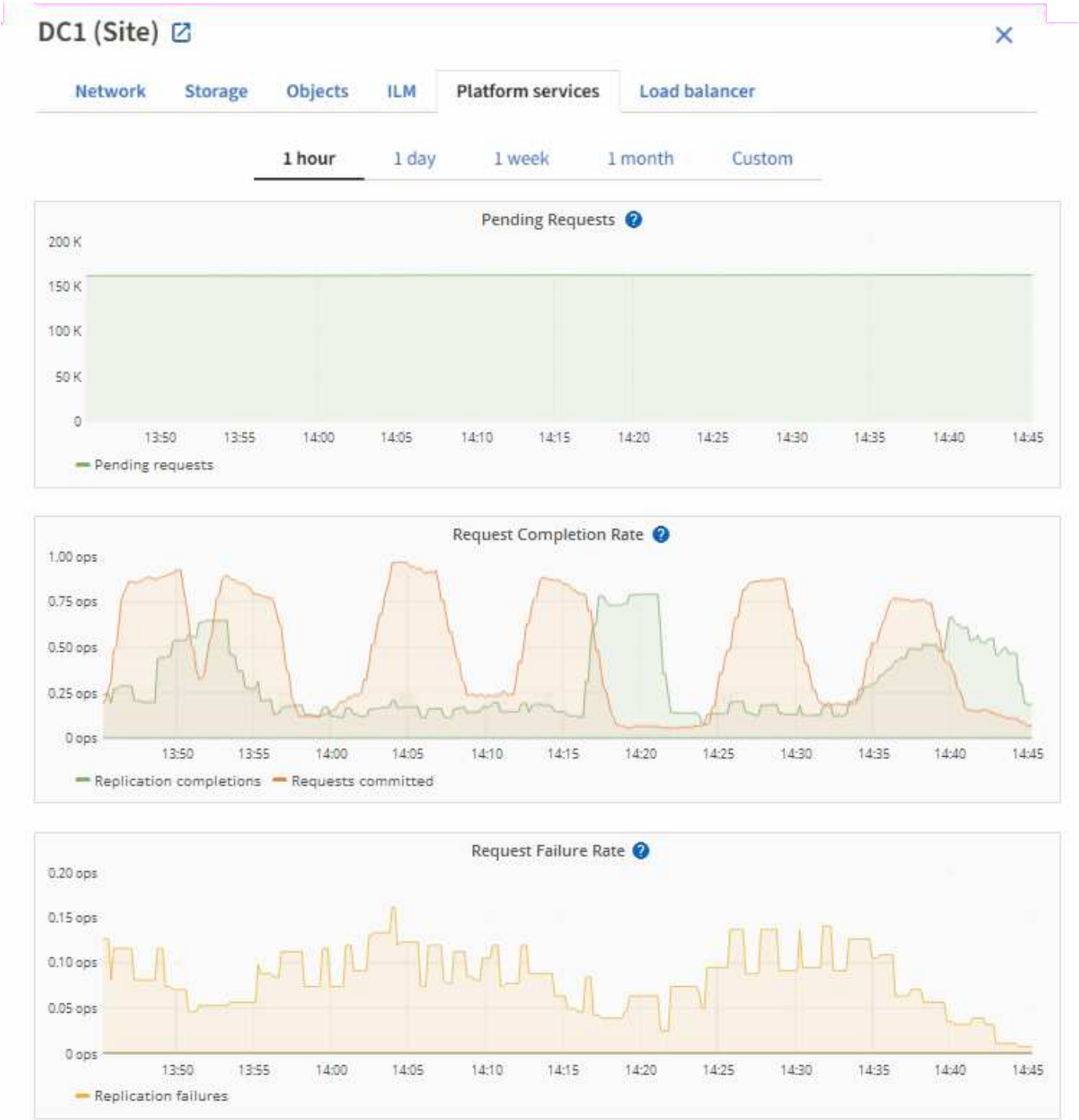
Monitor load balancing operations

Administer StorageGRID

## View the Platform services tab

The Platform services tab provides information about any S3 platform service operations at a site.

The Platform services tab is shown for each site. This tab provides information about S3 platform services, such as CloudMirror replication and the search integration service. Graphs on this tab display metrics such as the number of pending requests, request completion rate, and request failure rate.




For more information about S3 platform services, including troubleshooting details, see the instructions for administering StorageGRID.

#### View the SANtricity System Manager tab

The SANtricity System Manager tab enables you to access SANtricity System Manager without having to configure or connect the management port of the storage appliance. You can use this tab to review hardware diagnostic and environmental information as well as issues related to the drives.

The SANtricity System Manager tab is shown for storage appliance nodes.

Using SANtricity System Manager, you can do the following:

- View performance data such as storage array level performance, I/O latency, storage controller CPU utilization, and throughput
- Check hardware component status
- Perform support functions including viewing diagnostic data, and configuring E-Series AutoSupport

> To use SANtricity System Manager to configure a proxy for E-Series AutoSupport, see the instructions in administeringStorageGRID.

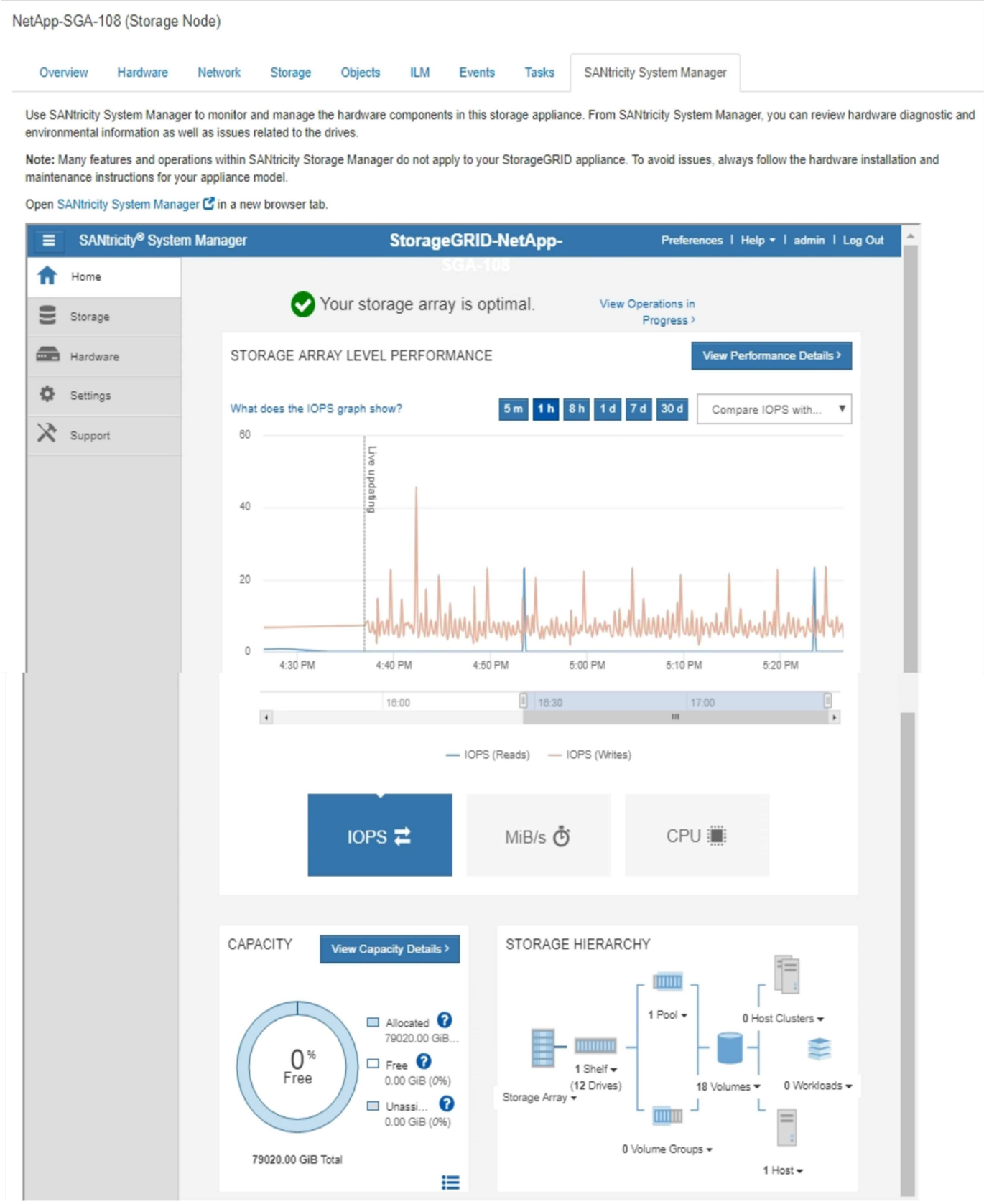
## Administer StorageGRID

To access SANtricity System Manager through Grid Manager, you must have the Storage Appliance Administrator permission or Root Access permission.

> You must have SANtricity firmware 8.70 (11.70) or higher to access SANtricity System Manager using the Grid Manager.

> Accessing SANtricity System Manager from the Grid Manager is generally meant only to monitor appliance hardware and configure E-Series AutoSupport. Many features and operations within SANtricity System Manager such as upgrading firmware do not apply to monitoring your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance.

The tab displays the home page of SANtricity System Manager.




You can use the SANtricity System Manager link to open the SANtricity System Manager in a new browser window for easier viewing.

To see details for storage array level performance and capacity usage, hover your cursor over each graph.

For more details on viewing the information accessible from the SANtricity System Manager tab, see NetApp E-Series and SANtricity documentation.

## Information you should monitor regularly

StorageGRID is a fault-tolerant, distributed storage system that is designed to continue operating even when errors occur, or when nodes or sites are unavailable. You must proactively monitor system health, workloads, and usage statistics so that you can take action to address potential issues before they affect the grid's efficiency or availability.

A busy system generates large amounts of information. This section provides guidance about the most important information to monitor on an ongoing basis.

| What to monitor | Frequency |
|---|---|
| The system health data shown on the Grid Manager Dashboard. Note if anything has changed from the previous day. | Daily |
| Rate at which Storage Node object and metadata capacity is being consumed | Weekly |
| Information lifecycle management operations | Weekly |
| Network connections and performance | Weekly |
| Node-level resources | Weekly |
| Tenant activity | Weekly |
| Capacity of the external archival storage system | Weekly |
| Load balancing operations | After the initial configuration and after any configuration changes |
| Availability of software hotfixes and software upgrades | Monthly |

### Monitor system health

You should monitor the overall health of your StorageGRID system on a daily basis.

#### About this task

The StorageGRID system is fault tolerant and can continue to operate even when parts of the grid are unavailable. The first sign of a potential issue with your StorageGRID system is likely to be an alert or an alarm (legacy system) and not necessarily an issue with system operations. Paying attention to system health can help you detect minor issues before they affect operations or grid efficiency.

The Health panel on the Grid Manager Dashboard provides a summary of issues that might be affecting your system. You should investigate any issues that are shown on the Dashboard.

To be notified of alerts as soon as they are triggered, you can set up email notifications for alerts or configure SNMP traps.

**Steps**

1. Sign in to the Grid Manager to view the Dashboard.
2. Review the information in the Health panel.

When issues exist, links appear that allow you to view additional details:

| Link | Indicates |
|---|---|
| Grid details | Appears if any nodes are disconnected (connection state Unknown or Administratively Down). Click the link, or click the blue or gray icon to determine which node or nodes are affected. |
| Current alerts | Appears if any alerts are currently active. Click the link, or click **Critical**, **Major**, or **Minor** to see the details on the **ALERTS** > **Current** page. |
| Recently resolved alerts | Appears if any alerts triggered in the past week are now resolved. Click the link to see the details on the **ALERTS** > **Resolved** page. |
| License | Appears if there is an issue with the software license for this StorageGRID system. Click the link to see the details on the **MAINTENANCE** > **System** > **License** page. |

**Related information**

- Administer StorageGRID
- Set up email notifications for alerts
- Use SNMP monitoring

#### Monitor node connection states

If one or more nodes are disconnected from the grid, critical StorageGRID operations might be affected. You must monitor node connection states and address any issues

promptly.

### What you'll need

- You must be signed in to the Grid Manager using a supported web browser.

### About this task

Nodes can have one of three connection states:

- **Not connected - Unknown** : The node is not connected to the grid for an unknown reason. For example, the network connection between nodes has been lost or the power is down. The **Unable to communicate with node** alert might also be triggered. Other alerts might be active as well. This situation requires immediate attention.

  > A node might appear as Unknown during managed shutdown operations. You can ignore the Unknown state in these cases.

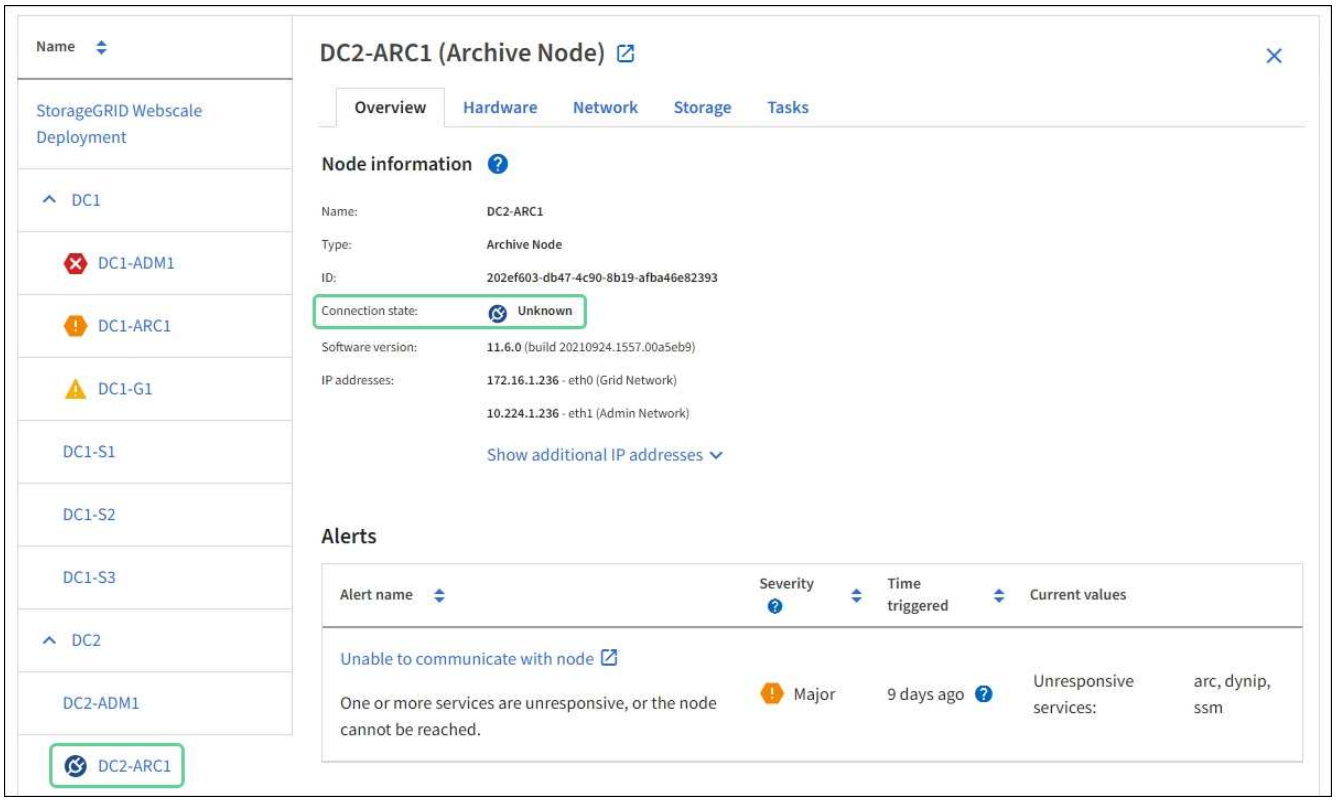
- **Not connected - Administratively down** : The node is not connected to the grid for an expected reason. For example, the node, or services on the node, has been gracefully shut down, the node is rebooting, or the software is being upgraded. One or more alerts might also be active.
- **Connected** : The node is connected to the grid.

### Steps

1. If a blue or gray icon appears on the Health panel of the Dashboard, click the icon or click **Grid details**. (The blue or gray icons and the **Grid details** link appear only if at least one node is disconnected from the grid.)

   The Overview page for the first blue node in the node tree appears. If there are no blue nodes, the Overview page for the first gray node in the tree appears.

   In the example, the Storage Node named DC1-S3 has a blue icon. The **Connection State** on the Node Information panel is **Unknown**, and the **Unable to communicate with node** alert is active. The alert indicates that one or more services are unresponsive, or the node cannot be reached.




2. If a node has a blue icon, follow these steps:
   a. Select each alert in the table, and follow the recommended actions.

      For example, you might need to restart a service that has stopped or restart the host for the node.

   b. If you are unable to bring the node back online, contact technical support.
3. If a node has a gray icon, follow these steps:

   Gray nodes are expected during maintenance procedures and might be associated with one or more alerts. Based on the underlying issue, these “administratively down” nodes often go back online with no intervention.

   a. Review the Alerts section, and determine if any alerts are affecting this node.
   b. If one or more alerts are active, select each alert in the table, and follow the recommended actions.
   c. If you are unable to bring the node back online, contact technical support.

**Related information**

Alerts reference

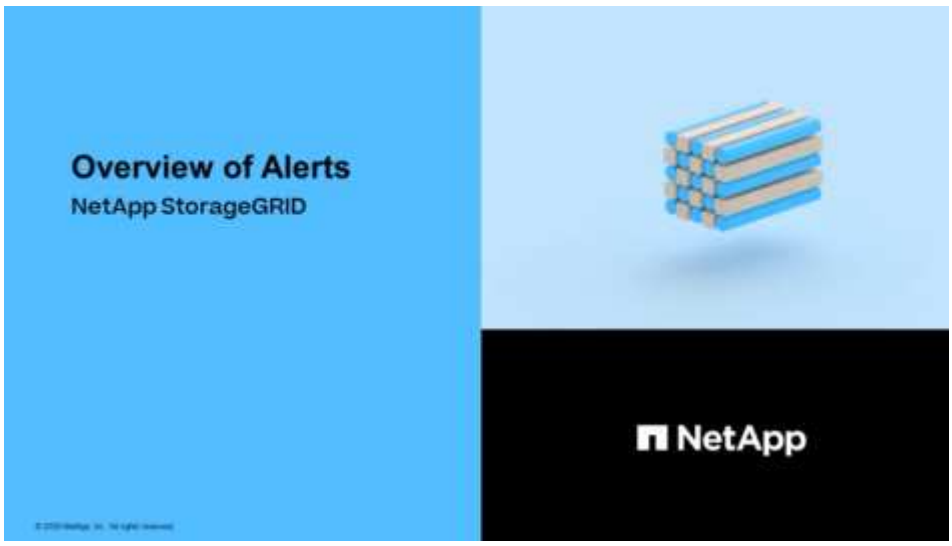
Recover and maintain

#### View current alerts

When an alert is triggered, an alert icon is displayed on the Dashboard. An alert icon is also displayed for the node on the Nodes page. An email notification might also be sent, unless the alert has been silenced.

**What you’ll need**

- You must be signed in to the Grid Manager using a supported web browser.
- Optionally, you have watched the video: Video: Overview of Alerts.

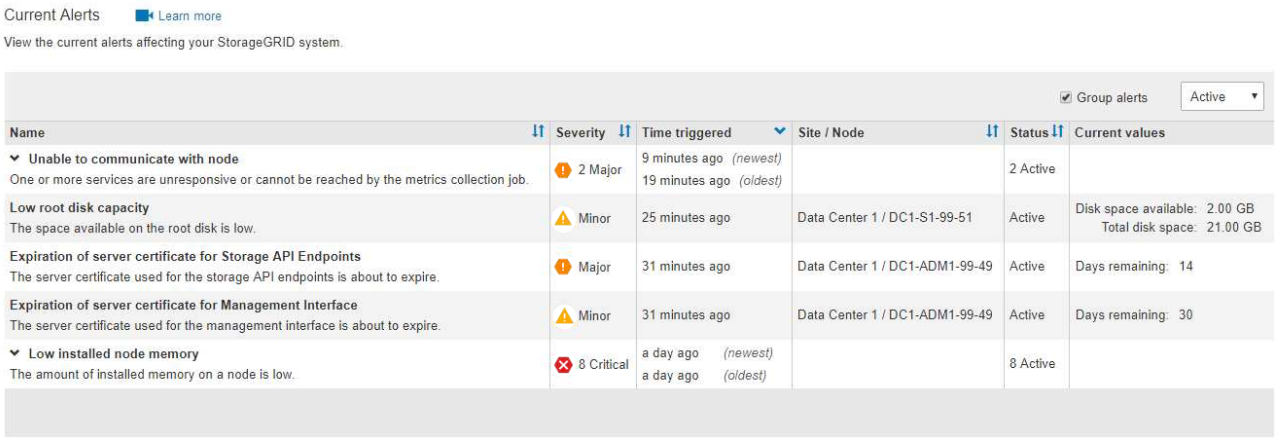



**Steps**

1. If one or more alerts are active, do either of the following:

   - From the Health panel on the Dashboard, click the alert icon or click **Current alerts**. (An alert icon and the **Current alerts** link appear only if at least one alert is currently active.)
   - Select **ALERTS** > **Current**.

     The Current Alerts page appears. It lists all alerts currently affecting your StorageGRID system.




     By default, alerts are shown as follows:

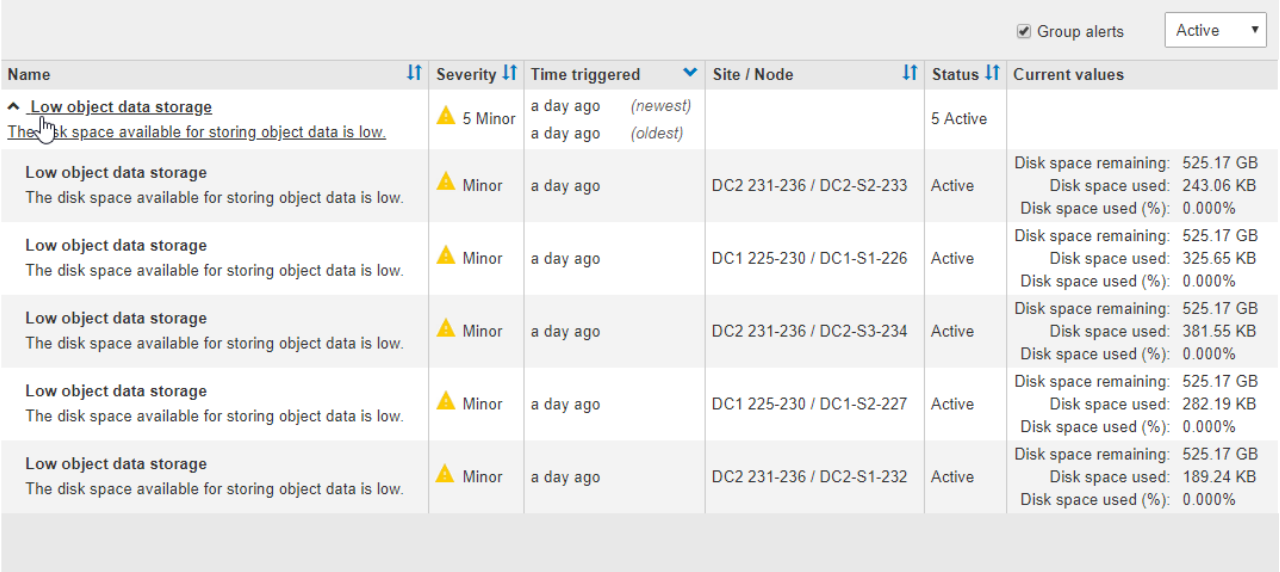
   - The most recently triggered alerts are shown first.
   - Multiple alerts of the same type are shown as a group.
   - Alerts that have been silenced are not shown.
   - For a specific alert on a specific node, if the thresholds are reached for more than one severity, only the most severe alert is shown. That is, if alert thresholds are reached for the minor, major, and critical severities, only the critical alert is shown.

   The Current Alerts page is refreshed every two minutes.

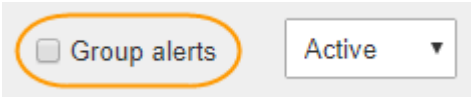
2. Review the information in the table.

| Column header | Description |
|---|---|
| Name | The name of the alert and its description. |
| Severity | The severity of the alert. If multiple alerts are grouped, the title row shows how many instances of that alert are occurring at each severity.<br><br>• **Critical** : An abnormal condition exists that has stopped the normal operations of a StorageGRID node or service. You must address the underlying issue immediately. Service disruption and loss of data might result if the issue is not resolved.<br><br>• **Major** : An abnormal condition exists that is either affecting current operations or approaching the threshold for a critical alert. You should investigate major alerts and address any underlying issues to ensure that the abnormal condition does not stop the normal operation of a StorageGRID node or service.<br><br>• **Minor** : The system is operating normally, but an abnormal condition exists that could affect the system's ability to operate if it continues. You should monitor and resolve minor alerts that do not clear on their own to ensure they do not result in a more serious problem. |
| Time triggered | How long ago the alert was triggered. If multiple alerts are grouped, the title row shows times for the most recent instance of the alert (*newest*) and the oldest instance of the alert (*oldest*). |
| Site/Node | The name of the site and node where the alert is occurring. If multiple alerts are grouped, the site and node names are not shown in the title row. |
| Status | Whether the alert is active or has been silenced. If multiple alerts are grouped and **All alerts** is selected in the drop-down, the title row shows how many instances of that alert are active and how many instances have been silenced. |
| Current values | The current value of the metric that caused the alert to be triggered. For some alerts, additional values are shown to help you understand and investigate the alert. For example, the values shown for a **Low object data storage** alert include the percentage of disk space used, the total amount of disk space, and the amount of disk space used.<br><br>**Note:** If multiple alerts are grouped, current values are not shown in the title row. |

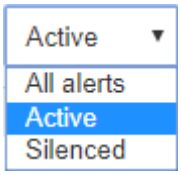
3. To expand and collapse groups of alerts:
   - To show the individual alerts in a group, click the down caret ⌄ in the heading, or click the group's name.
   - To hide the individual alerts in a group, click the up caret ⌃ in the heading, or click the group's name.




4. To display individual alerts instead of groups of alerts, unselect the **Group alerts** check box at the top of the table.




5. To sort alerts or alert groups, click the up/down arrows in each column header.
   - When **Group alerts** is selected, both the alert groups and the individual alerts within each group are sorted. For example, you might want to sort the alerts in a group by **Time triggered** to find the most recent instance of a specific alert.
   - When **Group alerts** is unselected, the entire list of alerts is sorted. For example, you might want to sort all alerts by **Node/Site** to see all alerts affecting a specific node.
6. To filter the alerts by status, use the drop-down menu at the top of the table.




   - Select **All alerts** to view all current alerts (both active and silenced alerts).
   - Select **Active** to view only the current alerts that are active.
   - Select **Silenced** to view only the current alerts that have been silenced. See Silence alert notifications.
7. To view details for a specific alert, select the alert from the table.

   A dialog box for the alert appears. See View a specific alert.

#### View resolved alerts

## You can search and view a history of alerts that have been resolved.

### What you'll need

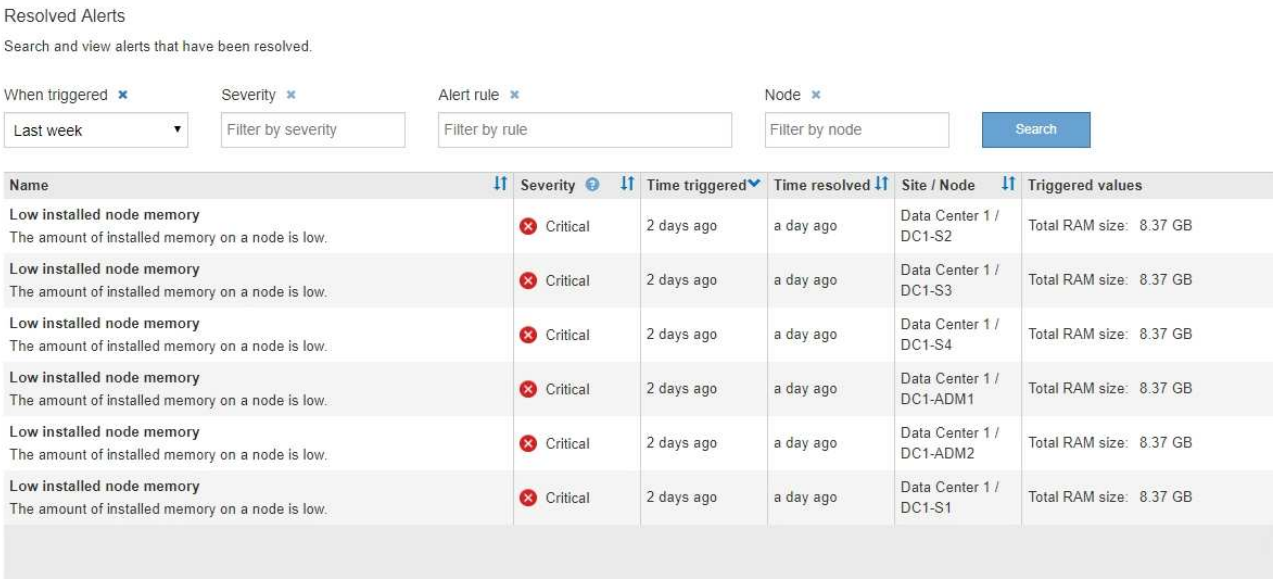
- You must be signed in to the Grid Manager using a supported web browser.

**Steps**

1. To view resolved alerts, do either of the following:
   - From the Health panel on the Dashboard, click **Recently resolved alerts**.

     The **Recently resolved alerts** link appears only if one or more alerts were triggered in the past week and are now resolved.

   - Select **ALERTS** > **Resolved**. The Resolved Alerts page appears. By default, resolved alerts that were triggered in the last week are shown, with the most recently triggered alerts shown first. The alerts on this page were previously shown on the Current Alerts page or in an email notification.




2. Review the information in the table.

| Column header | Description |
| --- | --- |
| Name | The name of the alert and its description. |

| Column header | Description |
| --- | --- |
| Severity | The severity of the alert.<br>• **Critical** : An abnormal condition exists that has stopped the normal operations of a StorageGRID node or service. You must address the underlying issue immediately. Service disruption and loss of data might result if the issue is not resolved.<br>• **Major** : An abnormal condition exists that is either affecting current operations or approaching the threshold for a critical alert. You should investigate major alerts and address any underlying issues to ensure that the abnormal condition does not stop the normal operation of a StorageGRID node or service.<br>• **Minor** : The system is operating normally, but an abnormal condition exists that could affect the system's ability to operate if it continues. You should monitor and resolve minor alerts that do not clear on their own to ensure they do not result in a more serious problem. |
| Time triggered | How long ago the alert was triggered. |
| Time resolved | How long ago the alert was resolved. |
| Site/Node | The name of the site and node where the alert occurred. |
| Triggered values | The value of the metric that caused the alert to be triggered. For some alerts, additional values are shown to help you understand and investigate the alert. For example, the values shown for a **Low object data storage** alert include the percentage of disk space used, the total amount of disk space, and the amount of disk space used. |

3. To sort the entire list of resolved alerts, click the up/down arrows in each column header.

   For example, you might want to sort resolved alerts by **Site/Node** to see the alerts that affected a specific node.

4. Optionally, filter the list of resolved alerts by using the drop-down menus at the top of the table.
   a. Select a time period from the **When triggered** drop-down menu to show resolved alerts based on how long ago they were triggered.

You can search for alerts that were triggered within the following time periods:

- Last hour
- Last day
- Last week (default view)
- Last month
- Any time period
- Custom (allows you to specify the start date and the end date for the time period)

b. Select one or more severities from the **Severity** drop-down menu to filter on resolved alerts of a specific severity.

c. Select one or more default or custom alert rules from the **Alert rule** drop-down menu to filter on resolved alerts related to a specific alert rule.

d. Select one or more nodes from the **Node** drop-down menu to filter on resolved alerts related to a specific node.

e. Click **Search**.

5. To view details for a specific resolved alert, select the alert from the table.

   A dialog box for the alert appears. See View a specific alert.

#### View a specific alert

You can view detailed information about an alert that is currently affecting your StorageGRID system or an alert that has been resolved. The details include recommended corrective actions, the time the alert was triggered, and the current value of the metrics related to this alert.

Optionally, you can silence a current alert or update the alert rule.

**What you'll need**

- You are signed in to the Grid Manager using a supported web browser.

**Steps**

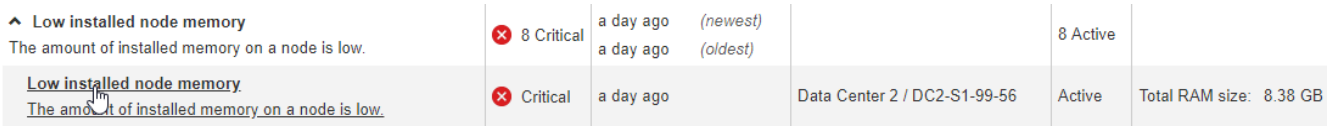
1. Do one of the following, based on whether you want to view a current or resolved alert:

| Column header | Description |
|---|---|
| Current alert | • From the Health panel on the Dashboard, click the **Current alerts** link. This link appears only if at least one alert is currently active. This link is hidden if there are no current alerts or if all current alerts have been silenced.<br>• Select **ALERTS** > **Current**.<br>• From the **NODES** page, select the **Overview** tab for a node that has an alert icon. Then, in the Alerts section, click the alert name. |

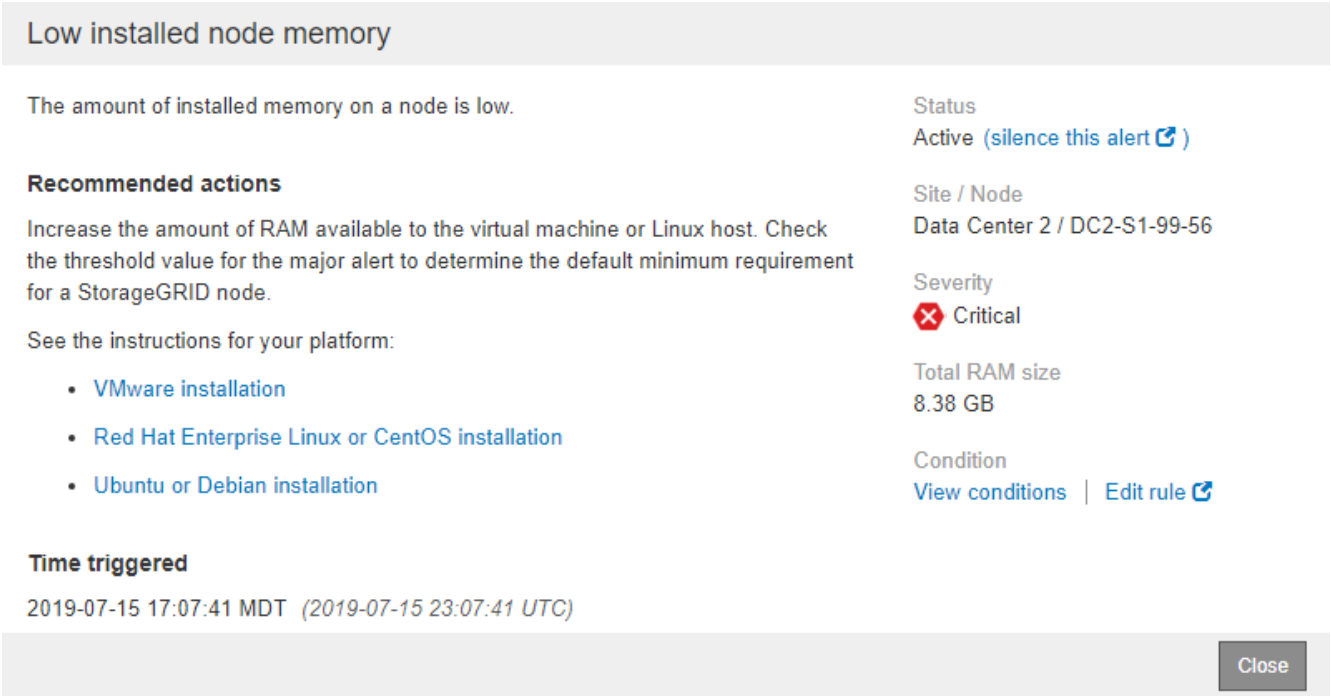
| Column header | Description |
| --- | --- |
| Resolved alert | • From the Health panel on the Dashboard, click the **Recently resolved alerts** link. (This link appears only if one or more alerts were triggered in the past week and are now resolved. This link is hidden if no alerts were triggered and resolved in the last week.)<br>• Select **ALERTS** > **Resolved**. |

2. As required, expand a group of alerts and then select the alert you want to view.

Select the alert, not the heading for a group of alerts.




A dialog box appears and provides details for the selected alert.




3. Review the alert details.

| Information | Description |
| --- | --- |
| *title* | The name of the alert. |
| *first paragraph* | The description of the alert. |
| Recommended actions | The recommended actions for this alert. |

| Information | Description |
| --- | --- |
| Time triggered | The date and time the alert was triggered in your local time and in UTC. |
| Time resolved | For resolved alerts only, the date and time the alert was resolved in your local time and in UTC. |
| Status | The status of the alert: Active, Silenced, or Resolved. |
| Site/Node | The name of the site and node affected by the alert. |
| Severity | The severity of the alert.<br>• **Critical** : An abnormal condition exists that has stopped the normal operations of a StorageGRID node or service. You must address the underlying issue immediately. Service disruption and loss of data might result if the issue is not resolved.<br>• **Major** : An abnormal condition exists that is either affecting current operations or approaching the threshold for a critical alert. You should investigate major alerts and address any underlying issues to ensure that the abnormal condition does not stop the normal operation of a StorageGRID node or service.<br>• **Minor** : The system is operating normally, but an abnormal condition exists that could affect the system's ability to operate if it continues. You should monitor and resolve minor alerts that do not clear on their own to ensure they do not result in a more serious problem. |
| *data values* | The current value of the metric for this alert. For some alerts, additional values are shown to help you understand and investigate the alert. For example, the values shown for a **Low metadata storage** alert include the percent of disk space used, the total amount of disk space, and the amount of disk space used. |

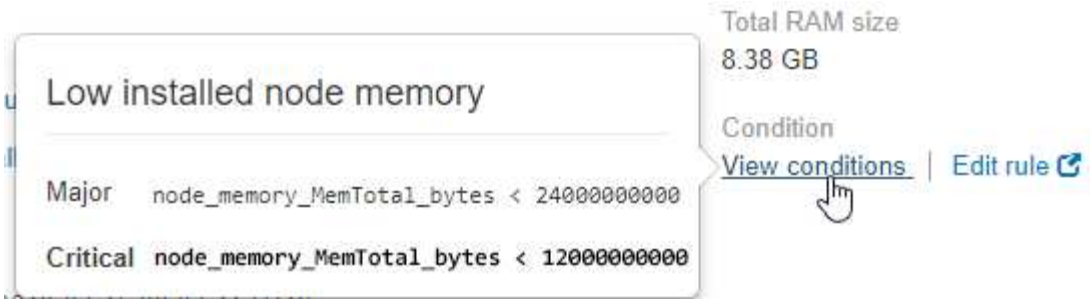
4. Optionally, click **silence this alert** to silence the alert rule that caused this alert to be triggered.

   You must have the Manage Alerts or Root access permission to silence an alert rule.

   > Be careful when deciding to silence an alert rule. If an alert rule is silenced, you might not detect an underlying problem until it prevents a critical operation from completing.

5. To view the current conditions for the alert rule:
   a. From the alert details, click **View conditions**.

      A pop-up appears, listing the Prometheus expression for each defined severity.




b. To close the pop-up, click anywhere outside of the pop-up.

6. Optionally, click **Edit rule** to edit the alert rule that caused this alert to be triggered:

   You must have the Manage Alerts or Root access permission to edit an alert rule.

   > Be careful when deciding to edit an alert rule. If you change trigger values, you might not detect an underlying problem until it prevents a critical operation from completing.

7. To close the alert details, click **Close**.

#### View legacy alarms

Alarms (legacy system) are triggered when system attributes reach alarm threshold values. You can view the currently active alarms from the Current Alarms page.

> While the legacy alarm system continues to be supported, the alert system offers significant benefits and is easier to use.

**What you'll need**

- You must be signed in to the Grid Manager using a supported web browser.

**Steps**

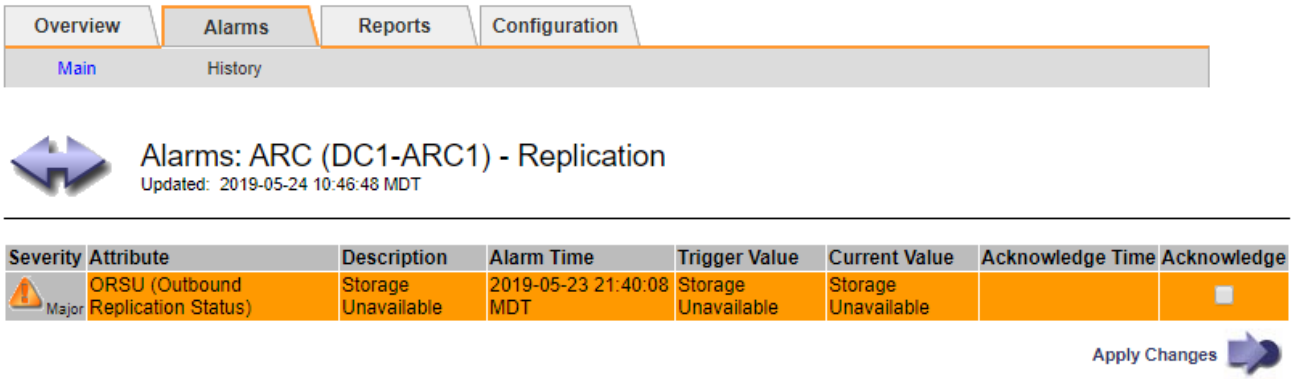
1. Select **SUPPORT** > **Alarms (legacy)** > **Current alarms**.

   The alarm icon indicates the severity of each alarm, as follows:

| Icon | Color | Alarm severity | Meaning |
|---|---|---|---|
| | Yellow | Notice | The node is connected to the grid, but an unusual condition exists that does not affect normal operations. |
| | Light Orange | Minor | The node is connected to the grid, but an abnormal condition exists that could affect operation in the future. You should investigate to prevent escalation. |
| | Dark Orange | Major | The node is connected to the grid, but an abnormal condition exists that currently affects operation. This requires prompt attention to prevent escalation. |
| | Red | Critical | The node is connected to the grid, but an abnormal condition exists that has stopped normal operations. You should address the issue immediately. |

2. To learn about the attribute that caused the alarm to be triggered, right click the attribute name in the table.
3. To view additional details about an alarm, click the service name in the table.

   The Alarms tab for the selected service appears (**SUPPORT** > **Tools** > **Grid topology** > ***Grid Node*** > ***Service*** > **Alarms**).




4. If you want to clear the count of current alarms, you can optionally do the following:
   - Acknowledge the alarm. An acknowledged alarm is no longer included in the count of legacy alarms unless it is triggered at the next severity level or it is resolved and occurs again.
   - Disable a particular Default alarm or Global Custom alarm for the entire system to prevent it from being triggered again.

**Related information**

Alarms reference (legacy system)

Acknowledge current alarms (legacy system)

Disable alarms (legacy system)

## Monitor storage capacity

Monitor the total usable space available to ensure that the StorageGRID system does not run out of storage space for objects or for object metadata.

StorageGRID stores object data and object metadata separately, and reserves a specific amount of space for a distributed Cassandra database that contains object metadata. Monitor the total amount of space consumed for objects and for object metadata, as well as trends in the amount of space consumed for each. This will enable you to plan ahead for the addition of nodes and avoid any service outages.

You can view storage capacity information for the entire grid, for each site, and for each Storage Node in your StorageGRID system.

### Monitor storage capacity for the entire grid

You must monitor the overall storage capacity for your grid to ensure that adequate free space remains for object data and object metadata. Understanding how storage capacity changes over time can help you plan to add Storage Nodes or storage volumes before the grid's usable storage capacity is consumed.

#### What you'll need

You are signed in to the Grid Manager using a supported web browser.

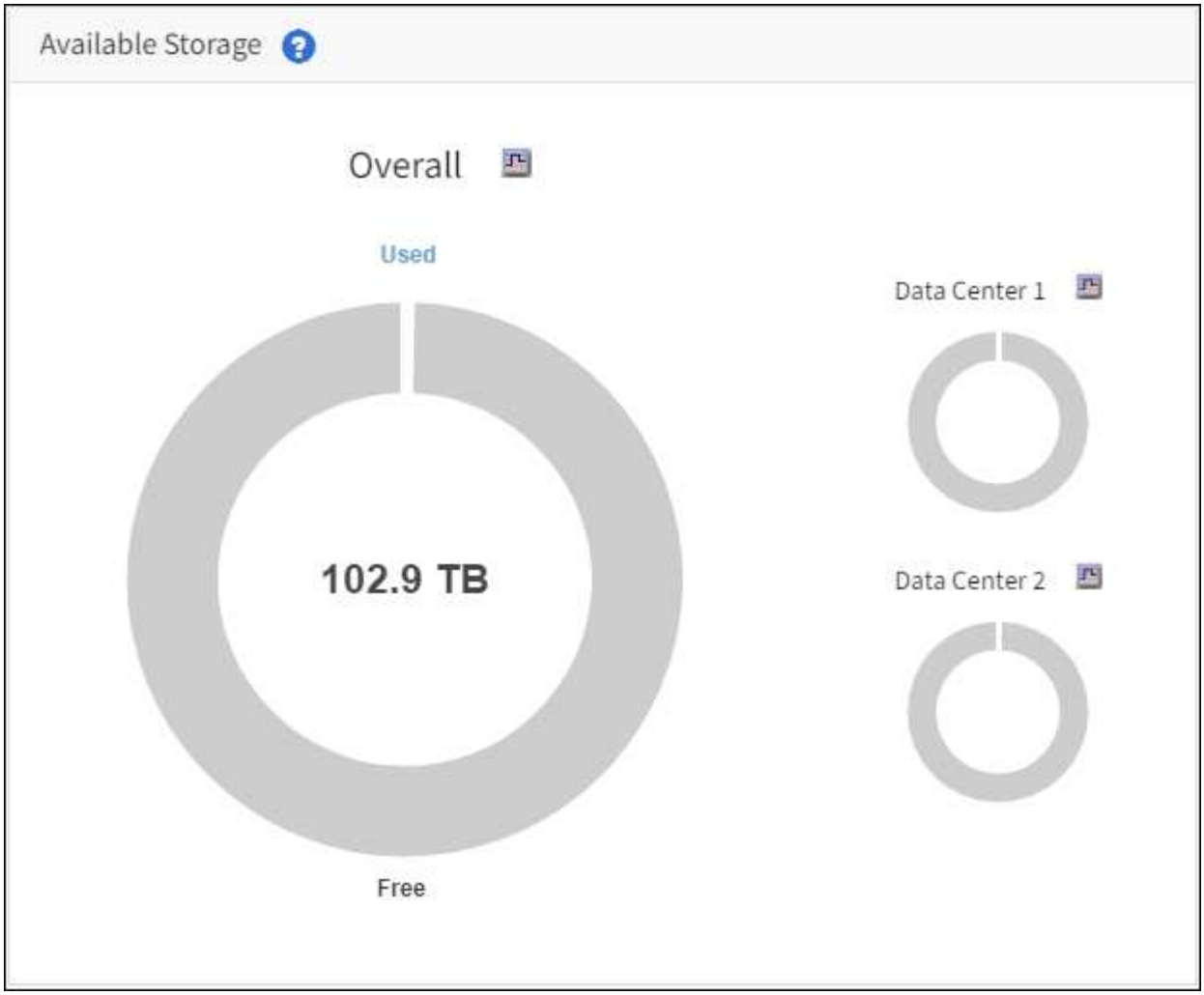
#### About this task

The Dashboard in the Grid Manager lets you quickly assess how much storage is available for the entire grid and for each data center. The Nodes page provides more detailed values for object data and object metadata.

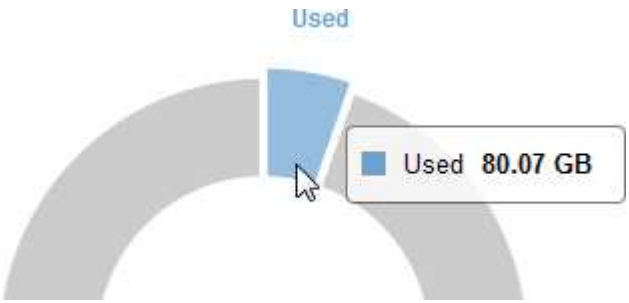
#### Steps

1. Assess how much storage is available for the entire grid and for each data center.
   a. Select **Dashboard**.
   b. In the Available Storage panel, note the overall summary of free and used storage capacity.

      The summary does not include archival media.




c. Place your cursor over the chart's Free or Used capacity sections to see exactly how much space is free or used.




d. For multi-site grids, review the chart for each data center.

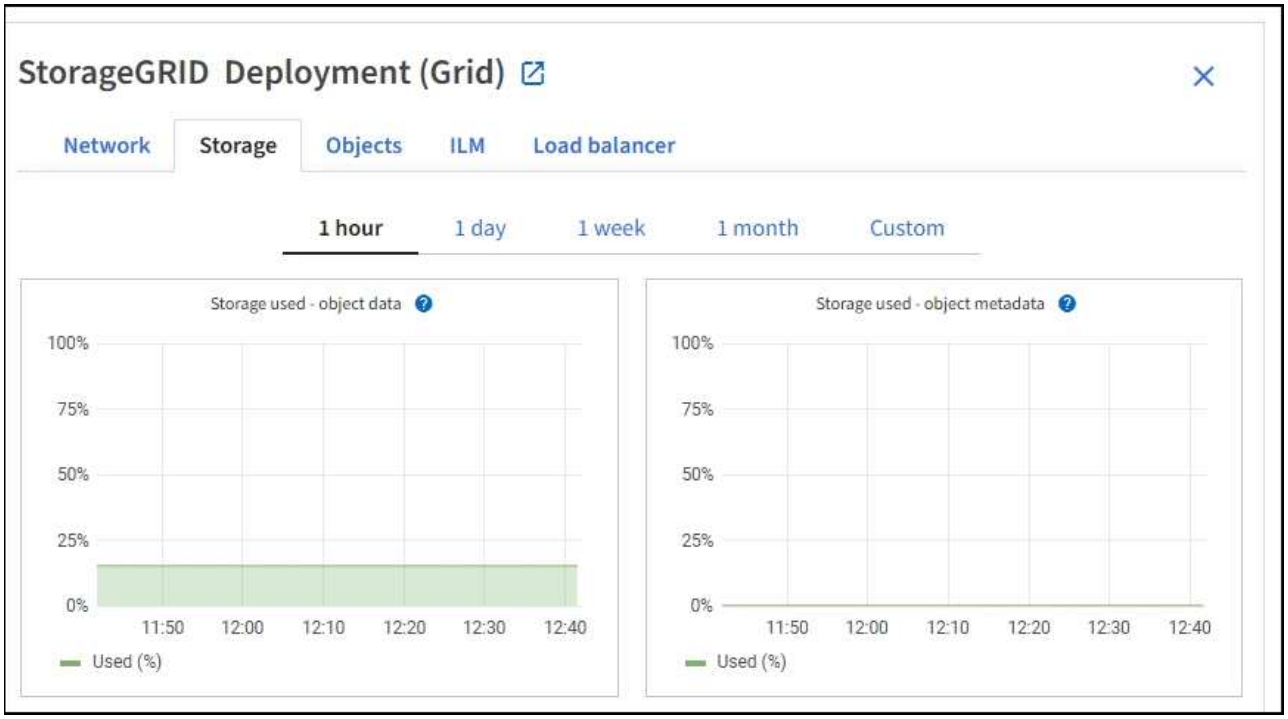
e. Click the chart icon for the overall chart or for an individual data center to view a graph showing capacity usage over time.

   A graph showing Percentage Storage Capacity Used (%) vs. Time appears.

2. Determine how much storage has been used and how much storage remains available for object data and object metadata.

   a. Select **NODES**.

   b. Select ***grid*** > **Storage**.




c. Hover your cursor over the **Storage used - object data** and the **Storage used - object metadata** charts to see how much object storage and object metadata storage is available for the entire grid, and how much has been used over time.

> The total values for a site or the grid do not include nodes that not have reported metrics for at least five minutes, such as offline nodes.

3. Plan to perform an expansion to add Storage Nodes or storage volumes before the grid's usable storage capacity is consumed.

   When planning the timing of an expansion, consider how long it will take to procure and install additional storage.

   > If your ILM policy uses erasure coding, you might prefer to expand when existing Storage Nodes are approximately 70% full to reduce the number of nodes that must be added.

   For more information on planning a storage expansion, see the instructions for expanding StorageGRID.

#### Monitor storage capacity for each Storage Node

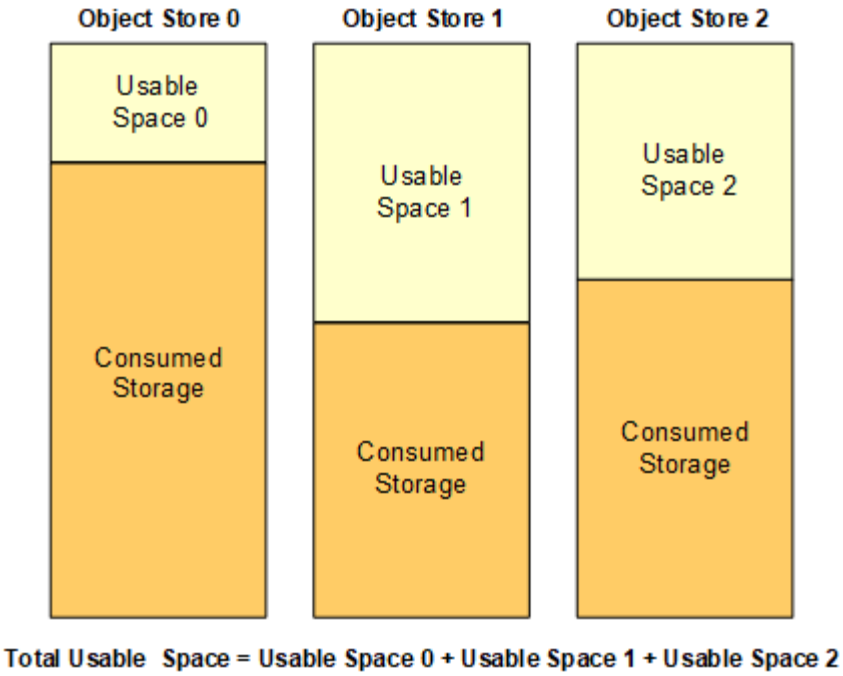
Monitor the total usable space for each Storage Node to ensure that the node has enough space for new object data.

**What you'll need**

- You are signed in to the Grid Manager using a supported web browser.

**About this task**

Usable space is the amount of storage space available to store objects. The total usable space for a Storage Node is calculated by adding together the available space on all object stores within the node.




**Steps**

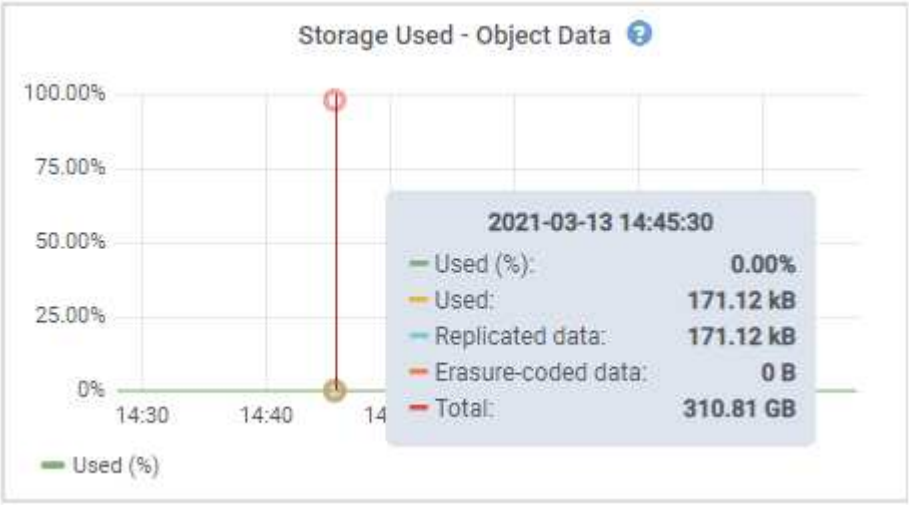
1. Select **NODES** > ***Storage Node*** > **Storage**.

   The graphs and tables for the node appear.

2. Hover your cursor over the Storage used - object data graph.

   The following values are shown:

   - **Used (%)**: The percentage of the Total usable space that has been used for object data.
   - **Used**: The amount of the Total usable space that has been used for object data.
   - **Replicated data**: An estimate of the amount of replicated object data on this node, site, or grid.
   - **Erasure-coded data**: An estimate of the amount of erasure-coded object data on this node, site, or grid.
   - **Total**: The total amount of usable space on this node, site, or grid. The Used value is the `storagegrid_storage_utilization_data_bytes` metric.



3. Review the Available values in the Volumes and Object stores tables, below the graphs.

To view graphs of these values, click the chart icons in the Available columns.

**Disk devices**

| Name | World Wide Name | I/O load | Read rate | Write rate |
|---|---|---|---|---|
| croot(8:1,sda1) | N/A | 0.04% | 0 bytes/s | 3 KB/s |
| cvloc(8:2,sda2) | N/A | 0.67% | 0 bytes/s | 50 KB/s |
| sdc(8:16,sdb) | N/A | 0.03% | 0 bytes/s | 4 KB/s |
| sdd(8:32,sdc) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |
| sde(8:48,sdd) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |

**Volumes**

| Mount point | Device | Status | Size | Available | Write cache status |
|---|---|---|---|---|---|
| / | croot | Online | 21.00 GB | 14.75 GB | Unknown |
| /var/local | cvloc | Online | 85.86 GB | 84.05 GB | Unknown |
| /var/local/rangedb/0 | sdc | Online | 107.32 GB | 107.17 GB | Enabled |
| /var/local/rangedb/1 | sdd | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/2 | sde | Online | 107.32 GB | 107.18 GB | Enabled |

**Object stores**

| ID | Size | Available | Replicated data | EC data | Object data (%) | Health |
|---|---|---|---|---|---|---|
| 0000 | 107.32 GB | 96.44 GB | 124.60 KB | 0 bytes | 0.00% | No Errors |
| 0001 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0002 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |

4. Monitor the values over time to estimate the rate at which usable storage space is being consumed.
5. To maintain normal system operations, add Storage Nodes, add storage volumes, or archive object data before usable space is consumed.

   When planning the timing of an expansion, consider how long it will take to procure and install additional storage.

> If your ILM policy uses erasure coding, you might prefer to expand when existing Storage Nodes are approximately 70% full to reduce the number of nodes that must be added.

For more information on planning a storage expansion, see the instructions for expanding StorageGRID.

The **Low object data storage** alert is triggered when insufficient space remains for storing object data on a Storage Node.

#### Monitor object metadata capacity for each Storage Node

Monitor the metadata usage for each Storage Node to ensure that adequate space remains available for essential database operations. You must add new Storage Nodes at each site before object metadata exceeds 100% of the allowed metadata space.

**What you'll need**

- You are signed in to the Grid Manager using a supported web browser.

**About this task**

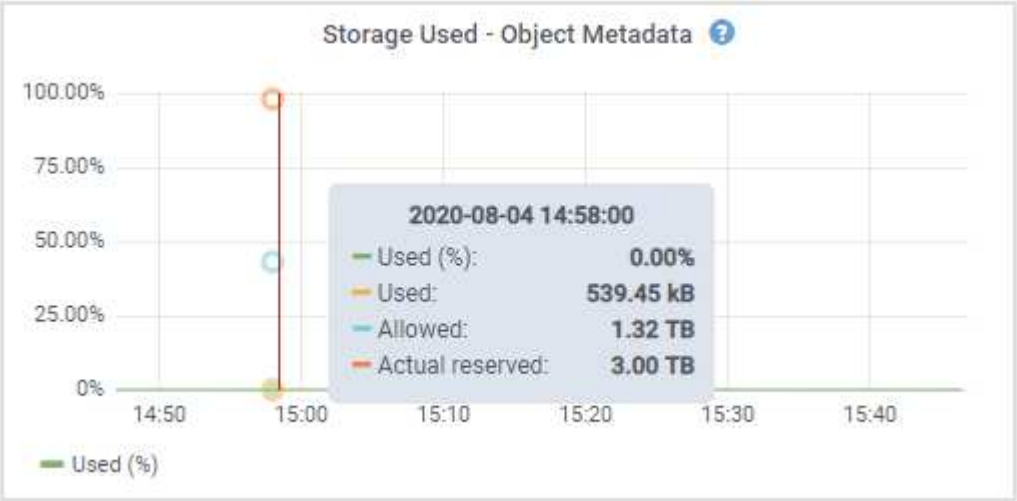
StorageGRID maintains three copies of object metadata at each site to provide redundancy and to protect object metadata from loss. The three copies are evenly distributed across all Storage Nodes at each site using the space reserved for metadata on storage volume 0 of each Storage Node.

In some cases, the grid's object metadata capacity might be consumed faster than its object storage capacity. For example, if you typically ingest large numbers of small objects, you might need to add Storage Nodes to increase metadata capacity even though sufficient object storage capacity remains.

Some of the factors that can increase metadata usage include the size and quantity of user metadata and tags, the total number of parts in a multipart upload, and the frequency of changes to ILM storage locations.

**Steps**

1. Select **NODES** > ***Storage Node*** > **Storage**.
2. Hover your cursor over the Storage used - object metadata graph to see the values for a specific time.



| Value | Description | Prometheus metric |
|---|---|---|
| Used (%) | The percentage of the allowed metadata space that has been used on this Storage Node. | `storagegrid_storage_utilization_metadata_bytes/ storagegrid_storage_utilization_metadata_allowed_bytes` |
| Used | The bytes of the allowed metadata space that have been used on this Storage Node. | `storagegrid_storage_utilization_metadata_bytes` |
| Allowed | The space allowed for object metadata on this Storage Node. To learn how this value is determine for each Storage Node, see the instructions for administering StorageGRID. | `storagegrid_storage_utilization_metadata_allowed_bytes` |
| Actual reserved | The actual space reserved for metadata on this Storage Node. Includes the allowed space and the required space for essential metadata operations. To learn how this value is calculated for each Storage Node, see the instructions for administering StorageGRID. | *Metric will be added in a future release.* |

> The total values for a site or the grid do not include nodes that have not reported metrics for at least five minutes, such as offline nodes.

3. If the **Used (%)** value is 70% or higher, expand your StorageGRID system by adding Storage Nodes to each site.

> The **Low metadata storage** alert is triggered when the **Used (%)** value reaches certain thresholds. Undesirable results can occur if object metadata uses more than 100% of the allowed space.

When you add the new nodes, the system automatically rebalances object metadata across all Storage Nodes within the site. See the instructions for expanding a StorageGRID system.

### Monitor information lifecycle management

The information lifecycle management (ILM) system provides data management for all objects stored on the grid. You must monitor ILM operations to understand if the grid can handle the current load, or if more resources are required.

#### What you'll need

You must be signed in to the Grid Manager using a supported web browser.

#### About this task

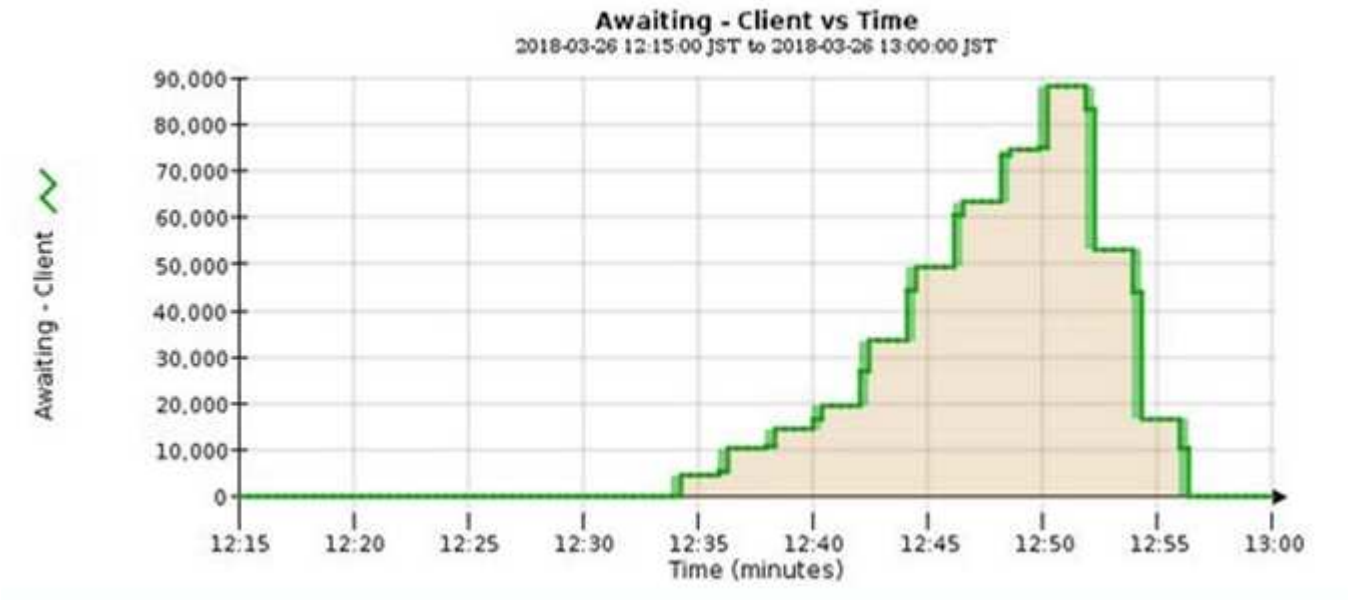
The StorageGRID system manages objects by applying the active ILM policy. The ILM policy and associated ILM rules determine how many copies are made, the type of copies that are created, where copies are placed, and the length of time each copy is retained.

Object ingest and other object-related activities can exceed the rate at which StorageGRID can evaluate ILM, causing the system to queue objects whose ILM placement instructions cannot be fulfilled in near real time. You can monitor whether StorageGRID is keeping up with client actions by charting the Awaiting - Client attribute.

To chart this attribute:

1. Sign in to the Grid Manager.
2. From the Dashboard, locate the **Awaiting - Client** entry in the Information Lifecycle Management (ILM) panel.
3. Click the chart icon .

The example chart shows a situation where the number of objects awaiting ILM evaluation temporarily increased in an unsustainable manner, then eventually decreased. Such a trend indicates that ILM was temporarily not fulfilled in near real time.




Temporary spikes in the chart of Awaiting - Client are to be expected. But if the value shown on the chart continues to increase and never declines, the grid requires more resources to operate efficiently: either more Storage Nodes, or, if the ILM policy places objects in remote locations, more network bandwidth.

You can further investigate ILM queues using the **NODES** page.

**Steps**

1. Select **NODES**.
2. Select ***grid name*** > **ILM**.
3. Hover your cursor over the ILM Queue graph to see the value of following attributes at a given point in time:
   - **Objects queued (from client operations)**: The total number of objects awaiting ILM evaluation because of client operations (for example, ingest).
   - **Objects queued (from all operations)**: The total number of objects awaiting ILM evaluation.
   - **Scan rate (objects/sec)**: The rate at which objects in the grid are scanned and queued for ILM.
   - **Evaluation rate (objects/sec)**: The current rate at which objects are being evaluated against the ILM

policy in the grid.

4. In the ILM Queue section, look at the following attributes.

> The ILM Queue section is included for the grid only. This information is not shown on the ILM tab for a site or Storage Node.

- **Scan Period - Estimated**: The estimated time to complete a full ILM scan of all objects.

  > A full scan does not guarantee that ILM has been applied to all objects.

- **Repairs Attempted**: The total number of object repair operations for replicated data that have been attempted. This count increments each time a Storage Node tries to repair a high-risk object. High-risk ILM repairs are prioritized if the grid becomes busy.

  > The same object repair might increment again if replication failed after the repair.

These attributes can be useful when you are monitoring the progress of Storage Node volume recovery. If the number of Repairs Attempted has stopped increasing and a full scan has been completed, the repair has probably completed.

### Monitor network connections and performance

Grid nodes must be able to communicate with one another to permit the grid to operate. The integrity of the network between nodes and sites, and the network bandwidth between sites, are critical to efficient operations.

#### What you'll need

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

Network connectivity and bandwidth are especially important if your information lifecycle management (ILM) policy copies replicated objects between sites or stores erasure-coded objects using a scheme that provides site-loss protection. If the network between sites is not available, network latency is too high, or network bandwidth is insufficient, some ILM rules might not be able to place objects where expected. This can lead to ingest failures (when the Strict ingest option is selected for ILM rules), or simply to poor ingest performance and ILM backlogs.

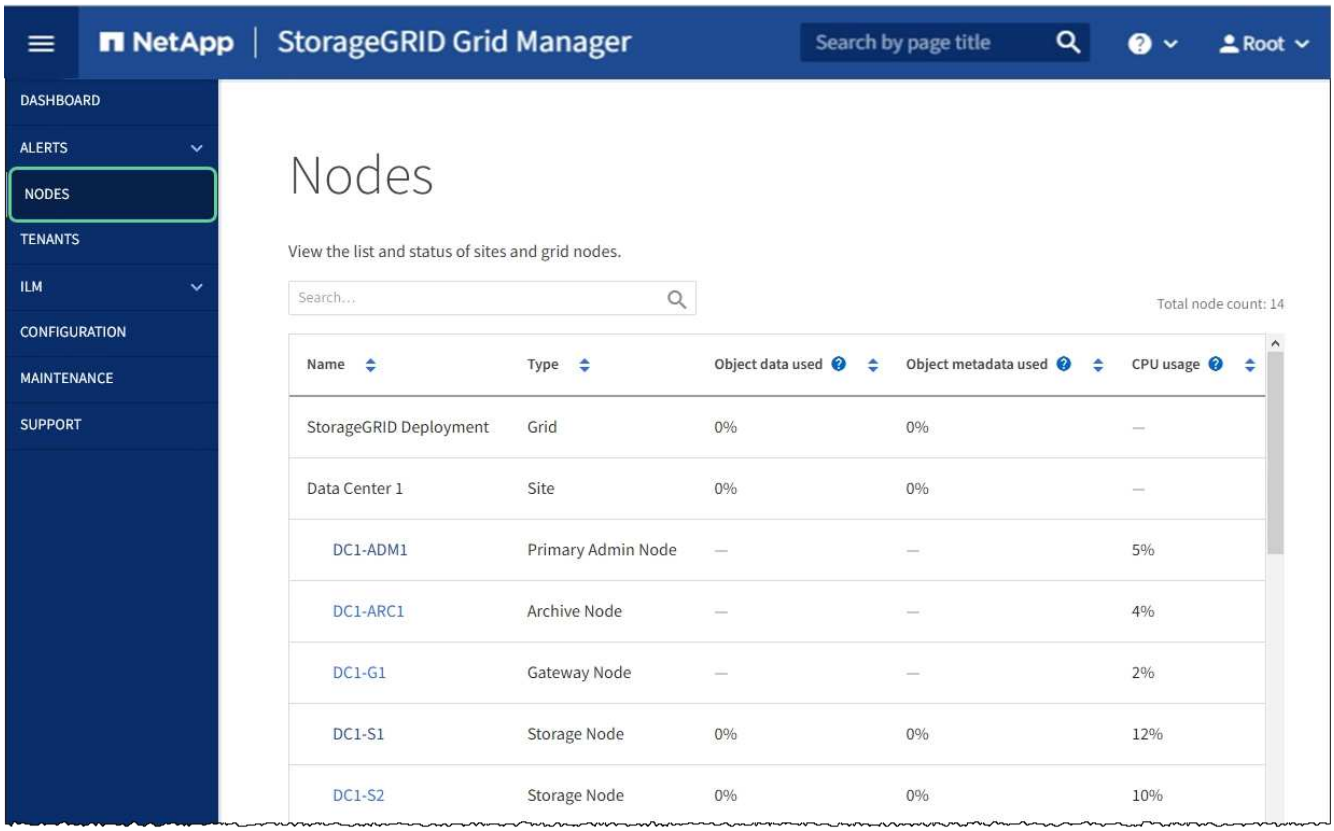
You can use the Grid Manager to monitor connectivity and network performance, so you can address any issues promptly.

Additionally, consider creating network traffic classification policies to provide monitoring and limiting for traffic related to specific tenants, buckets, subnets, or load balancer endpoints. See the instructions for administering StorageGRID.

#### Steps

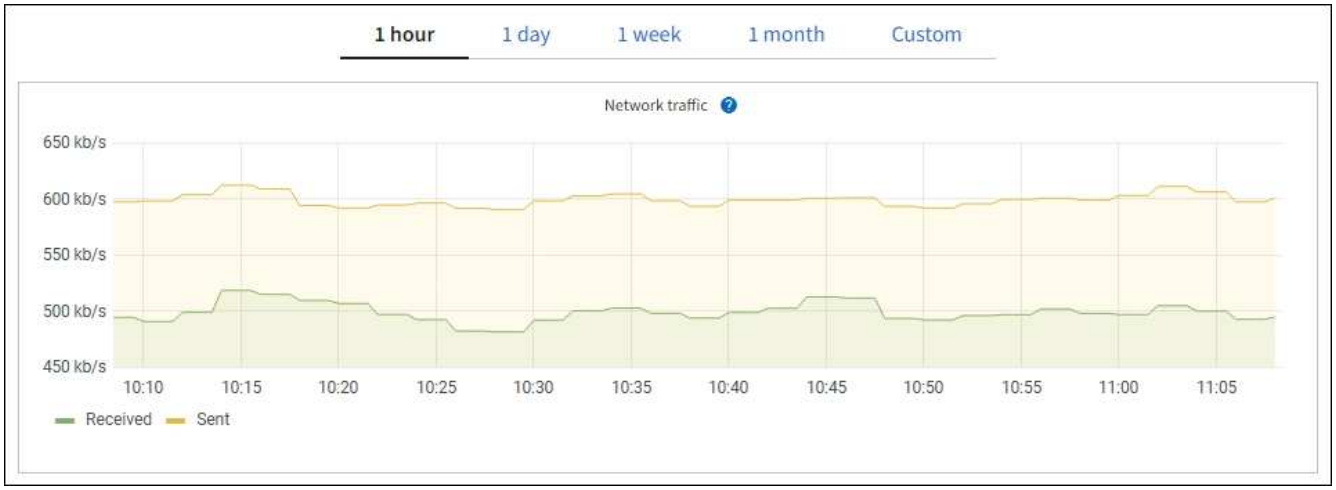
1. Select **NODES**.

   The Nodes page appears. Each node in the grid is listed in table format.

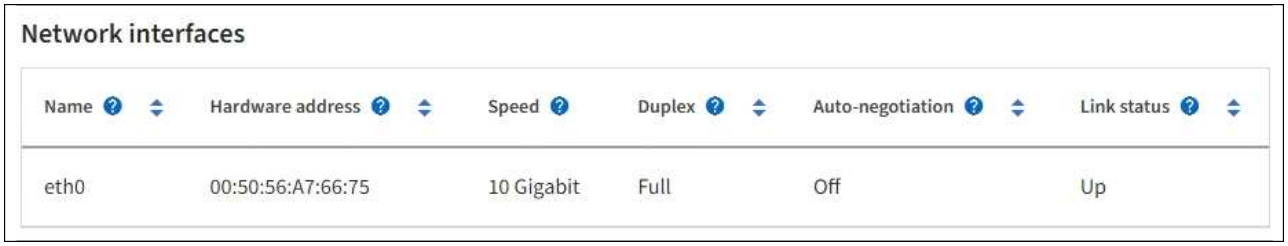



2. Select the grid name, a specific data center site, or a grid node, and then select the **Network** tab.

   The Network Traffic graph provides a summary of overall network traffic for the grid as a whole, the data center site, or for the node.




   a. If you selected a grid node, scroll down to review the **Network Interfaces** section of the page.



b. For grid nodes, scroll down to review the **Network Communication** section of the page.

The Receive and Transmit tables show how many bytes and packets have been received and sent across each network as well as other receive and transmission metrics.

**Network communication**

Receive

| Interface | Data | Packets | Errors | Dropped | Frame overruns | Frames |
|---|---|---|---|---|---|---|
| eth0 | 2.89 GB | 19,421,503 | 0 | 24,032 | 0 | 0 |

Transmit

| Interface | Data | Packets | Errors | Dropped | Collisions | Carrier |
|---|---|---|---|---|---|---|
| eth0 | 3.64 GB | 18,494,381 | 0 | 0 | 0 | 0 |

3. Use the metrics associated with your traffic classification policies to monitor network traffic.

a. Select **CONFIGURATION** > **Network** > **Traffic classification**.

The Traffic Classification Policies page appears, and the existing policies are listed in the table.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

Create | Edit | Remove | Metrics

| Name | Description | ID |
|---|---|---|
| ERP Traffic Control | Manage ERP traffic into the grid | cd9afbc7-b85e-4208-b6f8-7e8a79e2c574 |
| Fabric Pools | Monitor Fabric Pools | 223b0cbb-6968-4646-b32d-7665bddc894b |

Displaying 2 traffic classification policies.

b. To view graphs that show the networking metrics associated with a policy, select the radio button to the left of the policy, and then click **Metrics**.

c. Review the graphs to understand the network traffic associated with the policy.

If a traffic classification policy is designed to limit network traffic, analyze how often traffic is limited and decide if the policy continues to meet your needs. From time to time, adjust each traffic classification policy as needed.

To create, edit, or delete traffic classification policies, see the instructions for administering StorageGRID.

**Related information**

View the Network tab

Monitor node connection states

### Monitor node-level resources

You should monitor individual grid nodes to check their resource utilization levels.

#### What you'll need

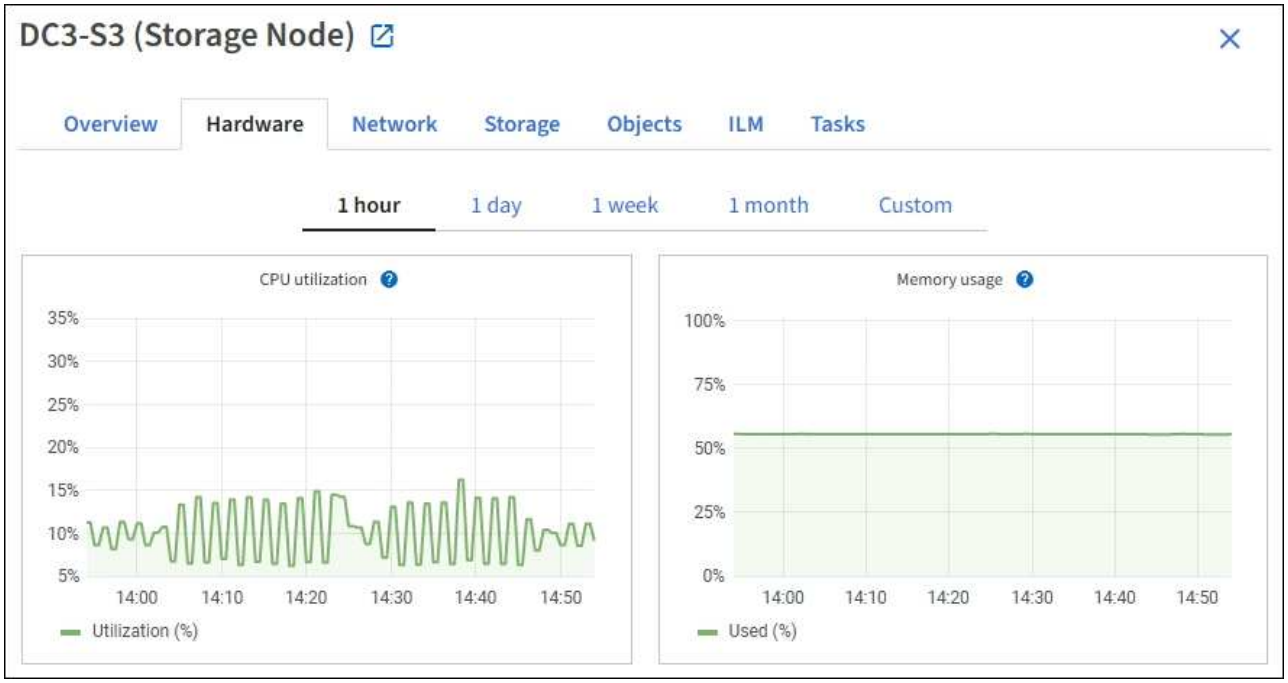
- You must be signed in to the Grid Manager using a supported web browser.

#### About this task

If nodes are consistently overloaded, more nodes might be required for efficient operations.

#### Steps

1. To view information about hardware utilization of a grid node:
   a. From the **NODES** page, select the node.
   b. Select the **Hardware** tab to display graphs of CPU Utilization and Memory Usage.




   c. To display a different time interval, select one of the controls above the chart or graph. You can display the information available for intervals of 1 hour, 1 day, 1 week, or 1 month. You can also set a custom interval, which allows you to specify date and time ranges.
   d. If the node is hosted on a storage appliance or a services appliance, scroll down to view the tables of components. The status of all components should be "Nominal." Investigate components that have any other status.

#### Related information

View information about appliance Storage Nodes

View information about appliance Admin Nodes and Gateway Nodes

### Monitor tenant activity

All client activity is associated with a tenant account. You can use the Grid Manager to monitor a tenant's storage usage or network traffic, or you can use the audit log or

Grafana dashboards to gather more detailed information about how tenants are using StorageGRID.

**What you'll need**

- You are signed in to the Grid Manager using a supported web browser.
- You have the Root Access or Administrator permission.

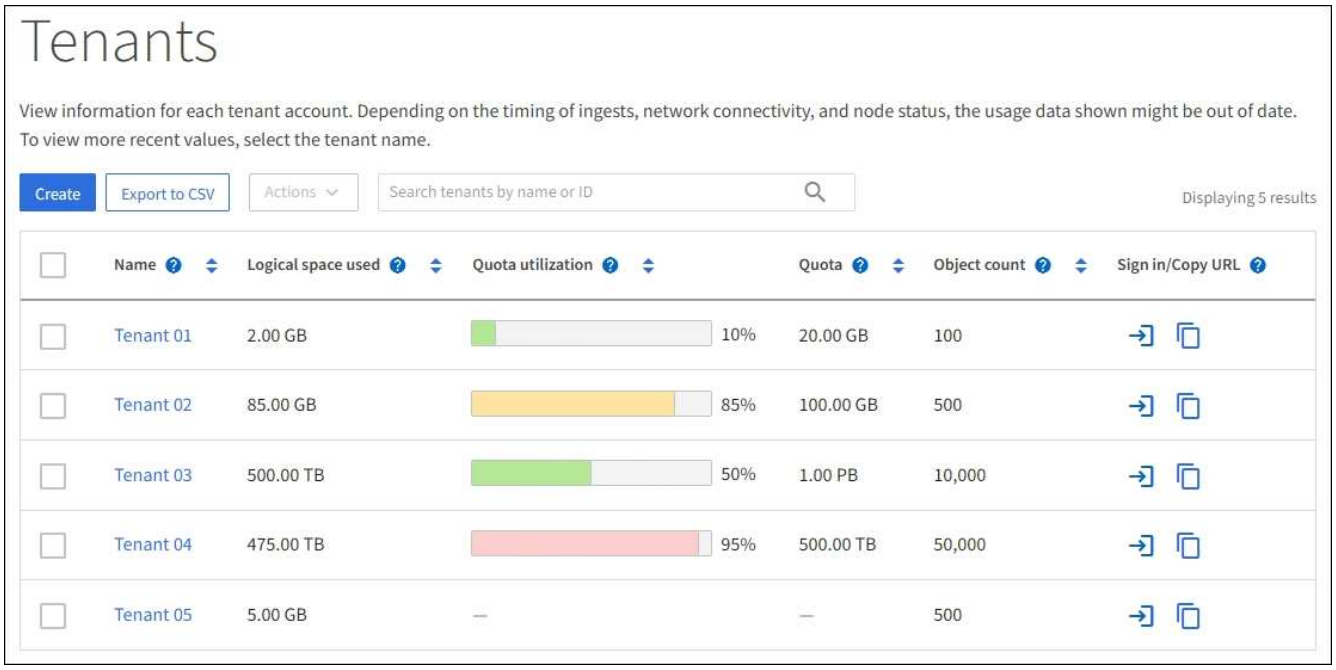
**About this task**

The space used values are estimates. These estimates are affected by the timing of ingests, network connectivity, and node status.

**Steps**

1. Select **TENANTS** to review the amount of storage used by all tenants.

   The Logical space used, Quota utilization, Quota, and Object count are listed for each tenant. If a quota is not set for a tenant, the Quota utilization and Quota fields contain a dash (—).




   You can sign in to a tenant account by selecting the sign-in link in the **Sign in/Copy URL** column of the table.

   You can copy the URL for a tenant's sign-in page by selecting the copy URL link in the **Sign in/Copy URL** column of the table.

2. Optionally, select **Export to CSV** to view and export a .csv file containing the usage values for all tenants.

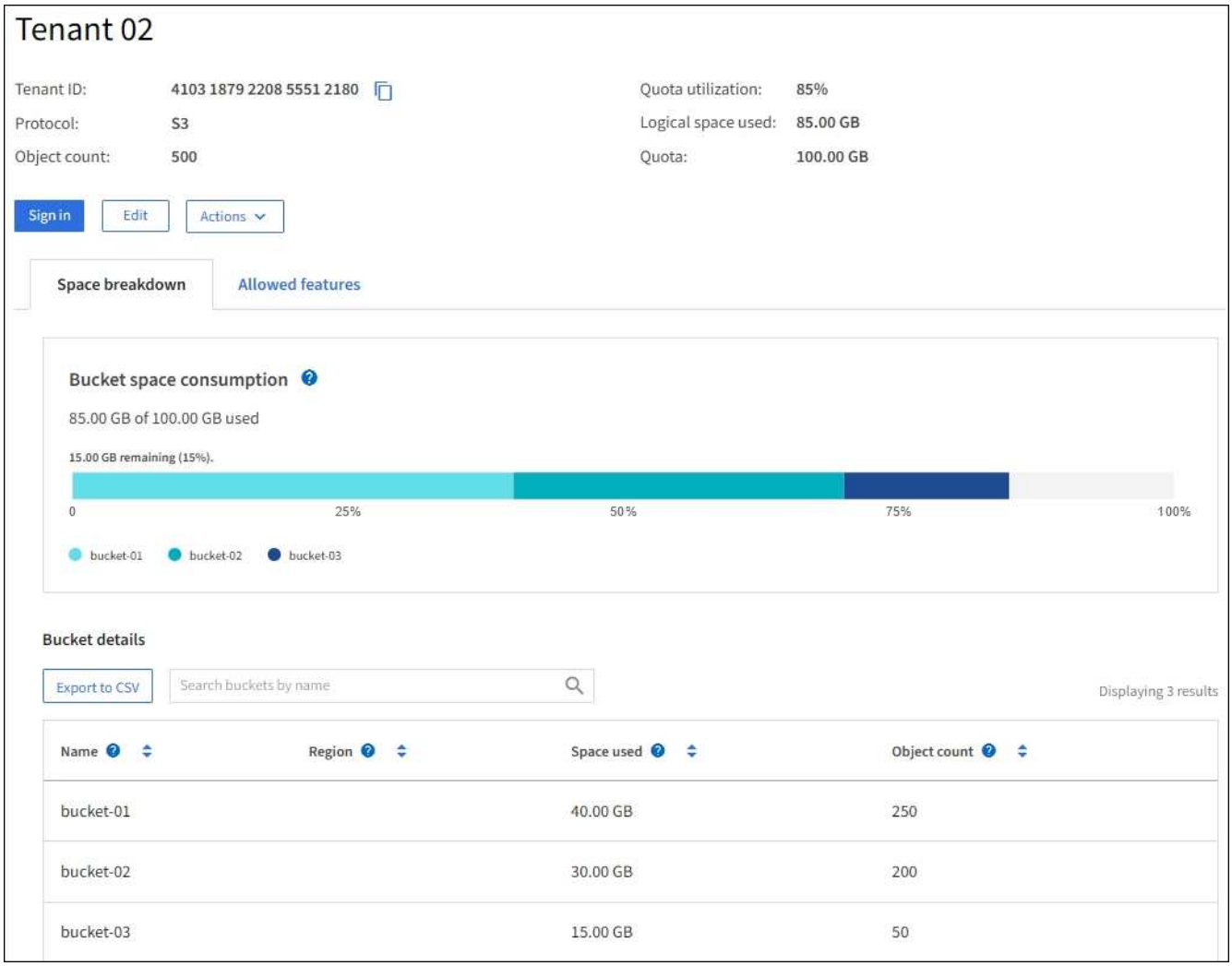
   You are prompted to open or save the `.csv` file.

   The contents of a .csv file look like the following example:

| Tenant ID | Display Name | Space Used (Bytes) | Quota utilization (%) | Quota (Bytes) | Object Count | Protocol |
|---|---|---|---|---|---|---|
| 12659822378459233654 | Tenant 01 | 2000000000 | 10 | 20000000000 | 100 | S3 |
| 99658234112547853685 | Tenant 02 | 85000000000 | 85 | 110000000 | 500 | S3 |
| 03521145586975586321 | Tenant 03 | 60500000000 | 50 | 150000 | 10000 | S3 |
| 44251365987569885632 | Tenant 04 | 4750000000 | 95 | 140000000 | 50000 | S3 |
| 36521587546689565123 | Tenant 05 | 5000000000 | Infinity | | 500 | S3 |

You can open the .csv file in a spreadsheet application or use it in automation.

3. To view details for a specific tenant, including usage charts, select the tenant account name from the Tenants page.




- **Tenant overview**

  The overview area for the tenant contains values for object count, quota utilization, logical space used, and the quota setting.

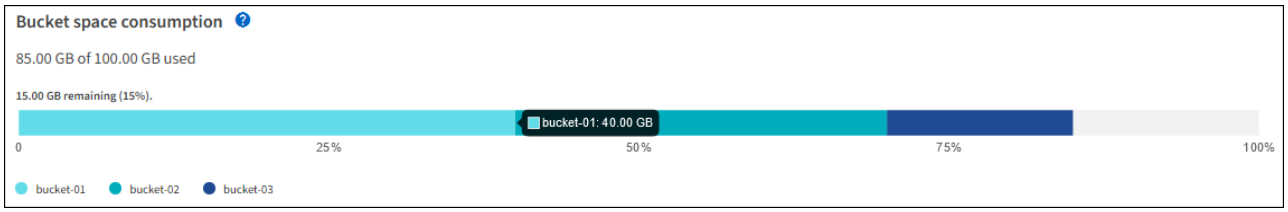
- **Space breakdown — Space consumption**

  The Space breakdown tab includes values for bucket (S3) or container (Swift) total space consumption as well as space used and object count for each bucket or container.

  If a quota was set for this tenant, the amount of quota used and remaining is displayed in text (for example, `85.00 GB of 100 GB used`). If no quota was set, the tenant has an unlimited quota, and

the text includes only an amount of space used (for example, `85.00 GB used`). The bar chart shows the percentage of quota in each bucket or container. If the tenant has exceeded the storage quota by more than 1% and by at least 1 GB, the chart shows the total quota and the excess amount.

You can place your cursor over the bar chart to see the storage used by each bucket or container. You can place your cursor over the free space segment to see the amount of storage quota remaining.




> Quota utilization is based on internal estimates and might be exceeded in some cases. For example, StorageGRID checks the quota when a tenant starts uploading objects and rejects new ingests if the tenant has exceeded the quota. However, StorageGRID does not take into account the size of the current upload when determining if the quota has been exceeded. If objects are deleted, a tenant might be temporarily prevented from uploading new objects until the quota utilization is recalculated. Quota utilization calculations can take 10 minutes or longer.

> A tenant's quota utilization indicates the total amount of object data the tenant has uploaded to StorageGRID (logical size). The quota utilization does not represent the space used to store copies of those objects and their metadata (physical size).

> You can enable the **Tenant quota usage high** alert to determine if tenants are consuming their quotas. If enabled, this alert is triggered when a tenant has used 90% of its quota. For more information, see the alerts reference.

- **Space breakdown — Bucket or container details**

  The **Bucket details** (S3) or **Container details** (Swift) table lists the buckets or containers for the tenant. Space used is the total amount of object data in the bucket or container. This value does not represent the storage space required for ILM copies and object metadata.

4. Optionally, select **Export to CSV** to view and export a .csv file containing the usage values for each bucket or container.

   The contents of an individual S3 tenant's .csv file look like the following example:

| Tenant ID | Bucket Name | Space Used (Bytes) | Number of Objects |
|---|---|---|---|
| 64796966429038923647 | bucket-01 | 88717711 | 14 |
| 64796966429038923647 | bucket-02 | 21747507 | 11 |
| 64796966429038923647 | bucket-03 | 15294070 | 3 |

   You can open the .csv file in a spreadsheet application or use it in automation.

5. If traffic classification policies are in place for a tenant, review the network traffic for that tenant.
   a. Select **CONFIGURATION** > **Network** > **Traffic classification**.

      The Traffic Classification Policies page appears, and the existing policies are listed in the table.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create | Edit | Remove | Metrics

| | Name | Description | ID |
|---|---|---|---|
| ○ | ERP Traffic Control | Manage ERP traffic into the grid | cd9afbc7-b85e-4208-b6f8-7e8a79e2c574 |
| ◉ | Fabric Pools | Monitor Fabric Pools | 223b0cbb-6968-4646-b32d-7665bddc894b |

Displaying 2 traffic classification policies.

b. Review the list of policies to identify the ones that apply to a specific tenant.

c. To view metrics associated with a policy, select the radio button to the left of the policy, and then click **Metrics**.

d. Analyze the graphs to determine how often the policy is limiting traffic and whether you need to adjust the policy.

   To create, edit, or delete traffic classification policies, see the instructions for administering StorageGRID.

6. Optionally, use the audit log for more granular monitoring of a tenant's activities.

   For instance, you can monitor the following types of information:

   - Specific client operations, such as PUT, GET, or DELETE
   - Object sizes
   - The ILM rule applied to objects
   - The source IP of client requests

     Audit logs are written to text files that you can analyze using your choice of log analysis tool. This allows you to better understand client activities, or to implement sophisticated chargeback and billing models.

     See the instructions for understanding audit messages for more information.

7. Optionally, use Prometheus metrics to report on tenant activity:

   - In the Grid Manager, select **SUPPORT** > **Tools** > **Metrics**. You can use existing dashboards, such as S3 Overview, to review client activities.

     > The tools available on the Metrics page are primarily intended for use by technical support. Some features and menu items within these tools are intentionally non-functional.

   - From the top of the Grid Manager, select the help icon and select **API Documentation**. You can use the metrics in the Metrics section of the Grid Management API to create custom alert rules and dashboards for tenant activity.

**Related information**

Alerts reference

Review audit logs

### Monitor archival capacity

You cannot directly monitor an external archival storage system's capacity through the StorageGRID system. However, you can monitor whether the Archive Node can still send object data to the archival destination, which might indicate that an expansion of archival media is required.

#### What you'll need

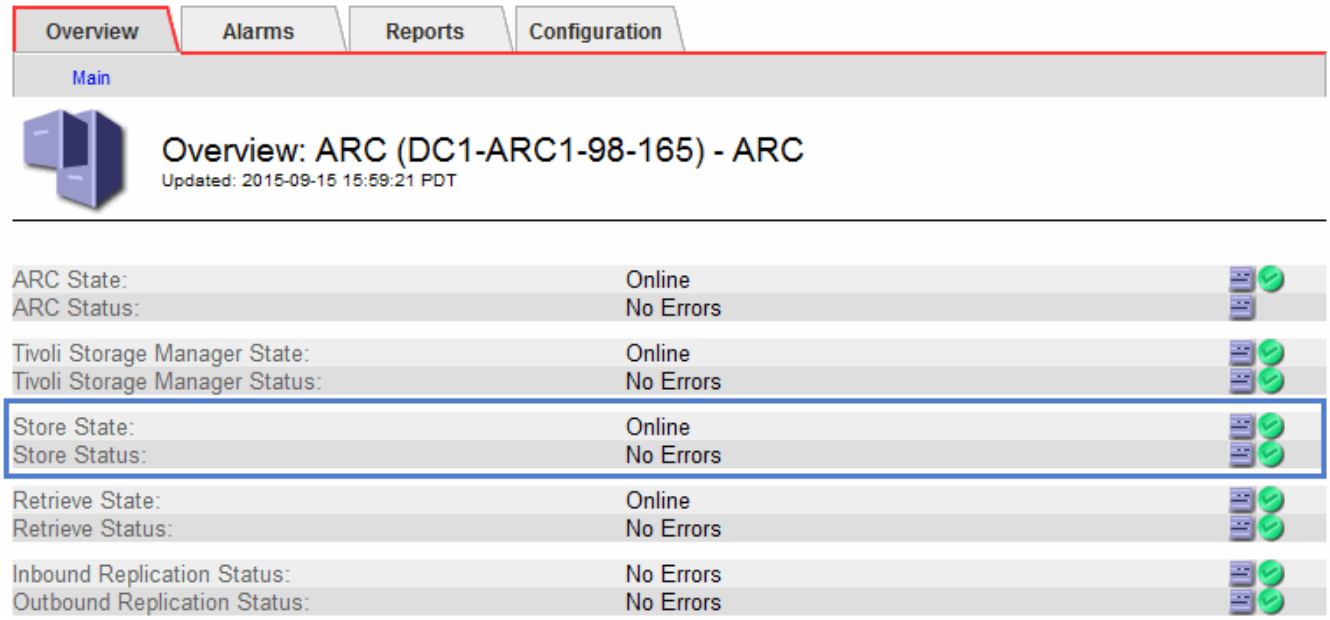
- You must be signed in to the Grid Manager using a supported web browser.
- You must have specific access permissions.

#### About this task

You can monitor the Store component to check if the Archive Node can still send object data to the targeted archival storage system. The Store Failures (ARVF) alarm might also indicate that the targeted archival storage system has reached capacity and can no longer accept object data.

#### Steps

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Select ***Archive Node*** > **ARC> Overview> Main**.
3. Check the Store State and Store Status attributes to confirm that the Store component is Online with No Errors.




An offline Store component or one with errors might indicate that targeted archival storage system can no longer accept object data because it has reached capacity.

### Monitor load balancing operations

If you are using a load balancer to manage client connections to StorageGRID, you

should monitor load balancing operations after you configure the system initially and after you make any configuration changes or perform an expansion.

**What you'll need**

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

**About this task**

You can use the Load Balancer service on Admin Nodes or Gateway Nodes, an external third-party load balancer, or the CLB service on Gateway Nodes to distribute client requests across multiple Storage Nodes.

> The CLB service is deprecated.

After configuring load balancing, you should confirm that object ingest and retrieval operations are being evenly distributed across Storage Nodes. Evenly distributed requests ensure that StorageGRID remains responsive to client requests under load and can help maintain client performance.

If you configured a high availability (HA) group of Gateway Nodes or Admin Nodes in active-backup mode, only one node in the group actively distributes client requests.

See the section on configuring client connections in the instructions for administering StorageGRID.

**Steps**

1. If S3 or Swift clients connect using the Load Balancer service, check that Admin Nodes or Gateway Nodes are actively distributing traffic as you expect:
   a. Select **NODES**.
   b. Select a Gateway Node or Admin Node.
   c. On the **Overview** tab, check if a node interface is in an HA group and if the node interface has the role of Master.

      Nodes with the role of Master and nodes that are not in an HA group should be actively distributing requests to clients.

   d. For each node that should be actively distributing client requests, select the **Load Balancer** tab.
   e. Review the chart of Load Balancer Request Traffic for the last week to ensure that the node has been actively distributing requests.

      Nodes in an active-backup HA group might take the Backup role from time to time. During that time the nodes do not distribute client requests.

   f. Review the chart of Load Balancer Incoming Request Rate for the last week to review the object throughput of the node.
   g. Repeat these steps for each Admin Node or Gateway Node in the StorageGRID system.
   h. Optionally, use traffic classification policies to view a more detailed breakdown of traffic being served by the Load Balancer service.
2. If S3 or Swift clients connect using the CLB service (deprecated), perform the following checks:
   a. Select **NODES**.
   b. Select a Gateway Node.

c. On the **Overview** tab, check if a node interface is in an HA group, and if the node interface has the role of Master.

   Nodes with the role of Master and nodes that are not in an HA group should be actively distributing requests to clients.

d. For each Gateway Node that should be actively distributing client requests, select **SUPPORT** > **Tools** > **Grid topology**.

e. Select ***Gateway Node*** > **CLB** > **HTTP** > **Overview** > **Main**.

f. Review the number of **Incoming Sessions - Established** to verify that the Gateway Node has been actively handling requests.

3. Verify that these requests are being evenly distributed to Storage Nodes.

   a. Select ***Storage Node*** > **LDR** > **HTTP**.

   b. Review the number of **Currently Established incoming Sessions**.

   c. Repeat for each Storage Node in the grid.

      The number of sessions should be roughly equal across all Storage Nodes.

#### Related information

Administer StorageGRID

View the Load Balancer tab

### Apply hotfixes or upgrade software if necessary

If a hotfix or a new version of StorageGRID software is available, you should assess whether the update is appropriate for your system, and install it if required.

#### About this task

StorageGRID hotfixes contain software changes that are made available outside of a feature or patch release. The same changes are included in a future release.

#### Steps

1. Go to the NetApp Downloads page for StorageGRID.

   NetApp Downloads: StorageGRID

2. Select the down arrow for the **Type/Select Version** field to see a list of the updates that are available to download:

   - **StorageGRID software versions**: 11.*x.y*
   - **StorageGRID hotfixes**: 11.*x.y.z*

3. Review the changes that are included in the update:

   a. Select the version from the pull-down menu, and click **Go**.

   b. Sign in using the username and password for your NetApp account.

   c. Read the End User License Agreement, select the check box, and then select **Accept & Continue**.

      The downloads page for the version you selected appears.

4. Learn about the changes included in the software version or hotfix.
    - For a new software version, see the “What’s new” topic in the instructions for upgrading StorageGRID.
    - For a hotfix, download the README file for a summary of the changes included in the hotfix.
5. If you decide a software update is required, locate the instructions before proceeding.
    - For a new software version, carefully follow the instructions for upgrading StorageGRID.
    - For a hotfix, locate the hotfix procedure in the recovery and maintenance instructions

**Related information**

Upgrade software

Recover and maintain

## Manage alerts and alarms

### Manage alerts and alarms: Overview

The StorageGRID alert system is designed to inform you about operational issues that require your attention. The legacy alarm system is deprecated.

#### Alert system

The alert system is designed to be your primary tool for monitoring any issues that might occur in your StorageGRID system. The alert system provides an easy-to-use interface for detecting, evaluating, and resolving issues.

Alerts are triggered at specific severity levels when alert rule conditions evaluate as true. When an alert is triggered, the following actions occur:

- An alert severity icon is shown on the Dashboard in the Grid Manager, and the count of Current Alerts is incremented.
- The alert is shown on the **NODES** summary page and on the **NODES** > ***node*** > **Overview** tab.
- An email notification is sent, assuming you have configured an SMTP server and provided email addresses for the recipients.
- An Simple Network Management Protocol (SNMP) notification is sent, assuming you have configured the StorageGRID SNMP agent.

#### Legacy alarm system

Like alerts, alarms are triggered at specific severity levels when attributes reach defined threshold values. However, unlike alerts, many alarms are triggered for events that you can safely ignore, which might result in an excessive number of email or SNMP notifications.

> The alarm system is deprecated and will be removed in a future release. If you are still using legacy alarms, you should fully transition to the alert system as soon as possible.

When an alarm is triggered, the following actions occur:

- The alarm appears on the **SUPPORT** > **Alarms (legacy)** > **Current alarms** page.

- An email notification is sent, assuming you have configured an SMTP server and configured one or more mailing lists.
- An SNMP notification might be sent, assuming you have configured the StorageGRID SNMP agent. (SNMP notifications are not sent for all alarms or alarm severities.)

### Compare alerts and alarms

There are a number of similarities between the alert system and the legacy alarm system, but the alert system offers significant benefits and is easier to use.

Refer to the following table to learn how to perform similar operations.

| | Alerts | Alarms (legacy system) |
|---|---|---|
| How do I see which alerts or alarms are active? | • Select the **Current alerts** link on the Dashboard.<br>• Select the alert on the **NODES** > **Overview** page.<br>• Select **ALERTS** > **Current**.<br><br>View current alerts | Select **SUPPORT** > **Alarms (legacy)** > **Current alarms**.<br><br>Manage alarms (legacy system) |
| What causes an alert or an alarm to be triggered? | Alerts are triggered when a Prometheus expression in an alert rule evaluates as true for the specific trigger condition and duration.<br><br>View alert rules | Alarms are triggered when a StorageGRID attribute reaches a threshold value.<br><br>Manage alarms (legacy system) |
| If an alert or alarm is triggered, how do I resolve the underlying problem? | The recommended actions for an alert are included in email notifications and are available from the Alerts pages in the Grid Manager.<br><br>As required, additional information is provided in the StorageGRID documentation.<br><br>Alerts reference | You can learn about an alarm by selecting the attribute name, or you can search for an alarm code in the StorageGRID documentation.<br><br>Alarms reference (legacy system) |
| Where can I see a list of alerts or alarms that have been resolved? | Select **ALERTS** > **Resolved**.<br><br>View resolved alerts | Select **SUPPORT** > **Alarms (legacy)** > **Historical alarms**.<br><br>Manage alarms (legacy system) |

| | Alerts | Alarms (legacy system) |
|---|---|---|
| Where do I manage the settings? | Select **ALERTS** > **Rules**.<br><br>Manage alerts | Select **SUPPORT**. Then, use the options in the **Alarms (legacy)** section of the menu.<br><br>Manage alarms (legacy system) |
| What user group permissions do I need? | • Anyone who can sign in to the Grid Manager can view current and resolved alerts.<br>• You must have the Manage Alerts permission to manage silences, alert notifications, and alert rules.<br><br>Administer StorageGRID | • Anyone who can sign in to the Grid Manager can view legacy alarms.<br>• You must have the Acknowledge Alarms permission to acknowledge alarms.<br>• You must have both the Grid Topology Page Configuration and Other Grid Configuration permissions to manage global alarms and email notifications.<br><br>Administer StorageGRID |
| How do I manage email notifications? | Select **ALERTS** > **Email setup**.<br><br>**Note:** Because alarms and alerts are independent systems, the email setup used for alarm and AutoSupport notifications is not used for alert notifications. However, you can use the same mail server for all notifications.<br><br>Set up email notifications for alerts | Select **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.<br><br>Manage alarms (legacy system) |
| How do I manage SNMP notifications? | Select **CONFIGURATION** > **Monitoring** > **SNMP agent**.<br><br>Use SNMP monitoring | Select **CONFIGURATION** > **Monitoring** > **SNMP agent**.<br><br>Use SNMP monitoring<br><br>**Note**: SNMP notifications are not sent for every alarm or alarm severity.<br><br>Alarms that generate SNMP notifications (legacy system) |

| | Alerts | Alarms (legacy system) |
|---|---|---|
| How do I control who receives notifications? | 1. Select **ALERTS** > **Email setup**.<br>2. In the **Recipients** section, enter an email address for each email list or person who should receive an email when an alert occurs.<br><br>Set up email notifications for alerts | 1. Select **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.<br>2. Creating a mailing list.<br>3. Select **Notifications**.<br>4. Select the mailing list.<br><br>Manage alarms (legacy system) |
| Which Admin Nodes send notifications? | A single Admin Node (the “preferred sender”).<br><br>Administer StorageGRID | A single Admin Node (the “preferred sender”).<br><br>Administer StorageGRID |
| How do I suppress some notifications? | 1. Select **ALERTS** > **Silences**.<br>2. Select the alert rule you want to silence.<br>3. Specify a duration for the silence.<br>4. Select the severity of alert you want to silence.<br>5. Select to apply the silence to the entire grid, a single site, or a single node.<br><br>**Note**: If you have enabled the SNMP agent, silences also suppress SNMP traps and informs.<br><br>Silence alert notifications | 1. Select **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.<br>2. Select **Notifications**.<br>3. Select a mailing list, and select **Suppress**.<br><br>Manage alarms (legacy system) |
| How do I suppress all notifications? | Select **ALERTS** > **Silences**.Then, select **All rules**.<br><br>**Note**: If you have enabled the SNMP agent, silences also suppress SNMP traps and informs.<br><br>Silence alert notifications | 1. Select **CONFIGURATION** > **System** > **Display options**.<br>2. Select the **Notification Suppress All** check box.<br><br>**Note**: Suppressing email notifications system wide also suppresses event-triggered AutoSupport emails.<br><br>Manage alarms (legacy system) |

| | Alerts | Alarms (legacy system) |
|---|---|---|
| How do I customize the conditions and triggers? | 1. Select **ALERTS** > **Rules**.<br>2. Select a default rule to edit, or select **Create custom rule**.<br><br>Edit alert rules<br><br>Create custom alert rules | 1. Select **SUPPORT** > **Alarms (legacy)** > **Global alarms**.<br>2. Create a Global Custom alarm to override a Default alarm or to monitor an attribute that does not have a Default alarm.<br><br>Manage alarms (legacy system) |
| How do I disable an individual alert or alarm? | 1. Select **ALERTS** > **Rules**.<br>2. Select the rule, and select **Edit rule**.<br>3. Unselect the **Enabled** check box.<br><br>Disable alert rules | 1. Select **SUPPORT** > **Alarms (legacy)** > **Global alarms**.<br>2. Select the rule, and select the Edit icon.<br>3. Unselect the **Enabled** check box.<br><br>Manage alarms (legacy system) |

## Manage alerts

### Manage alerts: overview

Alerts allow you to monitor various events and conditions within your StorageGRID system. You can manage alerts by creating custom alerts, editing or disabling the default alerts, setting up email notifications for alerts, and silencing alert notifications.

#### About StorageGRID alerts

The alert system provides an easy-to-use interface for detecting, evaluating, and resolving the issues that can occur during StorageGRID operation.

- The alert system focuses on actionable problems in the system. Alerts are triggered for events that require your immediate attention, not for events that can safely be ignored.
- The Current Alerts page provides a user-friendly interface for viewing current problems. You can sort the listing by individual alerts and alert groups. For example, you might want to sort all alerts by node/site to see which alerts are affecting a specific node. Or, you might want to sort the alerts in a group by time triggered to find the most recent instance of a specific alert.
- The Resolved Alerts page provides similar information as on the Current Alerts page, but it allows you to search and view a history of the alerts that have been resolved, including when the alert was triggered and when it was resolved.
- Multiple alerts of the same type are grouped into one email to reduce the number of notifications. In addition, multiple alerts of the same type are shown as a group on the Alerts page. You can expand and collapse alert groups to show or hide the individual alerts. For example, if several nodes report the **Unable to communicate with node** alert at about the same time, only one email is sent and the alert is shown as a group on the Alerts page.
- Alerts use intuitive names and descriptions to help you quickly understand the problem. Alert notifications include details about the node and site affected, the alert severity, the time when the alert rule was

triggered, and the current value of metrics related to the alert.

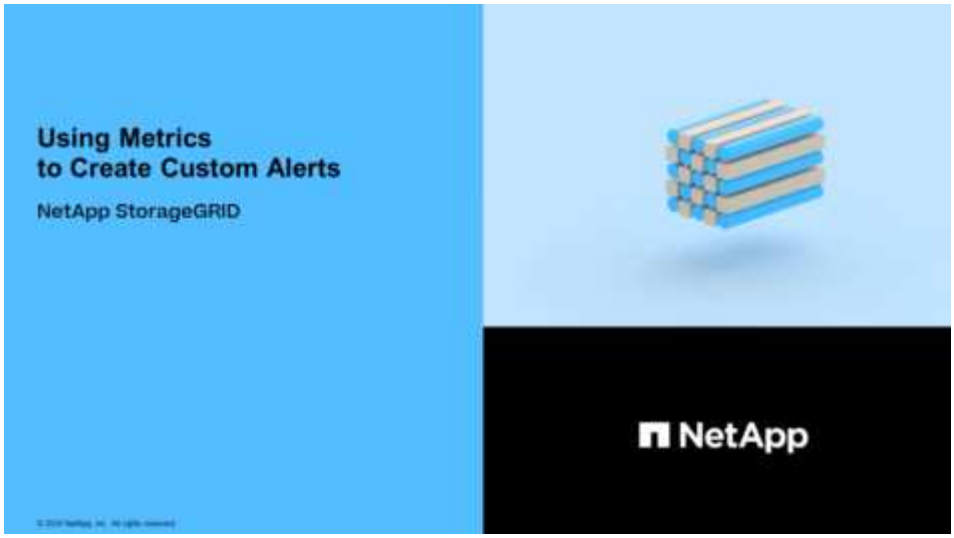
- Alert emails notifications and the alert listings on the Current Alerts and Resolved Alerts pages provide recommended actions for resolving an alert. These recommended actions often include direct links to the StorageGRID documentation center to make it easier to find and access more detailed troubleshooting procedures.
- If you need to temporarily suppress the notifications for an alert at one or more severity levels, you can easily silence a specific alert rule for a specified duration and for the entire grid, a single site, or a single node. You can also silence all alert rules, for example, during a planned maintenance procedure such as a software upgrade.
- You can edit the default alert rules as required. You can disable an alert rule completely, or change its trigger conditions and duration.
- You can create custom alert rules to target the specific conditions that are relevant to your situation and to provide your own recommended actions. To define the conditions for a custom alert, you create expressions using the Prometheus metrics available from the Metrics section of the Grid Management API.

**Learn more**

To learn more, review these videos:

- Video: Overview of Alerts

- Video: Using Metrics to Create Custom Alerts



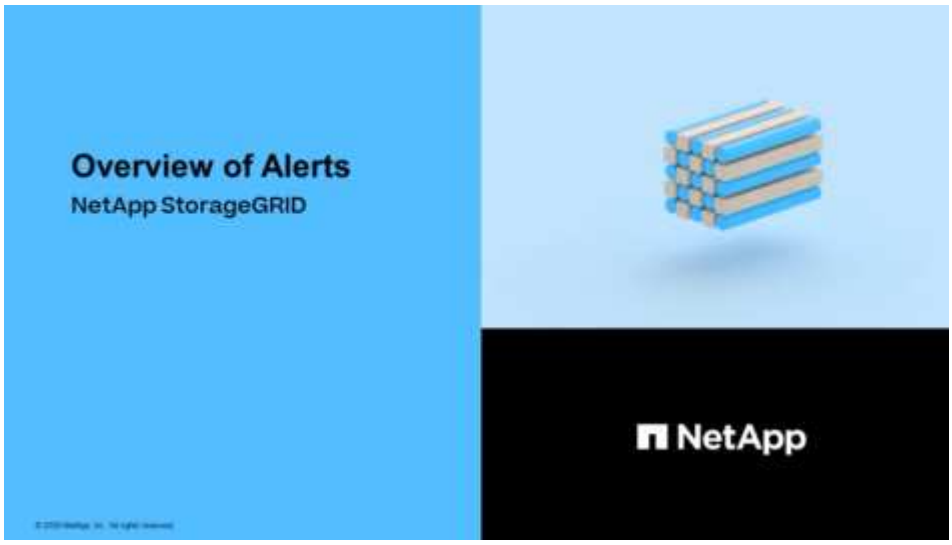

#### View alert rules

Alert rules define the conditions that trigger specific alerts. StorageGRID includes a set of default alert rules, which you can use as is or modify, or you can create custom alert rules.

You can view the list of all default and custom alert rules to learn which conditions will trigger each alert and to see whether any alerts are disabled.

#### What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have the Manage Alerts or Root Access permission.
- Optionally, you have watched the video: Video: Overview of Alerts




#### Steps

1. Select **ALERTS** > **Rules**.

   The Alert Rules page appears.

Alert Rules Learn more

Alert rules define which conditions trigger specific alerts.

You can edit the conditions for default alert rules to better suit your environment, or create custom alert rules that use your own conditions for triggering alerts.

Create custom rule | Edit rule | Remove custom rule

| Name | Conditions | Type | Status |
|---|---|---|---|
| **Appliance battery expired**<br>The battery in the appliance's storage controller has expired. | storagegrid_appliance_component_failure{type="REC_EXPIRED_BATTERY"}<br>*Major* > 0 | Default | Enabled |
| **Appliance battery failed**<br>The battery in the appliance's storage controller has failed. | storagegrid_appliance_component_failure{type="REC_FAILED_BATTERY"}<br>*Major* > 0 | Default | Enabled |
| **Appliance battery has insufficient learned capacity**<br>The battery in the appliance's storage controller has insufficient learned capacity. | storagegrid_appliance_component_failure{type="REC_BATTERY_WARN"}<br>*Major* > 0 | Default | Enabled |
| **Appliance battery near expiration**<br>The battery in the appliance's storage controller is nearing expiration. | storagegrid_appliance_component_failure{type="REC_BATTERY_NEAR_EXPIRATION"}<br>*Major* > 0 | Default | Enabled |
| **Appliance battery removed**<br>The battery in the appliance's storage controller is missing. | storagegrid_appliance_component_failure{type="REC_REMOVED_BATTERY"}<br>*Major* > 0 | Default | Enabled |
| **Appliance battery too hot**<br>The battery in the appliance's storage controller is overheated. | storagegrid_appliance_component_failure{type="REC_BATTERY_OVERTEMP"}<br>*Major* > 0 | Default | Enabled |
| **Appliance cache backup device failed**<br>A persistent cache backup device has failed. | storagegrid_appliance_component_failure{type="REC_CACHE_BACKUP_DEVICE_FAILED"}<br>*Major* > 0 | Default | Enabled |
| **Appliance cache backup device insufficient capacity**<br>There is insufficient cache backup device capacity. | storagegrid_appliance_component_failure{type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY"}<br>*Major* > 0 | Default | Enabled |
| **Appliance cache backup device write-protected**<br>A cache backup device is write-protected. | storagegrid_appliance_component_failure{type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED"}<br>*Major* > 0 | Default | Enabled |
| **Appliance cache memory size mismatch**<br>The two controllers in the appliance have different cache sizes. | storagegrid_appliance_component_failure{type="REC_CACHE_MEM_SIZE_MISMATCH"}<br>*Major* > 0 | Default | Enabled |

Displaying 62 alert rules.

2. Review the information in the alert rules table:

| Column header | Description |
|---|---|
| Name | The unique name and description of the alert rule. Custom alert rules are listed first, followed by default alert rules. The alert rule name is the subject for email notifications. |
| Conditions | The Prometheus expressions that determine when this alert is triggered. An alert can be triggered at one or more of the following severity levels, but a condition for each severity is not required.<br>• **Critical**: An abnormal condition exists that has stopped the normal operations of a StorageGRID node or service. You must address the underlying issue immediately. Service disruption and loss of data might result if the issue is not resolved.<br>• **Major**: An abnormal condition exists that is either affecting current operations or approaching the threshold for a critical alert. You should investigate major alerts and address any underlying issues to ensure that the abnormal condition does not stop the normal operation of a StorageGRID node or service.<br>• **Minor**: The system is operating normally, but an abnormal condition exists that could affect the system's ability to operate if it continues. You should monitor and resolve minor alerts that do not clear on their own to ensure they do not result in a more serious problem. |

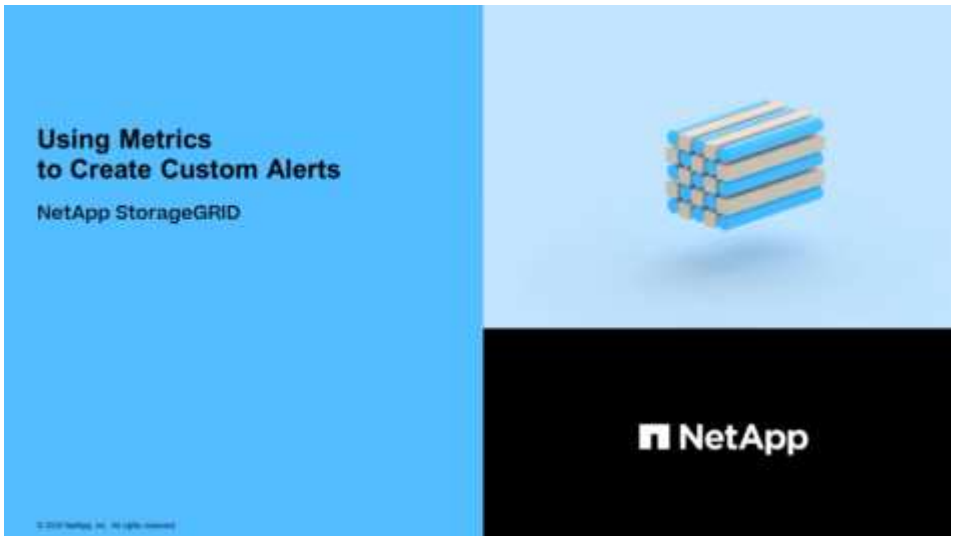
| Column header | Description |
| --- | --- |
| Type | The type of alert rule:<br>• **Default**: An alert rule provided with the system. You can disable a default alert rule or edit the conditions and duration for a default alert rule. You cannot remove a default alert rule.<br>• **Default***: A default alert rule that includes an edited condition or duration. As required, you can easily revert a modified condition back to the original default.<br>• **Custom**: An alert rule that you created. You can disable, edit, and remove custom alert rules. |
| Status | Whether this alert rule is currently enabled or disabled. The conditions for disabled alert rules are not evaluated, so no alerts are triggered. |

#### Create custom alert rules

You can create custom alert rules to define your own conditions for triggering alerts.

**What you'll need**

- You are signed in to the Grid Manager using a supported web browser
- You have the Manage Alerts or Root Access permission
- You are familiar with the commonly used Prometheus metrics
- You understand the syntax of Prometheus queries
- Optionally, you have watched the video: Video: Using Metrics to Create Custom Alerts




**About this task**

StorageGRID does not validate custom alerts. If you decide to create custom alert rules, follow these general guidelines:

- Look at the conditions for the default alert rules, and use them as examples for your custom alert rules.

- If you define more than one condition for an alert rule, use the same expression for all conditions. Then, change the threshold value for each condition.
- Carefully check each condition for typos and logic errors.
- Use only the metrics listed in the Grid Management API.
- When testing an expression using the Grid Management API, be aware that a “successful” response might simply be an empty response body (no alert triggered). To see if the alert is actually triggered, you can temporarily set a threshold to a value you expect to be true currently.

  For example, to test the expression `node_memory_MemTotal_bytes < 24000000000`, first execute `node_memory_MemTotal_bytes >= 0` and ensure you get the expected results (all nodes return a value). Then, change the operator and the threshold back to the intended values and execute again. No results indicate there are no current alerts for this expression.

- Do not assume a custom alert is working unless you have validated that the alert is triggered when expected.

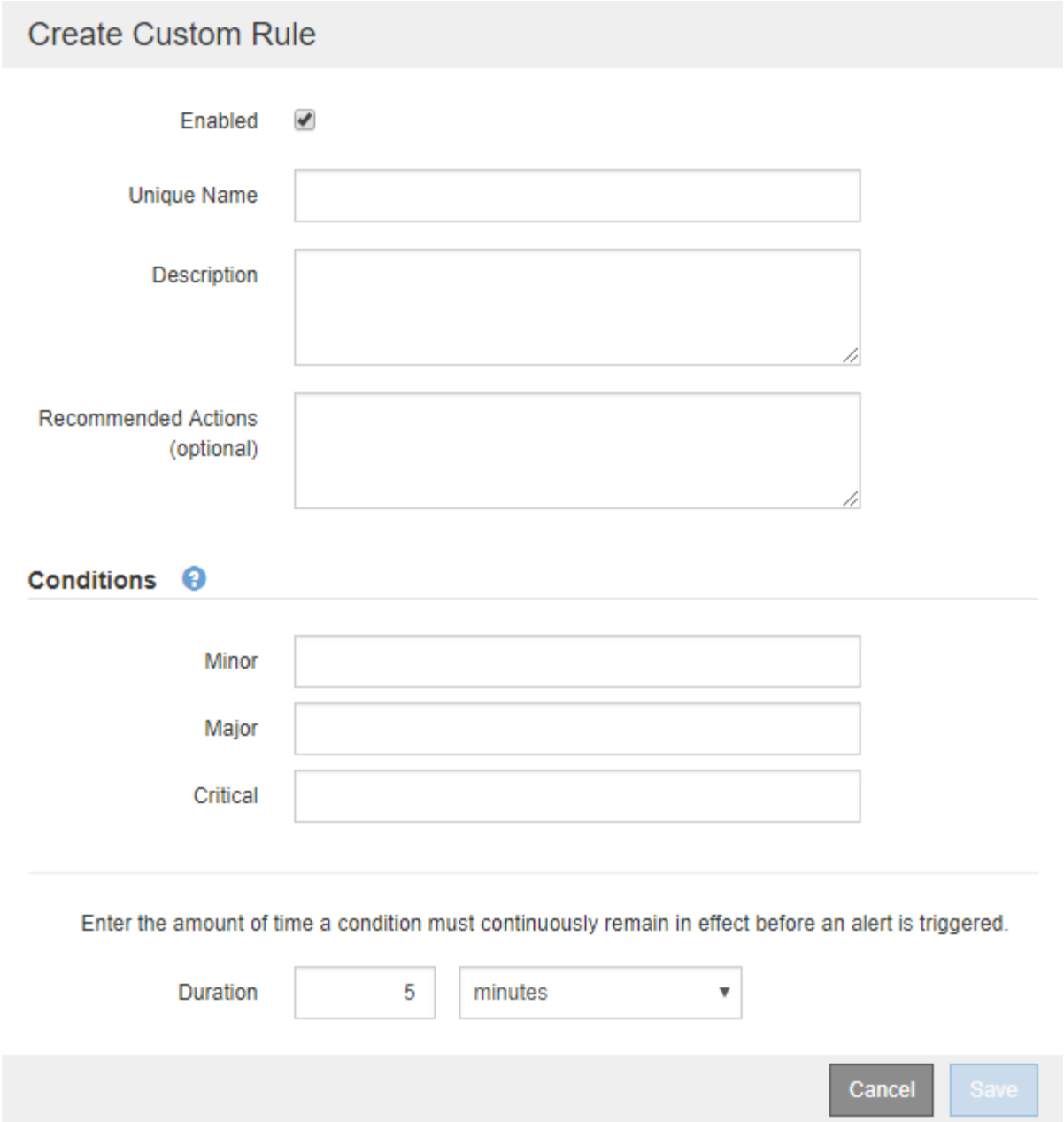
**Steps**

1. Select **ALERTS** > **Rules**.

   The Alert Rules page appears.

2. Select **Create custom rule**.

   The Create Custom Rule dialog box appears.




3. Select or unselect the **Enabled** check box to determine if this alert rule is currently enabled.

   If an alert rule is disabled, its expressions are not evaluated and no alerts are triggered.

4. Enter the following information:

| Field | Description |
|---|---|
| Unique Name | A unique name for this rule. The alert rule name is shown on the Alerts page and is also the subject for email notifications. Names for alert rules can be between 1 and 64 characters. |
| Description | A description of the problem that is occurring. The description is the alert message shown on the Alerts page and in email notifications. Descriptions for alert rules can be between 1 and 128 characters. |

| Field | Description |
| --- | --- |
| Recommended Actions | Optionally, the recommended actions to take when this alert is triggered. Enter recommended actions as plain text (no formatting codes). Recommended actions for alert rules can be between 0 and 1,024 characters. |

5. In the Conditions section, enter a Prometheus expression for one or more of the alert severity levels.

   A basic expression is usually of the form:

   ```
   [metric] [operator] [value]
   ```

   Expressions can be any length, but appear on a single line in the user interface. At least one expression is required.

   This expression causes an alert to be triggered if the amount of installed RAM for a node is less than 24,000,000,000 bytes (24 GB).

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

   To see available metrics and to test Prometheus expressions, select the help icon and follow the link to the Metrics section of the Grid Management API.

6. In the **Duration** field, enter the amount of time a condition must continuously remain in effect before the alert is triggered, and select a unit of time.

   To trigger an alert immediately when a condition becomes true, enter **0**. Increase this value to prevent temporary conditions from triggering alerts.

   The default is 5 minutes.

7. Select **Save**.

   The dialog box closes, and the new custom alert rule appears in the Alert Rules table.

#### Edit alert rules

You can edit an alert rule to change the trigger conditions, For a custom alert rule, you can also update the rule name, description, and recommended actions.

**What you'll need**

- You are signed in to the Grid Manager using a supported web browser.
- You have the Manage Alerts or Root Access permission.

**About this task**

When you edit a default alert rule, you can change the conditions for minor, major, and critical alerts; and the duration. When you edit a custom alert rule, you can also edit the rule's name, description, and recommended actions.

> Be careful when deciding to edit an alert rule. If you change trigger values, you might not detect an underlying problem until it prevents a critical operation from completing.

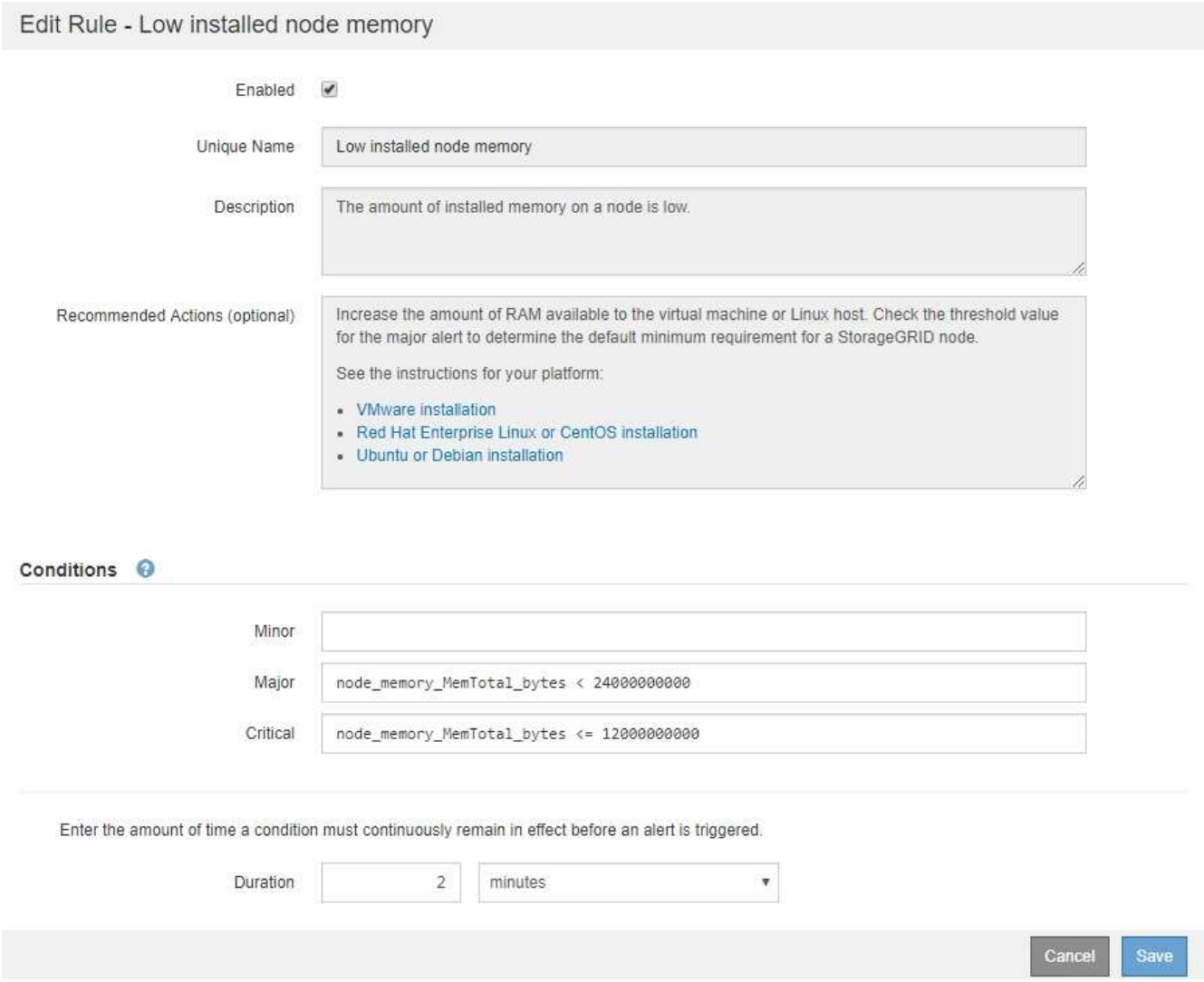
**Steps**

1. Select **ALERTS** > **Rules**.

   The Alert Rules page appears.

2. Select the radio button for the alert rule you want to edit.
3. Select **Edit rule**.

   The Edit Rule dialog box appears. This example shows a default alert rule—the Unique Name, Description, and Recommended Actions fields are disabled and cannot be edited.




4. Select or unselect the **Enabled** check box to determine if this alert rule is currently enabled.

   If an alert rule is disabled, its expressions are not evaluated and no alerts are triggered.

   > If you disable the alert rule for a current alert, you must wait a few minutes for the alert to no longer appear as an active alert.

   > In general, disabling a default alert rule is not recommended. If an alert rule is disabled, you might not detect an underlying problem until it prevents a critical operation from completing.

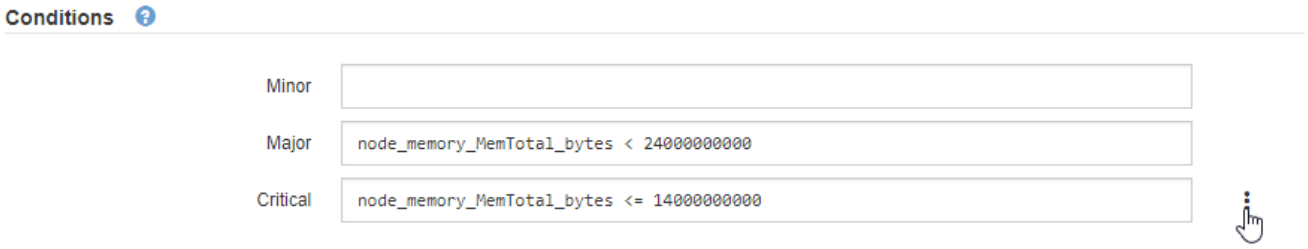
5. For custom alert rules, update the following information as required.

> You cannot edit this information for default alert rules.

| Field | Description |
|---|---|
| Unique Name | A unique name for this rule. The alert rule name is shown on the Alerts page and is also the subject for email notifications. Names for alert rules can be between 1 and 64 characters. |
| Description | A description of the problem that is occurring. The description is the alert message shown on the Alerts page and in email notifications. Descriptions for alert rules can be between 1 and 128 characters. |
| Recommended Actions | Optionally, the recommended actions to take when this alert is triggered. Enter recommended actions as plain text (no formatting codes). Recommended actions for alert rules can be between 0 and 1,024 characters. |

6. In the Conditions section, enter or update the Prometheus expression for one or more of the alert severity levels.

> If you want to restore a condition for an edited default alert rule back to its original value, select the three dots to the right of the modified condition.




> If you update the conditions for a current alert, your changes might not be implemented until the previous condition is resolved. The next time one of the conditions for the rule is met, the alert will reflect the updated values.

A basic expression is usually of the form:

```
[metric] [operator] [value]
```

Expressions can be any length, but appear on a single line in the user interface. At least one expression is required.

This expression causes an alert to be triggered if the amount of installed RAM for a node is less than 24,000,000,000 bytes (24 GB).

```
node_memory_MemTotal_bytes < 24000000000
```

7. In the **Duration** field, enter the amount of time a condition must continuously remain in effect before the

alert is triggered, and select the unit of time.

To trigger an alert immediately when a condition becomes true, enter **0**. Increase this value to prevent temporary conditions from triggering alerts.

The default is 5 minutes.

8. Select **Save**.

   If you edited a default alert rule, **Default*** appears in the Type column. If you disabled a default or custom alert rule, **Disabled** appears in the **Status** column.

#### Disable alert rules

## You can change the enabled/disabled state for a default or custom alert rule.

### What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have the Manage Alerts or Root Access permission.

### About this task

When an alert rule is disabled, its expressions are not evaluated and no alerts are triggered.

> In general, disabling a default alert rule is not recommended. If an alert rule is disabled, you might not detect an underlying problem until it prevents a critical operation from completing.

### Steps

1. Select **ALERTS** > **Rules**.

   The Alert Rules page appears.

2. Select the radio button for the alert rule you want to disable or enable.
3. Select **Edit rule**.

   The Edit Rule dialog box appears.

4. Select or unselect the **Enabled** check box to determine if this alert rule is currently enabled.

   If an alert rule is disabled, its expressions are not evaluated and no alerts are triggered.

   > If you disable the alert rule for a current alert, you must wait a few minutes for the alert to no longer display as an active alert.

5. Select **Save**.

   **Disabled** appears in the **Status** column.

#### Remove custom alert rules

## You can remove a custom alert rule if you no longer want to use it.

### What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have the Manage Alerts or Root Access permission.

**Steps**

1. Select **ALERTS** > **Rules**.

   The Alert Rules page appears.

2. Select the radio button for the custom alert rule you want to remove.

   You cannot remove a default alert rule.

3. Select **Remove custom rule**.

   A confirmation dialog box appears.

4. Select **OK** to remove the alert rule.

   Any active instances of the alert will be resolved within 10 minutes.

#### Manage alert notifications

### Set up SNMP notifications for alerts

If you want StorageGRID to send SNMP notifications when alerts occur, you must enable the StorageGRID SNMP agent and configure one or more trap destinations.

You can use the **CONFIGURATION** > **Monitoring** > **SNMP agent** option in the Grid Manager or the SNMP endpoints for the Grid Management API to enable and configure the StorageGRID SNMP agent. The SNMP agent supports all three versions of the SNMP protocol.

To learn how to configure the SNMP agent, see Use SNMP monitoring.

After you configure the StorageGRID SNMP agent, two types of event-driven notifications can be sent:

- Traps are notifications sent by the SNMP agent that do not require acknowledgment by the management system. Traps serve to notify the management system that something has happened within StorageGRID, such as an alert being triggered. Traps are supported in all three versions of SNMP.
- Informs are similar to traps, but they require acknowledgment by the management system. If the SNMP agent does not receive an acknowledgment within a certain amount of time, it resends the inform until an acknowledgment is received or the maximum retry value has been reached. Informs are supported in SNMPv2c and SNMPv3.

Trap and inform notifications are sent when a default or custom alert is triggered at any severity level. To suppress SNMP notifications for an alert, you must configure a silence for the alert. See Silence alert notifications.

Alert notifications are sent by whichever Admin Node is configured to be the preferred sender. By default, the primary Admin Node is selected. See the instructions for administering StorageGRID.

> Trap and inform notifications are also sent when certain alarms (legacy system) are triggered at specified severity levels or higher; however, SNMP notifications are not sent for every alarm or every alarm severity. See Alarms that generate SNMP notifications (legacy system).

### Set up email notifications for alerts

If you want email notifications to be sent when alerts occur, you must provide information about your SMTP server. You must also enter email addresses for the recipients of alert notifications.

#### What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have the Manage Alerts or Root Access permission.

#### About this task

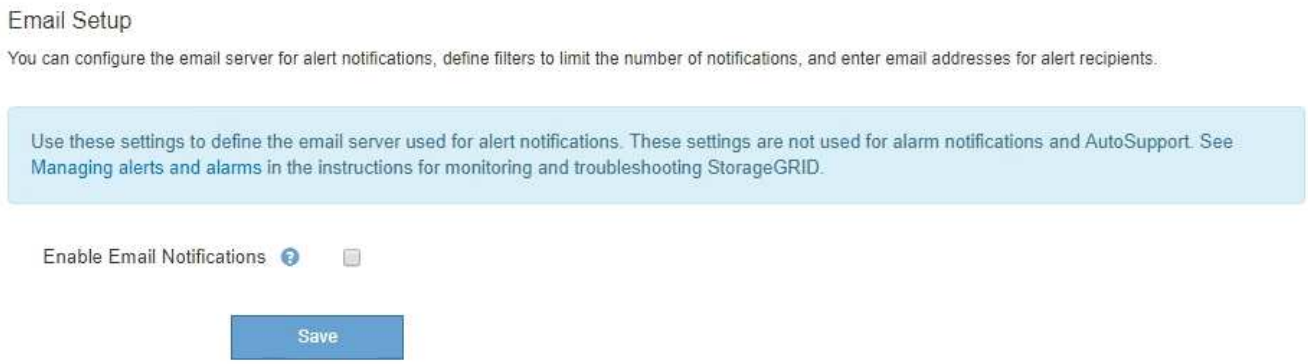
Because alarms and alerts are independent systems, the email setup used for alert notifications is not used for alarm notifications and AutoSupport messages. However, you can use the same email server for all notifications.

If your StorageGRID deployment includes multiple Admin Nodes, you can select which Admin Node should be the preferred sender of alert notifications. The same "preferred sender" is also used for alarm notifications and AutoSupport messages. By default, the primary Admin Node is selected. For details, see the instructions for administering StorageGRID.

#### Steps

1. Select **ALERTS** > **Email setup**.

   The Email Setup page appears.




2. Select the **Enable Email Notifications** check box to indicate that you want notification emails to be sent when alerts reach configured thresholds.

   The Email (SMTP) Server, Transport Layer Security (TLS), Email Addresses, and Filters sections appear.

3. In the Email (SMTP) Server section, enter the information StorageGRID needs to access your SMTP server.

   If your SMTP server requires authentication, you must provide both a username and a password.

| Field | Enter |
|---|---|
| Mail Server | The fully qualified domain name (FQDN) or IP address of the SMTP server. |

| Field | Enter |
| --- | --- |
| Port | The port used to access the SMTP server. Must be between 1 and 65535. |
| Username (optional) | If your SMTP server requires authentication, enter the username to authenticate with. |
| Password (optional) | If your SMTP server requires authentication, enter the password to authenticate with. |

4. In the Email Addresses section, enter email addresses for the sender and for each recipient.

   a. For the **Sender Email Address**, specify a valid email address to use as the From address for alert notifications.

      For example: `storagegrid-alerts@example.com`

   b. In the Recipients section, enter an email address for each email list or person who should receive an email when an alert occurs.

      Select the plus icon ✚ to add recipients.

5. If Transport Layer Security (TLS) is required for communications with the SMTP server, select **Require TLS** in the Transport Layer Security (TLS) section.

   a. In the **CA Certificate** field, provide the CA certificate that will be used to verify the identify of the SMTP server.

      You can copy and paste the contents into this field, or select **Browse** and select the file.

      You must provide a single file that contains the certificates from each intermediate issuing certificate

authority (CA). The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.

b. Select the **Send Client Certificate** check box if your SMTP email server requires email senders to provide client certificates for authentication.

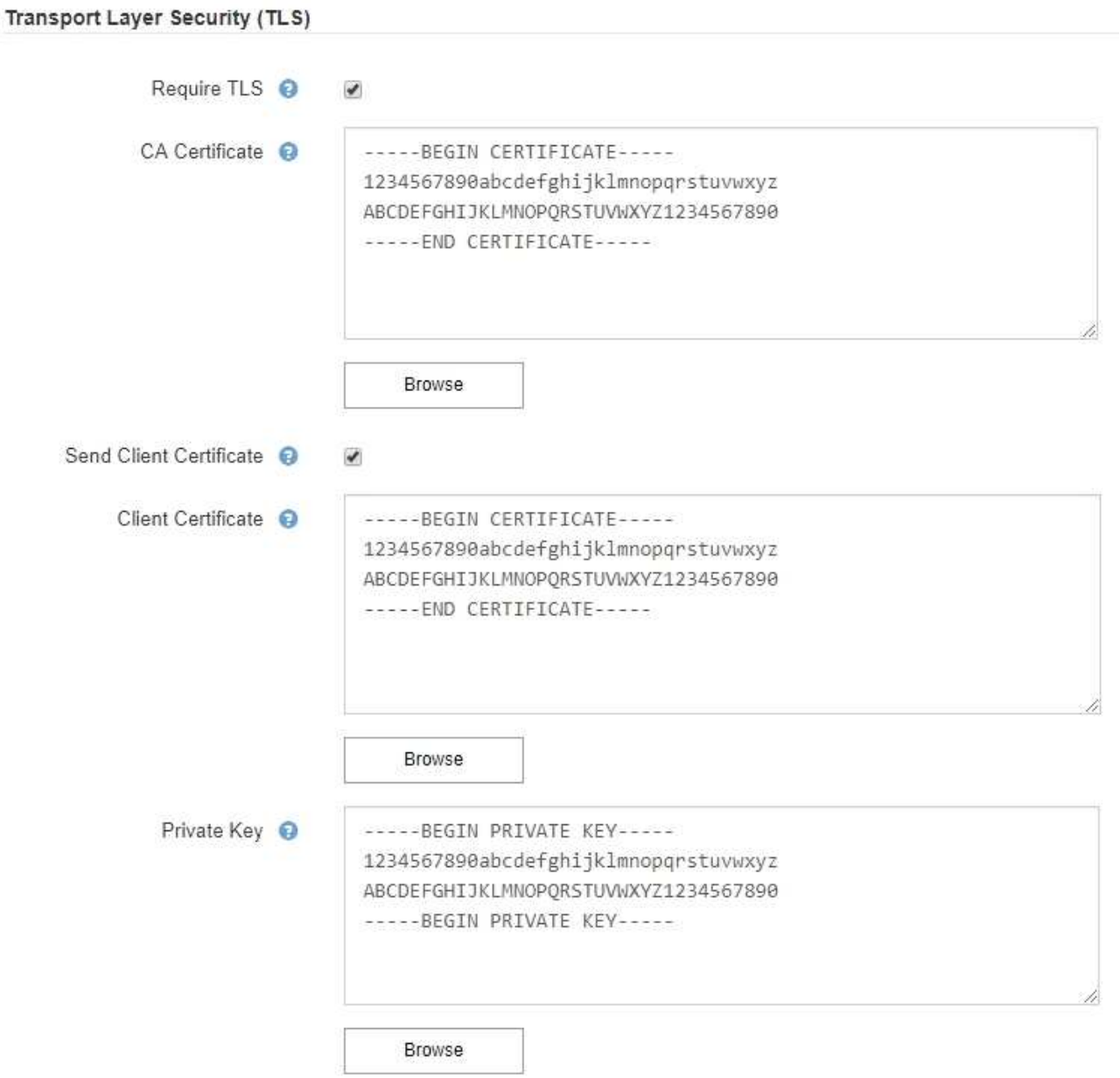
c. In the **Client Certificate** field, provide the PEM-encoded client certificate to send to the SMTP server.

   You can copy and paste the contents into this field, or select **Browse** and select the file.

d. In the **Private Key** field, enter the private key for the client certificate in unencrypted PEM encoding.

   You can copy and paste the contents into this field, or select **Browse** and select the file.

> If you need to edit the email setup, select the pencil icon to update this field.




6. In the Filters section, select which alert severity levels should result in email notifications, unless the rule for a specific alert has been silenced.

| Severity | Description |
| --- | --- |
| Minor, major, critical | An email notification is sent when the minor, major, or critical condition for an alert rule is met. |
| Major, critical | An email notification is sent when the major or critical condition for an alert rule is met. Notifications are not sent for minor alerts. |
| Critical only | An email notification is sent only when the critical condition for an alert rule is met. Notifications are not sent for minor or major alerts. |

7. When you are ready to test your email settings, perform these steps:
   a. Select **Send Test Email**.

      A confirmation message appears, indicating that a test email was sent.

   b. Check the inboxes of all email recipients and confirm that a test email was received.

      If the email is not received within a few minutes or if the **Email notification failure** alert is triggered, check your settings and try again.

   c. Sign in to any other Admin Nodes and send a test email to verify connectivity from all sites.

      When you test alert notifications, you must sign in to every Admin Node to verify connectivity. This is in contrast to testing alarm notifications and AutoSupport messages, where all Admin Nodes send the test email.

8. Select **Save**.

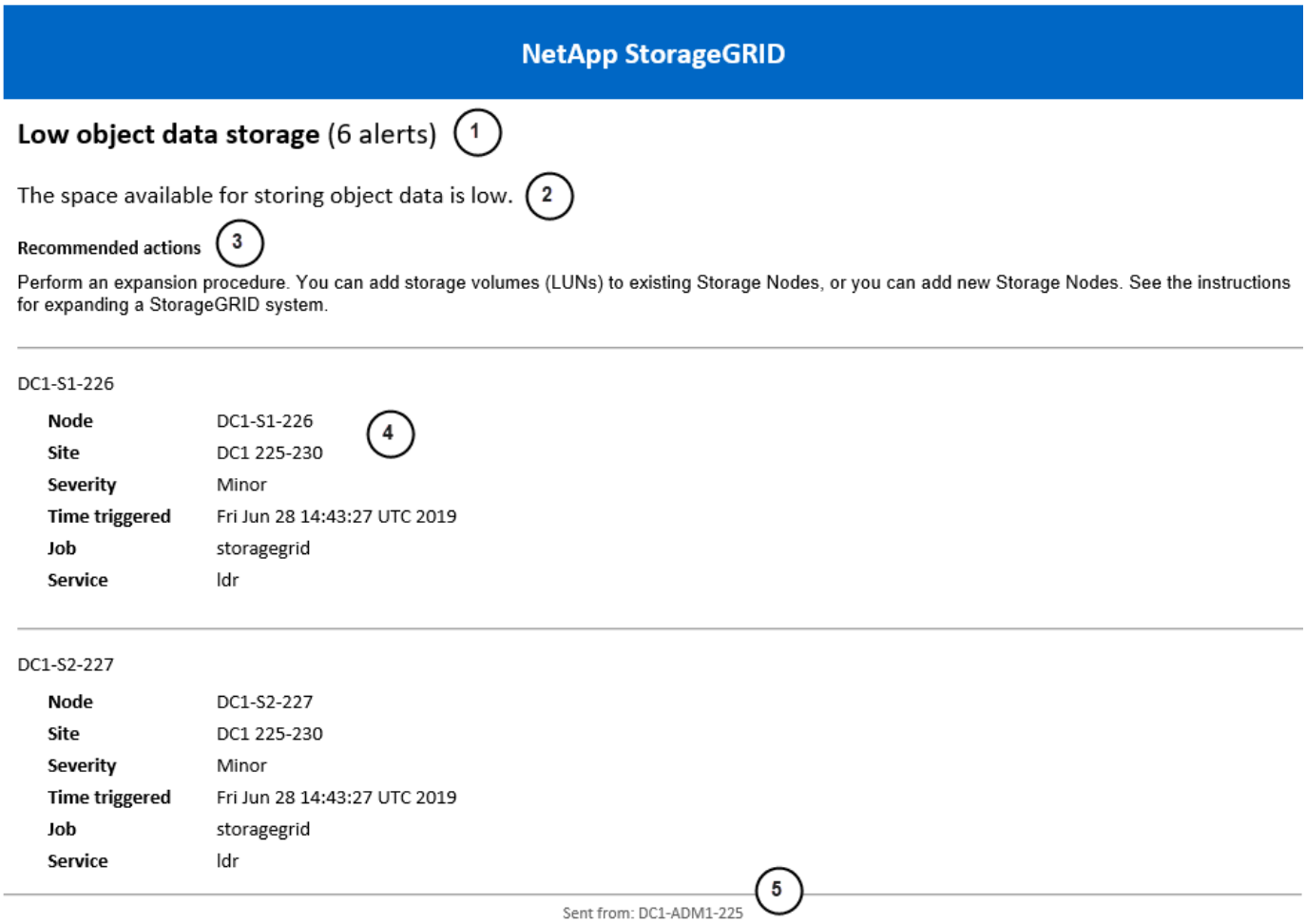
   Sending a test email does not save your settings. You must select **Save**.

   The email settings are saved.

### Information included in alert email notifications

After you configure the SMTP email server, email notifications are sent to the designated recipients when an alert is triggered, unless the alert rule is suppressed by a silence. See Silence alert notifications.

Email notifications include the following information:




| Callout | Description |
|---|---|
| 1 | The name of the alert, followed by the number of active instances of this alert. |
| 2 | The description of the alert. |
| 3 | Any recommended actions for the alert. |
| 4 | Details about each active instance of the alert, including the node and site affected, the alert severity, the UTC time when the alert rule was triggered, and the name of the affected job and service. |
| 5 | The hostname of the Admin Node that sent the notification. |

### How alerts are grouped

To prevent an excessive number of email notifications from being sent when alerts are triggered, StorageGRID attempts to group multiple alerts in the same notification.

Refer to the following table for examples of how StorageGRID groups multiple alerts in email notifications.

| Behavior | Example |
| --- | --- |
| Each alert notification applies only to alerts that have the same name. If two alerts with different names are triggered at the same time, two email notifications are sent. | • Alert A is triggered on two nodes at the same time. Only one notification is sent.<br>• Alert A is triggered on node 1, and Alert B is triggered on node 2 at the same time. Two notifications are sent—one for each alert. |
| For a specific alert on a specific node, if the thresholds are reached for more than one severity, a notification is sent only for the most severe alert. | • Alert A is triggered and the minor, major, and critical alert thresholds are reached. One notification is sent for the critical alert. |
| The first time an alert is triggered, StorageGRID waits 2 minutes before sending a notification. If other alerts with the same name are triggered during that time, StorageGRID groups all of the alerts in the initial notification. | 1. Alert A is triggered on node 1 at 08:00. No notification is sent.<br>2. Alert A is triggered on node 2 at 08:01. No notification is sent.<br>3. At 08:02, a notification is sent to report both instances of the alert. |
| If an another alert with the same name is triggered, StorageGRID waits 10 minutes before sending a new notification. The new notification reports all active alerts (current alerts that have not been silenced), even if they were reported previously. | 1. Alert A is triggered on node 1 at 08:00. A notification is sent at 08:02.<br>2. Alert A is triggered on node 2 at 08:05. A second notification is sent at 08:15 (10 minutes later). Both nodes are reported. |
| If there are multiple current alerts with the same name and one of those alerts is resolved, a new notification is not sent if the alert reoccurs on the node for which the alert was resolved. | 1. Alert A is triggered for node 1. A notification is sent.<br>2. Alert A is triggered for node 2. A second notification is sent.<br>3. Alert A is resolved for node 2, but it remains active for node 1.<br>4. Alert A is triggered again for node 2. No new notification is sent because the alert is still active for node 1. |
| StorageGRID continues to send email notifications once every 7 days until all instances of the alert are resolved or the alert rule is silenced. | 1. Alert A is triggered for node 1 on March 8. A notification is sent.<br>2. Alert A is not resolved or silenced. Additional notifications are sent on March 15, March 22, March 29, and so on. |

### Troubleshoot alert email notifications

If the **Email notification failure** alert is triggered or you are unable to receive the test alert email notification, follow these steps to resolve the issue.

#### What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have the Manage Alerts or Root Access permission.

**Steps**

1. Verify your settings.
   a. Select **ALERTS** > **Email setup**.
   b. Verify that the Email (SMTP) Server settings are correct.
   c. Verify that you have specified valid email addresses for the recipients.
2. Check your spam filter, and make sure that the email was not sent to a junk folder.
3. Ask your email administrator to confirm that emails from the sender address are not being blocked.
4. Collect a log file for the Admin Node, and then contact technical support.

   Technical support can use the information in the logs to help determine what went wrong. For example, the prometheus.log file might show an error when connecting to the server you specified.

   See Collect log files and system data.

### Silence alert notifications

Optionally, you can configure silences to temporarily suppress alert notifications.

**What you'll need**

- You are signed in to the Grid Manager using a supported web browser.
- You have the Manage Alerts or Root Access permission.

**About this task**

You can silence alert rules on the entire grid, a single site, or a single node and for one or more severities. Each silence suppresses all notifications for a single alert rule or for all alert rules.

If you have enabled the SNMP agent, silences also suppress SNMP traps and informs.

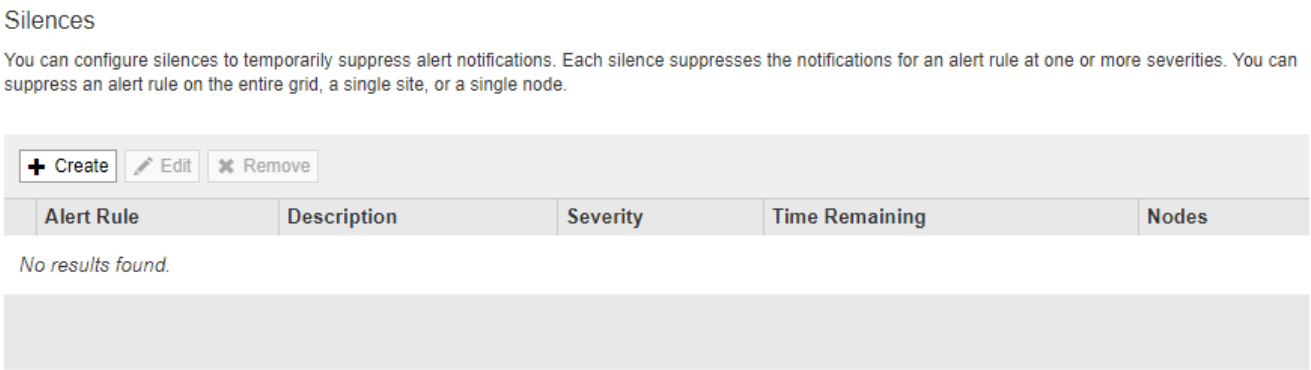
> Be careful when deciding to silence an alert rule. If you silence an alert, you might not detect an underlying problem until it prevents a critical operation from completing.

> Because alarms and alerts are independent systems, you cannot use this functionality to suppress alarm notifications.

**Steps**

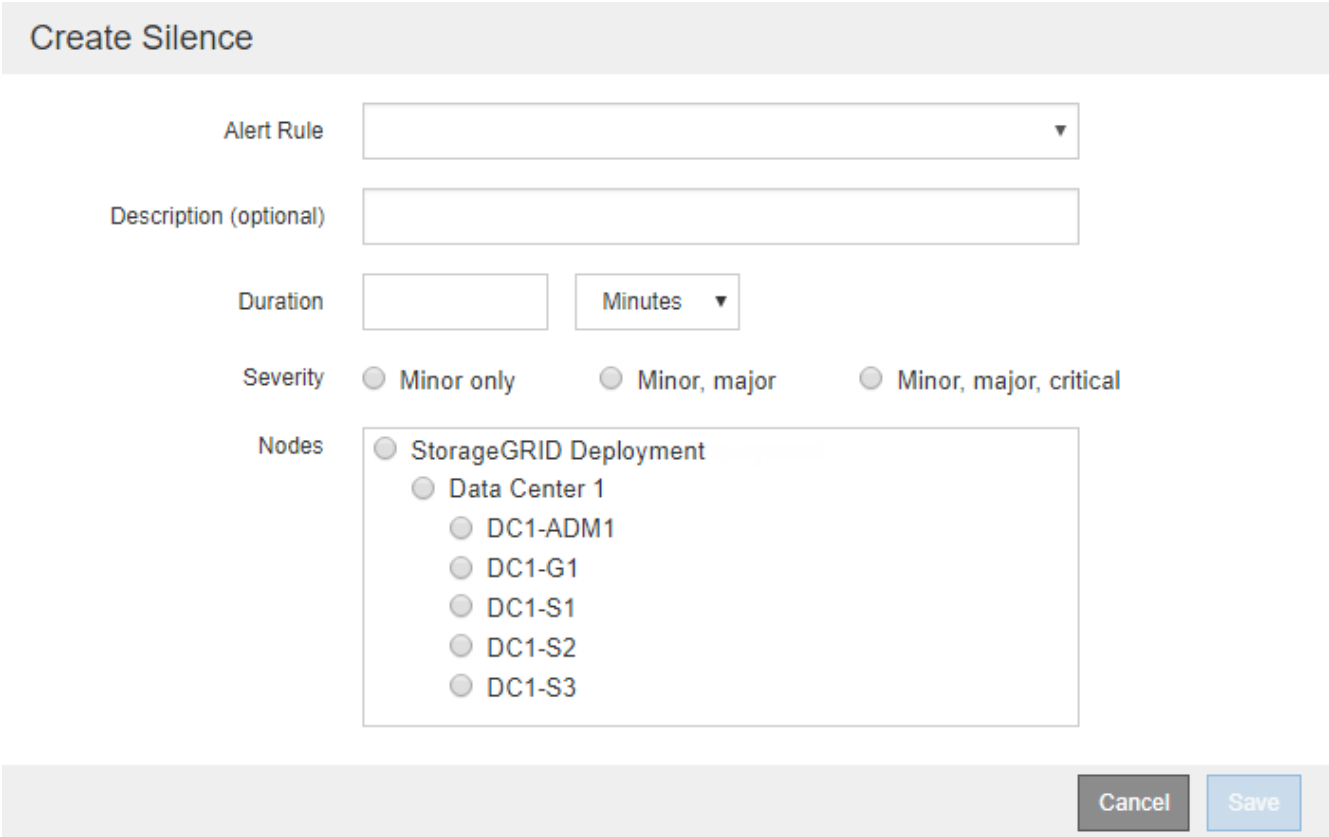
1. Select **ALERTS** > **Silences**.

   The Silences page appears.




2. Select **Create**.

   The Create Silence dialog box appears.




3. Select or enter the following information:

| Field | Description |
|---|---|
| Alert Rule | The name of the alert rule you want to silence. You can select any default or custom alert rule, even if the alert rule is disabled.<br><br>**Note:** Select **All rules** if you want to silence all alert rules using the criteria specified in this dialog box. |
| Description | Optionally, a description of the silence. For example, describe the purpose of this silence. |

| Field | Description |
| --- | --- |
| Duration | How long you want this silence to remain in effect, in minutes, hours, or days. A silence can be in effect from 5 minutes to 1,825 days (5 years).<br><br>**Note:** You should not silence an alert rule for an extended amount of time. If an alert rule is silenced, you might not detect an underlying problem until it prevents a critical operation from completing. However, you might need to use an extended silence if an alert is triggered by a specific, intentional configuration, such as might be the case for the **Services appliance link down** alerts and the **Storage appliance link down** alerts. |
| Severity | Which alert severity or severities should be silenced. If the alert is triggered at one of the selected severities, no notifications are sent. |
| Nodes | Which node or nodes you want this silence to apply to. You can suppress an alert rule or all rules on the entire grid, a single site, or a single node. If you select the entire grid, the silence applies to all sites and all nodes. If you select a site, the silence applies only to the nodes at that site.<br><br>**Note:** You cannot select more than one node or more than one site for each silence. You must create additional silences if you want to suppress the same alert rule on more than one node or more than one site at one time. |

4. Select **Save**.
5. If you want to modify or end a silence before it expires, you can edit or remove it.

| Option | Description |
| --- | --- |
| Edit a silence | a. Select **ALERTS** > **Silences**.<br>b. From the table, select the radio button for the silence you want to edit.<br>c. Select **Edit**.<br>d. Change the description, the amount of time remaining, the selected severities, or the affected node.<br>e. Select **Save**. |
| Remove a silence | a. Select **ALERTS** > **Silences**.<br>b. From the table, select the radio button for the silence you want to remove.<br>c. Select **Remove**.<br>d. Select **OK** to confirm you want to remove this silence.<br><br>**Note**: Notifications will now be sent when this alert is triggered (unless suppressed by another silence). If this alert is currently triggered, it might take few minutes for email or SNMP notifications to be sent and for the Alerts page to update. |

**Related information**

- Configure the SNMP agent

## Manage alarms (legacy system)

The StorageGRID alarm system is the legacy system used to identify trouble spots that sometimes occur during normal operation.

> While the legacy alarm system continues to be supported, the alert system offers significant benefits and is easier to use.

### Alarm classes (legacy system)

A legacy alarm can belong to one of two mutually exclusive alarm classes.

- Default alarms are provided with each StorageGRID system and cannot be modified. However, you can disable Default alarms or override them by defining Global Custom alarms.
- Global Custom alarms monitor the status of all services of a given type in the StorageGRID system. You can create a Global Custom alarm to override a Default alarm. You can also create a new Global Custom alarm. This can be useful for monitoring any customized conditions of your StorageGRID system.

### Alarm triggering logic (legacy system)

A legacy alarm is triggered when a StorageGRID attribute reaches a threshold value that evaluates to true against a combination of alarm class (Default or Global Custom) and alarm severity level.

| Icon | Color | Alarm severity | Meaning |
|---|---|---|---|
| | Yellow | Notice | The node is connected to the grid, but an unusual condition exists that does not affect normal operations. |
| | Light Orange | Minor | The node is connected to the grid, but an abnormal condition exists that could affect operation in the future. You should investigate to prevent escalation. |
| | Dark Orange | Major | The node is connected to the grid, but an abnormal condition exists that currently affects operation. This requires prompt attention to prevent escalation. |
| | Red | Critical | The node is connected to the grid, but an abnormal condition exists that has stopped normal operations. You should address the issue immediately. |

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

Note that a severity level of Normal does not trigger an alarm.

Attribute values are evaluated against the list of enabled alarms defined for that attribute. The list of alarms is checked in the following order to find the first alarm class with a defined and enabled alarm for the attribute:

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

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

### Alarm triggering example

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

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

| | **Global Custom alarm threshold (enabled)** | **Default alarm threshold (enabled)** |
|---|---|---|
| Notice | >= 1500 | >= 1000 |
| Minor | >= 15,000 | >= 1000 |
| Major | >=150,000 | >= 250,000 |

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

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

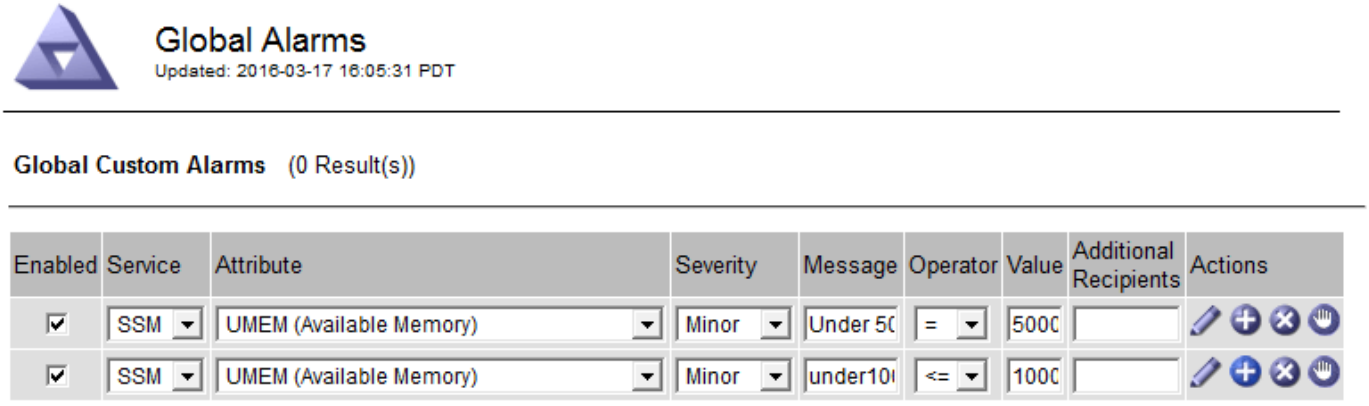
After the above scenario, if the Global Custom alarm is disabled, nothing changes. The attribute value must be reevaluated before a new alarm level is triggered.

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

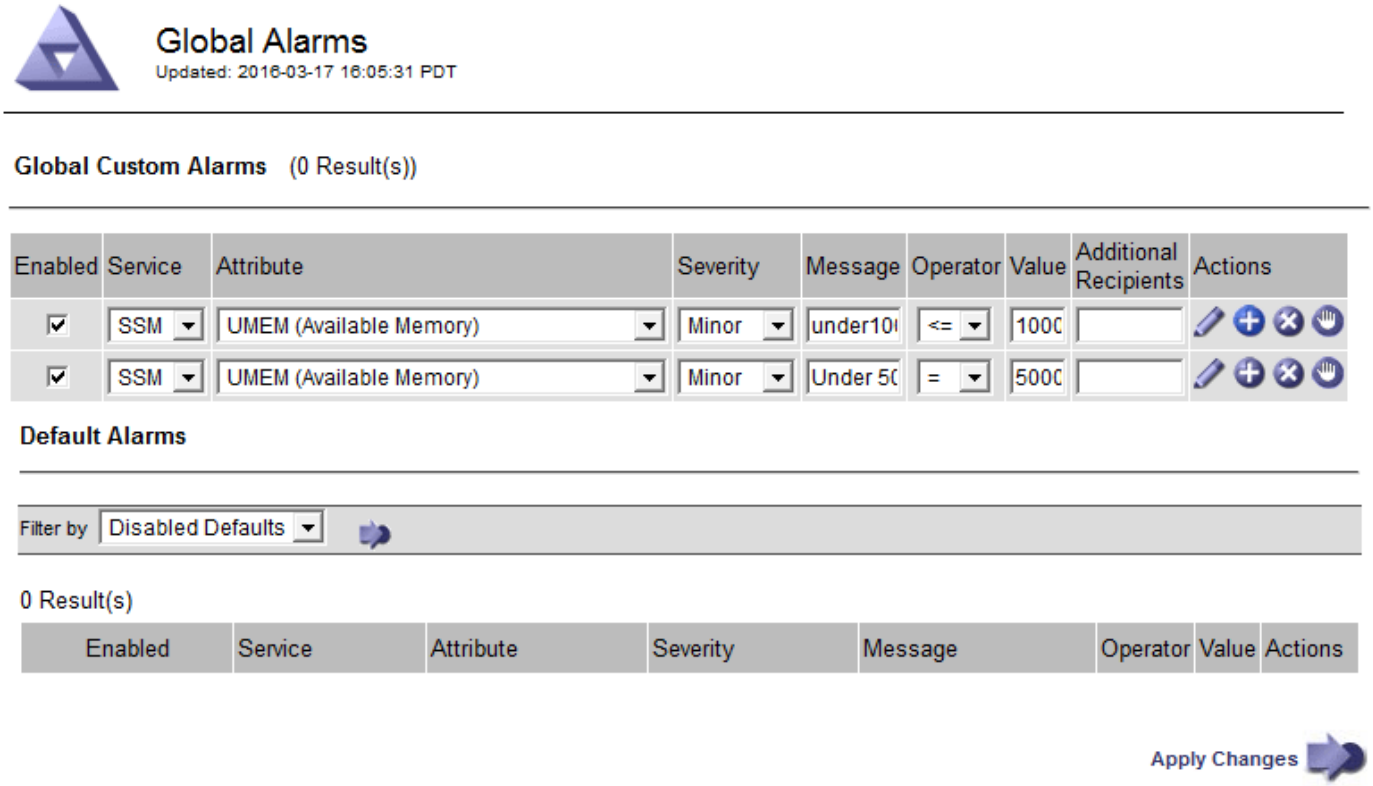
### Alarms of same severity

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

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




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




### Notifications

A notification reports the occurrence of an alarm or the change of state for a service. Alarm notifications can be sent in email or using SNMP.

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

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

### New services

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

### Alarms and tables

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

For example, the following table shows two critical Entries Available (VMFI) alarms. (Select **SUPPORT** > **Tools** > **Grid topology**. Then, select ***Storage Node*** > **SSM** > **Resources**.)

You can disable the VMFI alarm so that the Critical level VMFI alarm is not triggered (both currently Critical alarms would appear in the table as green); however, you cannot disable a single alarm in a table row so that one VMFI alarm displays as a Critical level alarm while the other remains green.

**Volumes**

| Mount Point | Device | Status | Size | Space Available | Total Entries | Entries Available | Write Cache |
|---|---|---|---|---|---|---|---|
| / | sda1 | Online | 10.6 GB | 7.46 GB | 655,360 | 559,263 | Enabled |
| /var/local | sda3 | Online | 63.4 GB | 59.4 GB | 3,932,160 | 3,931,842 | Unknown |
| /var/local/rangedb/0 | sdb | Online | 53.4 GB | 53.4 GB | 52,428,800 | 52,427,856 | Enabled |
| /var/local/rangedb/1 | sdc | Online | 53.4 GB | 53.4 GB | 52,428,800 | 52,427,848 | Enabled |
| /var/local/rangedb/2 | sdd | Online | 53.4 GB | 53.4 GB | 52,428,800 | 52,427,856 | Enabled |

#### Acknowledge current alarms (legacy system)

Legacy alarms are triggered when system attributes reach alarm threshold values. Optionally, if you want to reduce or clear the list of legacy alarms, you can acknowledge the alarms.

### What you'll need

- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Acknowledge Alarms permission.

### About this task

Because the legacy alarm system continues to be supported, the list of legacy alarms on the Current Alarms page is increased whenever a new alarm occurs. You can typically ignore the alarms (since alerts provide a better view of the system), or you can acknowledge the alarms.

> Optionally, when you have completely transitioned to the alert system, you can disable each legacy alarm to prevent it from being triggered and added to the count of legacy alarms.

When you acknowledge an alarm, it is no longer listed on the Current Alarms page in the Grid Manager, unless the alarm is triggered at the next severity level or it is resolved and occurs again.

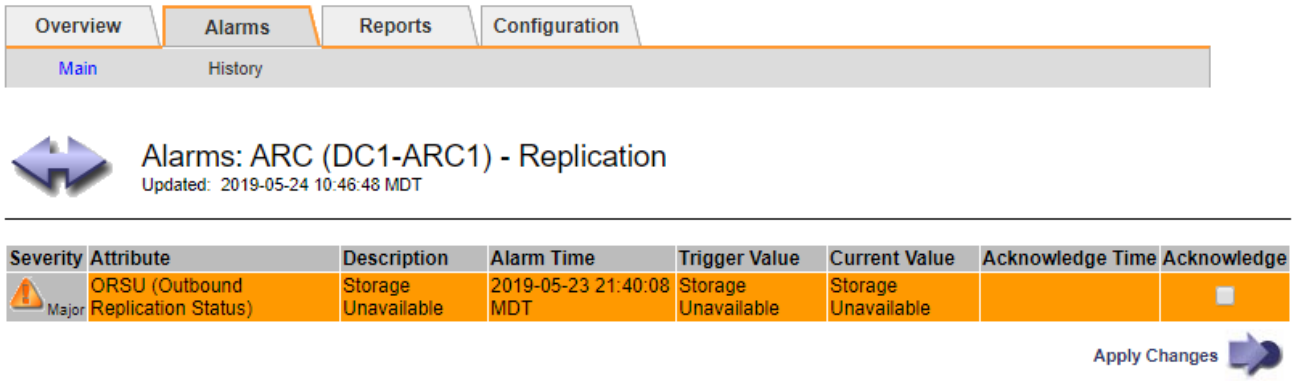
> While the legacy alarm system continues to be supported, the alert system offers significant benefits and is easier to use.

### Steps

1. Select **SUPPORT** > **Alarms (legacy)** > **Current alarms**.

2. Select the service name in the table.

   The Alarms tab for the selected service appears (**SUPPORT** > **Tools** > **Grid topology** > ***Grid Node*** > ***Service*** > **Alarms**).



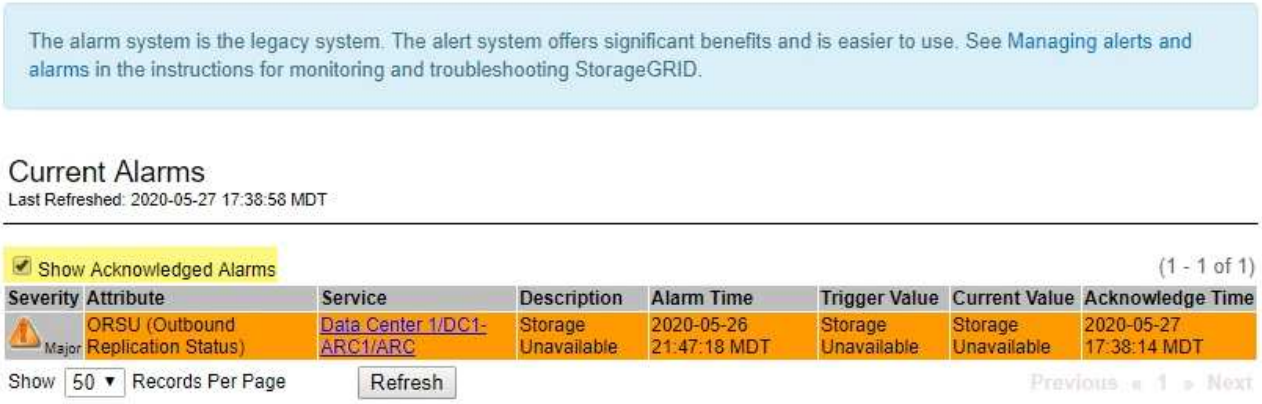

3. Select the **Acknowledge** check box for the alarm, and click **Apply Changes**.

   The alarm no longer appears on the Dashboard or the Current Alarms page.

   > When you acknowledge an alarm, the acknowledgment is not copied to other Admin Nodes. For this reason, if you view the Dashboard from another Admin Node, you might continue to see the active alarm.

4. As required, view acknowledged alarms.
   a. Select **SUPPORT** > **Alarms (legacy)** > **Current alarms**.
   b. Select **Show Acknowledged Alarms**.

      Any acknowledged alarms are shown.




#### View Default alarms (legacy system)

You can view the list of all Default legacy alarms.

#### What you'll need

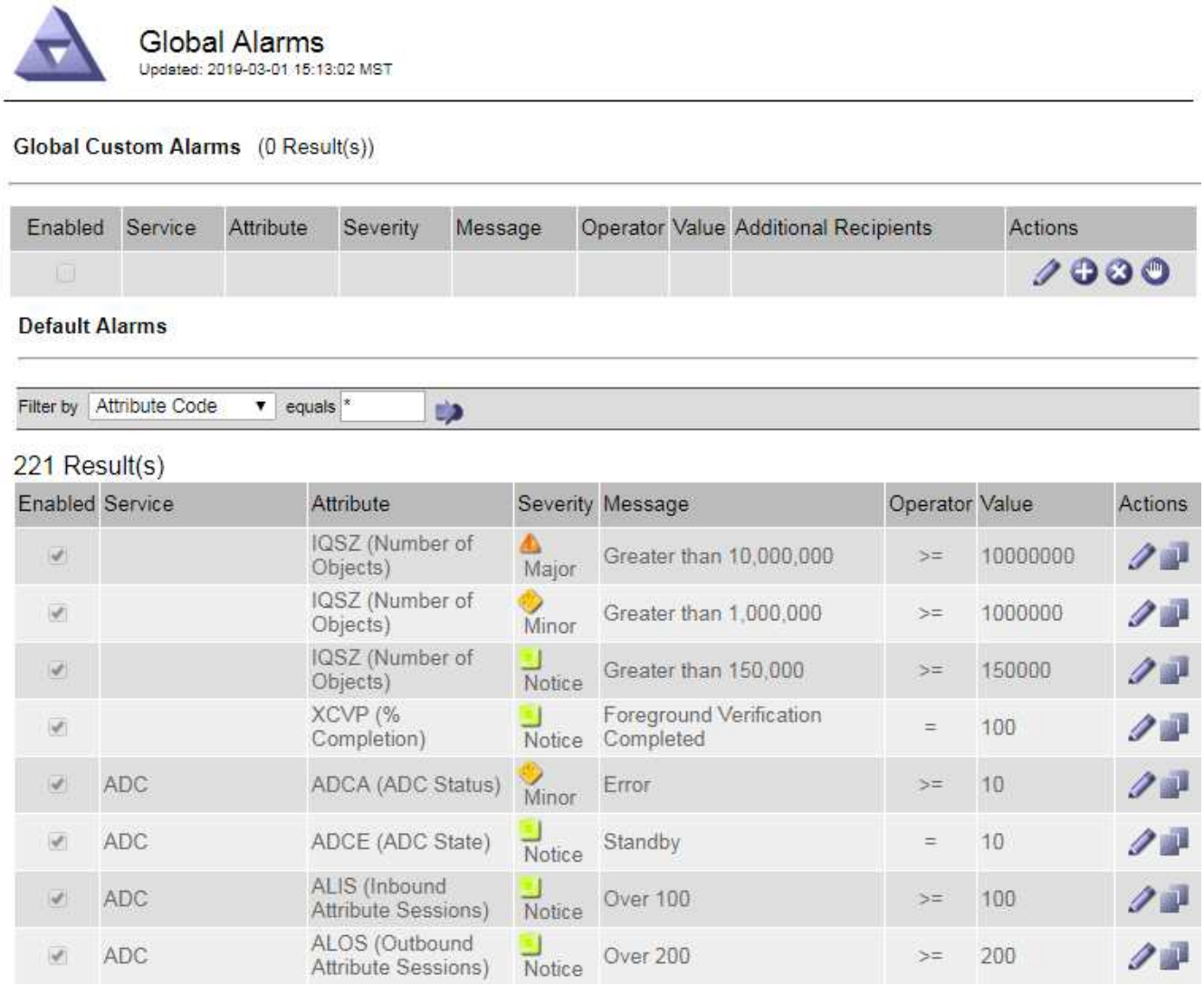
- You must be signed in to the Grid Manager using a supported web browser.
- You must have specific access permissions.

> While the legacy alarm system continues to be supported, the alert system offers significant benefits and is easier to use.

#### Steps

1. Select **SUPPORT** > **Alarms (legacy)** > **Global alarms**.
2. For Filter by, select **Attribute Code** or **Attribute Name**.
3. For equals, enter an asterisk: *
4. Click the arrow or press **Enter**.

   All Default alarms are listed.




#### Review historical alarms and alarm frequency (legacy system)

When troubleshooting an issue, you can review how often a legacy alarm was triggered in the past.

**What you'll need**

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

> While the legacy alarm system continues to be supported, the alert system offers significant benefits and is easier to use.

**Steps**

1. Follow these steps to get a list of all alarms triggered over a period of time.
   a. Select **SUPPORT** > **Alarms (legacy)** > **Historical alarms**.
   b. Do one of the following:
      - Click one of the time periods.
      - Enter a custom range, and click **Custom Query**.

2. Follow these steps to find out how often alarms have been triggered for a particular attribute.
   a. Select **SUPPORT** > **Tools** > **Grid topology**.
   b. Select ***grid node*** > ***service or component*** > **Alarms** > **History**.
   c. Select the attribute from the list.
   d. Do one of the following:
      - Click one of the time periods.
      - Enter a custom range, and click **Custom Query**.

        The alarms are listed in reverse chronological order.
   e. To return to the alarms history request form, click **History**.

#### Create Global Custom alarms (legacy system)

You might have used Global Custom alarms for the legacy system to address specific monitoring requirements. Global Custom alarms might have alarm levels that override Default alarms, or they might monitor attributes that do not have a Default alarm.

**What you'll need**

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

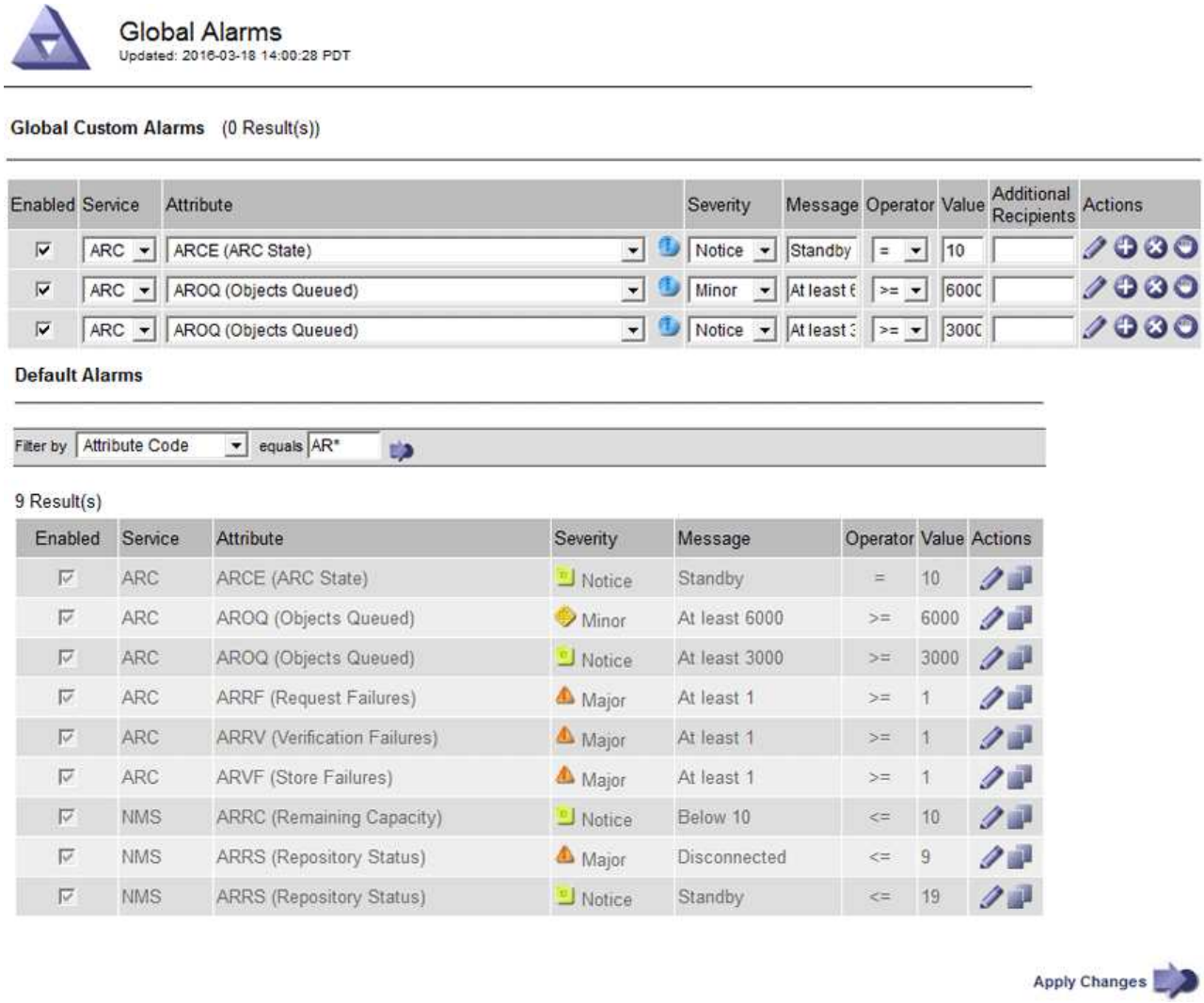
> While the legacy alarm system continues to be supported, the alert system offers significant benefits and is easier to use.

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

> Be very careful if you change alarm settings. For example, if you increase the threshold value for an alarm, you might not detect an underlying problem. Discuss your proposed changes with technical support before changing an alarm setting.

**Steps**

1. Select **SUPPORT** > **Alarms (legacy)** > **Global alarms**.
2. Add a new row to the Global Custom alarms table:
   - To add a new alarm, click **Edit** (if this is the first entry) or **Insert** .




- To modify a Default alarm, search for the Default alarm.
  i. Under Filter by, select either **Attribute Code** or **Attribute Name**.
  ii. Type a search string.

     Specify four characters or use wildcards (for example, A??? or AB*). Asterisks (*) represent multiple characters, and question marks (?) represent a single character.

  iii. Click the arrow , or press **Enter**.
  iv. In the list of results, click **Copy** next to the alarm you want to modify.

     The Default alarm is copied to the Global Custom alarms table.

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

| Heading | Description |
|---|---|
| Enabled | Select or unselect the check box to enable or disable the alarm. |

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

4. Click **Apply Changes**.

#### Disable alarms (legacy system)

The alarms in the legacy alarm system are enabled by default, but you can disable alarms that are not required. You can also disable the legacy alarms after you have completely transitioned to the new alert system.

> While the legacy alarm system continues to be supported, the alert system offers significant benefits and is easier to use.

### Disable a Default alarm (legacy system)

You can disable one of the legacy Default alarms for the entire system.

#### What you'll need

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

#### About this task

Disabling an alarm for an attribute that currently has an alarm triggered does not clear the current alarm. The alarm will be disabled the next time the attribute crosses the alarm threshold, or you can clear the triggered alarm.

> Do not disable any of the legacy alarms until you have completely transitioned to the new alert system. Otherwise, you might not detect an underlying problem until it has prevented a critical operation from completing.

#### Steps

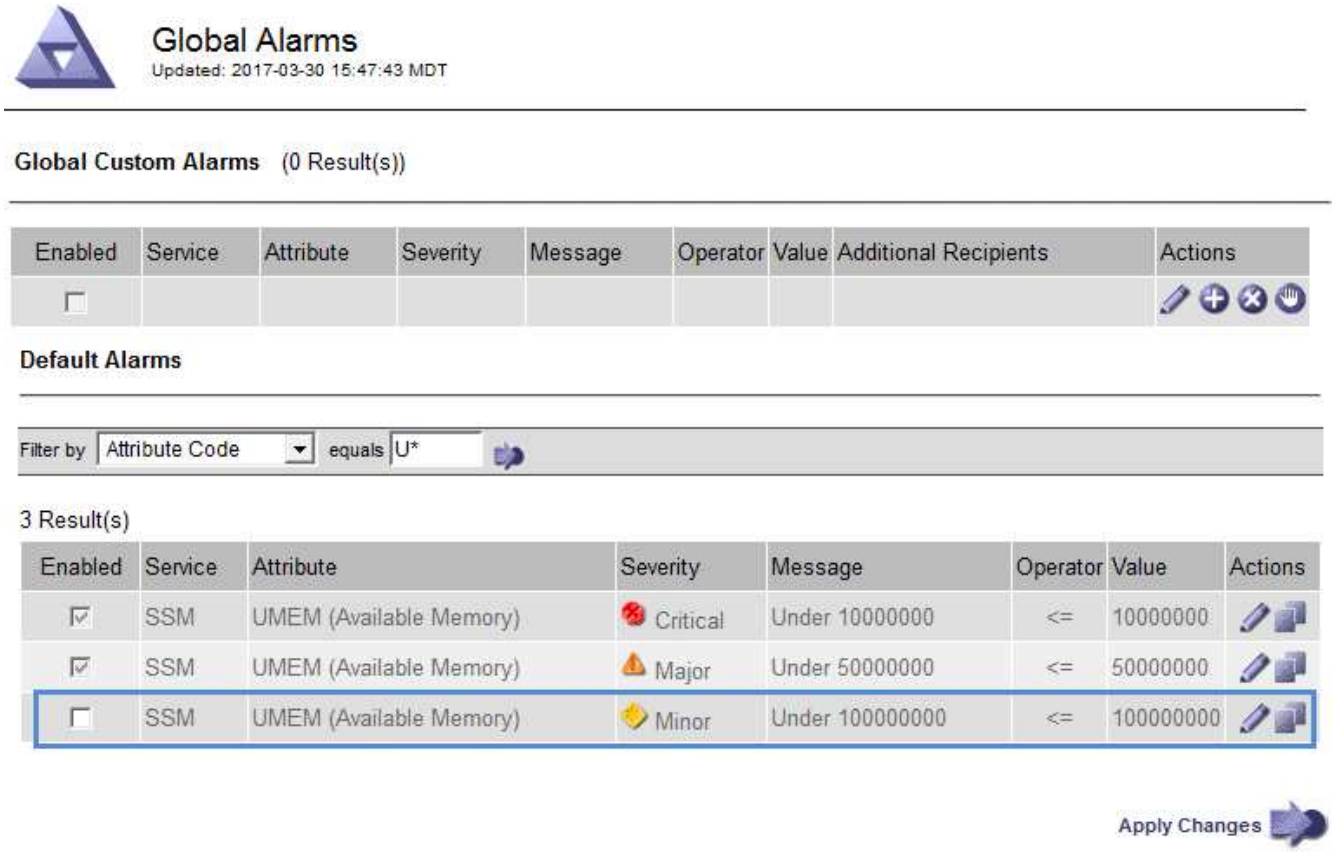
1. Select **SUPPORT** > **Alarms (legacy)** > **Global alarms**.
2. Search for the Default alarm to disable.
   a. In the Default Alarms section, select **Filter by** > **Attribute Code** or **Attribute Name**.
   b. Type a search string.

      Specify four characters or use wildcards (for example, A??? or AB*). Asterisks (*) represent multiple characters, and question marks (?) represent a single character.

   c. Click the arrow , or press **Enter**.

      > Selecting **Disabled Defaults** displays a list of all currently disabled Default alarms.

3. From the search results table, click the Edit icon for the alarm you want to disable.




The **Enabled** check box for the selected alarm becomes active.

4. Unselect the **Enabled** check box.
5. Click **Apply Changes**.

   The Default alarm is disabled.

### Disable Global Custom alarms (legacy system)

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

#### What you'll need

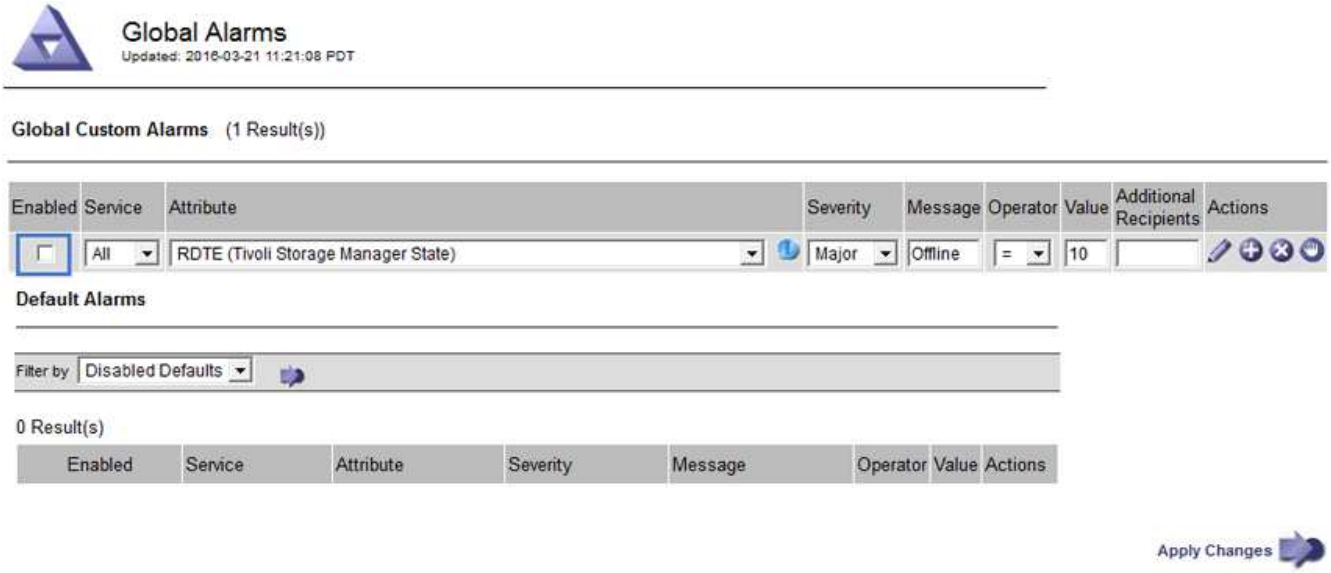
- You must be signed in to the Grid Manager using a supported web browser.
- You must have specific access permissions.

#### About this task

Disabling an alarm for an attribute that currently has an alarm triggered does not clear the current alarm. The alarm will be disabled the next time the attribute crosses the alarm threshold, or you can clear the triggered alarm.

#### Steps

1. Select **SUPPORT** > **Alarms (legacy)** > **Global alarms**.
2. In the Global Custom Alarms table, click **Edit** next to the alarm you want to disable.
3. Unselect the **Enabled** check box.




4. Click **Apply Changes**.

   The Global Custom alarm is disabled.

### Clear triggered alarms (legacy system)

If a legacy alarm is triggered, you can clear it instead of acknowledging it.

#### What you'll need

- You must have the `Passwords.txt` file.

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

1. Disable the alarm.
2. Log in to the primary Admin Node:
   a. Enter the following command: *`ssh admin@primary_Admin_Node_IP`*
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.
3. Restart the NMS service: `service nms restart`
4. Log out of the Admin Node: `exit`

   The alarm is cleared.

#### Configure notifications for alarms (legacy system)

StorageGRID system can automatically send email and SNMP notifications when an alarm is triggered or a service state changes.

By default, alarm email notifications are not sent. For email notifications, you must configure the email server and specify the email recipients. For SNMP notifications, you must configure the SNMP agent.

### Types of alarm notifications (legacy system)

When a legacy alarm is triggered, the StorageGRID system sends out two types of alarm notifications: severity level and service state.

#### Severity level notifications

An alarm email notification is sent when a legacy alarm is triggered at a selected severity level:

- Notice
- Minor
- Major
- Critical

A mailing list receives all notifications related to the alarm for the selected severity. A notification is also sent when the alarm leaves the alarm level — either by being resolved or by entering a different alarm severity level.

#### Service state notifications

A service state notification is sent when a service (for example, the LDR service or NMS service) enters the selected service state and when it leaves the selected service state. Service state notifications are send when a service enters or leaves ones of the following service states:

- Unknown
- Administratively Down

A mailing list receives all notifications related to changes in the selected state.

### Configure email server settings for alarms (legacy system)

If you want StorageGRID to send email notifications when a legacy alarm is triggered, you must specify the SMTP mail server settings. The StorageGRID system only sends email; it cannot receive email.

#### What you'll need

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

#### About this task

Use these settings to define the SMTP server used for legacy alarm email notifications and AutoSupport email messages. These settings are not used for alert notifications.

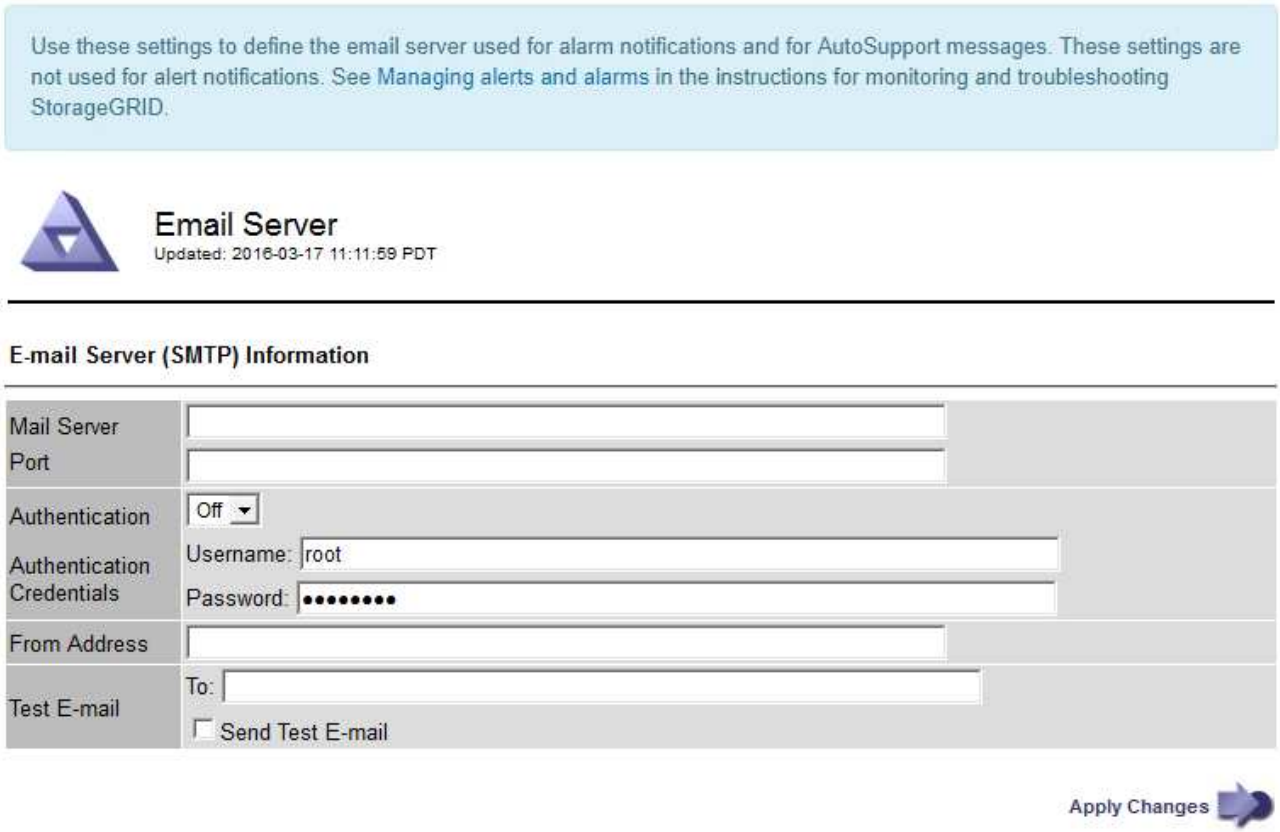
> If you use SMTP as the protocol for AutoSupport messages, you might have already configured an SMTP mail server. The same SMTP server is used for alarm email notifications, so you can skip this procedure. See the instructions for administering StorageGRID.

SMTP is the only protocol supported for sending email.

**Steps**

1. Select **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. From the Email menu, select **Server**.

   The Email Server page appears. This page is also used to configure the email server for AutoSupport messages.




3. Add the following SMTP mail server settings:

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

4. Under **From Address**, enter a valid email address that the SMTP server will recognize as the sending email address. This is the official email address from which the email message is sent.
5. Optionally, send a test email to confirm that your SMTP mail server settings are correct.
   a. In the **Test E-mail** > **To** box, add one or more addresses that you can access.

      You can enter a single email address or a comma-delineated list of email addresses. Because the NMS service does not confirm success or failure when a test email is sent, you must be able to check the test recipient's inbox.

   b. Select **Send Test E-mail**.
6. Click **Apply Changes**.

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

### Create alarm email templates (legacy system)

Email templates let you customize the header, footer, and subject line of a legacy alarm email notification. You can use email templates to send unique notifications that contain the same body text to different mailing lists.

#### What you'll need

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

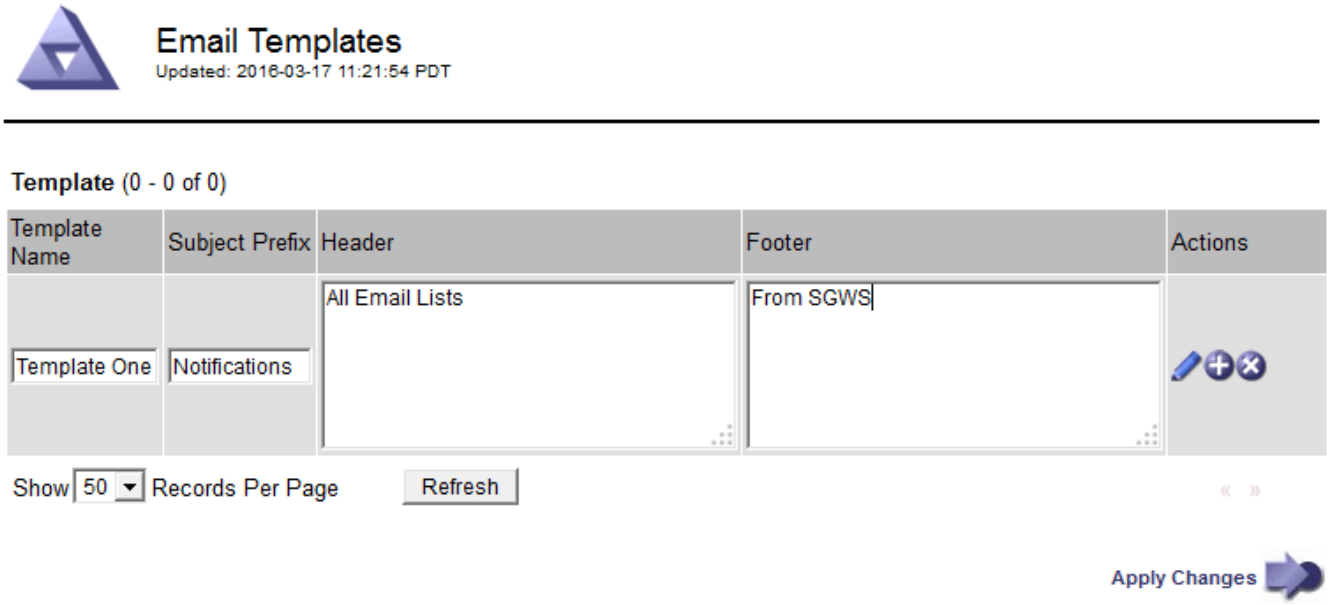
#### About this task

Use these settings to define the email templates used for legacy alarm notifications. These settings are not used for alert notifications.

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

#### Steps

1. Select **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. From the Email menu, select **Templates**.
3. Click **Edit** (or **Insert** if this is not the first template).




4. In the new row add the following:

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

5. Click **Apply Changes**.

   A new template for notifications is added.

### Create mailing lists for alarm notifications (legacy system)

Mailing lists let you notify recipients when a legacy alarm is triggered or when a service state changes. You must create at least one mailing list before any alarm email notifications can be sent. To send a notification to a single recipient, create a mailing list with one email address.

#### What you'll need

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

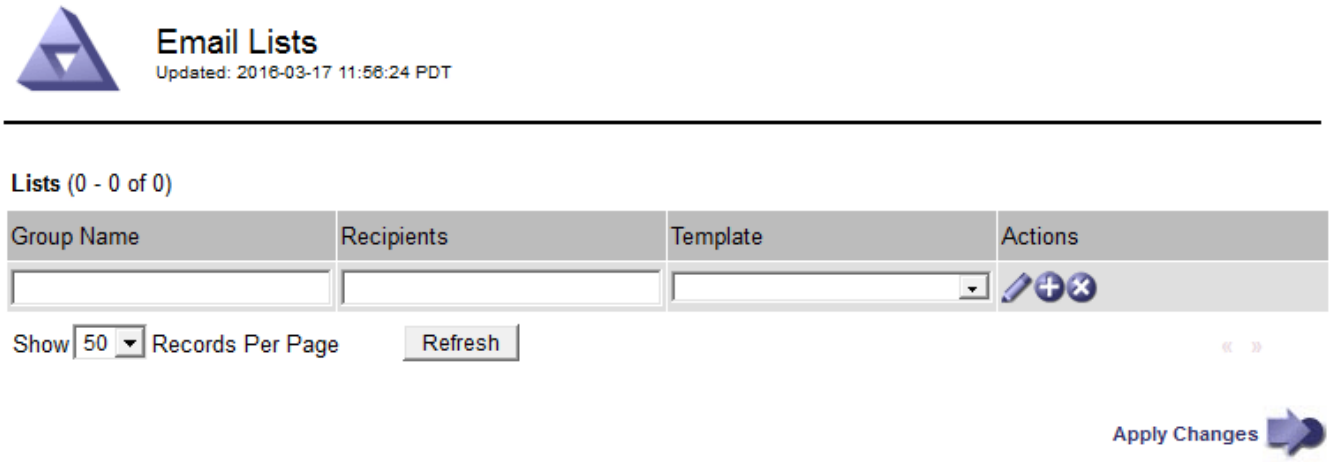
- If you want to specify an email template for the mailing list (custom header, footer, and subject line), you must have already created the template.

### About this task

Use these settings to define the mailing lists used for legacy alarm email notifications. These settings are not used for alert notifications.

### Steps

1. Select **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. From the Email menu, select **Lists**.
3. Click **Edit** (or *Insert* if this is not the first mailing list).




4. In the new row, add the following:

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

5. Click **Apply Changes**.

   A new mailing list is created.

### Configure email notifications for alarms (legacy system)

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

#### What you'll need

- You must be signed in to the Grid Manager using a supported web browser.
- You must have specific access permissions.
- You must have configured an email list.

#### About this task

Use these settings to configure notifications for legacy alarms. These settings are not used for alert notifications.

If an email address (or list) belongs to multiple mailing lists, only one email notification is sent when a notification triggering event occurs. For example, one group of administrators within your organization can be configured to receive notifications for all alarms regardless of severity. Another group might only require notifications for alarms with a severity of critical. You can belong to both lists. If a critical alarm is triggered, you receive only one notification.

#### Steps

1. Select **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. From the Email menu, select **Notifications**.
3. Click *Edit* (or *Insert* if this is not the first notification).
4. Under E-mail List, select the mailing list.
5. Select one or more alarm severity levels and service states.
6. Click **Apply Changes**.

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

### Suppress alarm notifications for a mailing list (legacy system)

You can suppress alarm notifications for a mailing list when you no longer want the mailing list to receive notifications about alarms. For example, you might want to suppress notifications about legacy alarms after you have transitioned to using alert email notifications.

#### What you'll need

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

Use these settings to suppress email notifications for the legacy alarm system. These settings do not apply to alert email notifications.

> While the legacy alarm system continues to be supported, the alert system offers significant benefits and is easier to use.

### Steps

1. Select **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. From the Email menu, select **Notifications**.
3. Click **Edit** next to the mailing list for which you want to suppress notifications.
4. Under Suppress, select the check box next to the mailing list you want to suppress, or select **Suppress** at the top of the column to suppress all mailing lists.
5. Click **Apply Changes**.

   Legacy alarm notifications are suppressed for the selected mailing lists.

## Suppress email notifications system wide

You can block the StorageGRID system's ability to send email notifications for legacy alarms and event-triggered AutoSupport messages.

### What you'll need

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

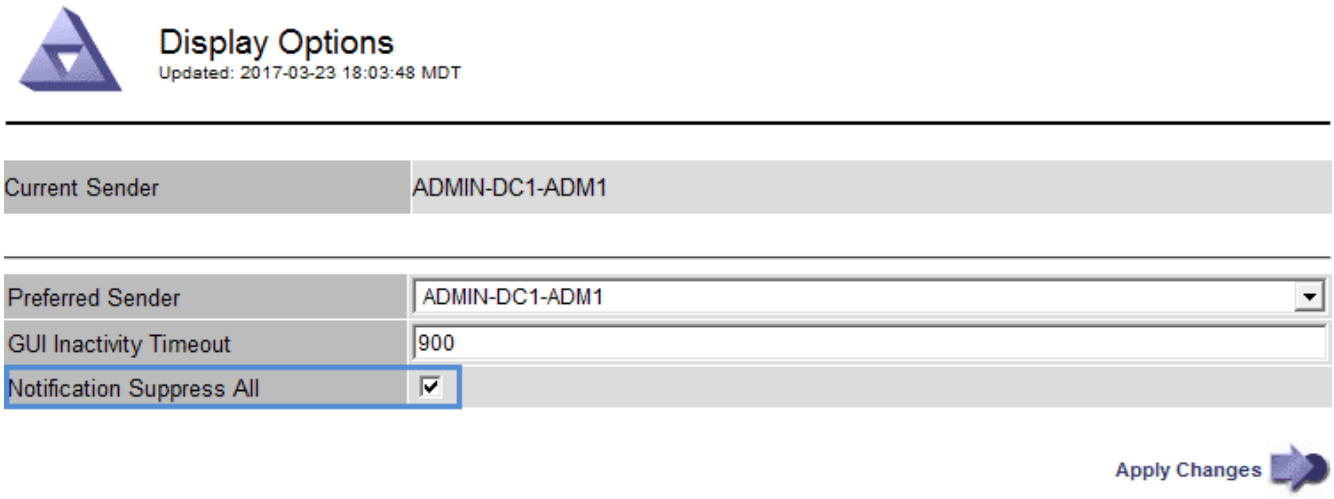
### About this task

Use this option to suppress email notifications for legacy alarms and event-triggered AutoSupport messages.

> This option does not suppress alert email notifications. It also does not suppress weekly or user-triggered AutoSupport messages.

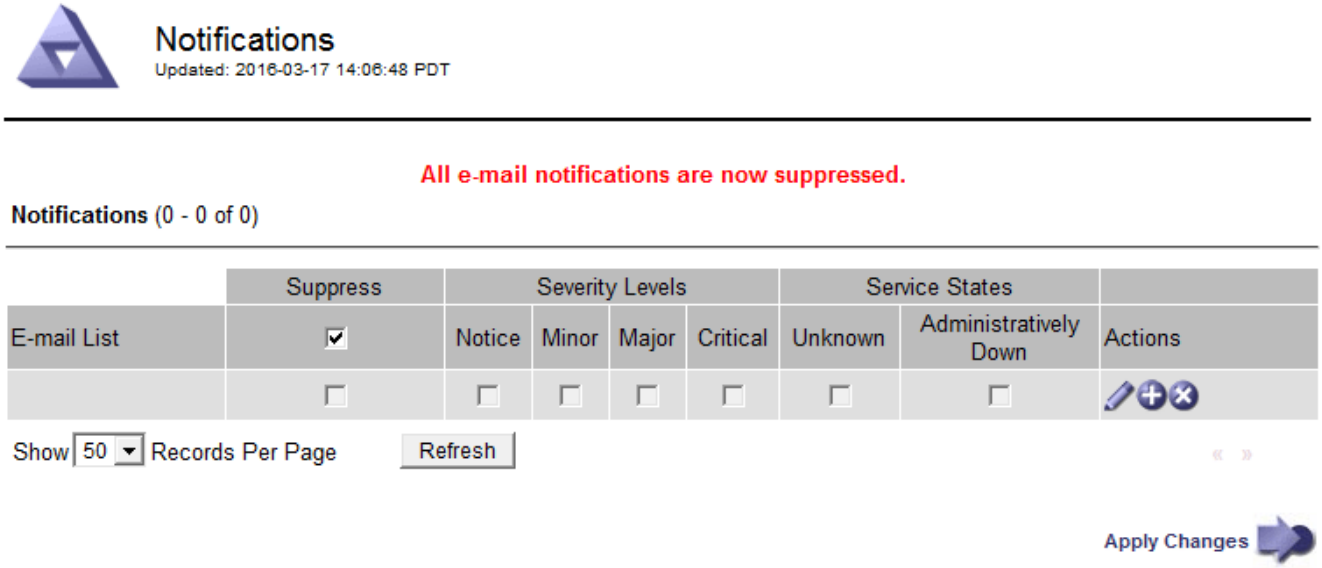
### Steps

1. Select **CONFIGURATION** > **System settings** > **Display options**.
2. From the Display Options menu, select **Options**.
3. Select **Notification Suppress All**.




4. Click **Apply Changes**.

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




## Configure audit messages and log destinations

Audit messages and logs record system activities and security events, and are essential tools for monitoring and troubleshooting. You can adjust audit levels to increase or decrease the type and number of audit messages recorded. Optionally, you can define any HTTP request headers you want to include in client read and write audit messages. You can also configure an external syslog server and change the destination of audit information.

For more information on audit messages, see Review audit logs.

### What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have Maintenance or Root access permissions.

### About this task

All StorageGRID nodes generate audit messages and logs to track system activity and events. By default, audit information is sent to the audit log on Admin Nodes. You can adjust audit levels to increase or decrease the type and number of audit messages recorded in the audit log. Optionally, you can configure audit information to be sent to a remote syslog server or to be stored temporarily on the originating nodes for manual collection.

### Change audit message levels in the audit log

You can set a different audit level for each of the following categories of messages in the audit log:

| Audit category | Description |
|---|---|
| System | By default, this level is set to Normal. See System audit messages. |
| Storage | By default, this level is set to Error. See Object storage audit messages. |

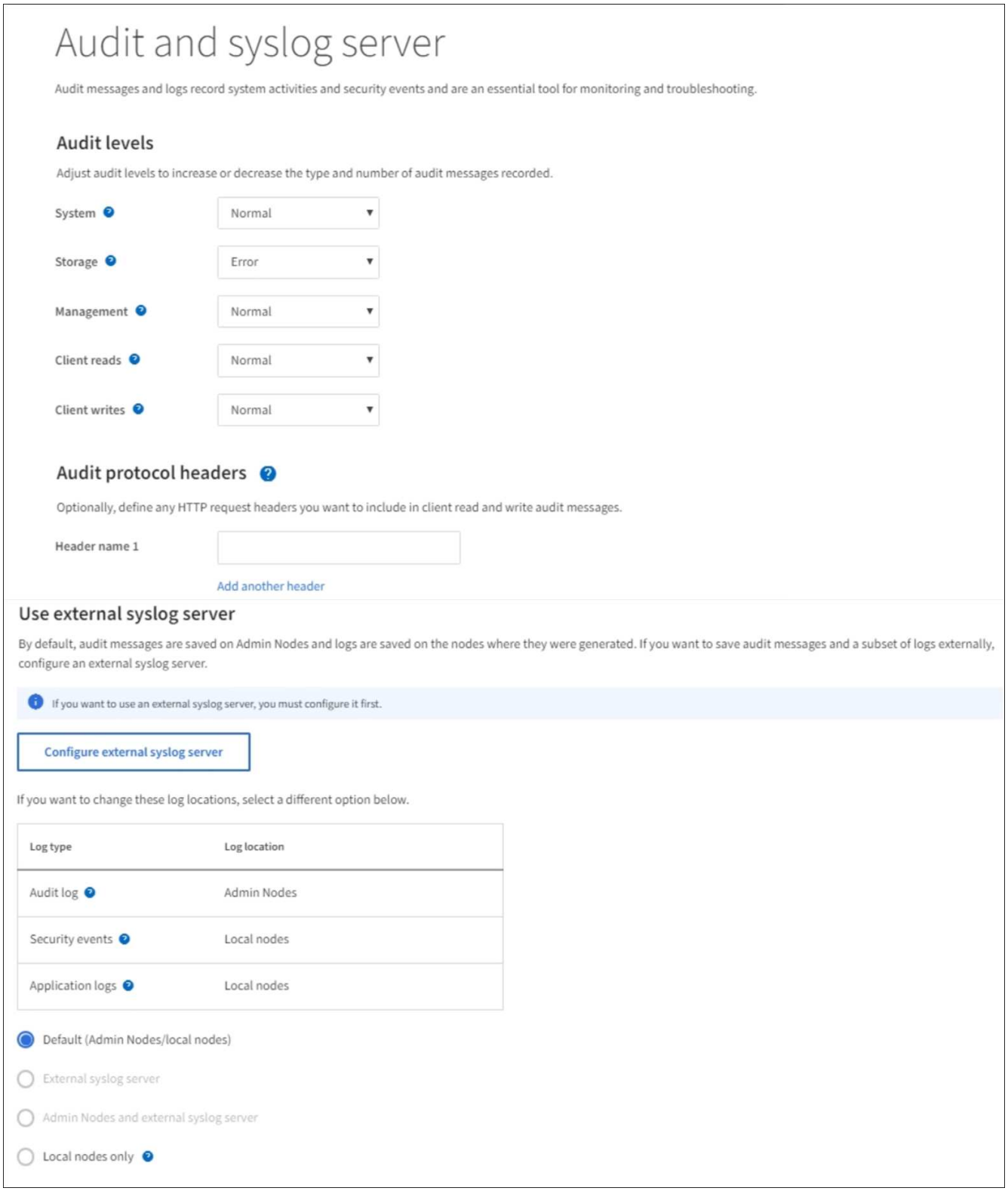
| Audit category | Description |
| --- | --- |
| Management | By default, this level is set to Normal. See Management audit message. |
| Client Reads | By default, this level is set to Normal. See Client read audit messages. |
| Client Writes | By default, this level is set to Normal. See Client write audit messages. |

These defaults apply if you initially installed StorageGRID using version 10.3 or later. If you have upgraded from an earlier version of StorageGRID, the default for all categories is set to Normal.

During upgrades, audit level configurations will not be effective immediately.

**Steps**

1. Select **CONFIGURATION** > **Monitoring** > **Audit and syslog server**.




2. For each category of audit message, select an audit level from the drop-down list:

| Audit level | Description |
|---|---|
| Off | No audit messages from the category are logged. |

| Audit level | Description |
| --- | --- |
| Error | Only error messages are logged—audit messages for which the result code was not "successful" (SUCS). |
| Normal | Standard transactional messages are logged—the messages listed in these instructions for the category. |
| Debug | Deprecated. This level behaves the same as the Normal audit level. |

The messages included for any particular level include those that would be logged at the higher levels. For example, the Normal level includes all of the Error messages.

3. Optionally, under **Audit protocol headers**, define any HTTP request headers you want to include in client read and write audit messages. Use an asterisk (*) as a wildcard to match zero or more characters. Use the escape sequence (*) to match a literal asterisk.

   Audit protocol headers apply to S3 and Swift requests only.

4. Select **Add another header** to create additional headers, if needed.

   When HTTP headers are found in a request, they are included in the audit message under the field HTRH.

   Audit protocol request headers are logged only if the audit level for **Client Reads** or **Client Writes** is not **Off**.

5. Select **Save**

   A green banner displays indicating your configuration has been saved successfully.

### Use an external syslog server

You can configure an external syslog server if you want to save audit information remotely.

- If you want to save audit information to an external syslog server, go to Configure an external syslog server.
- If you are not using an external syslog server, go to Select audit information destinations.

### Select audit information destinations

You can specify where audit logs, security event logs, and application logs are sent.

Some destination are available only if you are using an external syslog server. See Configure an external syslog server to configure an external syslog server.

For more information on StorageGRID software logs, see StorageGRID software logs.

1. On the Audit and syslog server page, select the destination for audit information from the listed options:

| Option | Description |
| --- | --- |
| Default (Admin nodes/local nodes) | Audit messages are sent to the audit log (`audit.log`) on the Admin Node, and security event logs and application logs are stored on the nodes where they were generated (also referred to as "the local node"). |
| External syslog server | Audit information is sent to an external syslog server and saved on the local node. The type of information sent depends upon how you configured the external syslog server. This option is enabled only after you have configured an external syslog server. |
| Admin Node and external syslog server | Audit messages are sent to the audit log (`audit.log`) on the Admin Node, and audit information is sent to the external syslog server and saved on the local node. The type of information sent depends upon how you configured the external syslog server. This option is enabled only after you have configured an external syslog server. |
| Local nodes only | No audit information is sent to an Admin Node or remote syslog server. Audit information is saved only on the nodes that generated it.<br><br>**Note**: StorageGRID periodically removes these local logs in a rotation to free up space. When the log file for a node reaches 1 GB, the existing file is saved, and a new log file is started. The rotation limit for the log is 21 files. When the 22nd version of the log file is created, the oldest log file is deleted. On average about 20 GB of log data is stored on each node. |

Audit information generated on every local node is stored in `/var/local/log/localaudit.log`

2. Select **Save**.

A warning message appears:

Change the log destination?

3. Confirm that you want to change the destination for audit information by selecting **OK**.

   A green banner appears notifying you that your audit configuration has been saved successfully.

   New logs are sent to the destinations you selected. Existing logs remain in their current location.

**Related information**

Considerations for external syslog server

Administer StorageGRID

Troubleshoot the external syslog server

## Use an external syslog server

### Considerations for external syslog server

Use the following guidelines to estimate the size of the external syslog server you need.

#### What is an external syslog server?

An external syslog server is a server outside of StorageGRID you can use to collect system audit information in a single location. Using an external syslog server enables you to configure the destinations of your audit information so you can reduce network traffic on your Admin Nodes and manage the information more efficiently. The types of audit information you can send to the external syslog server include:

- Audit logs containing the audit messages generated during normal system operation
- Security-related events such as logins and escalations to root
- Application logs that might be requested if it is necessary to open a support case to troubleshoot an issue you have encountered

#### How to estimate the size of the external syslog server

Normally, your grid is sized to achieve a required throughput, defined in terms of S3 operations per second or bytes per second. For example, you might have a requirement that your grid handle 1,000 S3 operations per second, or 2,000 MB per second, of object ingests and retrievals. You should size your external syslog server according to your grid's data requirements.

This section provides some heuristic formulas that help you estimate the rate and average size of log messages of various types that your external syslog server needs to be capable of handling, expressed in terms of the known or desired performance characteristics of the grid (S3 operations per second).

### Use S3 operations per second in estimation formulas

If your grid was sized for a throughput expressed in bytes per second, you must convert this sizing into S3 operations per second to use the estimation formulas. To convert grid throughput, you must first determine your average object size, which you can do using the information in existing audit logs and metrics (if any), or by using your knowledge of the applications that will use StorageGRID. For example, if your grid was sized to achieve a throughput of 2,000 MB/second, and your average object size is 2 MB, then your grid was sized to be able to handle 1,000 S3 operations per second (2,000 MB / 2 MB).

> The formulas for external syslog server sizing in the following sections provide common-case estimates (rather than worst-case estimates). Depending on your configuration and workload, you might see a higher or lower rate of syslog messages or volume of syslog data than the formulas predict. The formulas are meant to be used as guidelines only.

### Estimation formulas for audit logs

If you have no information about your S3 workload other than number of S3 operations per second your grid is expected to support, you can estimate the volume of audit logs your external syslog server will need to handle using the following formulas, under the assumption that you leave the Audit Levels set to the default values (all categories set to Normal, except Storage, which is set to Error):

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

For example, if your grid is sized for 1,000 S3 operations per second, your external syslog server should be sized to support 2,000 syslog messages per second and should be able to receive (and typically store) audit log data at a rate of 1.6 MB per second.

If you know more about your workload, more accurate estimations are possible. For audit logs, the most important additional variables are the percentage of S3 operations that are PUTs (vs. GETS), and the average size, in bytes, of the following S3 fields (4-character abbreviations used in the table are audit log field names):

| Code | Field | Description |
|---|---|---|
| SACC | S3 tenant account name (request sender) | The name of the tenant account for the user who sent the request. Empty for anonymous requests. |
| SBAC | S3 tenant account name (bucket owner) | The tenant account name for the bucket owner. Used to identify cross-account or anonymous access. |
| S3BK | S3 Bucket | The S3 bucket name. |
| S3KY | S3 Key | The S3 key name, not including the bucket name. Operations on buckets do not include this field. |

Let's use P to represent the percentage of S3 operations that are PUTs, where $0 \leq P \leq 1$ (so for a 100% PUT workload, P = 1, and for a 100% GET workload, P = 0).

Let's use K to represent the average size of the sum of the S3 account names, S3 Bucket, and S3 Key. Suppose the S3 account name is always my-s3-account (13 bytes), buckets have fixed-length names like /my/application/bucket-12345 (28 bytes), and objects have fixed-length keys like 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Then the value of K is 90 (13+13+28+36).

If you can determine values for P and K, you can estimate the volume of audit logs your external syslog server will need to handle using the following formulas, under the assumption that you leave the Audit Levels set to the defaults (all categories set to Normal, except Storage, which is set to Error):

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

For example, if your grid is sized for 1,000 S3 operations per second, your workload is 50% PUTs, and your S3 account names, bucket names, and object names average 90 bytes, your external syslog server should be sized to support 1,500 syslog messages per second and should be able to receive (and typically store) audit log data at a rate of approximately 1 MB per second.

### Estimation formulas for non-default audit levels

The formulas provided for audit logs assume the use of default audit level settings (all categories set to Normal, except Storage, which is set to Error). Detailed formulas for estimating the rate and average size of audit messages for non-default audit level settings are not available. However, the following table can be used to make a rough estimate of the rate; you can use the average size formula provided for audit logs, but be aware that it is likely to result in an over-estimate because the “extra” audit messages are, on average, smaller than the default audit messages.

| Condition | Formula |
|---|---|
| Replication: Audit levels all set to Debug or Normal | Audit log rate = 8 x S3 operations Rate |
| Erasure coding: audit levels all set to Debug or Normal | Use same formula as for default settings |

### Estimation formulas for security events

Security events are not correlated with S3 operations and typically produce a negligible volume of logs and data. For these reasons, no estimation formulas are provided.

### Estimation formulas for application logs

If you have no information about your S3 workload other than the number of S3 operations per second your grid is expected to support, you can estimate the volume of applications logs your external syslog server will need to handle using the following formulas:

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

So, for example, if your grid is sized for 1,000 S3 operations per second, your external syslog server should be sized to support 3,300 application logs per second and be able to receive (and store) application log data at a rate of about 1.2 MB per second.

If you know more about your workload, more accurate estimations are possible. For application logs, the most important additional variables are the data protection strategy (replication vs. erasure coding), the percentage of S3 operations that are PUTs (vs. GETs/other), and the average size, in bytes, of the following S3 fields (4-character abbreviations used in table are audit log field names):

| Code | Field | Description |
|---|---|---|
| SACC | S3 tenant account name (request sender) | The name of the tenant account for the user who sent the request. Empty for anonymous requests. |
| SBAC | S3 tenant account name (bucket owner) | The tenant account name for the bucket owner. Used to identify cross-account or anonymous access. |

| Code | Field | Description |
|---|---|---|
| S3BK | S3 Bucket | The S3 bucket name. |
| S3KY | S3 Key | The S3 key name, not including the bucket name. Operations on buckets do not include this field. |

#### Example sizing estimations

This section explains example cases of how to use the estimation formulas for grids with the following methods of data protection:

- Replication
- Erasure Coding

### If you use replication for data protection

Let P represent the percentage of S3 operations that are PUTs, where 0 ≤ P ≤ 1 (so for a 100% PUT workload, P = 1, and for a 100% GET workload, P = 0).

Let K represent the average size of the sum of the S3 account names, S3 Bucket, and S3 Key. Suppose the S3 account name is always my-s3-account (13 bytes), buckets have fixed-length names like /my/application/bucket-12345 (28 bytes), and objects have fixed-length keys like 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Then K has a value of 90 (13+13+28+36).

If you can determine values for P and K, you can estimate the volume of application logs your external syslog server will have to be able to handle using the following formulas.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

So, for example, if your grid is sized for 1,000 S3 operations per second, your workload is 50% PUTs, and your S3 account names, bucket names, and object names average 90 bytes, your external syslog server should be sized to support 1800 application logs per second, and will be receiving (and typically storing) application data at a rate of 0.5 MB per second.

### If you use erasure coding for data protection

Let P represent the percentage of S3 operations that are PUTs, where 0 ≤ P ≤ 1 (so for a 100% PUT workload, P = 1, and for a 100% GET workload, P = 0).

Let K represent the average size of the sum of the S3 account names, S3 Bucket, and S3 Key. Suppose the S3 account name is always my-s3-account (13 bytes), buckets have fixed-length names like /my/application/bucket-12345 (28 bytes), and objects have fixed-length keys like 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Then K has a value of 90 (13+13+28+36).

If you can determine values for P and K, you can estimate the volume of application logs your external syslog server will have to be able to handle using the following formulas.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

So, for example, if your grid is sized for 1,000 S3 operations per second, your workload is 50% PUTs, and your S3 account names, bucket names, and object names average 90 bytes, your external syslog server should be sized to support 2,250 application logs per second and should be able to receive and will be receive (and typically store) application data at a rate of 0.6 MB per second.

For more information on configuring audit message levels and an external syslog server, see the following:

- Configure an external syslog server
- Configure audit messages and log destinations

### Configure an external syslog server

If you want to save audit logs, application logs, and security event logs to a location outside of your grid, use this procedure to configure an external syslog server.

#### What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have Maintenance or Root access permissions.
- You have a syslog server with the capacity to receive and store the log files. For more information, see Considerations for external syslog server.
- You have the correct server and client certifications if you plan to use TLS or RELP/TLS.

#### About this task

If you want to send audit information to an external syslog server, you must configure the external server first.

Sending audit information to an external syslog server enables you to:

- Collect and manage audit information such as audit messages, application logs, and security events more efficiently
- Reduce network traffic on your Admin Nodes because audit information is transferred directly from the various Storage Nodes to the external syslog server, without having to go through an Admin Node

> When logs are sent to an external syslog server, single logs greater than 8192 bytes are truncated at the end of the message to conform with common limitations in external syslog server implementations.

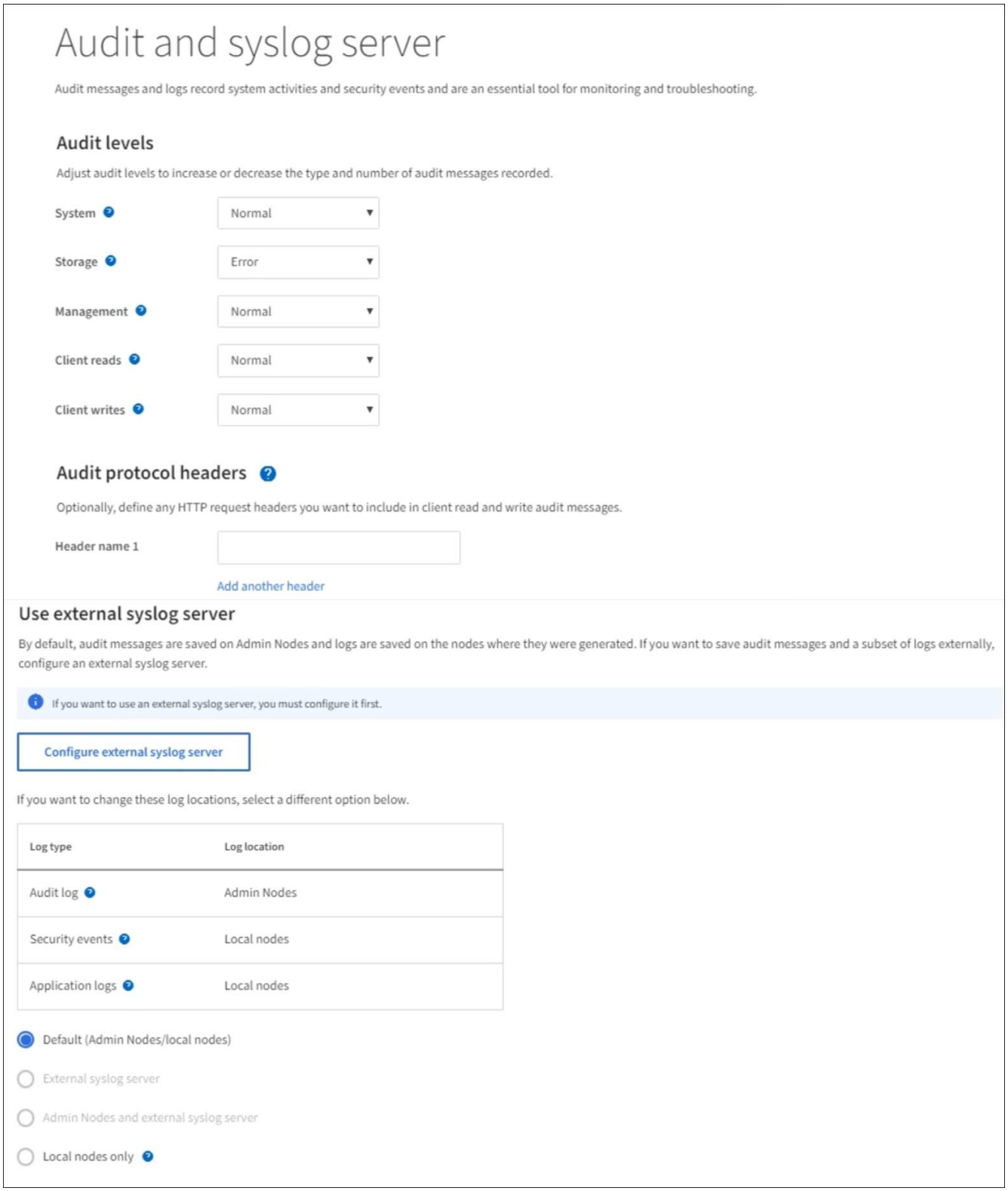
> To maximize the options for full data recovery in the event of a failure of the external syslog server, up to 20GB of local logs of audit records (localaudit.log) are maintained on each node.

If the configuration options available in this procedure are not flexible enough to meet your requirements, additional configuration options can be applied using the private API `audit-destinations` endpoints. For example, it is possible to use different syslog servers for different groups of nodes.

#### Access the syslog server configuration wizard

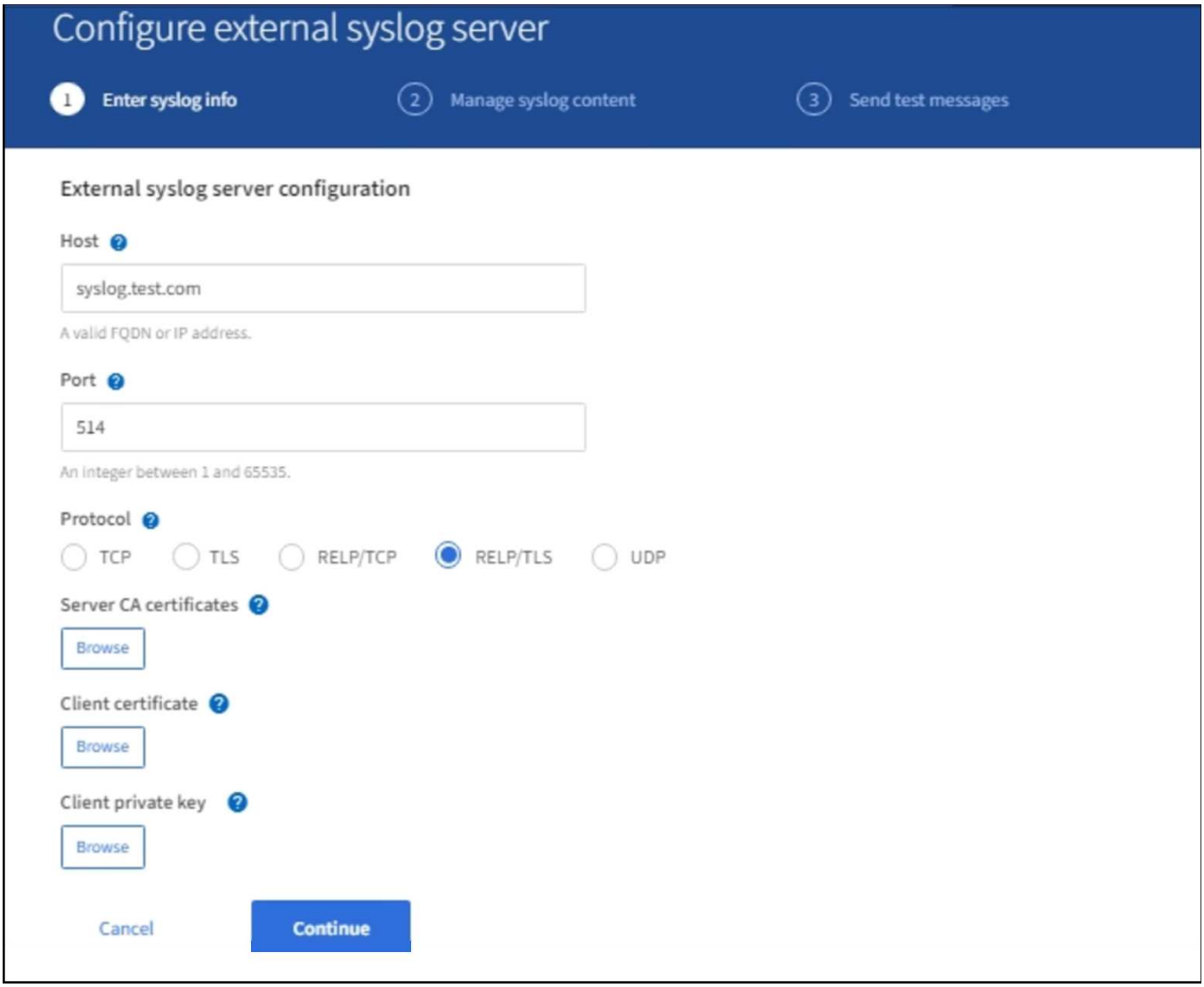
**Steps**

1. Select **CONFIGURATION** > **Monitoring** > **Audit and syslog server**.




2. From the Audit and syslog server page, select **Configure external syslog server**. If you have previously configured an external syslog server, select **Edit external syslog server**.

### Enter syslog info




1. Enter a valid fully qualified domain name or an IPv4 or IPv6 address for the external syslog server in the **Host** field.
2. Enter the destination port on the external syslog server (must be an integer between 1 and 65535). The default port is 514.
3. Select the protocol used to send audit information to the external syslog server.

   TLS or RELP/TLS is recommended. You must upload a server certificate to use either of these options.

   Using certificates helps secure the connections between your grid and the external syslog server. For more information, see Use StorageGRID security certificates.

   All protocol options require support by, and configuration of, the external syslog server. You must choose an option that is compatible with the external syslog server.

   > Reliable Event Logging Protocol (RELP) extends the functionality of the syslog protocol to provide reliable delivery of event messages. Using RELP can help prevent the loss of audit information if your external syslog server has to restart.

4. Select **Continue**.

5. If you selected **TLS** or **RELP/TLS**, upload the following certificates:

   - **Server CA certificates**: One or more trusted CA certificates for verifying the external syslog server (in PEM encoding). If omitted, the default Grid CA certificate will be used. The file you upload here might be a CA bundle.
   - **Client certificate**: The client certificate for authentication to the external syslog server (in PEM encoding).
   - **Client private key**: Private key for the client certificate (in PEM encoding).

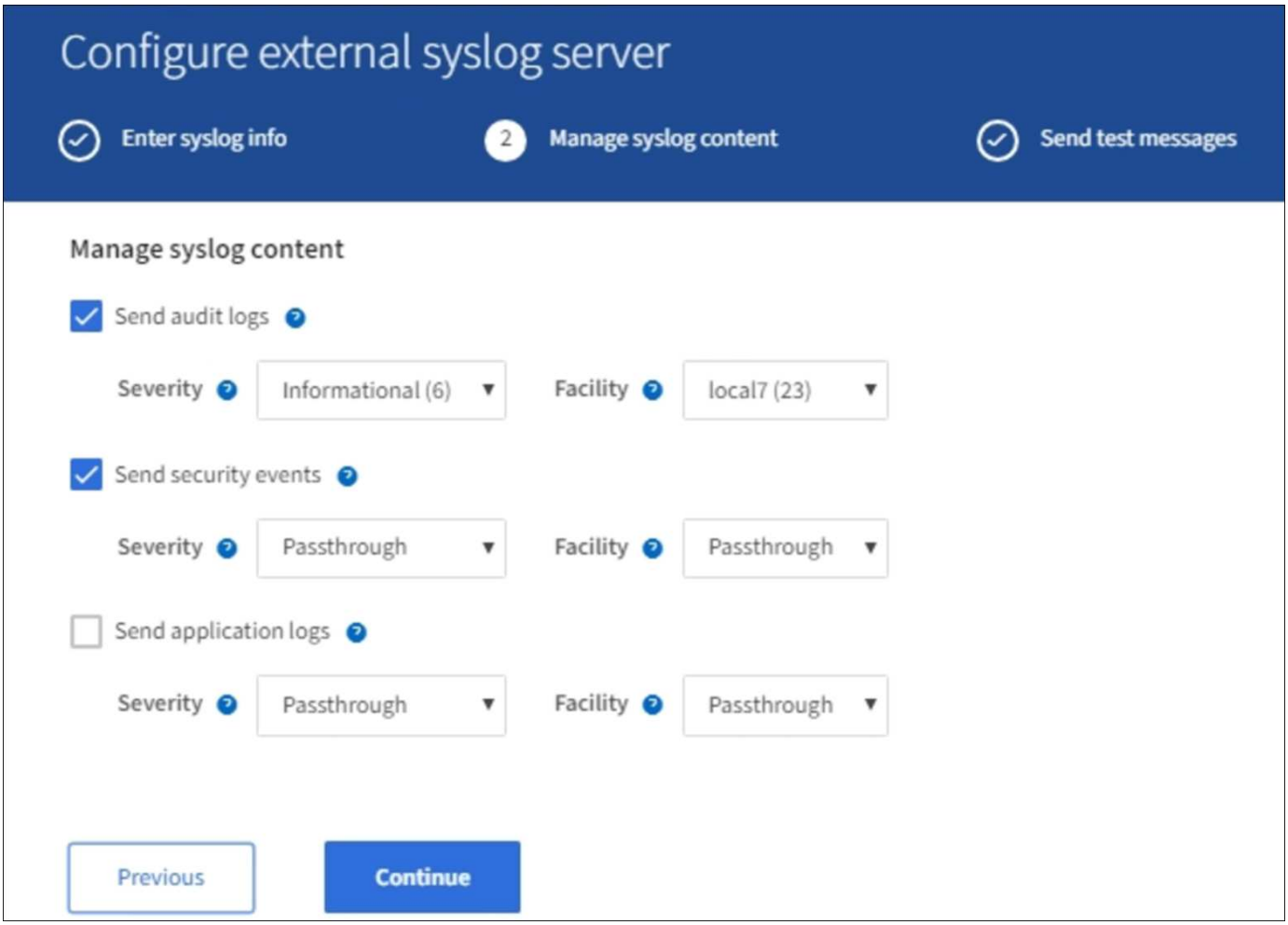
     > If you use a client certificate you must also use a client private key. If you provide an encrypted private key, you must also provide the passphrase. There is no significant security benefit from using an encrypted private key because the key and passphrase must be stored; using an unencrypted private key, if available, is recommended for simplicity.

     a. Select **Browse** for the certificate or key you want to use.
     b. Select the certificate file or key file.
     c. Select **Open** to upload the file.

   A green check appears next to the certificate or key file name, notifying you that it has been uploaded successfully.

6. Select **Continue**.

**Manage syslog content**




1. Select each type of audit information you want to send to the external syslog server.
   - **Send audit logs**: StorageGRID events and system activities
   - **Send security events**: Security events such as when an unauthorized user attempts to sign in or a user signs in as root
   - **Send application logs**: Log files useful for troubleshooting including:
     - bycast-err.log
     - bycast.log
     - jaeger.log
     - nms.log (Admin Nodes only)
     - prometheus.log
     - raft.log
     - hagroups.log
2. Use the drop-down menus to select the severity and facility (type of message) for the category of audit information you want to send.

   If you select **Passthrough** for severity and facility, the information sent to the remote syslog server will receive the same severity and facility as it did when logged locally onto the node. Setting facility and severity can help you aggregate the logs in customizable ways for easier analysis.

For more information on StorageGRID software logs, see StorageGRID software logs.

a. For **Severity**, select **Passthrough** if you want each message sent to the external syslog to have the same severity value as it does in the local syslog.

   For audit logs, if you select **Passthrough** the severity is 'info.'

   For security events, if you select **Passthrough**, the severity values are generated by the linux distribution on the nodes.

   For application logs, if you select **Passthrough**, the severities vary between 'info' and 'notice,' depending on what the issue is. For example, adding an NTP server and configuring an HA group gives a value of 'info,' while intentionally stopping the ssm or rsm service gives a value of 'notice.'

b. If you do not want to use the passthrough value, select a severity value between 0 and 7.

   The selected value will be applied to all messages of this type. Information about different severities will be lost when you choose to override severity with a fixed value.

| Severity | Description |
|---|---|
| 0 | Emergency: System is unusable |
| 1 | Alert: Action must be taken immediately |
| 2 | Critical: Critical conditions |
| 3 | Error: Error conditions |
| 4 | Warning: Warning conditions |
| 5 | Notice: Normal but significant condition |
| 6 | Informational: Informational messages |
| 7 | Debug: Debug-level messages |

c. For **Facility**, select **Passthrough** if you want each message sent to the external syslog to have the same facility value as it does in the local syslog.

   For audit logs, if you select **Passthrough** the facility sent to the external syslog server is 'local7.'

   For security events, if you select **Passthrough**, the facility values are generated by the linux distribution on the nodes.

   For application logs, if you select **Passthrough**, the application logs sent to the external syslog server have the following facility values:

| Application log | Passthrough value |
| --- | --- |
| bycast.log | user or daemon |
| bycast-err.log | user, daemon, local3, or local4 |
| jaeger.log | local2 |
| nms.log | local3 |
| prometheus.log | local4 |
| raft.log | local5 |
| hagroups.log | local6 |

d. If you do not want to use the passthrough value, select the facility value between 0 and 23.

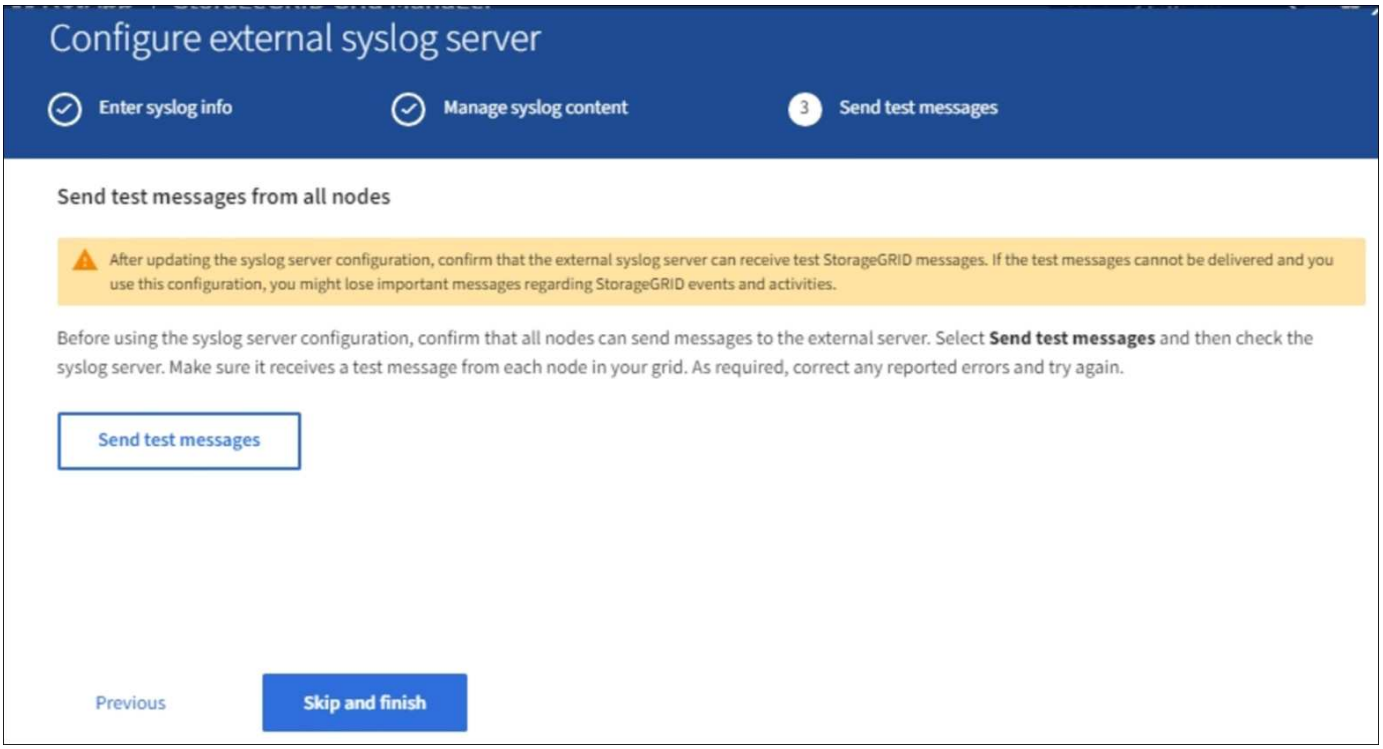
   The selected value will be applied to all messages of this type. Information about different facilities will be lost when you choose to override facility with a fixed value.

| Facility | Description |
| --- | --- |
| 0 | kern (kernel messages) |
| 1 | user (user-level messages) |
| 2 | mail |
| 3 | daemon (system daemons) |
| 4 | auth (security/authorization messages) |
| 5 | syslog (messages generated internally by syslogd) |
| 6 | lpr (line printer subsystem) |
| 7 | news (network news subsystem) |
| 8 | UUCP |
| 9 | cron (clock daemon) |
| 10 | security (security/authorization messages) |
| 11 | FTP |

| Facility | Description |
| --- | --- |
| 12 | NTP |
| 13 | logaudit (log audit) |
| 14 | logalert (log alert) |
| 15 | clock (clock daemon) |
| 16 | local0 |
| 17 | local1 |
| 18 | local2 |
| 19 | local3 |
| 20 | local4 |
| 21 | local5 |
| 22 | local6 |
| 23 | local7 |

3. Select **Continue**.

**Send test messages**




Before starting to use an external syslog server, you should request that all nodes in your grid send test messages to the external syslog server. You should use these test messages to help you validate your entire log collection infrastructure before you commit to sending data to the external syslog server.

> Do not use the external syslog server configuration until you confirm that the external syslog server received a test message from each node in your grid and that the message was processed as expected.

1. If you do not want to send test messages and you are certain your external syslog server is configured properly and can receive audit information from all the nodes in your grid, select **Skip and finish**.

   A green banner appears indicating your configuration has been saved successfully.

2. Otherwise, select **Send test messages**.

   Test results continuously appear on the page until you stop the test. While the test is in progress, your audit messages continue to be sent to your previously configured destinations.

3. If you receive any errors, correct them and select **Send test messages** again. See Troubleshooting the external syslog server to help you resolve any errors.

3. Wait until you see a green banner indicating all nodes have passed testing.
4. Check your syslog server to determine if test messages are being received and processed as expected.

   > If you are using UDP, check your entire log collection infrastructure. The UDP protocol does not allow for as rigorous error detection as the other protocols.

5. Select **Stop and finish**.

   You are returned to the **Audit and syslog server** page. A green banner appears notifying you that your syslog server configuration has been saved successfully.

Your StorageGRID audit information is not sent to the external syslog server until you select a destination that includes the external syslog server.

#### Select audit information destinations

You can specify where security event logs, application logs, and audit message logs are sent.

For more information on StorageGRID software logs, see StorageGRID software logs.

1. On the Audit and syslog server page, select the destination for audit information from the listed options:

| Option | Description |
|---|---|
| Default (Admin nodes/local nodes) | Audit messages are sent to the audit log (`audit.log`) on the Admin Node, and security event logs and application logs are stored on the nodes where they were generated (also referred to as "the local node"). |
| External syslog server | Audit information is sent to an external syslog server and saved on the local node. The type of information sent depends upon how you configured the external syslog server. This option is enabled only after you have configured an external syslog server. |
| Admin Node and external syslog server | Audit messages are sent to the audit log (`audit.log`) on the Admin Node, and audit information is sent to the external syslog server and saved on the local node. The type of information sent depends upon how you configured the external syslog server. This option is enabled only after you have configured an external syslog server. |
| Local nodes only | No audit information is sent to an Admin Node or remote syslog server. Audit information is saved only on the nodes that generated it.<br><br>**Note**: StorageGRID periodically removes these local logs in a rotation to free up space. When the log file for a node reaches 1 GB, the existing file is saved, and a new log file is started. The rotation limit for the log is 21 files. When the 22nd version of the log file is created, the oldest log file is deleted. On average about 20 GB of log data is stored on each node. |

Audit information generated on every local node is stored in `/var/local/log/localaudit.log`

2. Select **Save**. Then, select OK to accept the change to the log destination.
3. If you selected either **External syslog server** or **Admin Nodes and external syslog server** as the destination for audit information, an additional warning appears. Review the warning text.

You must confirm that the external syslog server can receive test StorageGRID messages.

4. Confirm that you want to change the destination for audit information by selecting **OK**.

   A green banner appears notifying you that your audit configuration has been saved successfully.

   New logs are sent to the destinations you selected. Existing logs remain in their current location.

**Related information**

Audit message overview

Configure audit messages and log destinations

System audit messages

Object storage audit messages

Management audit message

Client read audit messages

Administer StorageGRID

## Use SNMP monitoring

If you want to monitor StorageGRID using the Simple Network Management Protocol (SNMP), you must configure the SNMP agent that is included with StorageGRID.

- Configure the SNMP agent
- Update the SNMP agent

**Capabilities**

Each StorageGRID node runs an SNMP agent, or daemon, that provides a management information base (MIB). The StorageGRID MIB contains table and notification definitions for alerts and alarms. The MIB also contains system description information such as platform and model number for each node. Each StorageGRID node also supports a subset of MIB-II objects.

Initially, SNMP is disabled on all nodes. When you configure the SNMP agent, all StorageGRID nodes receive the same configuration.

The StorageGRID SNMP agent supports all three versions of the SNMP protocol. It provides read-only MIB access for queries, and it can send two types of event-driven notifications to a management system:

- **Traps** are notifications sent by the SNMP agent that do not require acknowledgment by the management system. Traps serve to notify the management system that something has happened within StorageGRID, such as an alert being triggered.

  Traps are supported in all three versions of SNMP.

- **Informs** are similar to traps, but they require acknowledgment by the management system. If the SNMP agent does not receive an acknowledgment within a certain amount of time, it resends the inform until an acknowledgment is received or the maximum retry value has been reached.

  Informs are supported in SNMPv2c and SNMPv3.

Trap and inform notifications are sent in the following cases:

- A default or custom alert is triggered at any severity level. To suppress SNMP notifications for an alert, you must configure a silence for the alert. Alert notifications are sent by whichever Admin Node is configured to be the preferred sender.

  Each alert is mapped to one of three trap types based on the severity level of the alert: activeMinorAlert, activeMajorAlert, and activeCriticalAlert. For descriptions of the alerts that can trigger these traps, see the Alerts reference.

- Certain alarms (legacy system) are triggered at specified severity levels or higher.

  SNMP notifications are not sent for every alarm or every alarm severity.

### SNMP version support

The table provides a high-level summary of what is supported for each SNMP version.

| | SNMPv1 | SNMPv2c | SNMPv3 |
|---|---|---|---|
| Queries | Read-only MIB queries | Read-only MIB queries | Read-only MIB queries |
| Query authentication | Community string | Community string | User-based Security Model (USM) user |
| Notifications | Traps only | Traps and informs | Traps and informs |
| Notification authentication | Default trap community or a custom community string for each trap destination | Default trap community or a custom community string for each trap destination | USM user for each trap destination |

### Limitations

- StorageGRID supports read-only MIB access. Read-write access is not supported.
- All nodes in the grid receive the same configuration.
- SNMPv3: StorageGRID does not support the Transport Support Mode (TSM).
- SNMPv3: The only authentication protocol supported is SHA (HMAC-SHA-96).
- SNMPv3: The only privacy protocol supported is AES.

### Access the MIB

You can access the MIB definition file at the following location on any StorageGRID node:

```
/usr/share/snmp/mibs/NETAPP-STORAGEGRID-MIB.txt
```

#### Related information

- Alerts reference
- Alarms reference (legacy system)

- Alarms that generate SNMP notifications (legacy system)
- Silence alert notifications

### Configure the SNMP agent

You can configure the StorageGRID SNMP agent if you want to use a third-party SNMP management system for read-only MIB access and notifications.

#### What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have the Root Access permission.

#### About this task

The StorageGRID SNMP agent supports all three versions of the SNMP protocol. You can configure the agent for one or more versions.

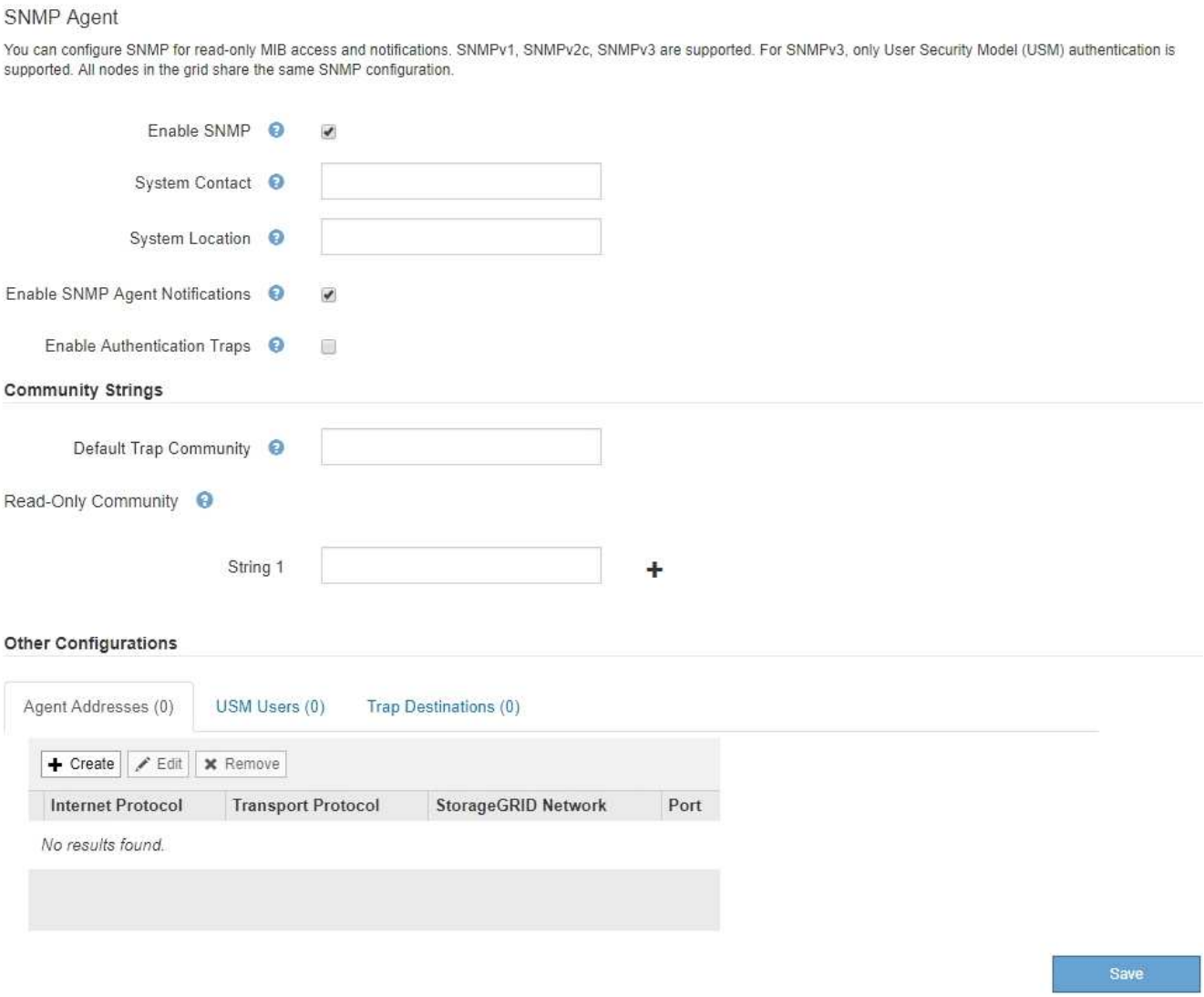
#### Steps

1. Select **CONFIGURATION** > **Monitoring** > **SNMP agent**.

   The SNMP Agent page appears.

2. To enable the SNMP agent on all grid nodes, select the **Enable SNMP** check box.

   The fields for configuring an SNMP agent appear.




3. In the **System Contact** field, enter the value you want StorageGRID to provide in SNMP messages for sysContact.

   The System Contact typically is an email address. The value you provide applies to all nodes in the StorageGRID system. **System Contact** can be a maximum of 255 characters.

4. In the **System Location** field, enter the value you want StorageGRID to provide in SNMP messages for sysLocation.

   The System Location can be any information that is useful for identifying where your StorageGRID system is located. For example, you might use the street address of a facility. The value you provide applies to all nodes in the StorageGRID system. **System Location** can be a maximum of 255 characters.

5. Keep the **Enable SNMP Agent Notifications** check box selected if you want the StorageGRID SNMP agent to send trap and inform notifications.

   If this check box is unselected, the SNMP agent supports read-only MIB access, but it does not send any SNMP notifications.

6. Select the **Enable Authentication Traps** check box if you want the StorageGRID SNMP agent to send an authentication trap if it receives an improperly authenticated protocol message.

7. If you use SNMPv1 or SNMPv2c, complete the Community Strings section.

   The fields in this section are used for community-based authentication in SNMPv1 or SNMPv2c. These fields do not apply to SNMPv3.

   a. In the **Default Trap Community** field, optionally enter the default community string you want to use for trap destinations.

      As required, you can provide a different ("custom") community string when you define a specific trap destination.

      **Default Trap Community** can be a maximum of 32 characters and cannot contain whitespace characters.

   b. For **Read-Only Community**, enter one or more community strings to allow read-only MIB access on IPv4 and IPv6 agent addresses. Click the plus sign + to add multiple strings.

      When the management system queries the StorageGRID MIB, it sends a community string. If the community string matches one of the values specified here, the SNMP agent sends a response to the management system.

      Each community string can be a maximum of 32 characters and cannot contain whitespace characters. Up to five strings are allowed.

      > To ensure the security of your StorageGRID system, do not use "public" as the community string. If you do not enter a community string, the SNMP agent uses the grid ID of your StorageGRID system as the community string.

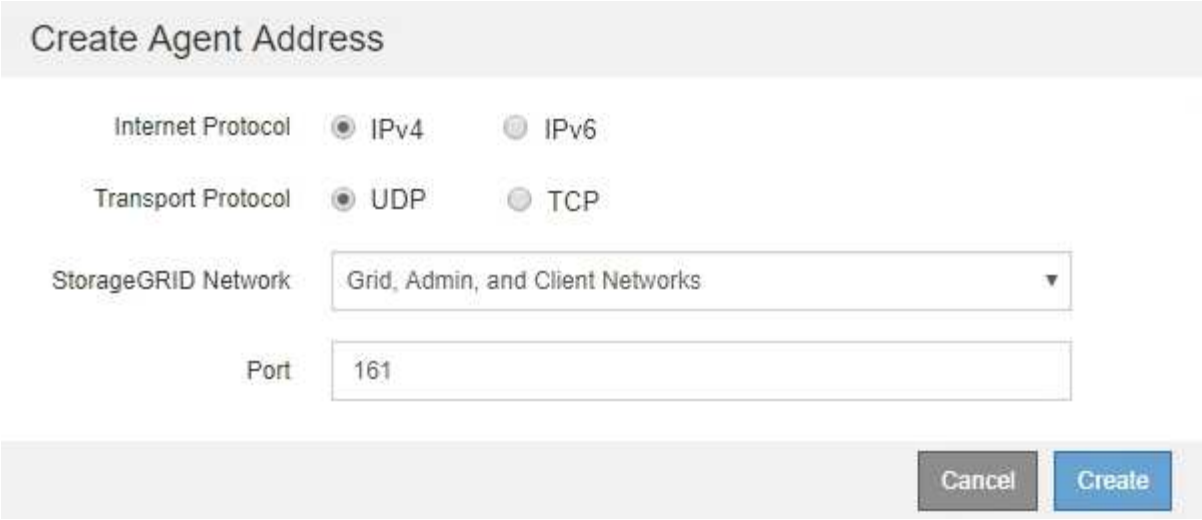
8. Optionally, select the Agent Addresses tab in the Other Configurations section.

   Use this tab to specify one or more "listening addresses." These are the StorageGRID addresses on which the SNMP agent can receive queries. Each agent address includes an internet protocol, a transport protocol, a StorageGRID network, and optionally a port.

   If you do not configure an agent address, the default listening address is UDP port 161 on all StorageGRID networks.

   a. Click **Create**.

      The Create Agent Address dialog box appears.




b. For **Internet Protocol**, select whether this address will use IPv4 or IPv6.

   By default, SNMP uses IPv4.

c. For **Transport Protocol**, select whether this address will use UDP or TCP.

   By default, SNMP uses UDP.

d. In the **StorageGRID Network** field, select which StorageGRID network the query will be received on.

   - Grid, Admin, and Client Networks: StorageGRID should listen for SNMP queries on all three networks.
   - Grid Network
   - Admin Network
   - Client Network

   > To ensure that client communications with StorageGRID remain secure, you should not create an agent address for the Client Network.

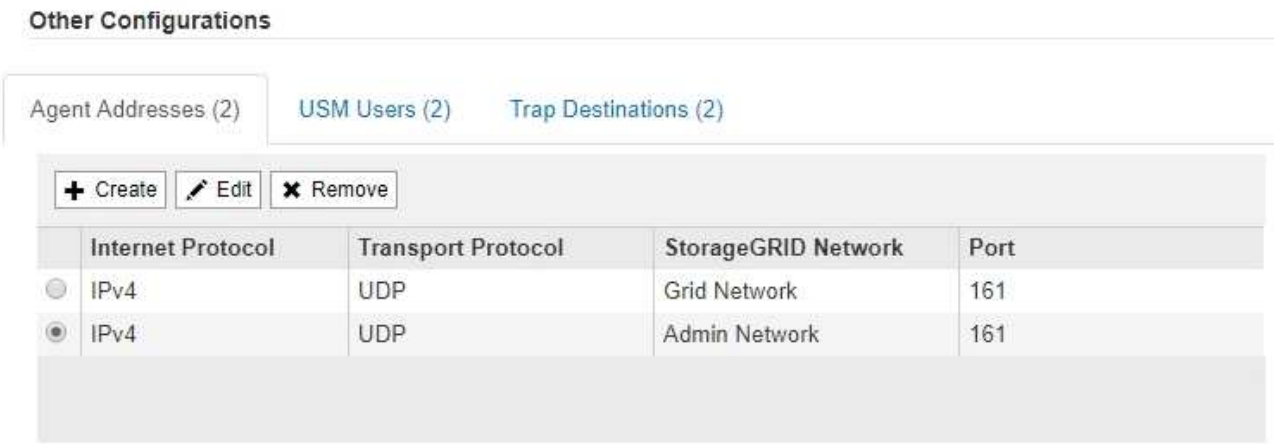
e. In the **Port** field, optionally enter the port number that the SNMP agent should listen on.

   The default UDP port for an SNMP agent is 161, but you can enter any unused port number.

   > When you save the SNMP agent, StorageGRID automatically opens the agent address ports on the internal firewall. You must ensure that any external firewalls allow access to these ports.

f. Click **Create**.

   The agent address is created and added to the table.



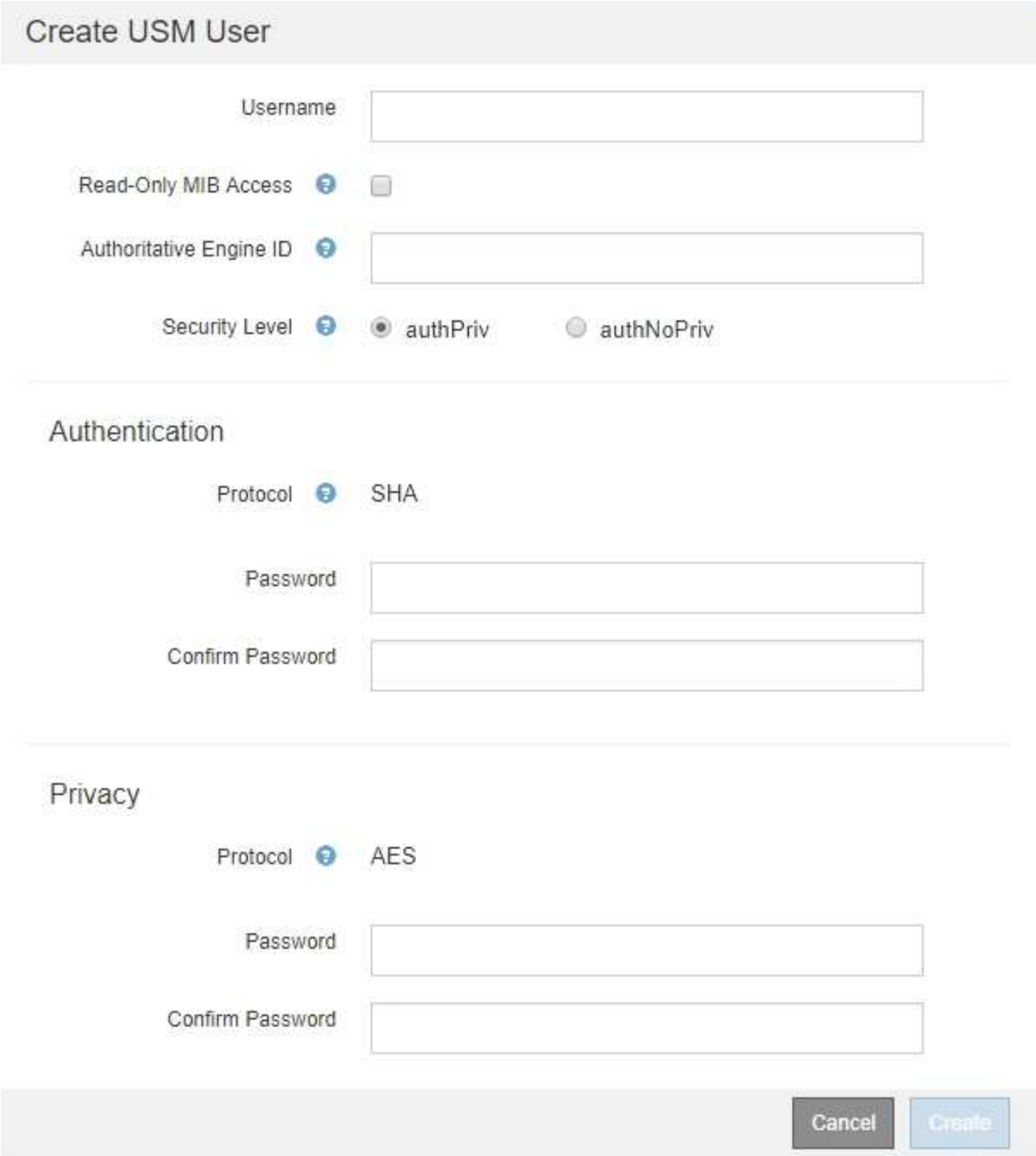

9. If you are using SNMPv3, select the USM Users tab in the Other Configurations section.

   Use this tab to define the USM users who are authorized to query the MIB or to receive traps and informs.

   > This step does not apply if you are only using SNMPv1 or SNMPv2c.

   a. Click **Create**.

      The Create USM User dialog box appears.




b. Enter a unique **Username** for this USM user.

   Usernames have a maximum of 32 characters and cannot contain whitespace characters. The username cannot be changed after the user is created.

c. Select the **Read-Only MIB Access** check box if this user should have read-only access to the MIB.

   If you select **Read-Only MIB Access**, the **Authoritative Engine ID** field is disabled.

   > USM users who have read-only MIB access cannot have engine IDs.

d. If this user will be used in an inform destination, enter the **Authoritative Engine ID** for this user.

> SNMPv3 inform destinations must have users with engine IDs. SNMPv3 trap destination cannot have users with engine IDs.

The authoritative engine ID can be from 5 to 32 bytes in hexadecimal.

e. Select a security level for the USM user.
   - **authPriv**: This user communicates with authentication and privacy (encryption). You must specify an authentication protocol and password and a privacy protocol and password.
   - **authNoPriv**: This user communicates with authentication and without privacy (no encryption). You must specify an authentication protocol and password.

f. Enter and confirm the password this user will use for authentication.

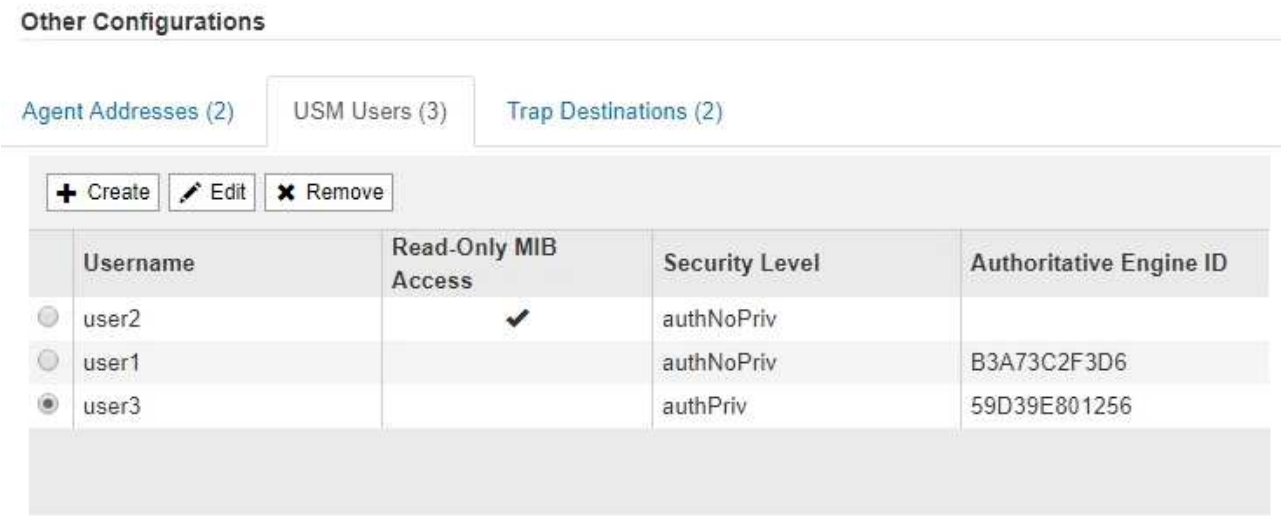
> The only authentication protocol supported is SHA (HMAC-SHA-96).

g. If you selected **authPriv**, enter and confirm the password this user will use for privacy.

> The only privacy protocol supported is AES.

h. Click **Create**.

   The USM user is created and added to the table.

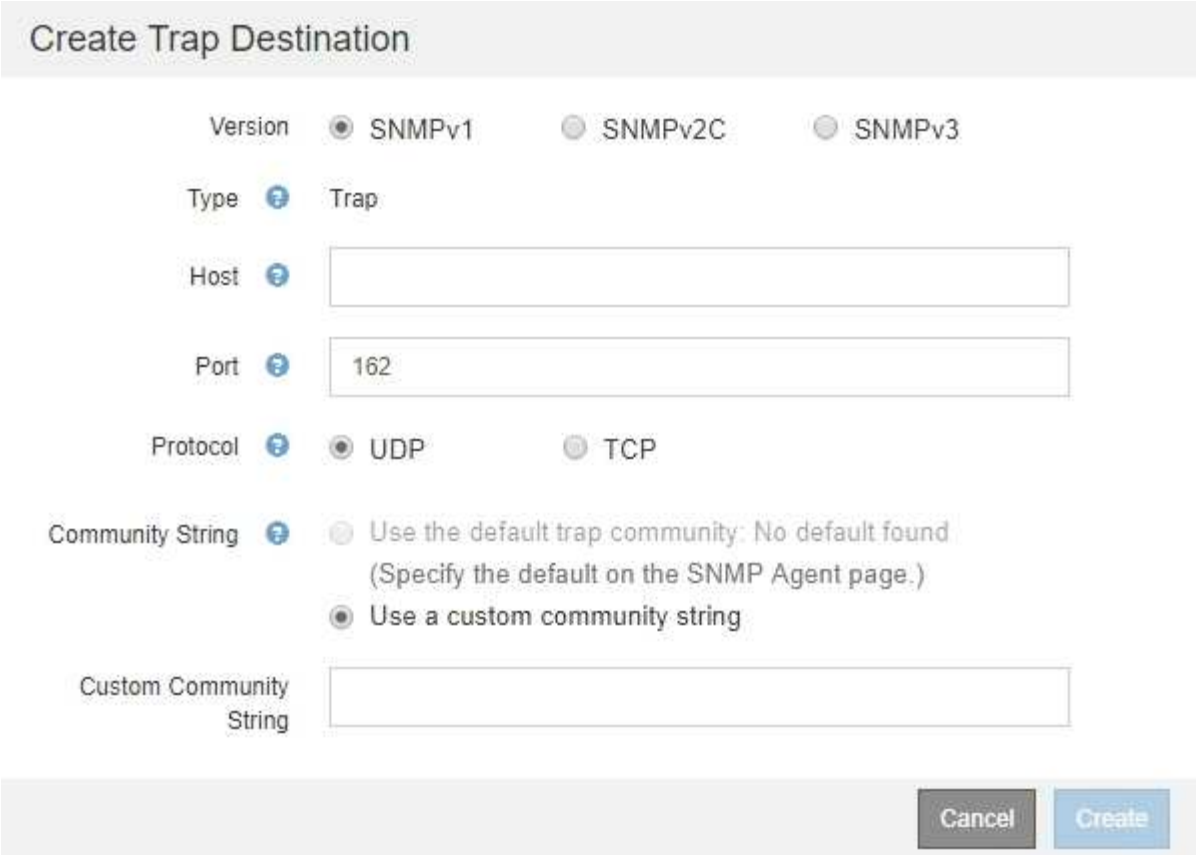



10. In the Other Configurations section, select the Trap Destinations tab.

The Trap Destinations tab allows you to define one or more destinations for StorageGRID trap or inform notifications. When you enable the SNMP agent and click **Save**, StorageGRID starts sending notifications to each defined destination. Notifications are sent when alerts and alarms are triggered. Standard notifications are also sent for the supported MIB-II entities (for example, ifDown and coldStart).

a. Click **Create**.

   The Create Trap Destination dialog box appears.




b. In the **Version** field, select which SNMP version will be used for this notification.

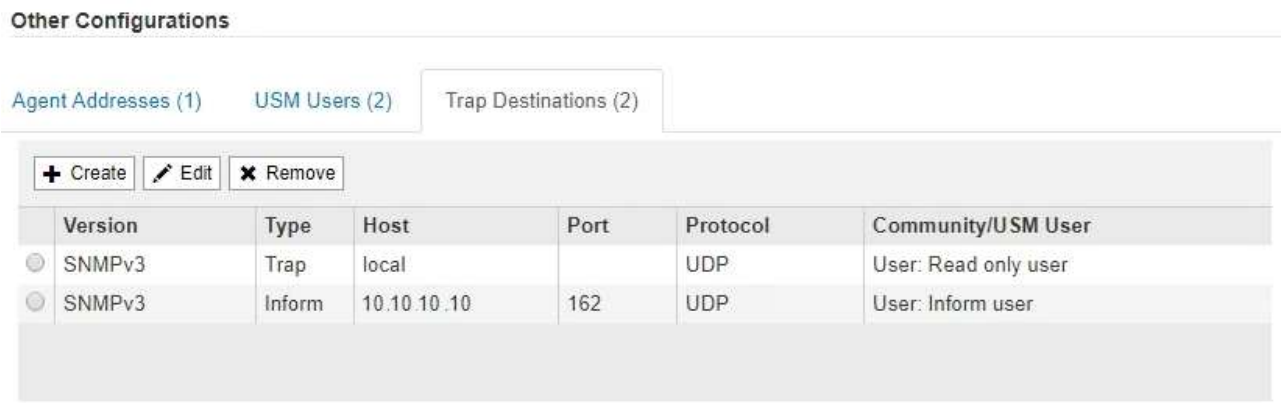
c. Complete the form, based on which version you selected

| Version | Specify this information |
|---|---|
| SNMPv1 | **Note:** For SNMPv1, the SNMP agent can only send traps. Informs are not supported.<br><br>i. In the **Host** field, enter an IPv4 or IPv6 address (or FQDN) to receive the trap.<br>ii. For **Port**, use the default (162), unless you must use another value. (162 is the standard port for SNMP traps.)<br>iii. For **Protocol**, use the default (UDP). TCP is also supported. (UDP is the standard SNMP trap protocol.)<br>iv. Use the default trap community, if one was specified on the SNMP Agent page, or enter a custom community string for this trap destination.<br><br>The custom community string can be a maximum of 32 characters and cannot contain whitespace. |

| Version | Specify this information |
| --- | --- |
| SNMPv2c | i. Select whether the destination will be used for traps or informs.<br>ii. In the **Host** field, enter an IPv4 or IPv6 address (or FQDN) to receive the trap.<br>iii. For **Port**, use the default (162), unless you must use another value. (162 is the standard port for SNMP traps.)<br>iv. For **Protocol**, use the default (UDP). TCP is also supported. (UDP is the standard SNMP trap protocol.)<br>v. Use the default trap community, if one was specified on the SNMP Agent page, or enter a custom community string for this trap destination.<br><br>The custom community string can be a maximum of 32 characters and cannot contain whitespace. |
| SNMPv3 | i. Select whether the destination will be used for traps or informs.<br>ii. In the **Host** field, enter an IPv4 or IPv6 address (or FQDN) to receive the trap.<br>iii. For **Port**, use the default (162), unless you must use another value. (162 is the standard port for SNMP traps.)<br>iv. For **Protocol**, use the default (UDP). TCP is also supported. (UDP is the standard SNMP trap protocol.)<br>v. Select the USM user that will be used for authentication.<br>◦ If you selected **Trap**, only USM users without authoritative engine IDs are shown.<br>◦ If you selected **Inform**, only USM users with authoritative engine IDs are shown. |

d. Click **Create**.

   The trap destination is created and added to the table.




11. When you have completed the SNMP agent configuration, click **Save**

    The new SNMP agent configuration becomes active.

#### Related information

Silence alert notifications

### Update the SNMP agent

You might want to disable SNMP notifications, update community strings, or add or remove agent addresses, USM users, and trap destinations.

#### What you'll need

- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Root Access permission.

#### About this task

Whenever you update the SNMP agent configuration, be aware that you must click **Save** at the bottom on the SNMP Agent page to commit any changes you have made on each tab.

#### Steps

1. Select **CONFIGURATION** > **Monitoring** > **SNMP agent**.

   The SNMP Agent page appears.

2. If you want to disable the SNMP agent on all grid nodes, unselect the **Enable SNMP** check box, and click **Save**.

   The SNMP agent is disabled for all grid nodes. If you later re-enable the agent, any previous SNMP configuration settings are retained.

3. Optionally, update the values you entered for **System Contact** and **System Location**.
4. Optionally, unselect the **Enable SNMP Agent Notifications** check box if you no longer want the StorageGRID SNMP agent to send trap and inform notifications.

   When this check box is unselected, the SNMP agent supports read-only MIB access, but it does not send any SNMP notifications.

5. Optionally, unselect the **Enable Authentication Traps** check box if you no longer want the StorageGRID SNMP agent to send an authentication trap when it receives an improperly authenticated protocol

message.

6. If you use SNMPv1 or SNMPv2c, optionally update the Community Strings section.

   The fields in this section are used for community-based authentication in SNMPv1 or SNMPv2c. These fields do not apply to SNMPv3.

   > If you want to remove the default community string, you must first ensure that all trap destinations use a custom community string.

7. If you want to update agent addresses, select the Agent Addresses tab in the Other Configurations section.

   **Other Configurations**

   Agent Addresses (2) | USM Users (2) | Trap Destinations (2)

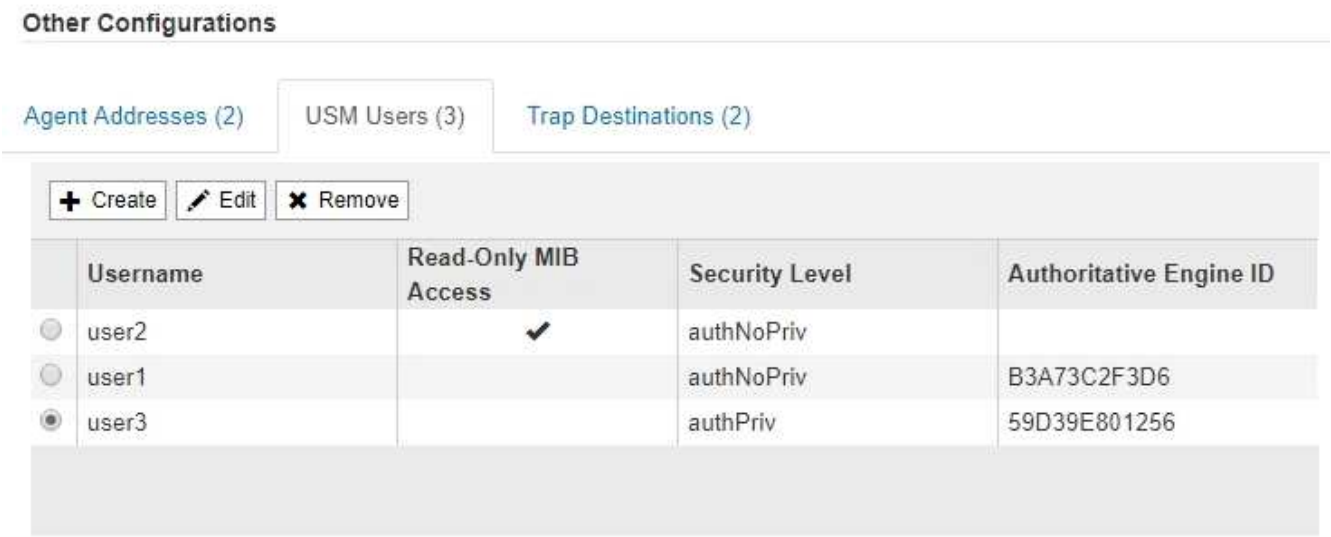
   + Create | Edit | ✖ Remove

   | | Internet Protocol | Transport Protocol | StorageGRID Network | Port |
   |---|---|---|---|---|
   | ○ | IPv4 | UDP | Grid Network | 161 |
   | ◉ | IPv4 | UDP | Admin Network | 161 |

   Use this tab to specify one or more “listening addresses.” These are the StorageGRID addresses on which the SNMP agent can receive queries. Each agent address includes an internet protocol, a transport protocol, a StorageGRID network, and a port.

   a. To add an agent address, click **Create**. Then, refer to the step for agent addresses in the instructions for configuring the SNMP agent.
   b. To edit an agent address, select the radio button for the address, and click **Edit**. Then, refer to the step for agent addresses in the instructions for configuring the SNMP agent.
   c. To remove an agent address, select the radio button for the address, and click **Remove**. Then, click **OK** to confirm that you want to remove this address.
   d. To commit your changes, click **Save** at the bottom of the SNMP Agent page.

8. If you want to update USM users, select the USM Users tab in the Other Configurations section.




Use this tab to define the USM users who are authorized to query the MIB or to receive traps and informs.

a. To add a USM user, click **Create**. Then, refer to the step for USM users in the instructions for configuring the SNMP agent.

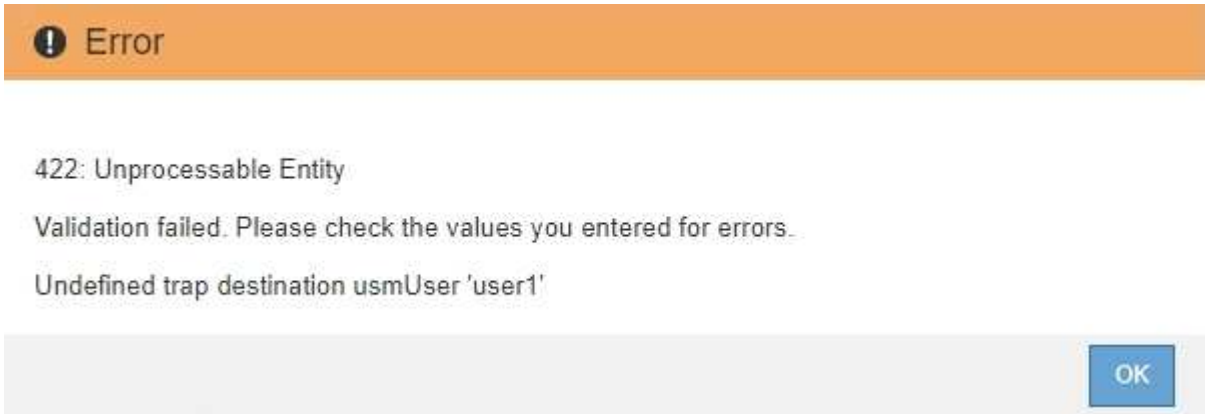
b. To edit a USM user, select the radio button for the user, and click **Edit**. Then, refer to the step for USM users in the instructions for configuring the SNMP agent.

   The username for an existing USM user cannot be changed. If you need to change a username, you must remove the user and create a new one.

   > If you add or remove a user's authoritative engine ID and that user is currently selected for a destination, you must edit or remove the destination, as described in step SNMP trap destination. Otherwise, a validation error occurs when you save the SNMP agent configuration.

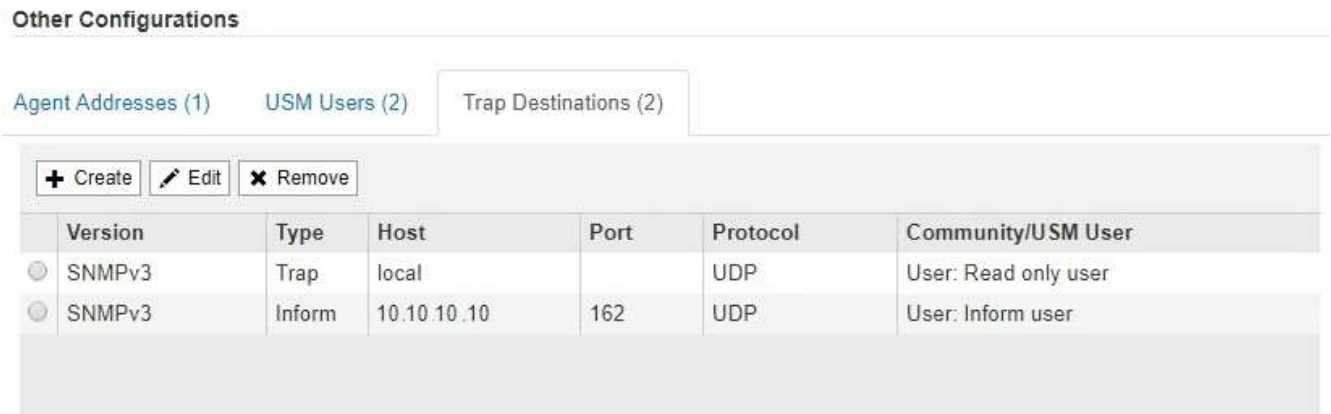
c. To remove a USM user, select the radio button for the user, and click **Remove**. Then, click **OK** to confirm that you want to remove this user.

   > If the user you removed is currently selected for a trap destination, you must edit or remove the destination, as described in step SNMP trap destination. Otherwise, a validation error occurs when you save the SNMP agent configuration.




d. To commit your changes, click **Save** at the bottom of the SNMP Agent page.

9. If you want to update trap destinations, select the Trap Destinations tab in the Other Configurations section.




The Trap Destinations tab allows you to define one or more destinations for StorageGRID trap or inform notifications. When you enable the SNMP agent and click **Save**, StorageGRID starts sending notifications to each defined destination. Notifications are sent when alerts and alarms are triggered. Standard notifications are also sent for the supported MIB-II entities (for example, ifDown and coldStart).

a. To add a trap destination, click **Create**. Then, refer to the step for trap destinations in the instructions for configuring the SNMP agent.
b. To edit a trap destination, select the radio button for the user, and click **Edit**. Then, refer to the step for trap destinations in the instructions for configuring the SNMP agent.
c. To remove a trap destination, select the radio button for the destination, and click **Remove**. Then, click **OK** to confirm that you want to remove this destination.
d. To commit your changes, click **Save** at the bottom of the SNMP Agent page.

10. When you have updated the SNMP agent configuration, click **Save**.

## Collect additional StorageGRID data

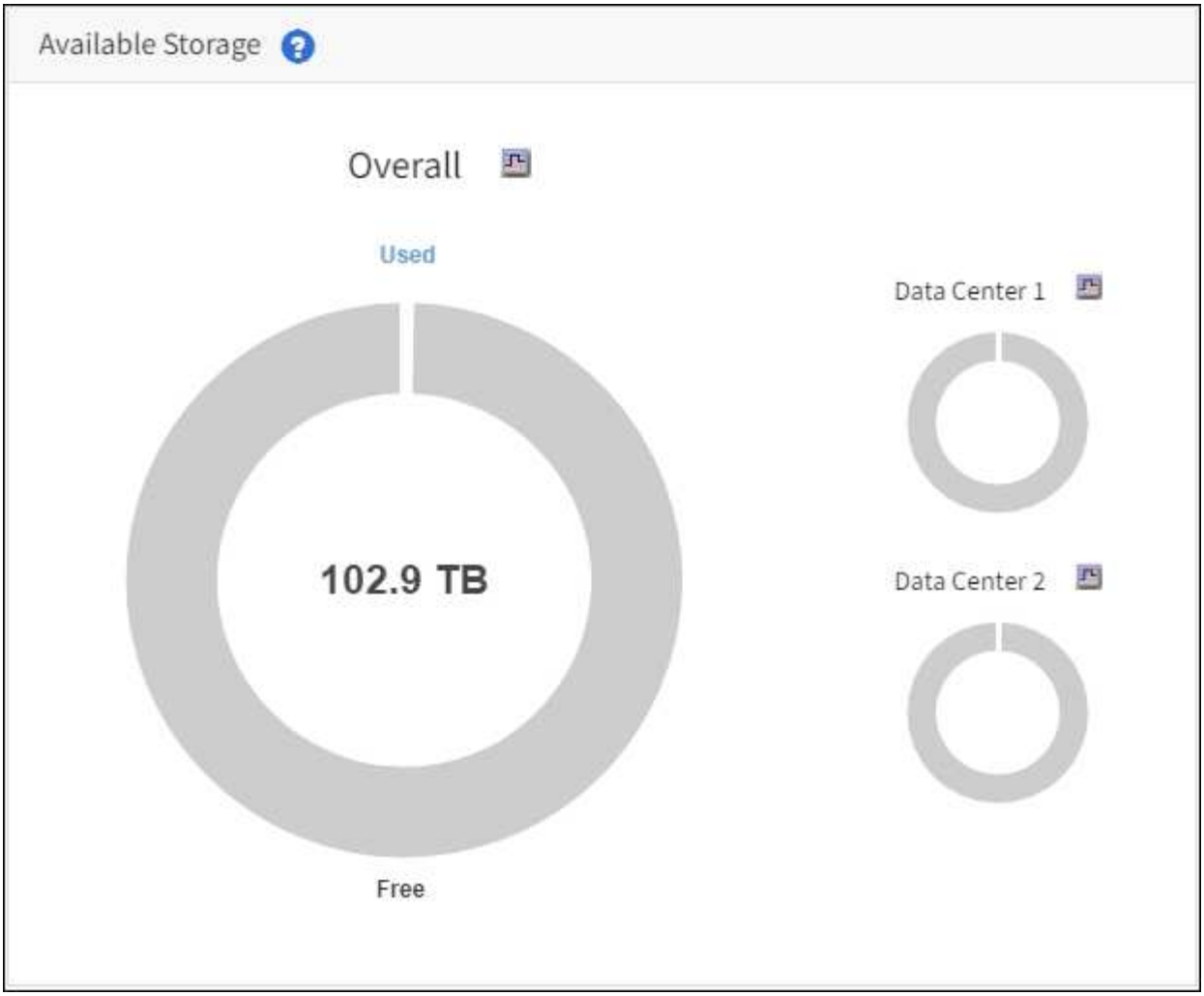
### Use charts and graphs

You can use charts and reports to monitor the state of the StorageGRID system and troubleshoot problems. The types of charts and reports available in the Grid Manager include donut charts (on the Dashboard only), graphs, and text reports.

#### Types of charts

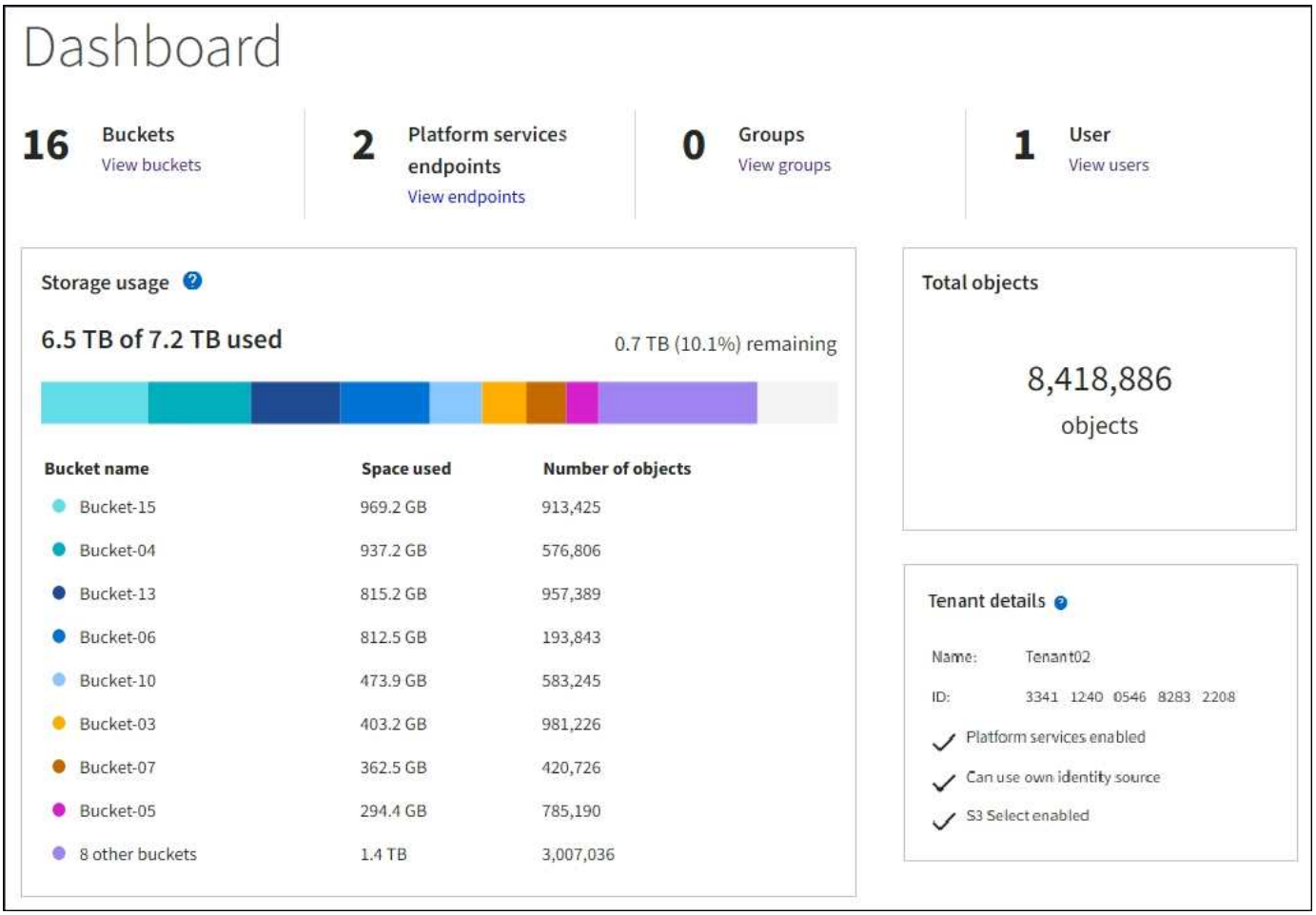
Charts and graphs summarize the values of specific StorageGRID metrics and attributes.

The Grid Manager Dashboard includes donut charts to summarize available storage for the grid and each site.




The Storage usage panel on the Tenant Manager Dashboard displays the following:

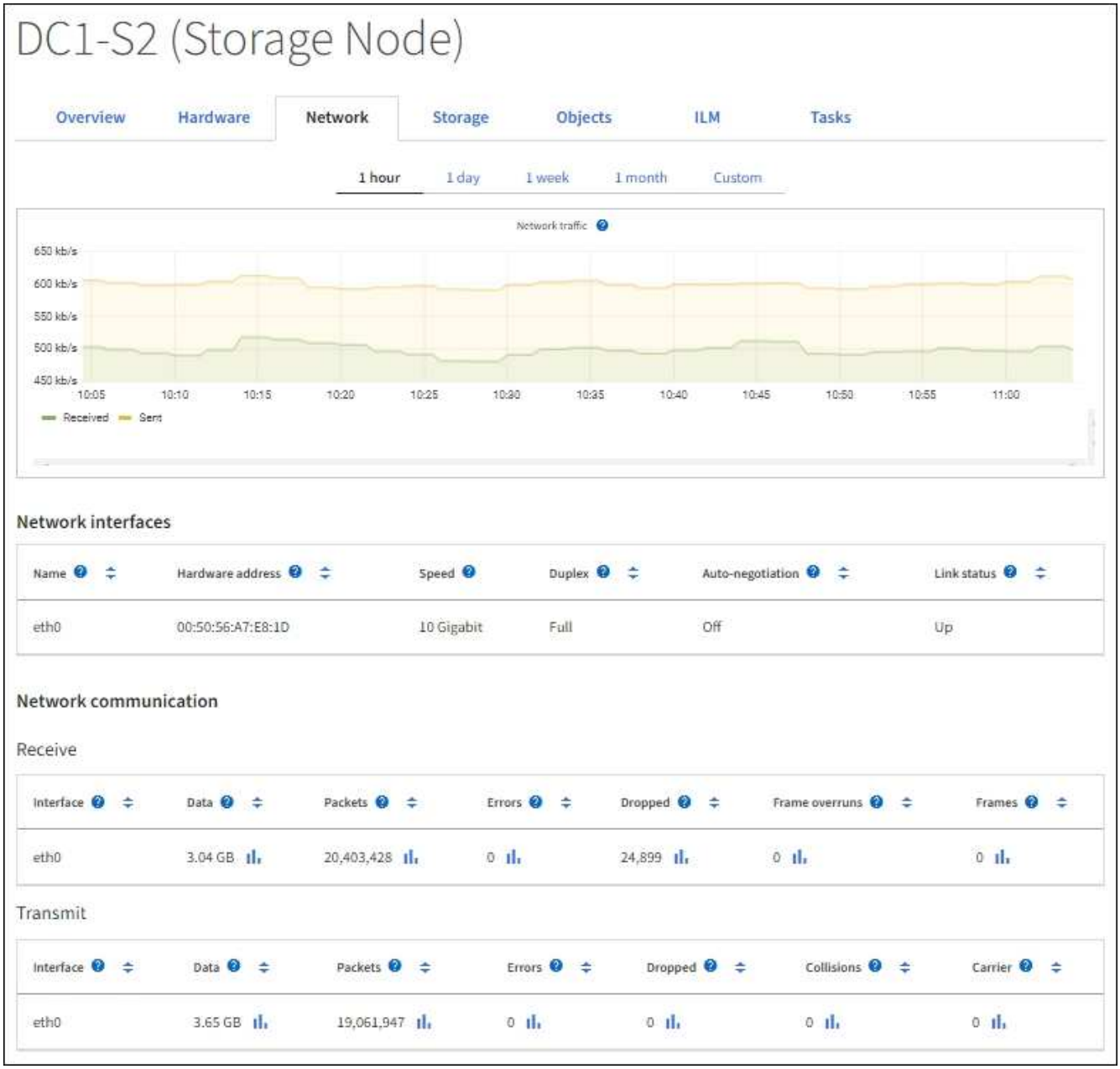
- A list of the largest buckets (S3) or containers (Swift) for the tenant
- A bar chart that represents the relative sizes of the largest buckets or containers
- The total amount of space used and, if a quota is set, the amount and percentage of space remaining




In addition, graphs that show how StorageGRID metrics and attributes change over time are available from the Nodes page and from the **SUPPORT** > **Tools** > **Grid topology** page.

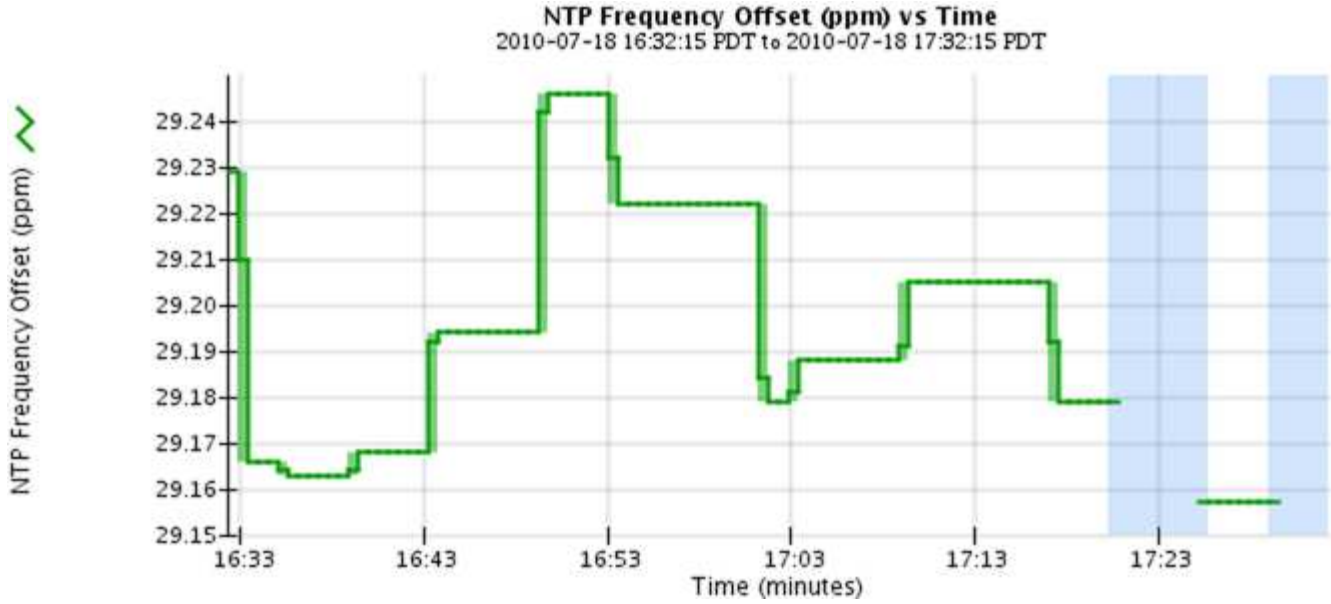
There are four types of graphs:

- **Grafana charts**: Shown on the Nodes page, Grafana charts are used to plot the values of Prometheus metrics over time. For example, the **NODES** > **Network** tab for a Storage Node includes a Grafana chart for network traffic.

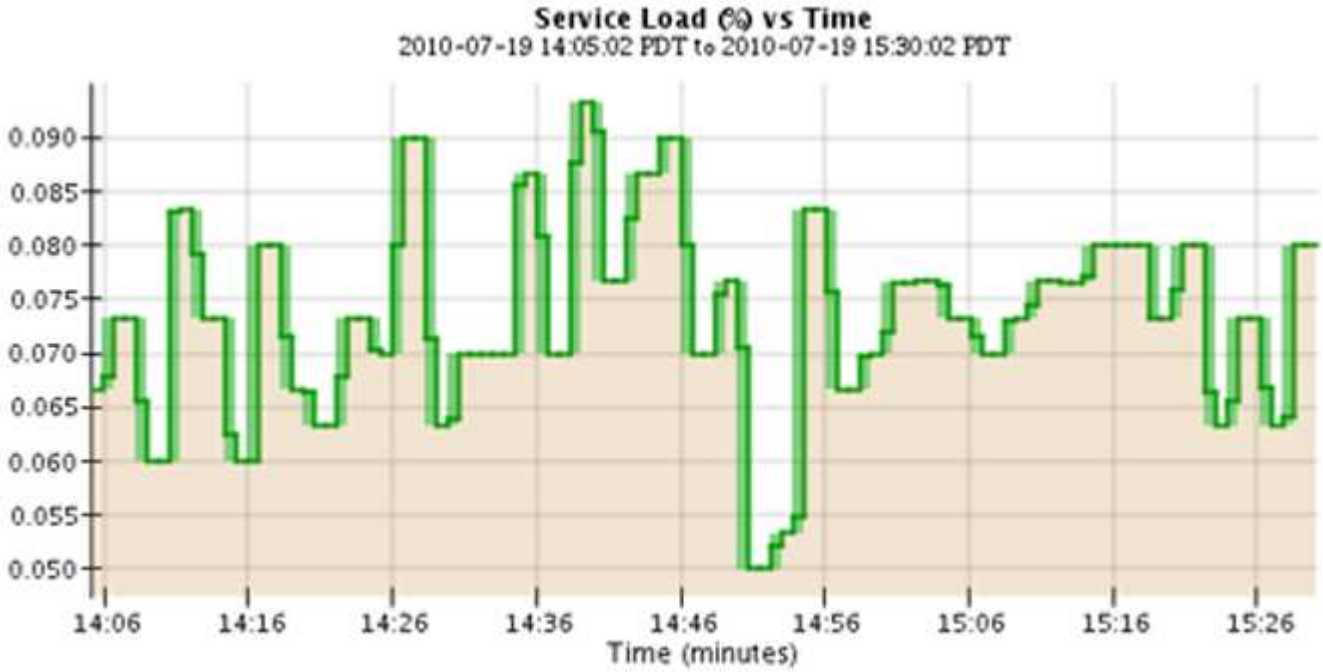



Grafana charts are also included on the pre-constructed dashboards available from the **SUPPORT** > **Tools** > **Metrics** page.

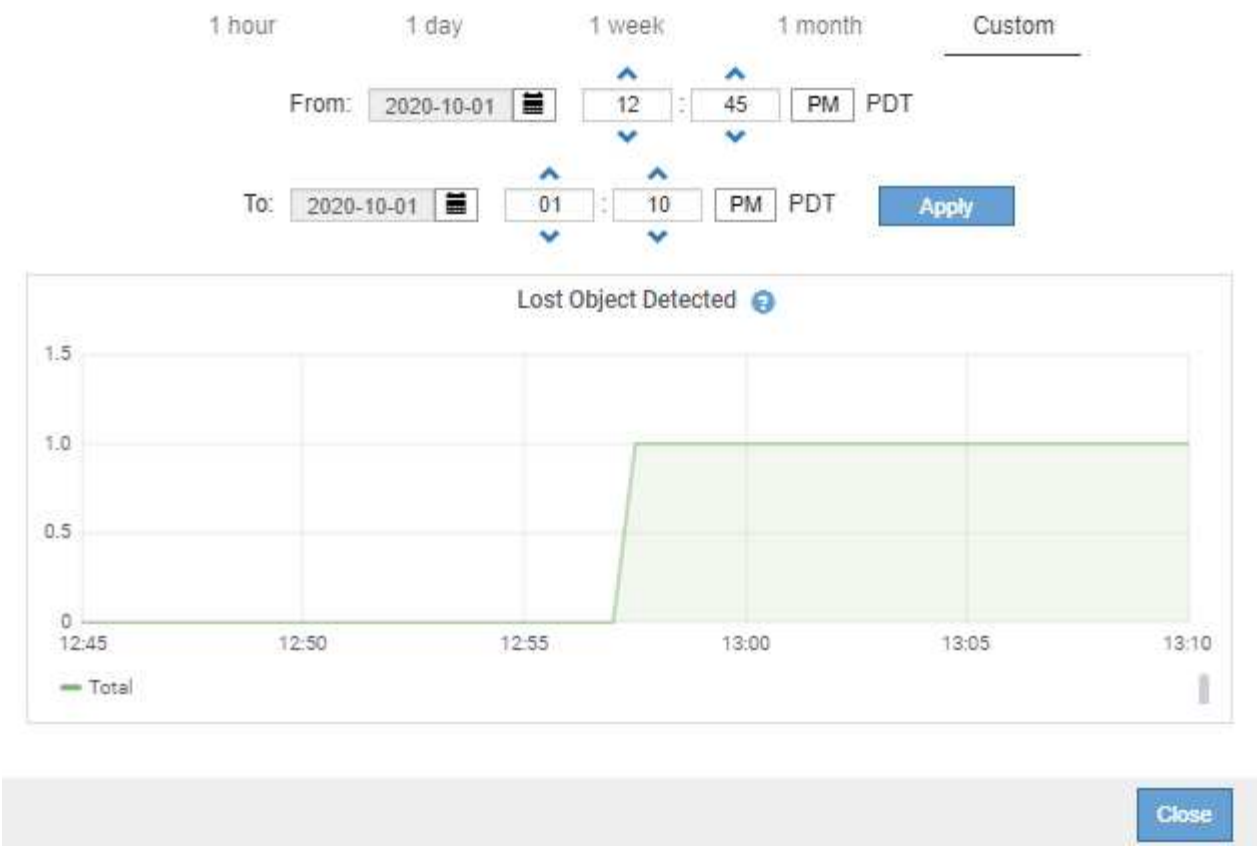
- **Line graphs**: Available from the Nodes page and from the **SUPPORT** > **Tools** > **Grid topology** page (select the chart icon after a data value), line graphs are used to plot the values of StorageGRID attributes that have a unit value (such as NTP Frequency Offset, in ppm). The changes in the value are plotted in regular data intervals (bins) over time.



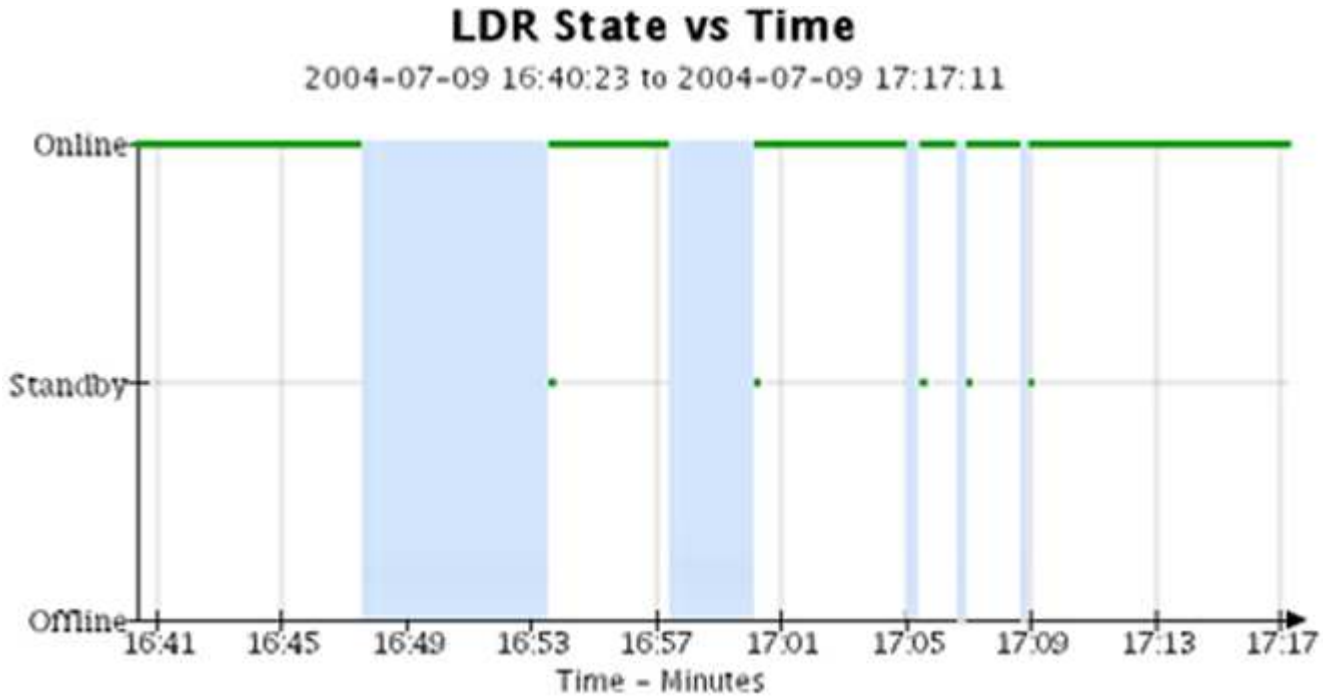

- **Area graphs**: Available from the Nodes page and from the **SUPPORT** > **Tools** > **Grid topology** page (select the chart icon after a data value), area graphs are used to plot volumetric attribute quantities, such as object counts or service load values. Area graphs are similar to line graphs, but include a light brown shading below the line. The changes in the value are plotted in regular data intervals (bins) over time.




- Some graphs are denoted with a different type of chart icon and have a different format:




- **State graph**: Available from the **SUPPORT** > **Tools** > **Grid topology** page (select the chart icon after a data value), state graphs are used to plot attribute values that represent distinct states such as a service state that can be online, standby, or offline. State graphs are similar to line graphs, but the transition is discontinuous; that is, the value jumps from one state value to another.




**Related information**

View the Nodes page

View the Grid Topology tree

Review support metrics

#### Chart legend

The lines and colors used to draw charts have specific meaning.

| Sample | Meaning |
|---|---|
| | Reported attribute values are plotted using dark green lines. |
| | Light green shading around dark green lines indicates that the actual values in that time range vary and have been “binned” for faster plotting. The dark line represents the weighted average. The range in light green indicates the maximum and minimum values within the bin. Light brown shading is used for area graphs to indicate volumetric data. |
|  | Blank areas (no data plotted) indicate that the attribute values were unavailable. The background can be blue, gray, or a mixture of gray and blue, depending on the state of the service reporting the attribute. |
|  | Light blue shading indicates that some or all of the attribute values at that time were indeterminate; the attribute was not reporting values because the service was in an unknown state. |
| | Gray shading indicates that some or all of the attribute values at that time were not known because the service reporting the attributes was administratively down. |
| | A mixture of gray and blue shading indicates that some of the attribute values at the time were indeterminate (because the service was in an unknown state), while others were not known because the service reporting the attributes was administratively down. |

#### Display charts and graphs

The Nodes page contains the charts and graphs you should access regularly to monitor attributes such as storage capacity and throughput. In some cases, especially when working with technical support, you can use the **SUPPORT** > **Tools** > **Grid topology** page to access additional charts.

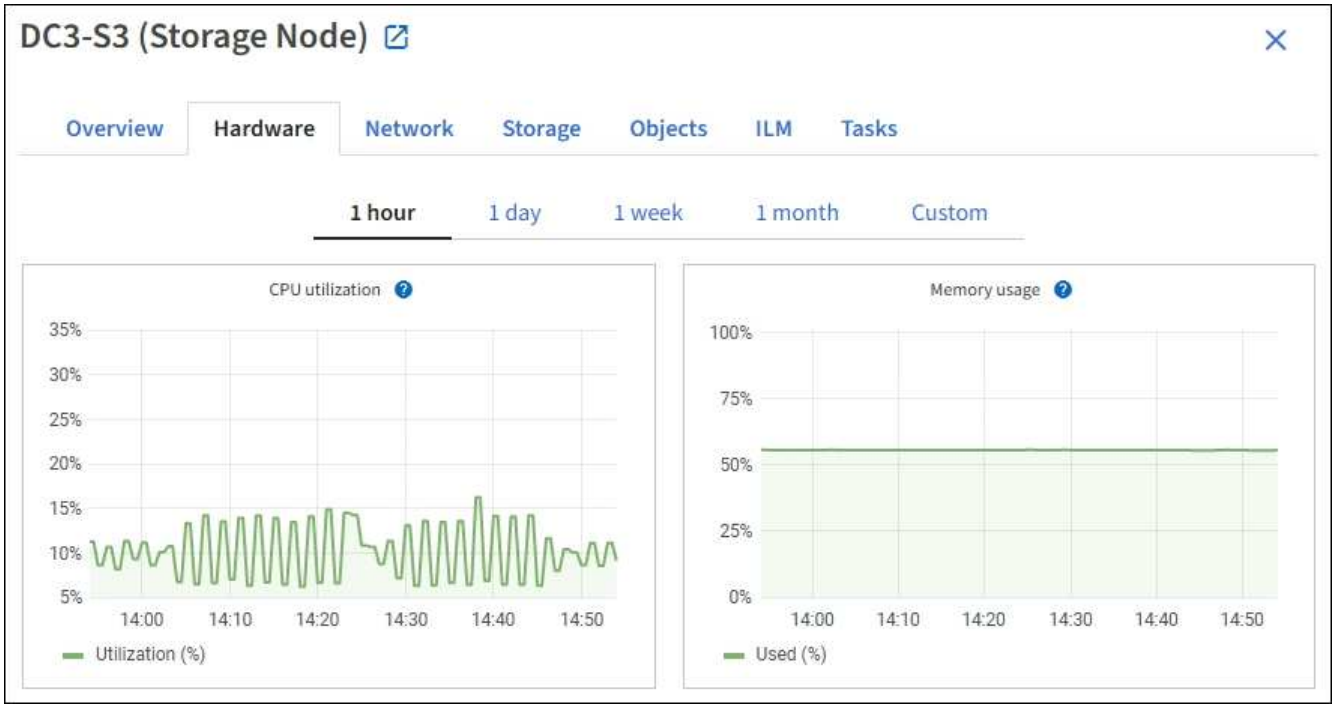
#### What you’ll need

You must be signed in to the Grid Manager using a supported web browser.

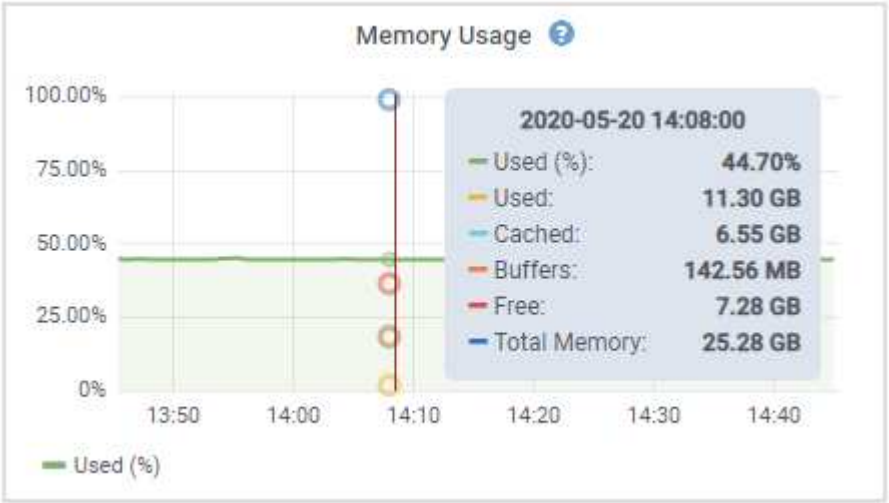
#### Steps

1. Select **NODES**. Then, select a node, a site, or the entire grid.
2. Select the tab for which you want to view information.

   Some tabs include one or more Grafana charts, which are used to plot the values of Prometheus metrics over time. For example, the **NODES** > **Hardware** tab for a node includes two Grafana charts.




3. Optionally, hover your cursor over the chart to see more detailed values for a particular point in time.

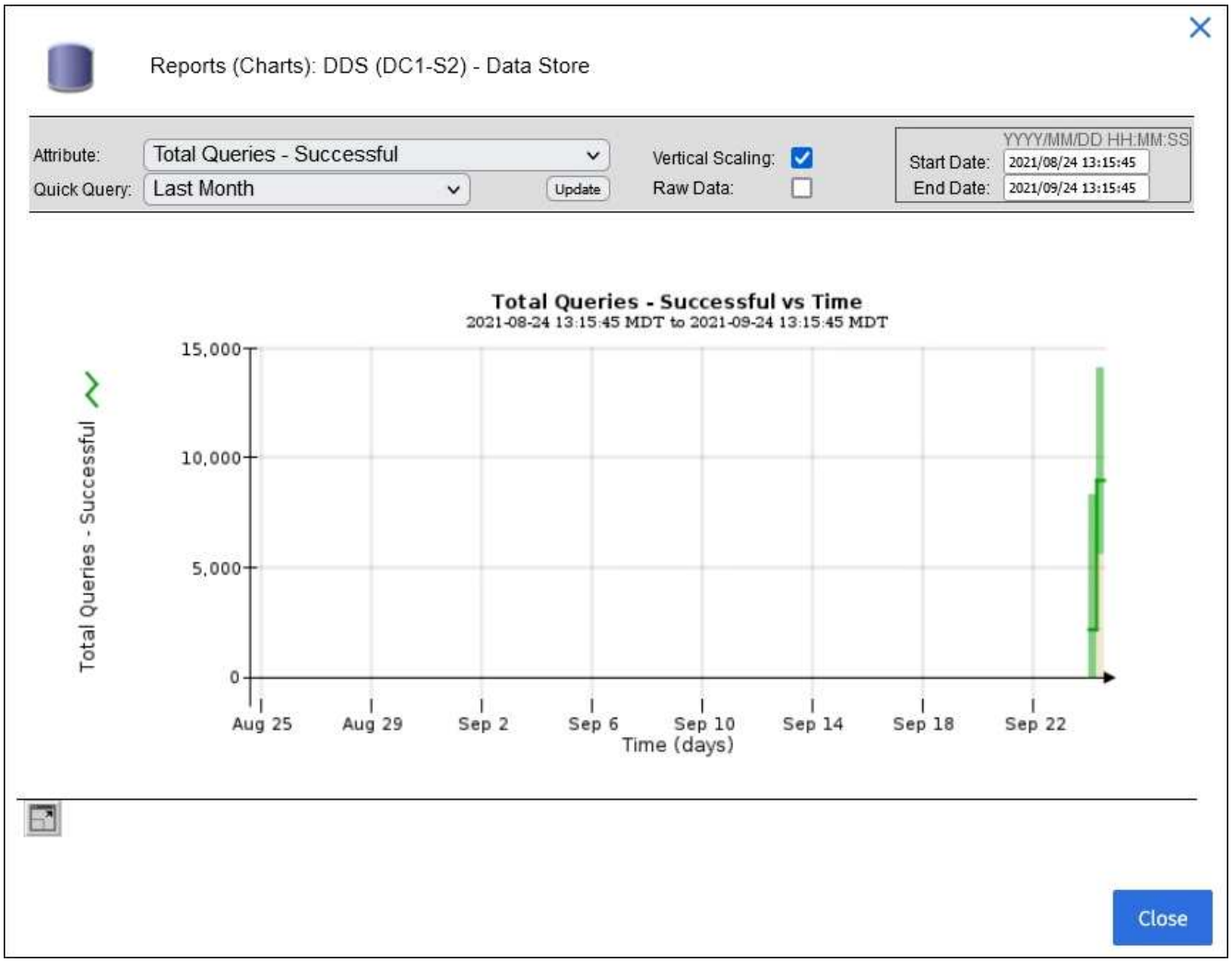



4. As required, you can often display a chart for a specific attribute or metric. From the table on the Nodes page, select the chart icon to the right of the attribute name.

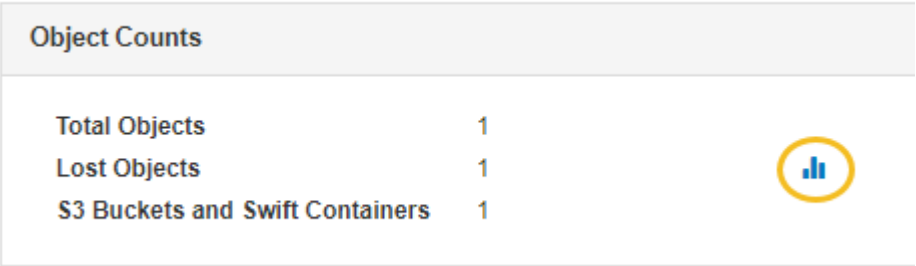
> Charts are not available for all metrics and attributes.

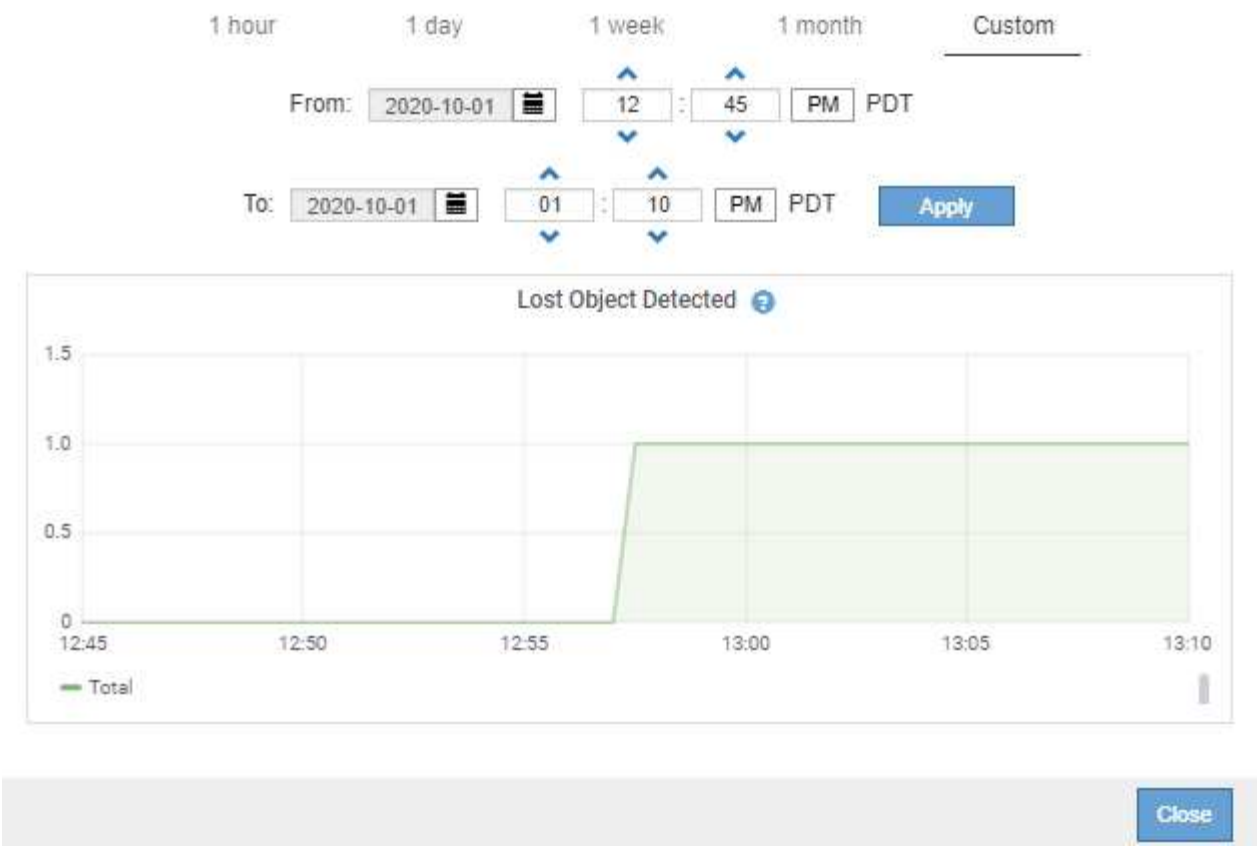
**Example 1**: From the Objects tab for a Storage Node, you can select the chart icon to see the total number of successful metadata store queries for the Storage Node.

Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 MDT
Total Queries - Successful
32,000
31,000
30,000
29,000
13:25
13:35
13:45
13:55
14:05
14:15
Time (minutes)
Close

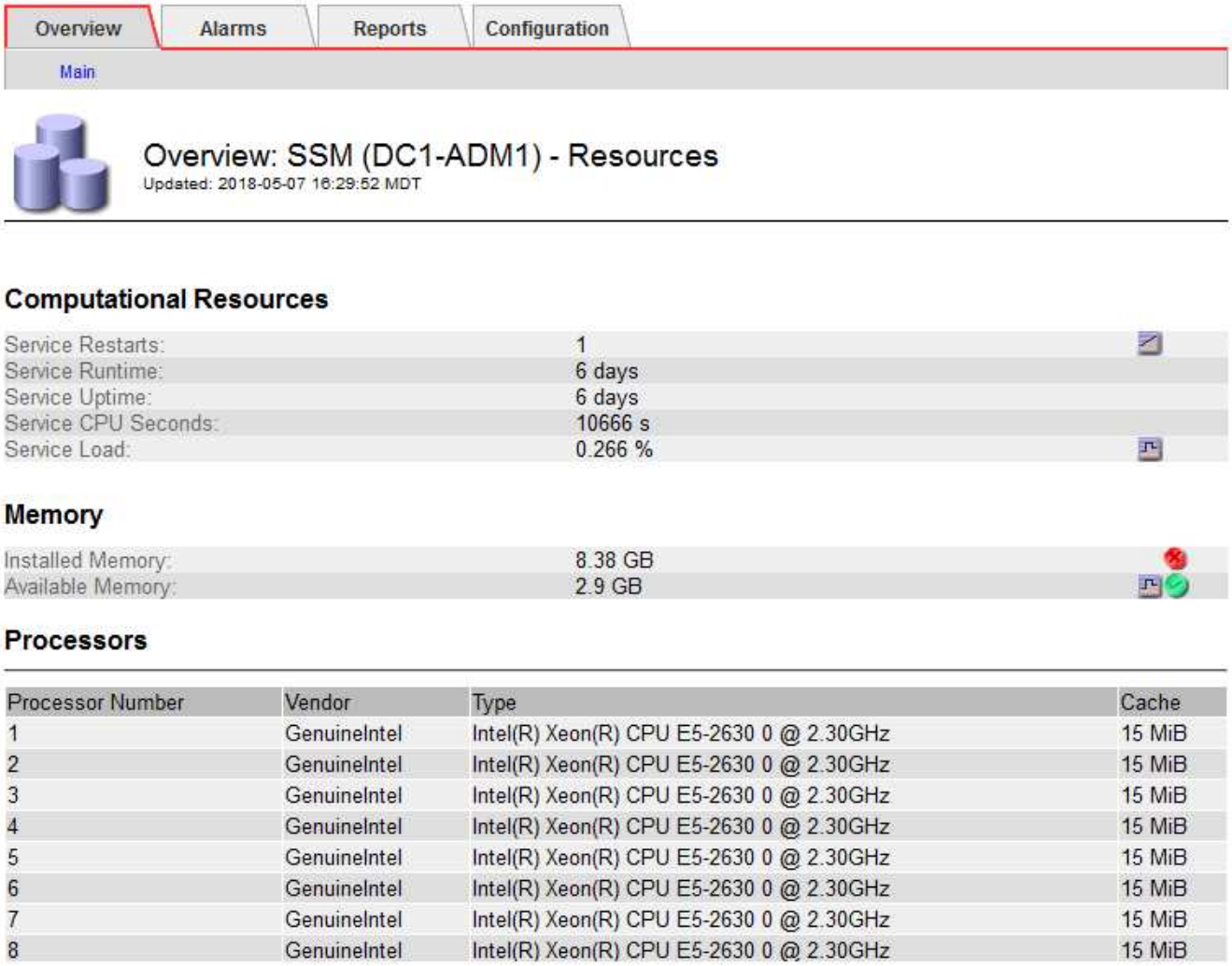



**Example 2**: From the Objects tab for a Storage Node, you can select the chart icon to see the Grafana graph of the count of lost objects detected over time.






5. To display charts for attributes that are not shown on the Node page, select **SUPPORT** > **Tools** > **Grid topology**.
6. Select ***grid node*** > ***component or service*** > **Overview** > **Main**.




7. Select the chart icon next to the attribute.

   The display automatically changes to the **Reports** > **Charts** page. The chart displays the attribute's data over the past day.

#### Generate charts

Charts display a graphical representation of attribute data values. You can report on a data center site, grid node, component, or service.

**What you'll need**

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

**Steps**

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Select ***grid node*** > ***component or service*** > **Reports** > **Charts**.
3. Select the attribute to report on from the **Attribute** drop-down list.
4. To force the Y-axis to start at zero, deselect the **Vertical Scaling** check box.
5. To show values at full precision, select the **Raw Data** check box, or to round values to a maximum of three

decimal places (for example, for attributes reported as percentages), deselect the **Raw Data** check box.

6. Select the time period to report on from the **Quick Query** drop-down list.

   Select the Custom Query option to select a specific time range.

   The chart appears after a few moments. Allow several minutes for tabulation of long time ranges.

7. If you selected Custom Query, customize the time period for the chart by entering the **Start Date** and **End Date**.

   Use the format *YYYY/MM/DDHH:MM:SS* in local time. Leading zeros are required to match the format. For example, 2017/4/6 7:30:00 fails validation. The correct format is: 2017/04/06 07:30:00.

8. Select **Update**.

   A chart is generated after a few seconds. Allow several minutes for tabulation of long time ranges. Depending on the length of time set for the query, either a raw text report or aggregate text report is displayed.

### Use text reports

Text reports display a textual representation of attribute data values that have been processed by the NMS service. There are two types of reports generated depending on the time period you are reporting on: raw text reports for periods less than a week, and aggregate text reports for time periods greater than a week.

#### Raw text reports

A raw text report displays details about the selected attribute:

- Time Received: Local date and time that a sample value of an attribute's data was processed by the NMS service.
- Sample Time: Local date and time that an attribute value was sampled or changed at the source.
- Value: Attribute value at sample time.

## Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

| Time Received | Sample Time | Value |
|---|---|---|
| 2010-07-19 15:58:09 | 2010-07-19 15:58:09 | 0.016 % |
| 2010-07-19 15:56:06 | 2010-07-19 15:56:06 | 0.024 % |
| 2010-07-19 15:54:02 | 2010-07-19 15:54:02 | 0.033 % |
| 2010-07-19 15:52:00 | 2010-07-19 15:52:00 | 0.016 % |
| 2010-07-19 15:49:57 | 2010-07-19 15:49:57 | 0.008 % |
| 2010-07-19 15:47:54 | 2010-07-19 15:47:54 | 0.024 % |
| 2010-07-19 15:45:50 | 2010-07-19 15:45:50 | 0.016 % |
| 2010-07-19 15:43:47 | 2010-07-19 15:43:47 | 0.024 % |
| 2010-07-19 15:41:43 | 2010-07-19 15:41:43 | 0.032 % |
| 2010-07-19 15:39:40 | 2010-07-19 15:39:40 | 0.024 % |
| 2010-07-19 15:37:37 | 2010-07-19 15:37:37 | 0.008 % |
| 2010-07-19 15:35:34 | 2010-07-19 15:35:34 | 0.016 % |
| 2010-07-19 15:33:31 | 2010-07-19 15:33:31 | 0.024 % |
| 2010-07-19 15:31:27 | 2010-07-19 15:31:27 | 0.032 % |
| 2010-07-19 15:29:24 | 2010-07-19 15:29:24 | 0.032 % |
| 2010-07-19 15:27:21 | 2010-07-19 15:27:21 | 0.049 % |
| 2010-07-19 15:25:18 | 2010-07-19 15:25:18 | 0.024 % |
| 2010-07-19 15:21:12 | 2010-07-19 15:21:12 | 0.016 % |
| 2010-07-19 15:19:09 | 2010-07-19 15:19:09 | 0.008 % |
| 2010-07-19 15:17:07 | 2010-07-19 15:17:07 | 0.016 % |

#### Aggregate text reports

An aggregate text report displays data over a longer period of time (usually a week) than a raw text report. Each entry is the result of summarizing multiple attribute values (an aggregate of attribute values) by the NMS service over time into a single entry with average, maximum, and minimum values that are derived from the aggregation.

Each entry displays the following information:

- Aggregate Time: Last local date and time that the NMS service aggregated (collected) a set of changed attribute values.
- Average Value: The average of the attribute's value over the aggregated time period.
- Minimum Value: The minimum value over the aggregated time period.
- Maximum Value: The maximum value over the aggregated time period.

**Text Results for Attribute Send to Relay Rate**

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

| Aggregate Time | Average Value | Minimum Value | Maximum Value |
|---|---|---|---|
| 2010-07-19 15:59:52 | 0.271072196 Messages/s | 0.266649743 Messages/s | 0.274983464 Messages/s |
| 2010-07-19 15:53:52 | 0.275585378 Messages/s | 0.266562352 Messages/s | 0.283302736 Messages/s |
| 2010-07-19 15:49:52 | 0.279315709 Messages/s | 0.233318712 Messages/s | 0.333313579 Messages/s |
| 2010-07-19 15:43:52 | 0.28181323 Messages/s | 0.241651024 Messages/s | 0.374976601 Messages/s |
| 2010-07-19 15:39:52 | 0.284233141 Messages/s | 0.249982001 Messages/s | 0.324971987 Messages/s |
| 2010-07-19 15:33:52 | 0.325752083 Messages/s | 0.266641993 Messages/s | 0.358306197 Messages/s |
| 2010-07-19 15:29:52 | 0.278531507 Messages/s | 0.274984766 Messages/s | 0.283320999 Messages/s |
| 2010-07-19 15:23:52 | 0.281437642 Messages/s | 0.274981961 Messages/s | 0.291577735 Messages/s |
| 2010-07-19 15:17:52 | 0.261563307 Messages/s | 0.258318006 Messages/s | 0.266655787 Messages/s |
| 2010-07-19 15:13:52 | 0.265159147 Messages/s | 0.258318557 Messages/s | 0.26663986 Messages/s |

#### Generate text reports

Text reports display a textual representation of attribute data values that have been processed by the NMS service. You can report on a data center site, grid node, component, or service.

**What you'll need**

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

**About this task**

For attribute data that is expected to be continuously changing, this attribute data is sampled by the NMS service (at the source) at regular intervals. For attribute data that changes infrequently (for example, data based on events such as state or status changes), an attribute value is sent to the NMS service when the value changes.

The type of report displayed depends on the configured time period. By default, aggregate text reports are generated for time periods longer than one week.

Gray text indicates the service was administratively down during the time it was sampled. Blue text indicates the service was in an unknown state.

**Steps**

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Select ***grid node*** > ***component or service*** > **Reports** > **Text**.
3. Select the attribute to report on from the **Attribute** drop-down list.
4. Select the number of results per page from the **Results per Page** drop-down list.
5. To round values to a maximum of three decimal places (for example, for attributes reported as percentages), unselect the **Raw Data** check box.
6. Select the time period to report on from the **Quick Query** drop-down list.

   Select the Custom Query option to select a specific time range.

   The report appears after a few moments. Allow several minutes for tabulation of long time ranges.

7. If you selected Custom Query, you need to customize the time period to report on by entering the **Start Date** and **End Date**.

   Use the format `YYYY/MM/DDHH:MM:SS` in local time. Leading zeros are required to match the format. For example, 2017/4/6 7:30:00 fails validation. The correct format is: 2017/04/06 07:30:00.

8. Click **Update**.

   A text report is generated after a few moments. Allow several minutes for tabulation of long time ranges. Depending on the length of time set for the query, either a raw text report or aggregate text report is displayed.

#### Export text reports

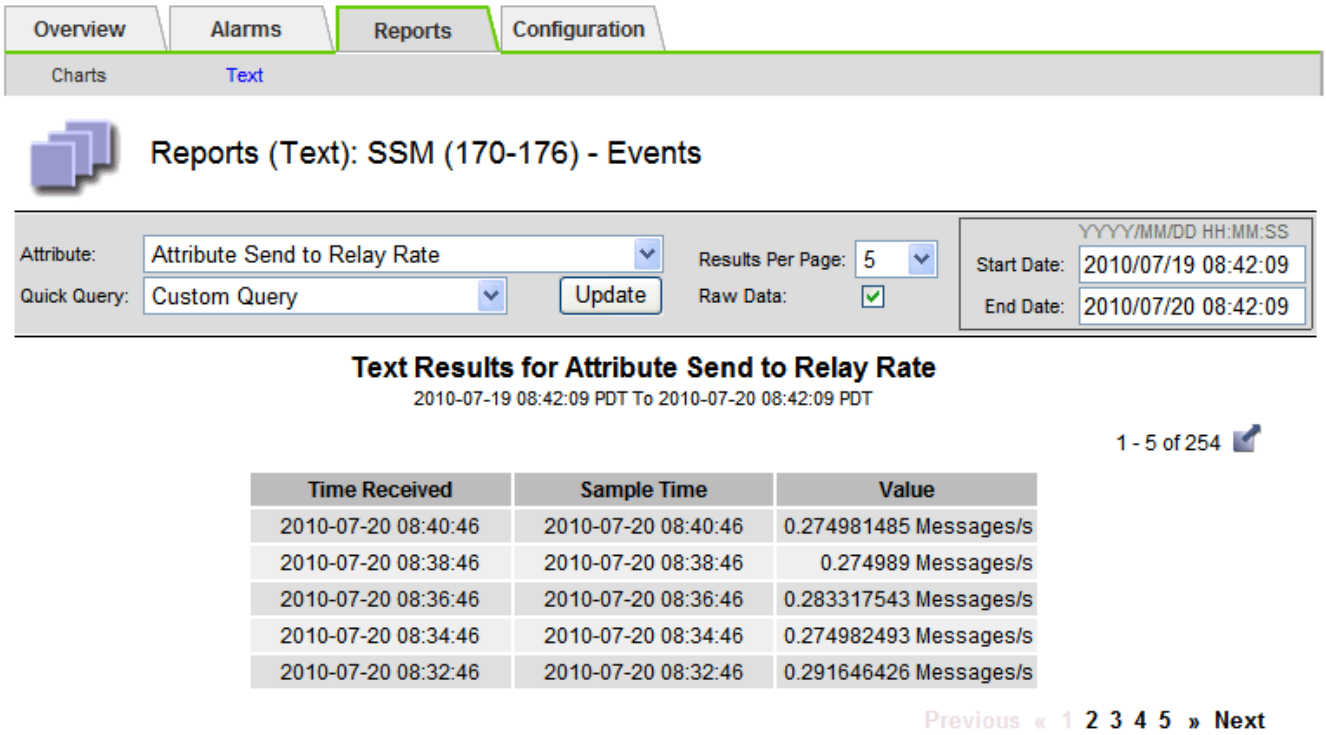
Exported text reports open a new browser tab, which enables you to select and copy the data.

### About this task

The copied data can then be saved into a new document (for example, a spreadsheet) and used to analyze the performance of the StorageGRID system.

### Steps

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Create a text report.
3. Click *Export*.




   The Export Text Report window opens displaying the report.

```
Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U
```

4. Select and copy the contents of the Export Text Report window.

   This data can now be pasted into a third-party document such as a spreadsheet.

### Monitor PUT and GET performance

You can monitor the performance of certain operations, such as object store and retrieve, to help identify changes that might require further investigation.

#### About this task

To monitor PUT and GET performance, you can run S3 and Swift commands directly from a workstation or by using the open-source S3tester application. Using these methods allows you to assess performance independently of factors that are external to StorageGRID, such as issues with a client application or issues with an external network.

When performing tests of PUT and GET operations, use the following guidelines:

- Use object sizes comparable to the objects that you typically ingest into your grid.
- Perform operations against both local and remote sites.

Messages in the audit log indicate the total time required to run certain operations. For example, to determine the total processing time for an S3 GET request, you can review the value of the TIME attribute in the SGET audit message. You can also find the TIME attribute in the audit messages for the following operations:

- **S3**: DELETE, GET, HEAD, Metadata Updated, POST, PUT
- **Swift**: DELETE, GET, HEAD, PUT

When analyzing results, look at the average time required to satisfy a request, as well as the overall throughput that you can achieve. Repeat the same tests regularly and record the results, so that you can identify trends that may require investigation.

- You can download S3tester from github.

### Monitor object verification operations

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

#### What you'll need

- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Maintenance or Root Access permission.

#### About this task

Two verification processes work together to ensure data integrity:

- **Background verification** runs automatically, continuously checking the correctness of object data.

  Background verification automatically and continuously checks all Storage Nodes to determine if there are corrupt copies of replicated and erasure-coded object data. If problems are found, the StorageGRID system automatically attempts to replace the corrupt object data from copies stored elsewhere in the system. Background verification does not run on Archive Nodes or on objects in a Cloud Storage Pool.

  > The **Unidentified corrupt object detected** alert is triggered if the system detects a corrupt object that cannot be corrected automatically.

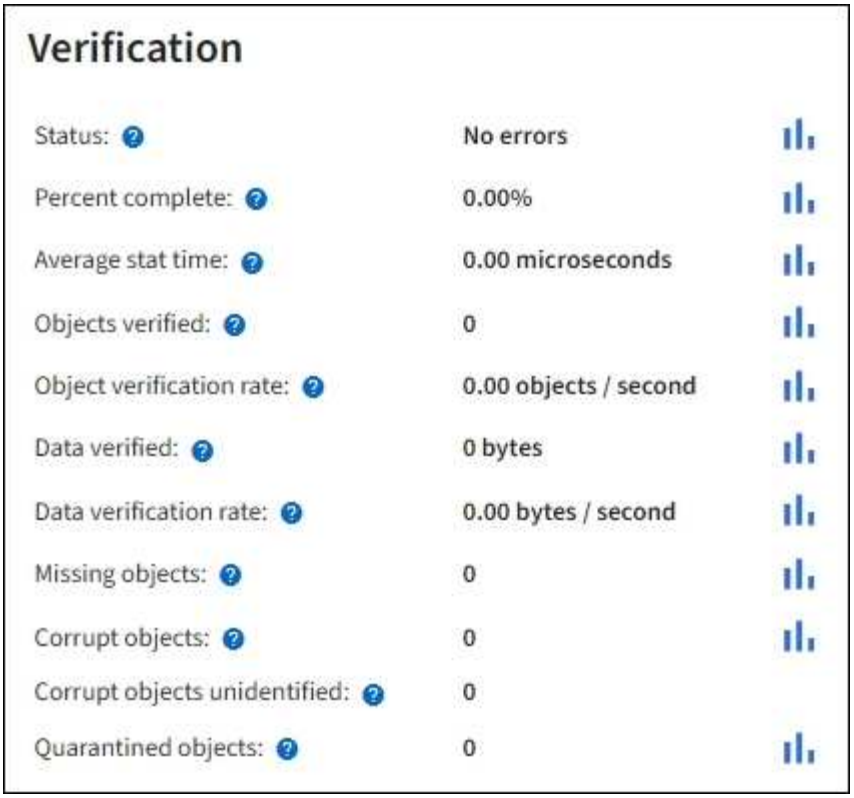
- **Object existence check** can be triggered by a user to more quickly verify the existence (although not the correctness) of object data.

  Object existence check verifies whether all expected replicated copies of objects and erasure-coded fragments exist on a Storage Node. Object existence check provides a way to verify the integrity of storage devices, especially if a recent hardware issue could have affected data integrity.

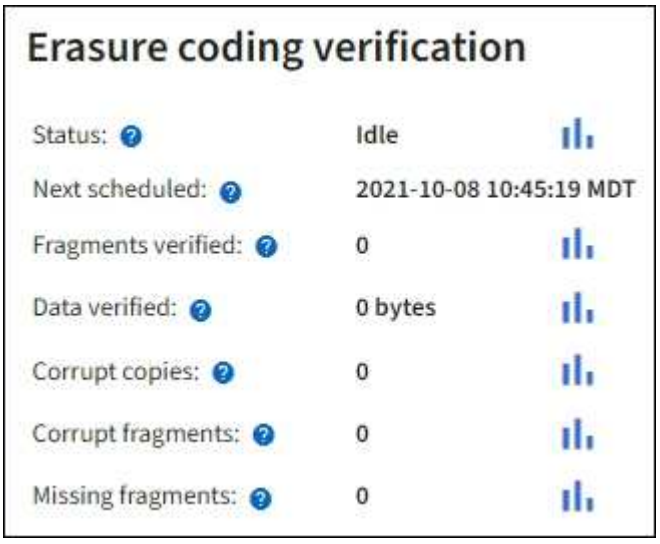
You should review the results from background verifications and object existence checks regularly. Investigate any instances of corrupt or missing object data immediately to determine the root cause.

#### Steps

1. Review the results from background verifications:
   a. Select **NODES** > ***Storage Node*** > **Objects**.
   b. Check the verification results:
      - To check replicated object data verification, look at the attributes in the Verification section.

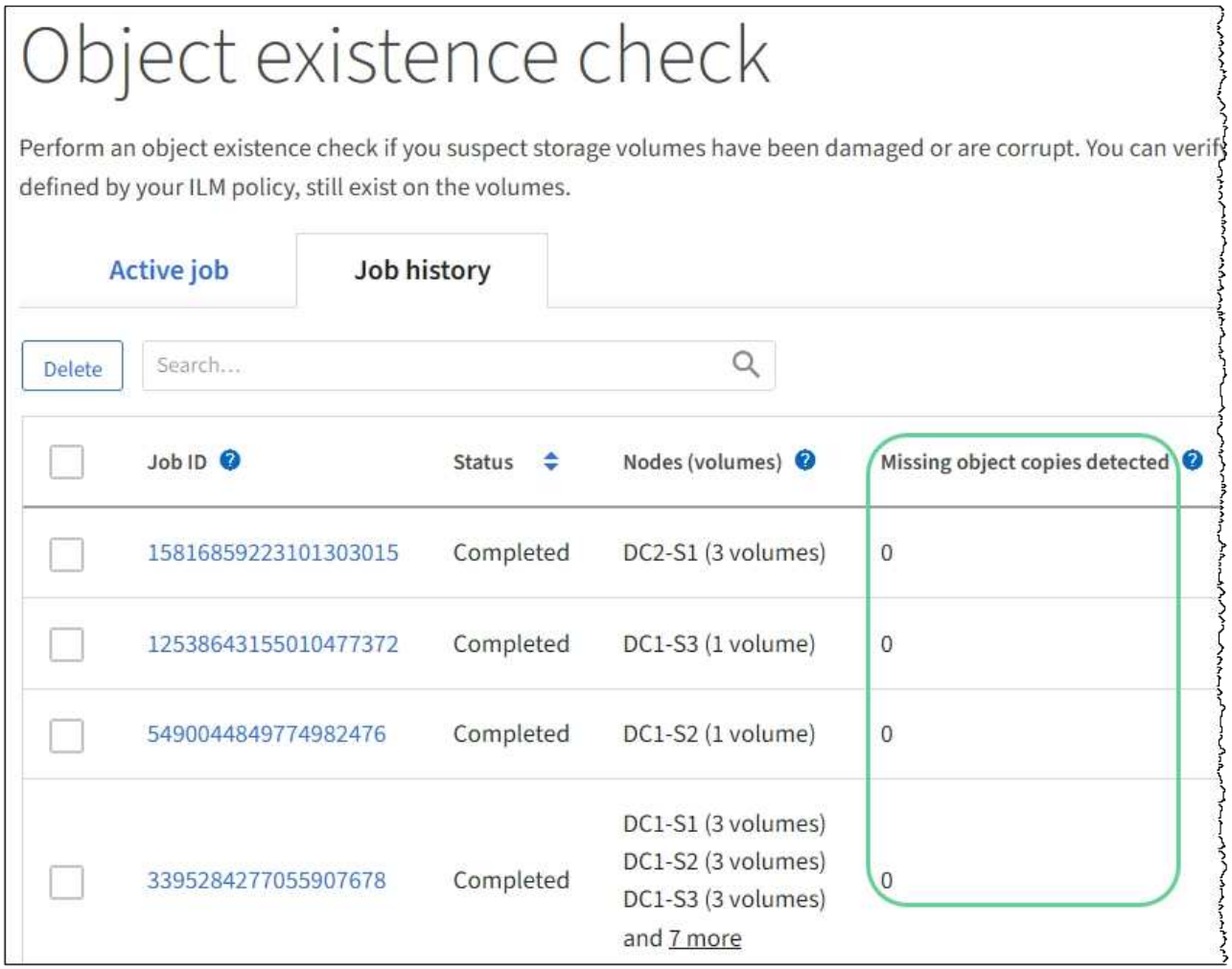



- To check erasure-coded fragment verification, select ***Storage Node*** > **ILM** and look at the attributes in the Erasure coding verification section.




Select the question mark ? next to an attribute's name to display help text.

2. Review the results from object existence check jobs:
   a. Select **MAINTENANCE** > **Object existence check** > **Job history**.
   b. Scan the Missing object copies detected column. If any jobs resulted in 100 or more missing object copies and the Objects lost alert has been triggered, contact technical support.




**Monitor events**

You can monitor events that are detected by a grid node, including custom events that you have created to track events that are logged to the syslog server. The Last Event message shown in the Grid Manager provides more information about the most recent event.

Event messages are also listed in the `/var/local/log/bycast-err.log` log file. See the Log files reference.

The SMTT (Total events) alarm can be repeatedly triggered by issues such as network problems, power outages or upgrades. This section has information on investigating events so that you can better understand why these alarms have occurred. If an event occurred because of a known issue, it is safe to reset the event counters.

**Steps**

1. Review the system events for each grid node:
   a. Select **SUPPORT** > **Tools** > **Grid topology**.
   b. Select ***site*** > ***grid node*** > **SSM** > **Events** > **Overview** > **Main**.
2. Generate a list of previous event messages to help isolate issues that occurred in the past:

a. Select **SUPPORT** > **Tools** > **Grid topology**.

b. Select ***site*** > ***grid node*** > **SSM** > **Events** > **Reports**.

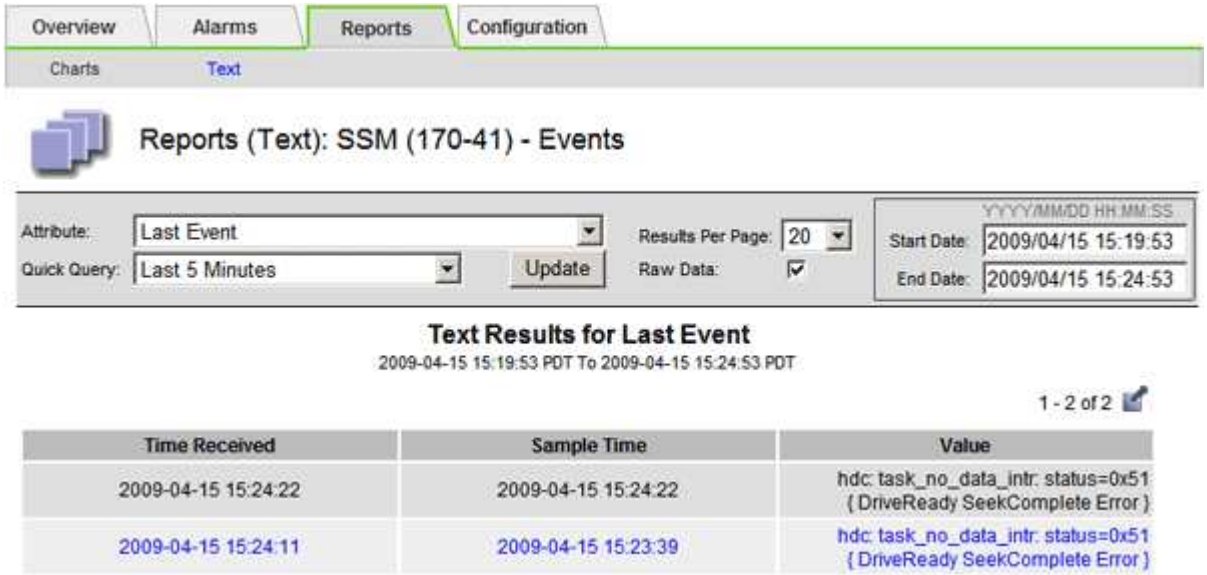
c. Select **Text**.

The **Last Event** attribute is not shown in the charts view. To view it:

d. Change **Attribute** to **Last Event**.

e. Optionally, select a time period for **Quick Query**.

f. Select **Update**.




#### Create custom syslog events

Custom events allow you to track all kernel, daemon, error and critical level user events logged to the syslog server. A custom event can be useful for monitoring the occurrence of system log messages (and thus network security events and hardware faults).

#### About this task

Consider creating custom events to monitor recurring problems. The following considerations apply to custom events.

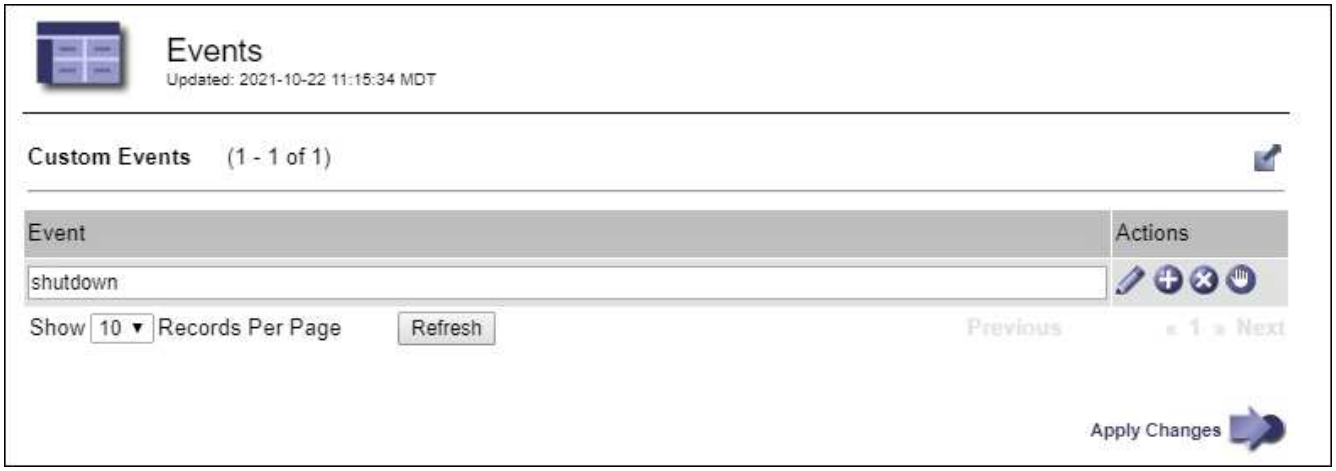
- After a custom event is created, every occurrence of it is monitored.
- To create a custom event based on keywords in the `/var/local/log/messages` files, the logs in those files must be:
  - Generated by the kernel
  - Generated by daemon or user program at the error or critical level

**Note:** Not all entries in the `/var/local/log/messages` files will be matched unless they satisfy the requirements stated above.

#### Steps

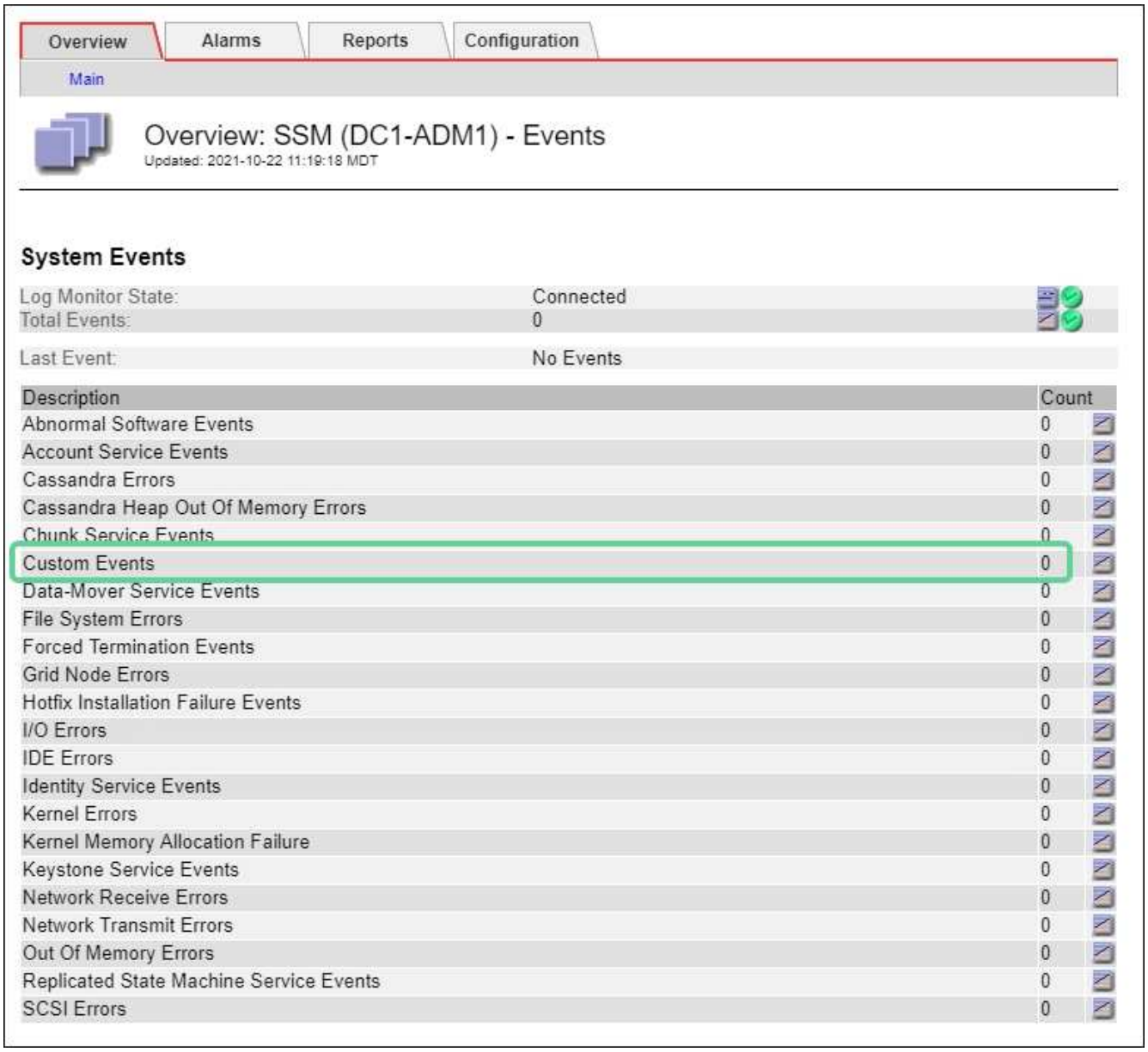
1. Select **SUPPORT** > **Alarms (legacy)** > **Custom events**.
2. Click **Edit** (or **Insert** if this is not the first event).

3. Enter a custom event string, for example, shutdown




4. Select **Apply Changes**.
5. Select **SUPPORT** > **Tools** > **Grid topology**.
6. Select ***grid node*** > **SSM** > **Events**.
7. Locate the entry for Custom Events in the Events table, and monitor the value for **Count**.

   If the count increases, a custom event you are monitoring is being triggered on that grid node.



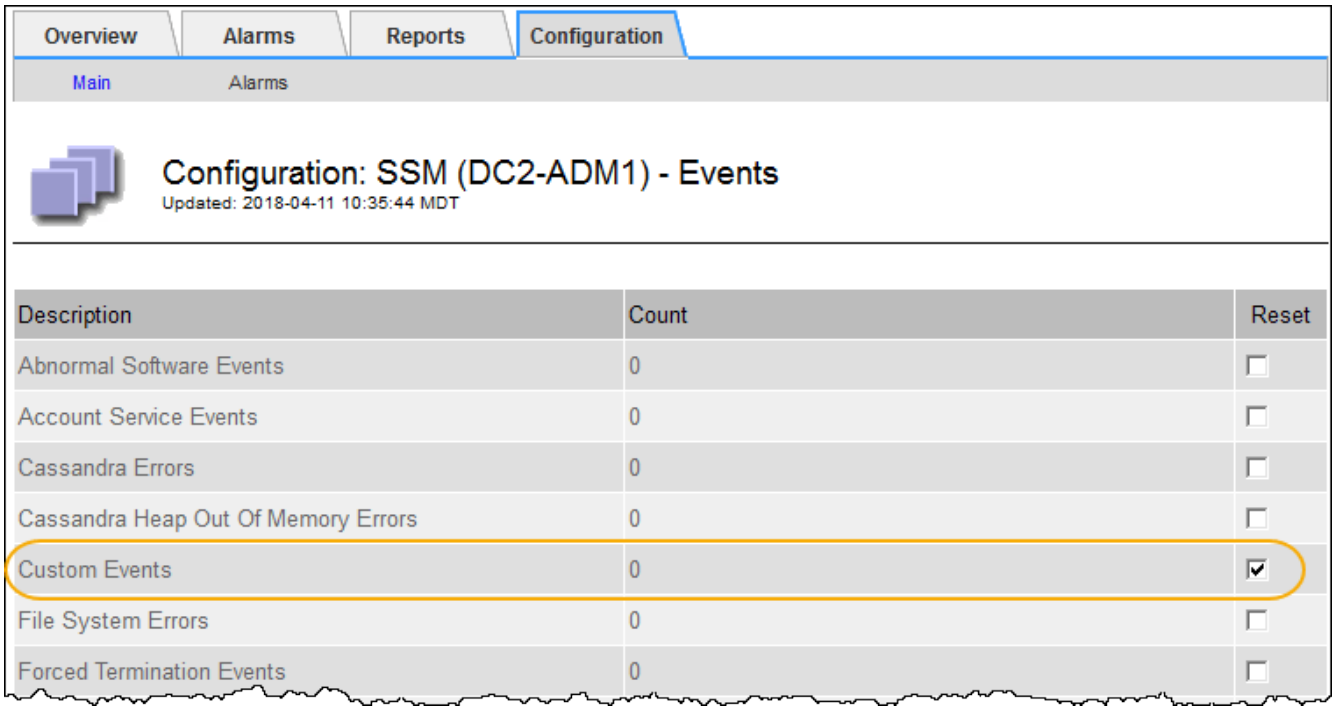

#### Reset the count of custom events to zero

If you want to reset the counter only for custom events, you must use the Grid Topology page in the Support menu.

### About this task

Resetting a counter causes the alarm to be triggered by the next event. In contrast, when you acknowledge an alarm, that alarm is only re-triggered if the next threshold level is reached.

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Select ***grid node*** > **SSM** > **Events** > **Configuration** > **Main**.
3. Select the **Reset** check box for Custom Events.




4. Select **Apply Changes**.

**Review audit messages**

Audit messages can help you get a better understanding of the detailed operations of your StorageGRID system. You can use audit logs to troubleshoot issues and to evaluate performance.

During normal system operation, all StorageGRID services generate audit messages, as follows:

- System audit messages are related to the auditing system itself, grid node states, system-wide task activity, and service backup operations.
- Object storage audit messages are related to the storage and management of objects within StorageGRID, including object storage and retrievals, grid-node to grid-node transfers, and verifications.
- Client read and write audit messages are logged when an S3 or Swift client application makes a request to create, modify, or retrieve an object.
- Management audit messages log user requests to the Management API.

Each Admin Node stores audit messages in text files. The audit share contains the active file (audit.log) as well as compressed audit logs from previous days. Each node in the grid also stores a copy of the audit information generated on the node.

For easy access to audit logs, you can configure client access to the audit share for both NFS and CIFS (CIFS is deprecated). You can also access audit log files directly from the command line of the Admin Node.

Optionally, you can change the destination of audit logs and send audit information to an external syslog server. Local logs of audit records continue to be generated and stored when an external syslog server is configured. See Configure audit messages and log destinations.

For details on the audit log file, the format of audit messages, the types of audit messages, and the tools available to analyze audit messages, see the instructions for audit messages. To learn how to configure audit

client access, see the instructions for administering StorageGRID.

**Related information**

Review audit logs

Administer StorageGRID

### Collect log files and system data

You can use the Grid Manager to retrieve log files and system data (including configuration data) for your StorageGRID system.

**What you'll need**

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

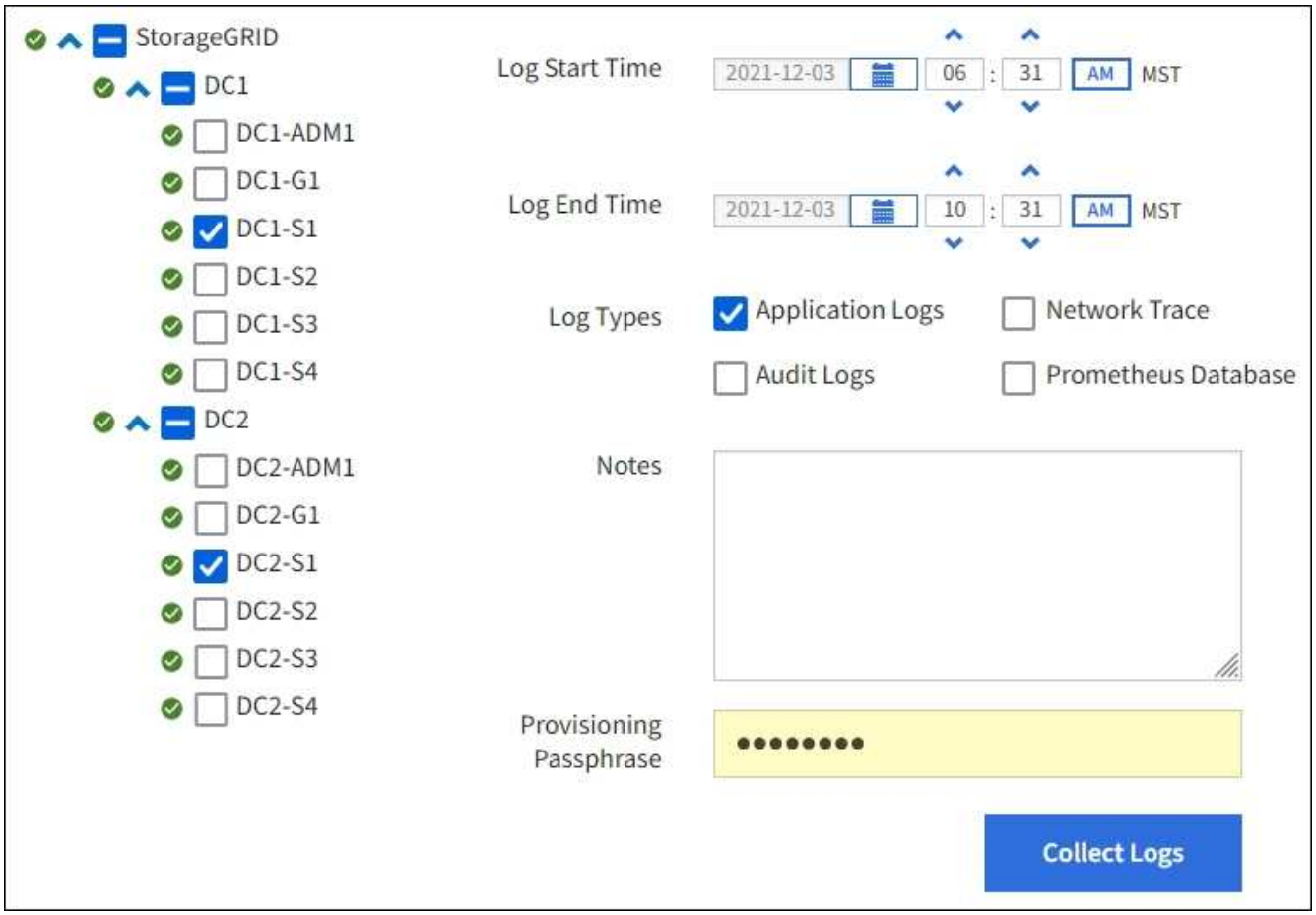
**About this task**

You can use the Grid Manager to gather log files, system data, and configuration data from any grid node for the time period that you select. Data is collected and archived in a .tar.gz file that you can then download to your local computer.

Optionally, you can change the destination of audit logs and send audit information to an external syslog server. Local logs of audit records continue to be generated and stored when an external syslog server is configured. See Configure audit messages and log destinations.

**Steps**

1. Select **SUPPORT** > **Tools** > **Logs**.




2. Select the grid nodes for which you want to collect log files.

   As required, you can collect log files for the entire grid or an entire data center site.

3. Select a **Start Time** and **End Time** to set the time range of the data to be included in the log files.

   If you select a very long time period or collect logs from all nodes in a large grid, the log archive could become too large to be stored on a node, or too large to be collected to the primary Admin Node for download. If this occurs, you must restart log collection with a smaller set of data.

4. Select the types of logs you want to collect.
   - **Application Logs**: Application-specific logs that technical support uses most frequently for troubleshooting. The logs collected are a subset of the available application logs.
   - **Audit Logs**: Logs containing the audit messages generated during normal system operation.
   - **Network Trace**: Logs used for network debugging.
   - **Prometheus Database**: Time series metrics from the services on all nodes.
5. Optionally, enter notes about the log files you are gathering in the **Notes** text box.

   You can use these notes to give technical support information about the problem that prompted you to collect the log files. Your notes are added to a file called `info.txt`, along with other information about the log file collection. The `info.txt` file is saved in the log file archive package.

6. Enter the provisioning passphrase for your StorageGRID system in the **Provisioning Passphrase** text box.

7. Select **Collect Logs**.

   When you submit a new request, the previous collection of log files is deleted.

   You can use the Logs page to monitor the progress of log file collection for each grid node.

   If you receive an error message about log size, try collecting logs for a shorter time period or for fewer nodes.

8. Select **Download** when log file collection is complete.

   The *.tar.gz* file contains all log files from all grid nodes where log collection was successful. Inside the combined *.tar.gz* file, there is one log file archive for each grid node.

#### After you finish

You can re-download the log file archive package later if you need to.

Optionally, you can select **Delete** to remove the log file archive package and free up disk space. The current log file archive package is automatically removed the next time you collect log files.

### Manually trigger an AutoSupport message

To assist technical support in troubleshooting issues with your StorageGRID system, you can manually trigger an AutoSupport message to be sent.

#### What you'll need

- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Root Access or Other Grid Configuration permission.

#### Steps

1. Select **SUPPORT** > **Tools** > **AutoSupport**.

   The AutoSupport page appears with the **Settings** tab selected.

2. Select **Send User-Triggered AutoSupport**.

   StorageGRID attempts to send an AutoSupport message to technical support. If the attempt is successful, the **Most Recent Result** and **Last Successful Time** values on the **Results** tab are updated. If there is a problem, the **Most Recent Result** value updates to "Failed," and StorageGRID does not try to send the AutoSupport message again.

   > After sending an User-triggered AutoSupport message, refresh the AutoSupport page in your browser after 1 minute to access the most recent results.

#### Related information

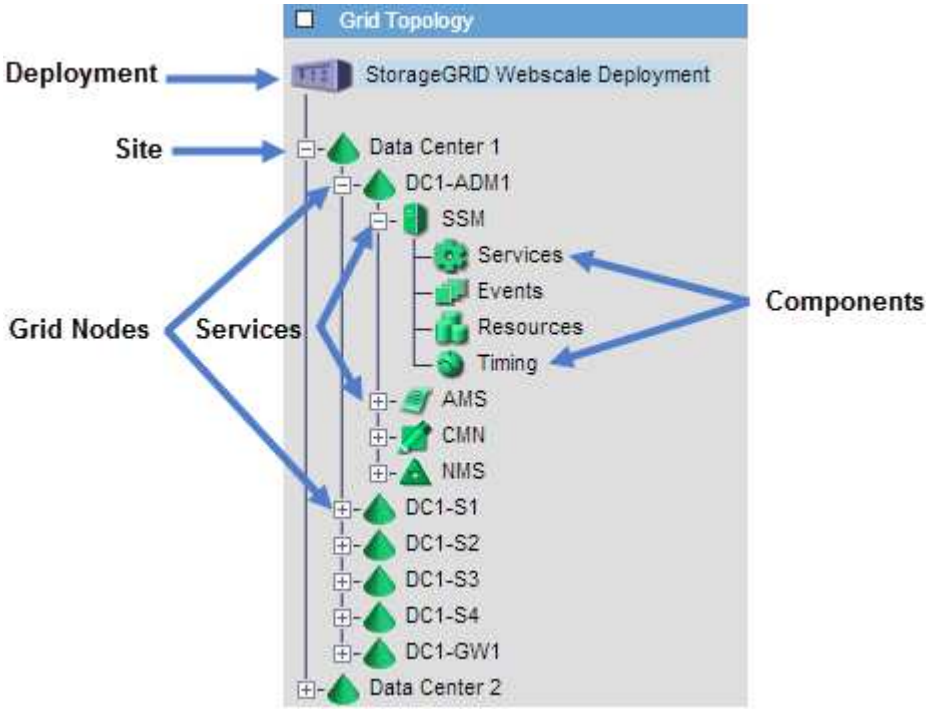
Configure email server settings for alarms (legacy system)

### View the Grid Topology tree

The Grid Topology tree provides access to detailed information about StorageGRID system elements, including sites, grid nodes, services, and components. In most cases,

you only need to access the Grid Topology tree when instructed in the documentation or when working with technical support.

To access the Grid Topology tree, select **SUPPORT** > **Tools** > **Grid topology**.




To expand or collapse the Grid Topology tree, click ⊞ or ⊟ at the site, node, or service level. To expand or collapse all items in the entire site or in each node, hold down the **<Ctrl>** key and click.

### Review support metrics

When troubleshooting an issue, you can work with technical support to review detailed metrics and charts for your StorageGRID system.

#### What you'll need

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

#### About this task

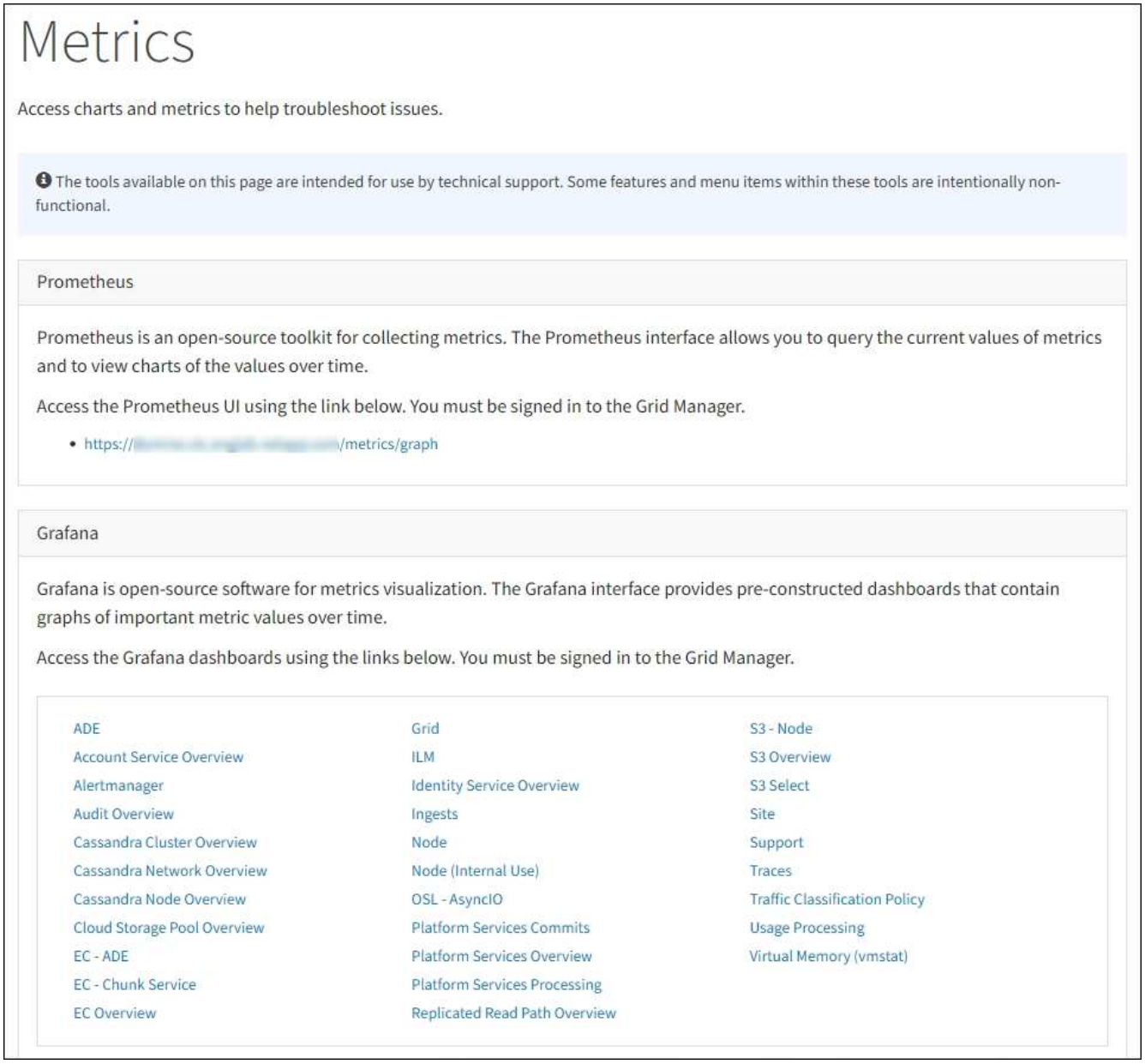
The Metrics page allows you to access the Prometheus and Grafana user interfaces. Prometheus is open-source software for collecting metrics. Grafana is open-source software for metrics visualization.

> The tools available on the Metrics page are intended for use by technical support. Some features and menu items within these tools are intentionally non-functional and are subject to change. See the list of commonly used Prometheus metrics.

#### Steps

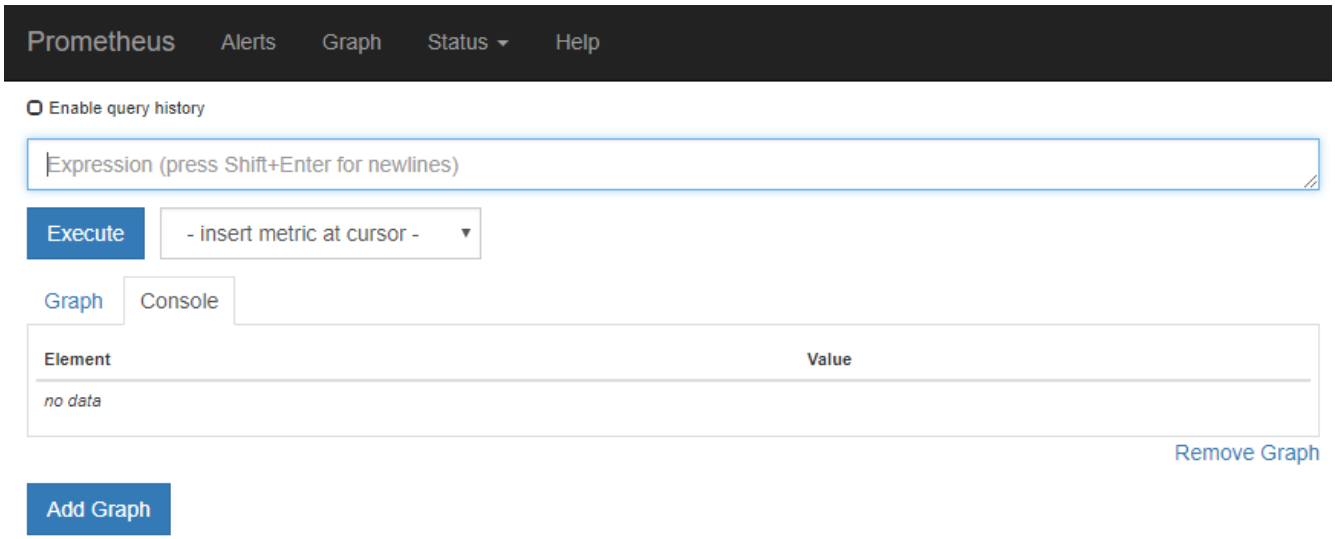
1. As directed by technical support, select **SUPPORT** > **Tools** > **Metrics**.

   An example of the Metrics page is shown here:




2. To query the current values of StorageGRID metrics and to view graphs of the values over time, click the link in the Prometheus section.

   The Prometheus interface appears. You can use this interface to execute queries on the available StorageGRID metrics and to graph StorageGRID metrics over time.




> Metrics that include *private* in their names are intended for internal use only and are subject to change between StorageGRID releases without notice.

3. To access pre-constructed dashboards containing graphs of StorageGRID metrics over time, click the links in the Grafana section.

   The Grafana interface for the link you selected appears.

### Run diagnostics

When troubleshooting an issue, you can work with technical support to run diagnostics on your StorageGRID system and review the results.

- Review support metrics
- Commonly used Prometheus metrics

#### What you'll need

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

#### About this task

The Diagnostics page performs a set of diagnostic checks on the current state of the grid. Each diagnostic check can have one of three statuses:

-

- **Normal**: All values are within the normal range.
- **Attention**: One or more of the values are outside of the normal range.
- **Caution**: One or more of the values are significantly outside of the normal range.

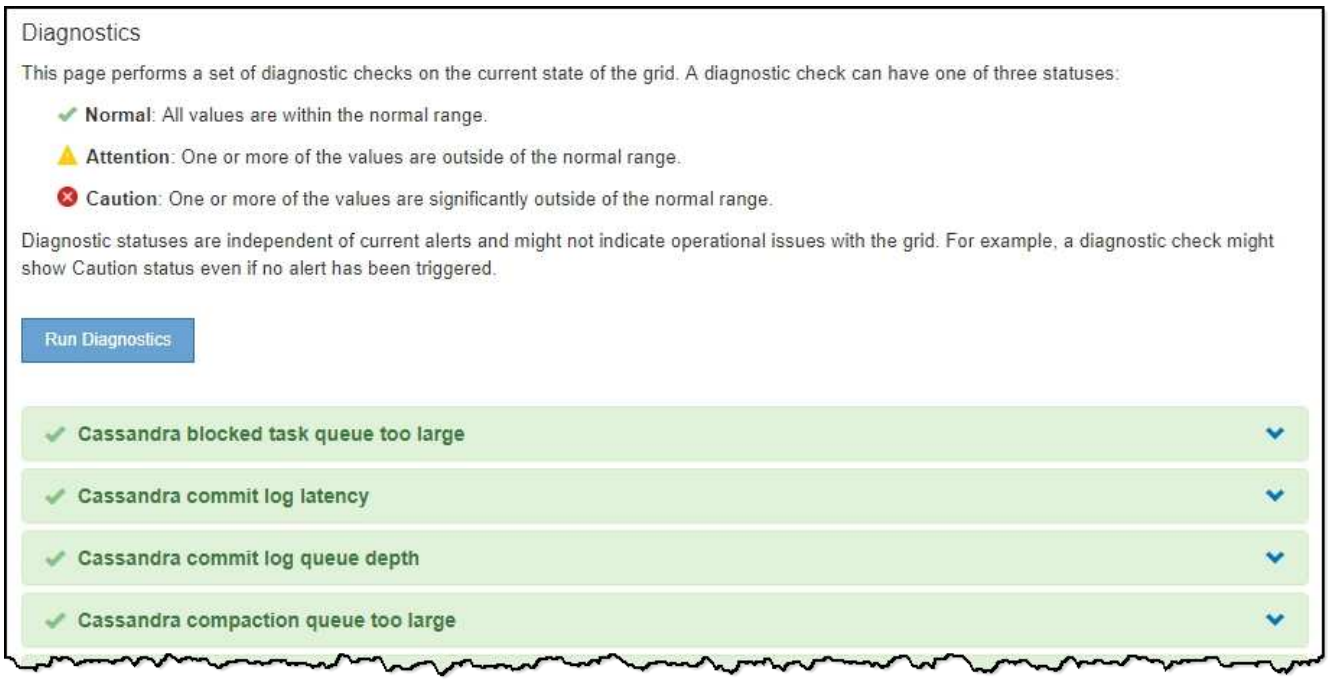
Diagnostic statuses are independent of current alerts and might not indicate operational issues with the grid. For example, a diagnostic check might show Caution status even if no alert has been triggered.

**Steps**

1. Select **SUPPORT** > **Tools** > **Diagnostics**.

   The Diagnostics page appears and lists the results for each diagnostic check. The results are sorted by severity (Caution, Attention, and then Normal). Within each severity, the results are sorted alphabetically.

   In this example, all diagnostics have a Normal status.




2. To learn more about a specific diagnostic, click anywhere in the row.

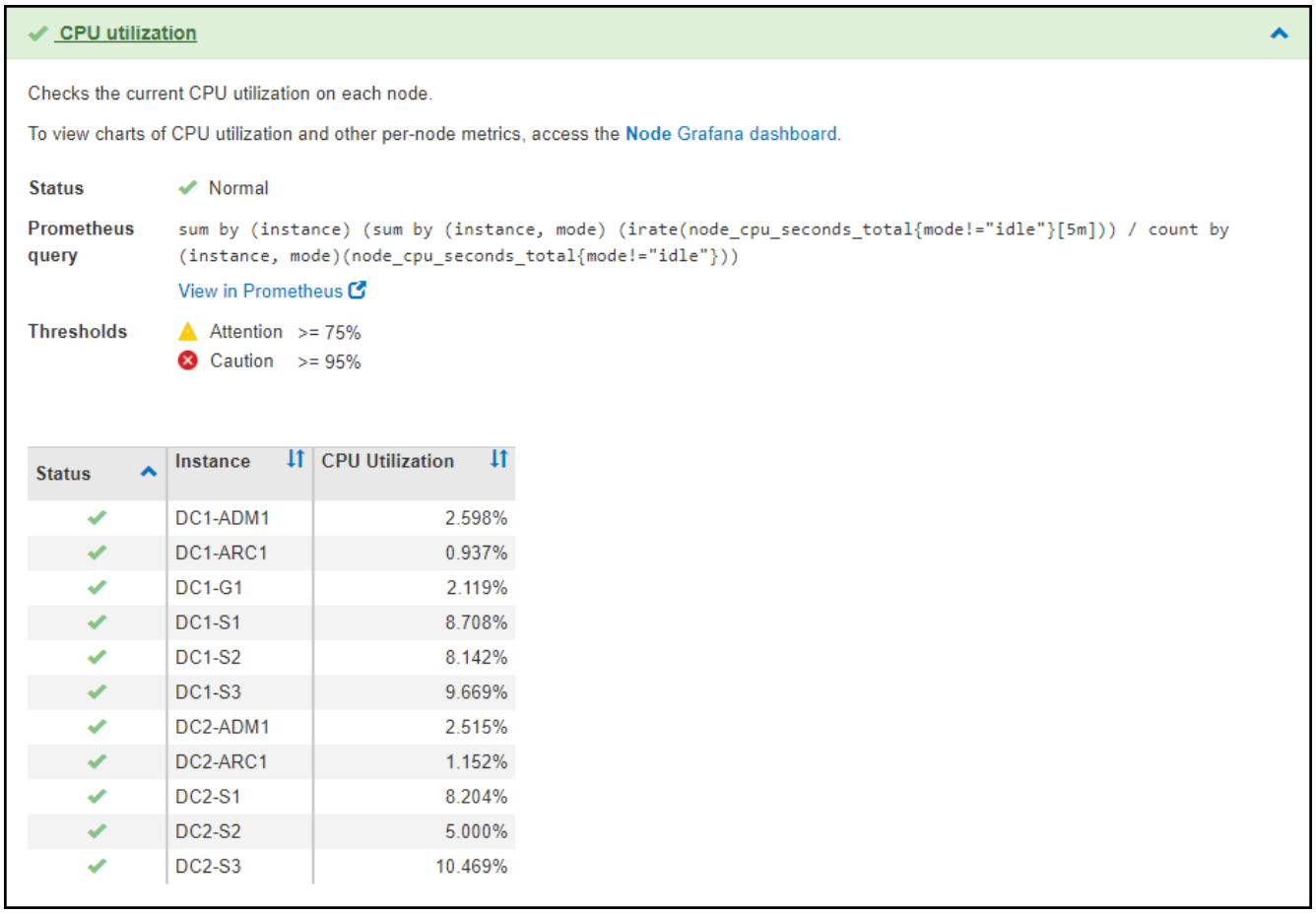
   Details about the diagnostic and its current results appear. The following details are listed:

   - **Status**: The current status of this diagnostic: Normal, Attention, or Caution.
   - **Prometheus query**: If used for the diagnostic, the Prometheus expression that was used to generate the status values. (A Prometheus expression is not used for all diagnostics.)
   - **Thresholds**: If available for the diagnostic, the system-defined thresholds for each abnormal diagnostic status. (Threshold values are not used for all diagnostics.)

     You cannot change these thresholds.

   - **Status values**: A table showing the status and the value of the diagnostic throughout the StorageGRID system. In this example, the current CPU utilization for every node in a StorageGRID system is shown. All node values are below the Attention and Caution thresholds, so the overall status of the diagnostic

is Normal.



CPU utilization

Checks the current CPU utilization on each node.

To view charts of CPU utilization and other per-node metrics, access the **Node** Grafana dashboard.

**Status** Normal

**Prometheus query**

```
sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode)(node_cpu_seconds_total{mode!="idle"}))
```

View in Prometheus

**Thresholds** Attention >= 75%
Caution >= 95%

| Status | Instance | CPU Utilization |
|---|---|---|
| ✔ | DC1-ADM1 | 2.598% |
| ✔ | DC1-ARC1 | 0.937% |
| ✔ | DC1-G1 | 2.119% |
| ✔ | DC1-S1 | 8.708% |
| ✔ | DC1-S2 | 8.142% |
| ✔ | DC1-S3 | 9.669% |
| ✔ | DC2-ADM1 | 2.515% |
| ✔ | DC2-ARC1 | 1.152% |
| ✔ | DC2-S1 | 8.204% |
| ✔ | DC2-S2 | 5.000% |
| ✔ | DC2-S3 | 10.469% |

3. **Optional**: To see Grafana charts related to this diagnostic, click the **Grafana dashboard** link.

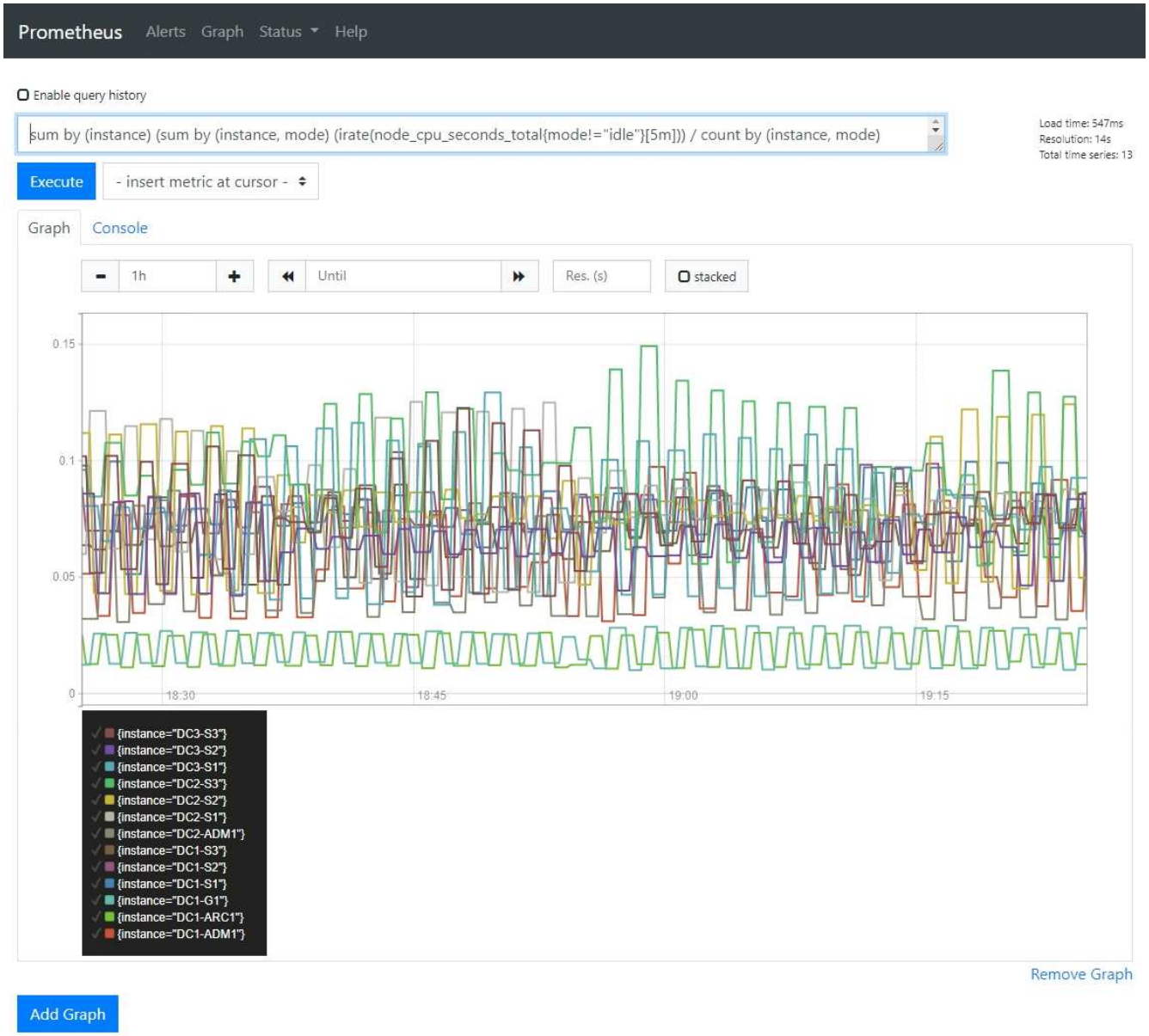
   This link is not displayed for all diagnostics.

   The related Grafana dashboard appears. In this example, the Node dashboard appears showing CPU Utilization over time for this node as well as other Grafana charts for the node.

   > You can also access the pre-constructed Grafana dashboards from the Grafana section of the **SUPPORT** > **Tools** > **Metrics** page.

4. **Optional**: To see a chart of the Prometheus expression over time, click **View in Prometheus**.

   A Prometheus graph of the expression used in the diagnostic appears.




### Create custom monitoring applications

You can build custom monitoring applications and dashboards using the StorageGRID metrics available from the Grid Management API.

If you want to monitor metrics that are not displayed on an existing page of the Grid Manager, or if you want to create custom dashboards for StorageGRID, you can use the Grid Management API to query StorageGRID metrics.

You can also access Prometheus metrics directly with an external monitoring tool, such as Grafana. Using an external tool requires that you upload or generate an administrative client certificate to allow StorageGRID to authenticate the tool for security. See the instructions for administering StorageGRID.

To view the metrics API operations, including the complete list of the metrics that are available, go to the Grid Manager. From the top of the page, select the help icon and select **API Documentation** > **metrics**.

**metrics** Operations on metrics

| | | |
|---|---|---|
| GET | `/grid/metric-labels/{label}/values` | Lists the values for a metric label |
| GET | `/grid/metric-names` | Lists all available metric names |
| GET | `/grid/metric-query` | Performs an instant metric query at a single point in time |
| GET | `/grid/metric-query-range` | Performs a metric query over a range of time |

The details of how to implement a custom monitoring application are beyond the scope of this documentation.

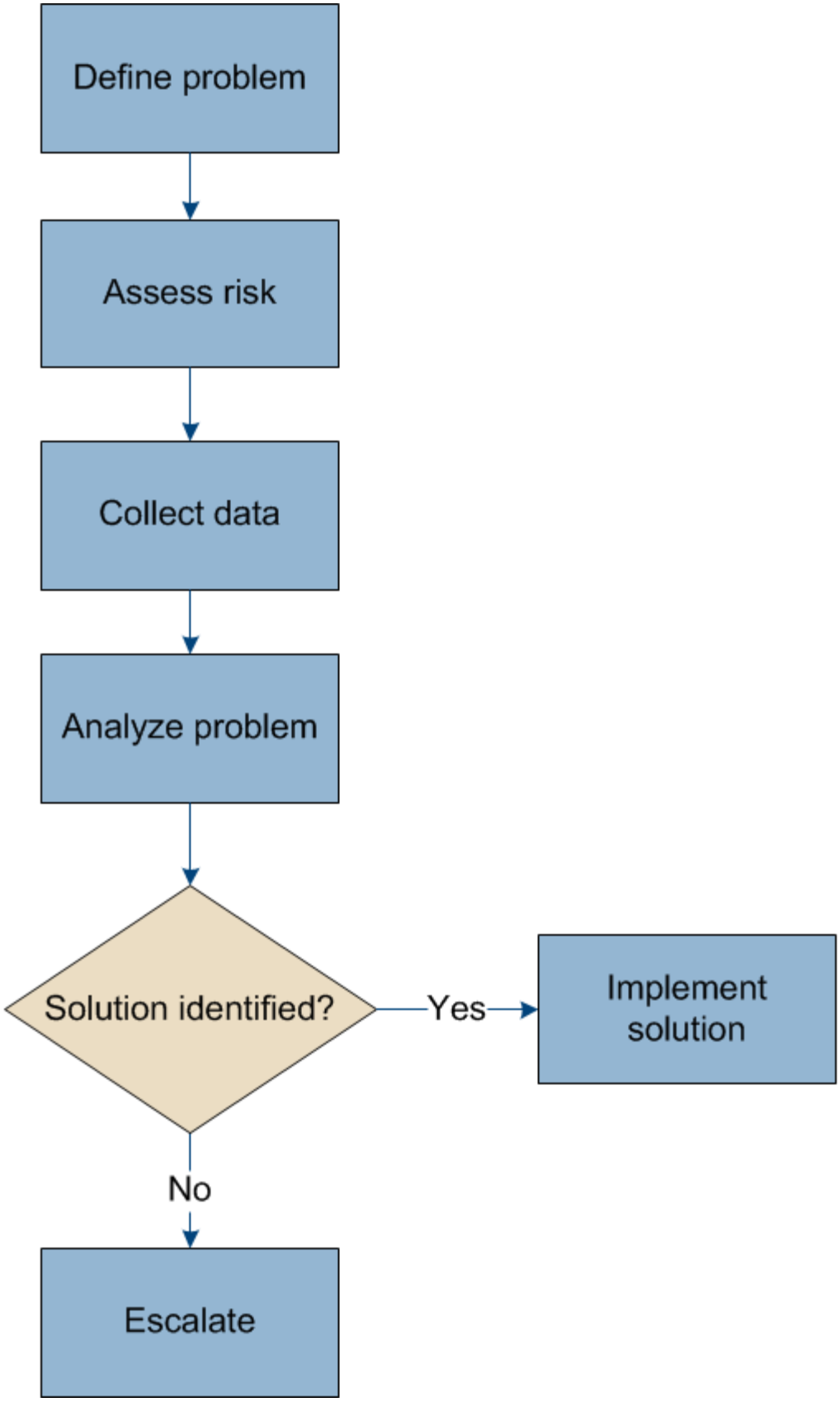
## Troubleshoot a StorageGRID system

### Troubleshoot a StorageGRID system

If you encounter a problem when using a StorageGRID system, refer to the tips and guidelines in this section for help in determining and resolving the issue.

#### Overview of problem determination

If you encounter a problem when administering a StorageGRID system, you can use the process outlined in this figure to identify and analyze the issue. In many cases, you can resolve problems on your own; however, you might need to escalate some issues to technical support.




**Define the problem**

The first step to solving a problem is to define the problem clearly.

This table provides examples of the types of information that you might collect to define a problem:

| Question | Sample response |
|---|---|
| What is the StorageGRID system doing or not doing? What are its symptoms? | Client applications are reporting that objects cannot be ingested into StorageGRID. |
| When did the problem start? | Object ingest was first denied at about 14:50 on January 8, 2020. |
| How did you first notice the problem? | Notified by client application. Also received alert email notifications. |
| Does the problem happen consistently, or only sometimes? | Problem is ongoing. |
| If the problem happens regularly, what steps cause it to occur | Problem happens every time a client tries to ingest an object. |
| If the problem happens intermittently, when does it occur? Record the times of each incident that you are aware of. | Problem is not intermittent. |
| Have you seen this problem before? How often have you had this problem in the past? | This is the first time I have seen this issue. |

### Assess the risk and impact on the system

After you have defined the problem, assess its risk and impact on the StorageGRID system. For example, the presence of critical alerts does not necessarily mean that the system is not delivering core services.

This table summarizes the impact the example problem is having on system operations:

| Question | Sample response |
|---|---|
| Can the StorageGRID system ingest content? | No. |
| Can client applications retrieve content? | Some objects can be retrieved and others cannot. |
| Is data at risk? | No. |
| Is the ability to conduct business severely affected? | Yes, because client applications cannot store objects to the StorageGRID system and data cannot be retrieved consistently. |

### Collect data

After you have defined the problem and have assessed its risk and impact, collect data for analysis. The type of data that is most useful to collect depends upon the nature of the problem.

| Type of data to collect | Why collect this dat | Instructions |
| --- | --- | --- |
| Create timeline of recent changes | Changes to your StorageGRID system, its configuration, or its environment can cause new behavior. | • Create a timeline of recent changes |
| Review alerts and alarms | Alerts and alarms can help you quickly determine the root cause of a problem by providing important clues as to the underlying issues that might be causing it.<br><br>Review the list of current alerts and alarms to see if StorageGRID has identified the root cause of a problem for you.<br><br>Review alerts and alarms triggered in the past for additional insights. | • View current alerts<br>• View legacy alarms<br>• View resolved alerts<br>• Review historical alarms and alarm frequency (legacy system) |
| Monitor events | Events include any system error or fault events for a node, including errors such as network errors. Monitor events to learn more about issues or to help with troubleshooting. | • Monitor events |
| Identify trends using charts and text reports | Trends can provide valuable clues about when issues first appeared, and can help you understand how quickly things are changing. | • Use charts and graphs<br>• Use text reports |
| Establish baselines | Collect information about the normal levels of various operational values. These baseline values, and deviations from these baselines, can provide valuable clues. | • Establish baselines |
| Perform ingest and retrieval tests | To troubleshoot performance issues with ingest and retrieval, use a workstation to store and retrieve objects. Compare results against those seen when using the client application. | • Monitor PUT and GET performance |
| Review audit messages | Review audit messages to follow StorageGRID operations in detail. The details in audit messages can be useful for troubleshooting many types of issues, including performance issues. | • Review audit messages |
| Check object locations and storage integrity | If you are having storage problems, verify that objects are being placed where you expect. Check the integrity of object data on a Storage Node. | • Monitor object verification operations<br>• Confirm object data locations<br>• Verify object integrity |

| Type of data to collect | Why collect this dat | Instructions |
| --- | --- | --- |
| Collect data for technical support | Technical support might ask you to collect data or review specific information to help troubleshoot issues. | • Collect log files and system data<br>• Manually trigger an AutoSupport message<br>• Review support metrics |

### Create a timeline of recent changes

When a problem occurs, you should consider what has changed recently and when those changes occurred.

- Changes to your StorageGRID system, its configuration, or its environment can cause new behavior.
- A timeline of changes can help you identify which changes might be responsible for an issue, and how each change might have affected its development.

Create a table of recent changes to your system that includes information about when each change occurred and any relevant details about the change, such information about what else was happening while the change was in progress:

| Time of change | Type of change | Details |
| --- | --- | --- |
| For example:<br>• When did you start the node recovery?<br>• When did the software upgrade complete?<br>• Did you interrupt the process? | What happened? What did you do? | Document any relevant details about the change. For example:<br>• Details of the network changes.<br>• Which hotfix was installed.<br>• How client workloads changed.<br>Make sure to note if more than one change was happening at the same time. For example, was this change made while an upgrade was in progress? |

#### Examples of significant recent changes

Here are some examples of potentially significant changes:

- Was the StorageGRID system recently installed, expanded, or recovered?
- Has the system been upgraded recently? Was a hotfix applied?
- Has any hardware been repaired or changed recently?
- Has the ILM policy been updated?
- Has the client workload changed?
- Has the client application or its behavior changed?
- Have you changed load balancers, or added or removed a high availability group of Admin Nodes or Gateway Nodes?

- Have any tasks been started that might take a long time to complete? Examples include:
  - Recovery of a failed Storage Node
  - Storage Node decommissioning
- Have any changes been made to user authentication, such as adding a tenant or changing LDAP configuration?
- Is data migration taking place?
- Were platform services recently enabled or changed?
- Was compliance enabled recently?
- Have Cloud Storage Pools been added or removed?
- Have any changes been made to storage compression or encryption?
- Have there been any changes to the network infrastructure? For example, VLANs, routers, or DNS.
- Have any changes been made to NTP sources?
- Have any changes been made to the Grid, Admin, or Client Network interfaces?
- Have any configuration changes been made to the Archive Node?
- Have any other changes been made to the StorageGRID system or its environment?

### Establish baselines

You can establish baselines for your system by recording the normal levels of various operational values. In the future, you can compare current values to these baselines to help detect and resolve abnormal values.

| Property | Value | How to obtain |
|---|---|---|
| Average storage consumption | GB consumed/day<br><br>Percent consumed/day | Go to the Grid Manager. On the Nodes page, select the entire grid or a site and go to the Storage tab.<br><br>On the Storage Used - Object Data chart, find a period where the line is fairly stable. Hover your cursor over the chart to estimate how much storage is consumed each day<br><br>You can collect this information for the entire system or for a specific data center. |

| Property | Value | How to obtain |
| --- | --- | --- |
| Average metadata consumption | GB consumed/day<br><br>Percent consumed/day | Go to the Grid Manager. On the Nodes page, select the entire grid or a site and go to the Storage tab.<br><br>On the Storage Used - Object Metadata chart, find a period where the line is fairly stable. Hover your cursor over the chart to estimate how much metadata storage is consumed each day<br><br>You can collect this information for the entire system or for a specific data center. |
| Rate of S3/Swift operations | Operations/second | Go to the Dashboard in the Grid Manager. In the Protocol Operations section, view the values for S3 rate and the Swift rate.<br><br>To see ingest and retrieval rates and counts for a specific site or node, select **NODES** > ***site or Storage Node*** > **Objects**. Hover your cursor over the Ingest and Retrieve chart for S3 or Swift. |
| Failed S3/Swift operations | Operations | Select **SUPPORT** > **Tools** > **Grid topology**. On the Overview tab in the API Operations section, view the value for S3 Operations - Failed or Swift Operations - Failed. |
| ILM evaluation rate | Objects/second | From the Nodes page, select ***grid*** > **ILM**.<br><br>On the ILM Queue chart, find a period where the line is fairly stable. Hover your cursor over the chart to estimate a baseline value for **Evaluation rate** for your system. |
| ILM scan rate | Objects/second | Select **NODES** > ***grid*** > **ILM**.<br><br>On the ILM Queue chart, find a period where the line is fairly stable. Hover your cursor over the chart to estimate a baseline value for **Scan rate** for your system. |

| Property | Value | How to obtain |
| --- | --- | --- |
| Objects queued from client operations | Objects/second | Select **NODES** > ***grid*** > **ILM**.<br><br>On the ILM Queue chart, find a period where the line is fairly stable. Hover your cursor over the chart to estimate a baseline value for **Objects queued (from client operations)** for your system. |
| Average query latency | Milliseconds | Select **NODES** > ***Storage Node*** > **Objects**. In the Queries table, view the value for Average Latency. |

### 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.

### Escalation information checklist

If you cannot resolve the problem on your own, contact technical support. Before contacting technical support, gather the information listed in the following table to facilitate problem resolution.

| ✔ | Item | Notes |
| --- | --- | --- |
| | Problem statement | What are the problem symptoms? When did the problem start? Does it happen consistently or intermittently? If intermittently, what times has it occurred?<br><br>Define the problem |
| | Impact assessment | What is the severity of the problem? What is the impact to the client application?<br><br>• Has the client connected successfully before?<br>• Can the client ingest, retrieve, and delete data? |
| | StorageGRID System ID | Select **MAINTENANCE** > **System** > **License**. The StorageGRID System ID is shown as part of the current license. |

| ✓ | Item | Notes |
|---|---|---|
| | Software version | From the top of the Grid Manager, select the help icon and select **About** to see the StorageGRID version. |
| | Customization | Summarize how your StorageGRID system is configured. For example, list the following:<br>• Does the grid use storage compression, storage encryption, or compliance?<br>• Does ILM make replicated or erasure coded objects? Does ILM ensure site redundancy? Do ILM rules use the Strict, Balanced, or Dual Commit ingest behaviors? |
| | Log files and system data | Collect log files and system data for your system. Select **SUPPORT** > **Tools** > **Logs**.<br><br>You can collect logs for the entire grid, or for selected nodes.<br><br>If you are collecting logs only for selected nodes, be sure to include at least one Storage Node that has the ADC service. (The first three Storage Nodes at a site include the ADC service.)<br><br>Collect log files and system data |
| | Baseline information | Collect baseline information regarding ingest operations, retrieval operations, and storage consumption.<br><br>Establish baselines |
| | Timeline of recent changes | Create a timeline that summarizes any recent changes to the system or its environment.<br><br>Create a timeline of recent changes |
| | History of efforts to diagnose the issue | If you have taken steps to diagnose or troubleshoot the issue yourself, make sure to record the steps you took and the outcome. |

## Troubleshoot object and storage issues

### Confirm object data locations

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.

**What you'll need**

- You must have an object identifier, which can be one of:
  - **UUID**: The object's Universally Unique Identifier. Enter the UUID in all uppercase.
  - **CBID**: The object's unique identifier within StorageGRID . You can obtain an object's CBID from the audit log. Enter the CBID in all uppercase.
  - **S3 bucket and object key**: When an object is ingested through the S3 interface, the client application uses a bucket and object key combination to store and identify the object.
  - **Swift container and object name**: When an object is ingested through the Swift interface, the client application uses a container and object name combination to store and identify the object.

**Steps**

1. Select **ILM** > **Object metadata lookup**.
2. Type the object's identifier in the **Identifier** field.

   You can enter a UUID, CBID, S3 bucket/object-key, or Swift container/object-name.

3. If you want to look up a specific version of the object, enter the version ID (optional).

4. Select **Look Up**.

   The object metadata lookup results appear. This page lists the following types of information:

   - System metadata, including the object ID (UUID), the version ID (optional), the object name, the name of the container, the tenant account name or ID, the logical size of the object, the date and time the object was first created, and the date and time the object was last modified.
   - Any custom user metadata key-value pairs associated with the object.
   - For S3 objects, any object tag key-value pairs associated with the object.
   - For replicated object copies, the current storage location of each copy.
   - For erasure-coded object copies, the current storage location of each fragment.
   - For object copies in a Cloud Storage Pool, the location of the object, including the name of the external bucket and the object's unique identifier.
   - For segmented objects and multipart objects, a list of object segments including segment identifiers and data sizes. For objects with more than 100 segments, only the first 100 segments are shown.

- All object metadata in the unprocessed, internal storage format. This raw metadata includes internal system metadata that is not guaranteed to persist from release to release.

  The following example shows the object metadata lookup results for an S3 test object that is stored as two replicated copies.

**System Metadata**

| | |
|---|---|
| Object ID | A12E96FF-B13F-4905-9E9E-45373F6E7DA8 |
| Name | testobject |
| Container | source |
| Account | t-1582139188 |
| Size | 5.24 MB |
| Creation Time | 2020-02-19 12:15:59 PST |
| Modified Time | 2020-02-19 12:15:59 PST |

**Replicated Copies**

| Node | Disk Path |
|---|---|
| 99-97 | /var/local/rangedb/2/p/06/0B/00nM8H$\|TFbnQQ}\|CV2E |
| 99-99 | /var/local/rangedb/1/p/12/0A/00nM8H$\|TFboW28\|CXG% |

**Raw Metadata**


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


**Related information**

Manage objects with ILM

Use S3

Use Swift

#### Object store (storage volume) failures

The underlying storage on a Storage Node is divided into object stores. Object stores are also known as storage volumes.

You can view object store information for each Storage Node. Object stores are shown at the bottom of the **NODES** > ***Storage Node*** > **Storage** page.

## Disk devices

| Name | World Wide Name | I/O load | Read rate | Write rate |
|---|---|---|---|---|
| sdc(8:16,sdb) | N/A | 0.05% | 0 bytes/s | 4 KB/s |
| sde(8:48,sdd) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |
| sdf(8:64,sde) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |
| sdg(8:80,sdf) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |
| sdd(8:32,sdc) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |
| croot(8:1,sda1) | N/A | 0.04% | 0 bytes/s | 4 KB/s |
| cvloc(8:2,sda2) | N/A | 0.95% | 0 bytes/s | 52 KB/s |

## Volumes

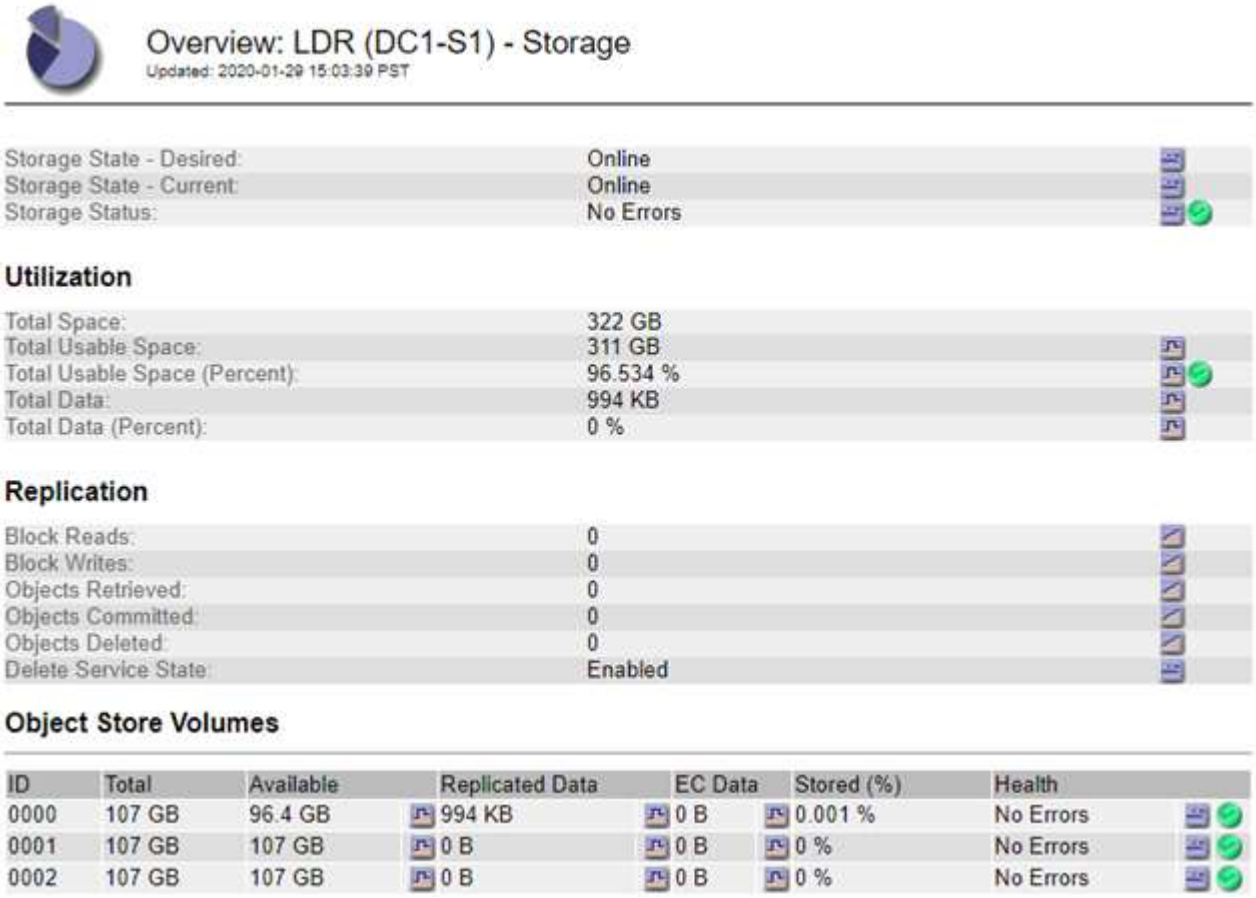
| Mount point | Device | Status | Size | Available | Write cache status |
|---|---|---|---|---|---|
| / | croot | Online | 21.00 GB | 14.73 GB | Unknown |
| /var/local | cvloc | Online | 85.86 GB | 80.94 GB | Unknown |
| /var/local/rangedb/0 | sdc | Online | 107.32 GB | 107.17 GB | Enabled |
| /var/local/rangedb/1 | sdd | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/2 | sde | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/3 | sdf | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/4 | sdg | Online | 107.32 GB | 107.18 GB | Enabled |

## Object stores

| ID | Size | Available | Replicated data | EC data | Object data (%) | Health |
|---|---|---|---|---|---|---|
| 0000 | 107.32 GB | 96.44 GB | 1.55 MB | 0 bytes | 0.00% | No Errors |
| 0001 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0002 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0003 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0004 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |

To see more details about each Storage Node, follow these steps:

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Select ***site*** > ***Storage Node*** > **LDR** > **Storage** > **Overview** > **Main**.




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 go to the **Configuration** tab and place the Storage Node in a read-only state so that the StorageGRID system can use it for data retrieval while you prepare for a full recovery of the server.

**Related information**

Recover and maintain

#### Verify object integrity

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

There are two verification processes: background verification and object existence check (formerly called foreground verification). They work together to ensure data integrity. Background verification runs automatically, and continuously checks the correctness of object data. Object existence check can be triggered by a user to more quickly verify the existence (although not the correctness) of objects.

### What is background verification?

The background verification process automatically and continuously checks Storage Nodes for corrupt copies of object data, and automatically attempts to repair any issues that it finds.

Background verification checks the integrity of replicated objects and erasure-coded objects, as follows:

- **Replicated objects**: If the background verification process finds a replicated object that is corrupt, the corrupt copy is removed from its location and quarantined elsewhere on the Storage Node. Then, a new uncorrupted copy is generated and placed to satisfy the active ILM policy. The new copy might not be placed on the Storage Node that was used for the original copy.

  > Corrupt object data is quarantined rather than deleted from the system, so that it can still be accessed. For more information on accessing quarantined object data, contact technical support.

- **Erasure-coded objects**: If the background verification process detects that a fragment of an erasure-coded object is corrupt, StorageGRID automatically attempts to rebuild the missing fragment in place on the same Storage Node, using the remaining data and parity fragments. If the corrupted fragment cannot be rebuilt, an attempt is made to retrieve another copy of the object. If retrieval is successful, an ILM evaluation is performed to create a replacement copy of the erasure-coded object.

  The background verification process checks objects on Storage Nodes only. It does not check objects on Archive Nodes or in a Cloud Storage Pool. Objects must be older than four days to qualify for background verification.

Background verification runs at a continuous rate that is designed not to interfere with ordinary system activities. Background verification cannot be stopped. However you can increase the background verification rate to more quickly verify the contents of a Storage Node if you suspect a problem.

### Alerts and alarms (legacy) related to background verification

If the system detects a corrupt object that it cannot correct automatically (because the corruption prevents the object from being identified), the **Unidentified corrupt object detected** alert is triggered.

If background verification cannot replace a corrupted object because it cannot locate another copy, the **Objects lost** alert is triggered.

### Change the background verification rate

You can change the rate at which background verification checks replicated object data on a Storage Node if you have concerns about data integrity.

#### What you'll need

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

#### About this task

You can change the Verification Rate for background verification on a Storage Node:

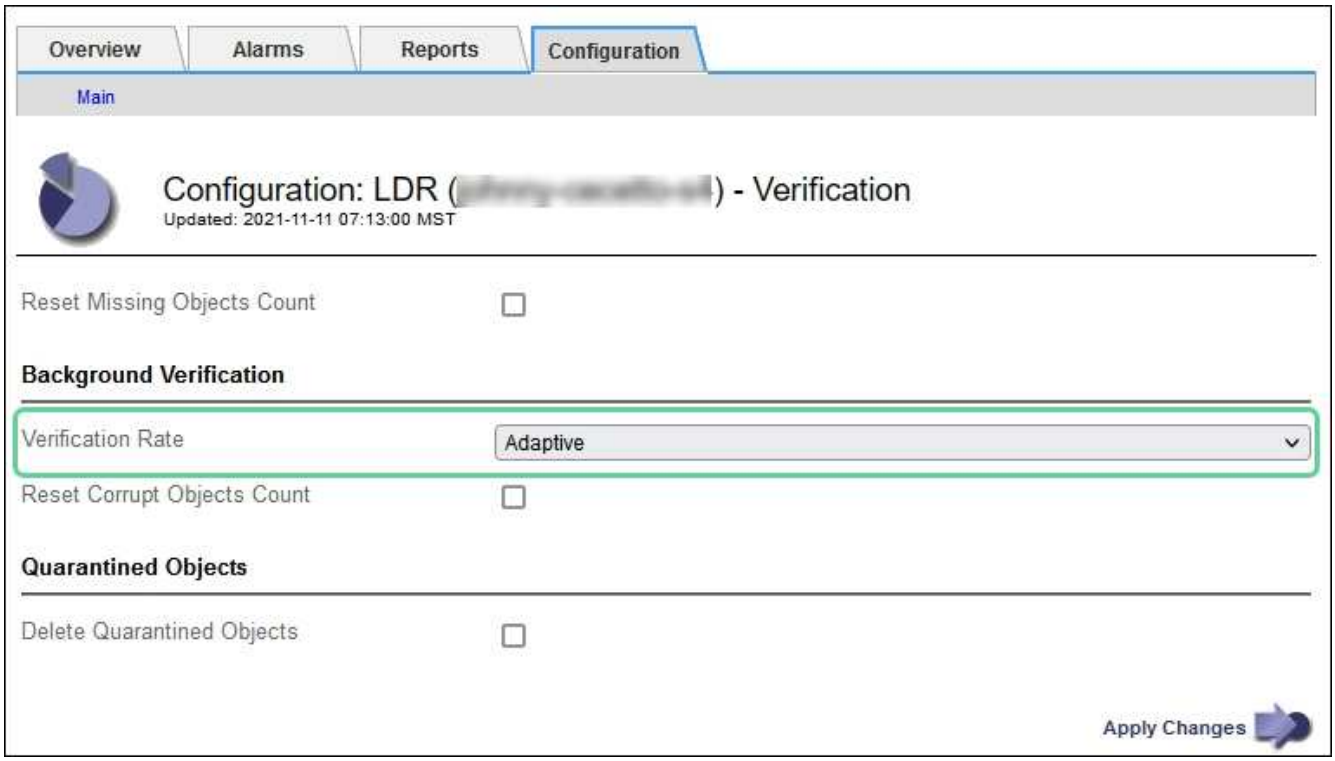
- Adaptive: Default setting. The task is designed to verify at a maximum of 4 MB/s or 10 objects/s (whichever is exceeded first).

- High: Storage verification proceeds quickly, at a rate that can slow ordinary system activities.

Use the High verification rate only when you suspect that a hardware or software fault might have corrupted object data. After the High priority background verification completes, the Verification Rate automatically resets to Adaptive.

**Steps**

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Select ***Storage Node*** > **LDR** > **Verification**.
3. Select **Configuration** > **Main**.
4. Go to **LDR** > **Verification** > **Configuration** > **Main**.
5. Under Background Verification, select **Verification Rate** > **High** or **Verification Rate** > **Adaptive**.




> Setting the Verification Rate to High triggers the VPRI (Verification Rate) legacy alarm at the Notice level.

6. Click **Apply Changes**.
7. Monitor the results of background verification for replicated objects.
   a. Go to **NODES** > ***Storage Node*** > **Objects**.
   b. In the Verification section, monitor the values for **Corrupt Objects** and **Corrupt Objects Unidentified**.

      If background verification finds corrupt replicated object data, the **Corrupt Objects** metric is incremented, and StorageGRID attempts to extract the object identifier from the data, as follows:

      - If the object identifier can be extracted, StorageGRID automatically creates a new copy of the object data. The new copy can be made anywhere in the StorageGRID system that satisfies the active ILM policy.

    - If the object identifier cannot be extracted (because it has been corrupted), the **Corrupt Objects Unidentified** metric is incremented, and the **Unidentified corrupt object detected** alert is triggered.

  c. If corrupt replicated object data is found, contact technical support to determine the root cause of the corruption.

8. Monitor the results of background verification for erasure-coded objects.

   If background verification finds corrupt fragments of erasure-coded object data, the Corrupt Fragments Detected attribute is incremented. StorageGRID recovers by rebuilding the corrupt fragment in place on the same Storage Node.

   a. Select **SUPPORT** > **Tools** > **Grid topology**.
   b. Select ***Storage Node*** > **LDR** > **Erasure Coding**.
   c. In the Verification Results table, monitor the Corrupt Fragments Detected (ECCD) attribute.

9. After corrupt objects have been automatically restored by the StorageGRID system, reset the count of corrupt objects.

   a. Select **SUPPORT** > **Tools** > **Grid topology**.
   b. Select ***Storage Node*** > **LDR** > **Verification** > **Configuration**.
   c. Select **Reset Corrupt Object Count**.
   d. Click **Apply Changes**.

10. If you are confident that quarantined objects are not required, you can delete them.

    > If the **Objects lost** alert or the LOST (Lost Objects) legacy alarm was triggered, technical support might want to access quarantined objects to help debug the underlying issue or to attempt data recovery.

    a. Select **SUPPORT** > **Tools** > **Grid topology**.
    b. Select ***Storage Node*** > **LDR** > **Verification** > **Configuration**.
    c. Select **Delete Quarantined Objects**.
    d. Select **Apply Changes**.

**What is object existence check?**

Object existence check verifies whether all expected replicated copies of objects and erasure-coded fragments exist on a Storage Node. Object existence check does not verify the object data itself (background verification does that); instead, it provides a way to verify the integrity of storage devices, especially if a recent hardware issue could have affected data integrity.

Unlike background verification, which occurs automatically, you must manually start an object existence check job.

Object existence check reads the metadata for every object stored in StorageGRID and verifies the existence of both replicated object copies and erasure-coded object fragments. Any missing data is handled as follows:

- **Replicated copies**: If a copy of replicated object data is missing, StorageGRID automatically attempts to replace the copy from a copy stored elsewhere in the system. The Storage Node runs an existing copy through an ILM evaluation, which will determine that the current ILM policy is no longer being met for this object because another copy is missing. A new copy is generated and placed to satisfy the system's active

ILM policy. This new copy might not be placed in the same location where the missing copy was stored.

- **Erasure-coded fragments**: If a fragment of an erasure-coded object is missing, StorageGRID automatically attempts to rebuild the missing fragment in place on the same Storage Node using the remaining fragments. If the missing fragment cannot be rebuilt (because too many fragments have been lost), ILM attempts to find another copy of the object, which it can use to generate a new erasure-coded fragment.

### Run object existence check

You create and run one object existence check job at a time. When you create a job, you select the Storage Nodes and volumes you want to verify. You also select the consistency control for the job.

#### What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have the Maintenance or Root Access permission.
- You have ensured that the Storage Nodes you want to check are online. Select **NODES** to view the table of nodes. Ensure that no alert icons appear next to the node name for the nodes you want to check.
- You have ensured that the following procedures are **not** running on the nodes you want to check:
  - Grid expansion to add a Storage Node
  - Storage Node decommission
  - Recovery of a failed storage volume
  - Recovery of a Storage Node with a failed system drive
  - EC rebalance
  - Appliance node clone

Object existence check does not provide useful information while these procedures are in progress.

#### About this task

An object existence check job can take days or weeks to complete, depending on the number of objects in the grid, the selected storage nodes and volumes, and the selected consistency control. You can run only one job at a time, but you can select multiple Storage Nodes and volumes at the same time.

#### Steps

1. Select **MAINTENANCE** > **Tasks** > **Object existence check**.
2. Select **Create job**. The Create an object existence check job wizard appears.
3. Select the nodes containing the volumes you want to verify. To select all online nodes, select the **Node name** check box in the column header.

   You can search by node name or site.

   You cannot select nodes that are not connected to the grid.

4. Select **Continue**.
5. Select one or more volumes for each node in the list. You can search for volumes using the storage volume number or node name.

   To select all volumes for each node you selected, select the **Storage volume** check box in the column header.

6. Select **Continue**.
7. Select the consistency control for the job.

   The consistency control determines how many copies of object metadata are used for the object existence check.

   - **Strong-site**: Two copies of metadata at a single site.
   - **Strong-global**: Two copies of metadata at each site.
   - **All** (default): All three copies of metadata at each site.

     For more information about consistency control, see the descriptions in the wizard.

8. Select **Continue**.
9. Review and verify your selections. You can select **Previous** to go to a previous step in the wizard to update your selections.

   An Object existence check job is generated and runs until one of the following occurs:

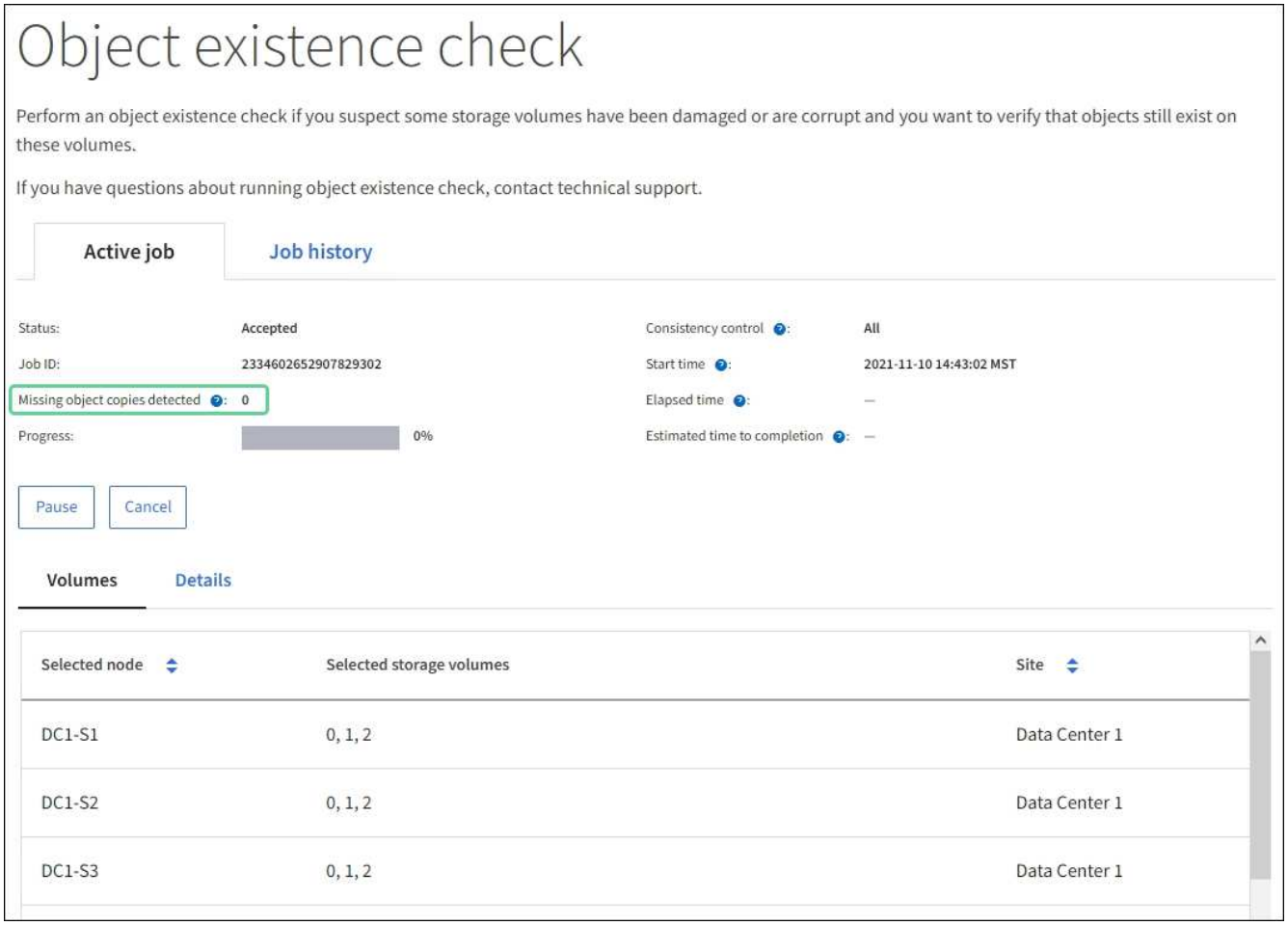
   - The job completes.
   - You pause or cancel the job. You can resume a job that you have paused, but you cannot resume a job that you have canceled.
   - The job stalls. The **Object existence check has stalled** alert is triggered. Follow the corrective actions specified for the alert.
   - The job fails. The **Object existence check has failed** alert is triggered. Follow the corrective actions specified for the alert.
   - A “Service unavailable” or an “Internal server error” message appears. After one minute, refresh the page to continue monitoring the job.

     > As needed, you can navigate away from the Object existence check page and return to continue monitoring the job.

10. As the job runs, view the **Active job** tab and note the value of Missing object copies detected.

    This value represents the total number of missing copies of replicated objects and erasure-coded objects with one or more missing fragments.

    If the number of Missing object copies detected is greater than 100, there might be an issue with the Storage Node’s storage.




11. After the job has completed, take any additional required actions:
    - If Missing object copies detected is zero, then no issues were found. No action is required.
    - If Missing object copies detected is greater than zero and the **Objects lost** alert has not been triggered, then all missing copies were repaired by the system. Verify that any hardware issues have been corrected to prevent future damage to object copies.
    - If Missing object copies detected is greater than zero and the **Objects lost** alert has been triggered, then data integrity could be affected. Contact technical support.
    - You can investigate lost object copies by using grep to extract the LLST audit messages: `grep LLST audit_file_name`.

      This procedure is similar to the one for investigating lost objects, although for object copies you search for `LLST` instead of `OLST`.

12. If you selected the strong-site or strong-global consistency control for the job, wait approximately three weeks for metadata consistency and then rerun the job on the same volumes again.

    When StorageGRID has had time to achieve metadata consistency for the nodes and volumes included in the job, rerunning the job could clear erroneously reported missing object copies or cause additional object copies to be checked if they were missed.

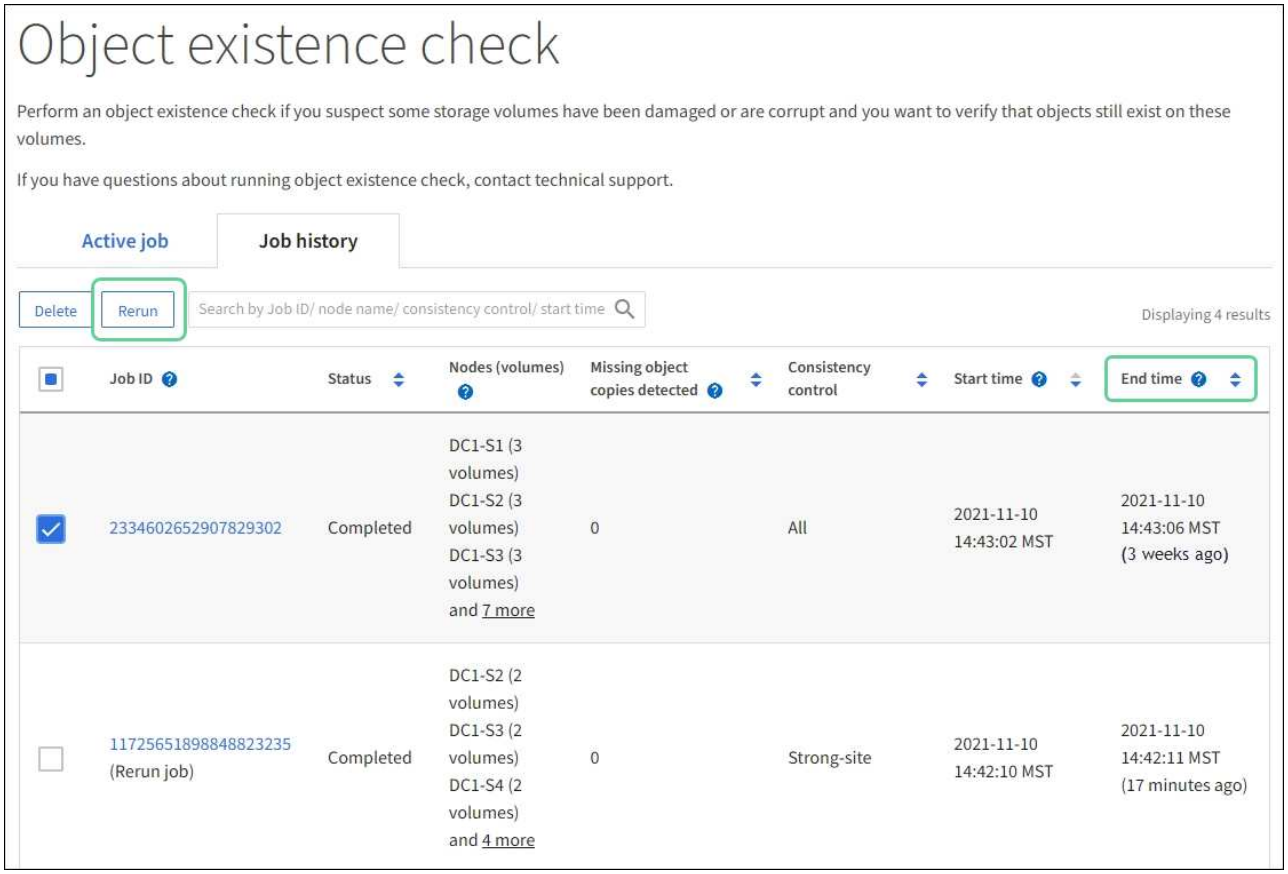
    a. Select **MAINTENANCE** > **Object existence check** > **Job history**.

    b. Determine which jobs are ready to be rerun:

       i. Look at the **End time** column to determine which jobs were run more than three weeks ago.

ii. For those jobs, scan the Consistency control column for strong-site or strong-global.

c. Select the check box for each job you want to rerun, then select **Rerun**.




d. In the Rerun jobs wizard, review the selected nodes and volumes and the consistency control.

e. When you are ready to rerun the jobs, select **Rerun**.

The Active job tab appears. All the jobs you selected are rerun as one job at a consistency control of strong-site. A **Related jobs** field in the Details section lists the job IDs for the original jobs.

**After you finish**

If you still have concerns about data integrity, go to **SUPPORT** > **Tools** > **Grid topology** > ***site*** > ***Storage Node*** > **LDR** > **Verification** > **Configuration** > **Main** and increase the Background Verification Rate. Background verification checks the correctness of all stored object data and repairs any issues that it finds. Finding and repairing potential issues as quickly as possible reduces the risk of data loss.

#### Troubleshoot lost and missing object data

Objects can be retrieved for several reasons, including read requests from a client application, background verifications of replicated object data, ILM re-evaluations, and the restoration of object data during the recovery of a Storage Node.

The StorageGRID system uses location information in an object's metadata to determine from which location to retrieve the object. If a copy of the object is not found in the expected location, the system attempts to retrieve another copy of the object from elsewhere in the system, assuming that the ILM policy contains a rule to make two or more copies of the object.

If this retrieval is successful, the StorageGRID system replaces the missing copy of the object. Otherwise, the

**Objects lost** alert is triggered, as follows:

- For replicated copies, if another copy cannot be retrieved, the object is considered lost, and the alert is triggered.
- For erasure coded copies, if a copy cannot be retrieved from the expected location, the Corrupt Copies Detected (ECOR) attribute is incremented by one before an attempt is made to retrieve a copy from another location. If no other copy is found, the alert is triggered.

You should investigate all **Objects lost** alerts immediately to determine the root cause of the loss and to determine if the object might still exist in an offline, or otherwise currently unavailable, Storage Node or Archive Node.

In the case where object data without copies is lost, there is no recovery solution. However, you must reset the Lost objects counter to prevent known lost objects from masking any new lost objects.

#### Related information

Investigate lost objects

Reset lost and missing object counts

### Investigate lost objects

When the **Objects lost** alert is triggered, you must investigate immediately. Collect information about the affected objects and contact technical support.

#### What you'll need

- You must be signed in to the Grid Manager using a supported web browser.
- You must have specific access permissions.
- You must have the `Passwords.txt` file.

#### About this task

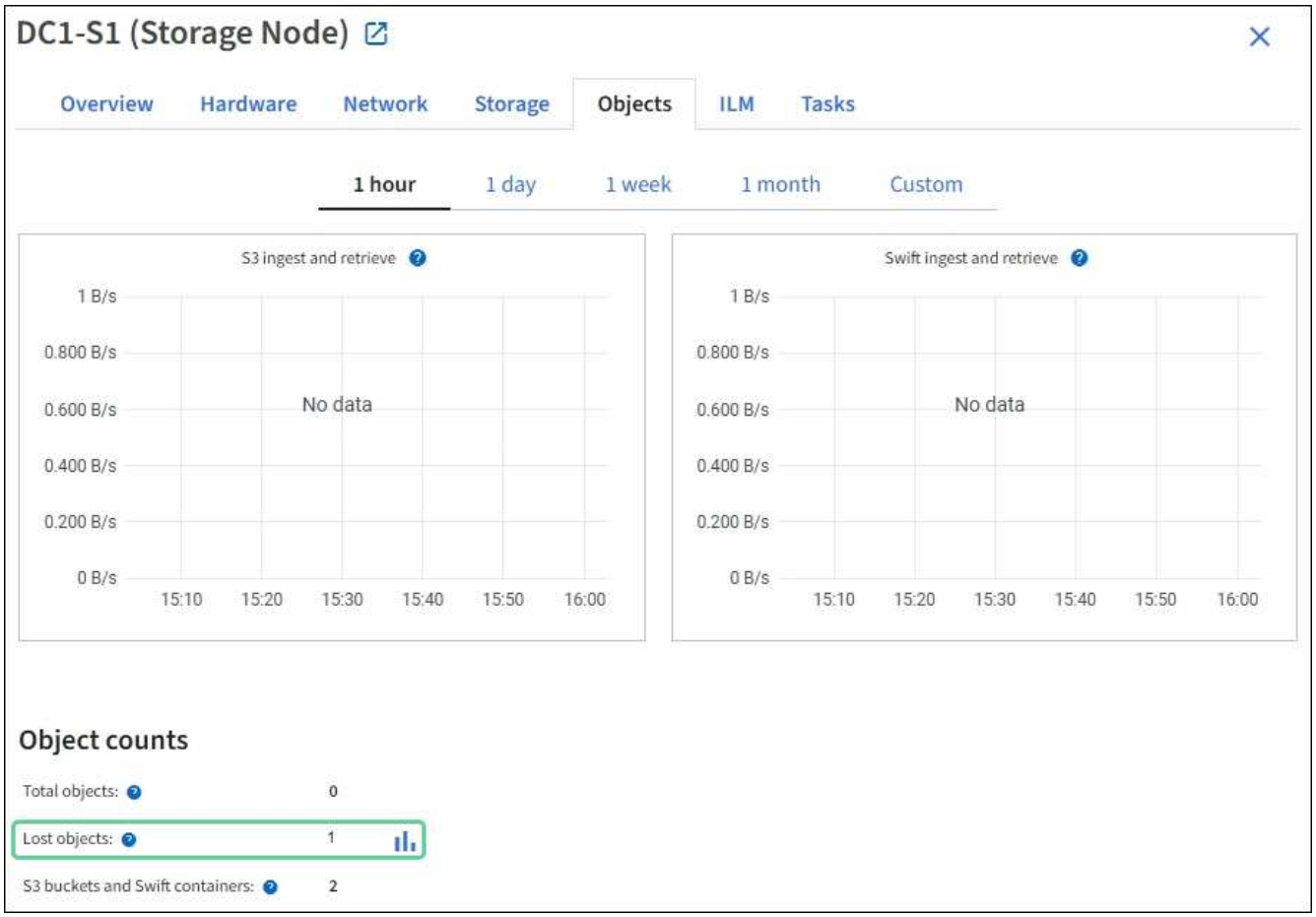
The **Objects lost** alert indicates that StorageGRID believes that there are no copies of an object in the grid. Data might have been permanently lost.

Investigate lost object alerts immediately. You might need to take action to prevent further data loss. In some cases, you might be able to restore a lost object if you take prompt action.

#### Steps

1. Select **NODES**.
2. Select ***Storage Node*** > **Objects**.
3. Review the number of Lost objects shown in the Object counts table.

   This number indicates the total number of objects this grid node detects as missing from the entire StorageGRID system. The value is the sum of the Lost objects counters of the Data store component within the LDR and DDS services.




4. From an Admin Node, access the audit log to determine the unique identifier (UUID) of the object that triggered the **Objects lost** alert:
   a. Log in to the grid node:
      i. Enter the following command: `ssh admin@grid_node_IP`
      ii. Enter the password listed in the `Passwords.txt` file.
      iii. Enter the following command to switch to root: `su -`
      iv. Enter the password listed in the `Passwords.txt` file. When you are logged in as root, the prompt changes from `$` to `#`.
   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 UUID value included in the message.

```
>Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):926026C4-00A4-449B-
AC72-BCCA72DD1311]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Use the `ObjectByUUID` command to find the object by its identifier (UUID), and then determine if data is at risk.
   a. Telnet to localhost 1402 to access the LDR console.
   b. Enter: `/proc/OBRP/ObjectByUUID UUID_value`

      In this first example, the object with `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` has two locations listed.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
```

```
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.934425"
        }
    ]
}
```


In the second example, the object with `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` has no locations listed.

```
ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    }
}
```

c. Review the output of /proc/OBRP/ObjectByUUID, and take the appropriate action:

| Metadata | Conclusion |
| --- | --- |
| No object found ("ERROR":"" ) | If the object is not found, the message "ERROR":"" is returned.<br><br>If the object is not found, you can reset the count of **Objects lost** to clear the alert. The lack of an object indicates that the object was intentionally deleted. |
| Locations > 0 | If there are locations listed in the output, the **Objects lost** alert might be a false positive.<br><br>Confirm that the objects exist. Use the Node ID and filepath listed in the output to confirm that the object file is in the listed location.<br><br>(The procedure for searching for potentially lost objects explains how to use the Node ID to find the correct Storage Node.)<br><br>If the objects exist, you can reset the count of **Objects lost** to clear the alert. |
| Locations = 0 | If there are no locations listed in the output, the object is potentially missing. You can try to search for and restore the object yourself, or you can contact technical support.<br><br>Technical support might ask you to determine if there is a storage recovery procedure in progress. That is, has a *repair-data* command been issued on any Storage Node, and is the recovery still in progress? See the information about restoring object data to a storage volume. |

**Related information**

Review audit logs

### Search for and restore potentially lost objects

It might be possible to find and restore objects that have triggered a Lost Objects (LOST) alarm and a **Object lost** alert and that you have identified as potentially lost.

**What you'll need**

- You must have the UUID of any lost object, as identified in "Investigating lost objects."
- You must have the `Passwords.txt` file.

**About this task**

You can follow this procedure to look for replicated copies of the lost object elsewhere in the grid. In most cases, the lost object will not be found. However, in some cases, you might be able to find and restore a lost replicated object if you take prompt action.

Contact technical support for assistance with this procedure.

**Steps**

1. From an Admin Node, search the audit logs for possible object locations:
   a. Log in to the grid node:
      i. Enter the following command: `ssh admin@grid_node_IP`
      ii. Enter the password listed in the `Passwords.txt` file.
      iii. Enter the following command to switch to root: `su -`
      iv. Enter the password listed in the `Passwords.txt` file. When you are logged in as root, the prompt changes from `$` to `#`.
   b. Change to the directory where the audit logs are located: `cd /var/local/audit/export/`
   c. Use grep to extract the audit messages associated with the potentially lost object and send them to an output file. Enter: `grep uuid-valueaudit_file_name > output_file_name`

      For example:

      ```
      Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
      messages_about_lost_object.txt
      ```

   d. Use grep to extract the Location Lost (LLST) audit messages from this output file. Enter: `grep LLST output_file_name`

      For example:

      ```
      Admin: # grep LLST messages_about_lost_objects.txt
      ```

      An LLST audit message looks like this sample message.

      ```
      [AUDT:\[NOID\(UI32\):12448208\][CBIL(UI64):0x38186FE53E3C49A5]
      [UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
      [PCLD\(CSTR\):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
      [TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):
      1581535134379225][ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CL
      SM]
      [ATID(UI64):7086871083190743409]]
      ```

   e. Find the PCLD field and the NOID field in the LLST message.

      If present, the value of PCLD is the complete path on disk to the missing replicated object copy. The value of NOID is the node id of the LDR where a copy of the object might be found.

      If you find an object location, you might be able to restore the object.

   f. Find the Storage Node for this LDR node ID.

      There are two ways to use the node ID to find the Storage Node:

- In the Grid Manager, select **SUPPORT** > **Tools** > **Grid topology**. Then select ***Data Center*** > ***Storage Node*** > **LDR**. The LDR node ID is in the Node Information table. Review the information for each Storage Node until you find the one that hosts this LDR.
- Download and unzip the Recovery Package for the grid. There is a *\docs* directory in the SAID package. If you open the index.html file, the Servers Summary shows all node IDs for all grid nodes.

2. Determine if the object exists on the Storage Node indicated in the audit message:
   a. Log in to the grid node:
      i. Enter the following command: `ssh admin@grid_node_IP`
      ii. Enter the password listed in the `Passwords.txt` file.
      iii. Enter the following command to switch to root: `su -`
      iv. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

   b. Determine if the file path for the object exists.

For the file path of the object, use the value of PCLD from the LLST audit message.

For example, enter:

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

**Note**: Always enclose the object file path in single quotes in commands to escape any special characters.

- If the object path is not found, the object is lost and cannot be restored using this procedure. Contact technical support.
- If the object path is found, continue with step Restore the object to StorageGRID. You can attempt to restore the found object back to StorageGRID.

1. If the object path was found, attempt to restore the object to StorageGRID:
   a. From the same Storage Node, change the ownership of the object file so that it can be managed by StorageGRID. Enter: `chown ldr-user:bycast 'file_path_of_object'`
   b. Telnet to localhost 1402 to access the LDR console. Enter: `telnet 0 1402`
   c. Enter: `cd /proc/STOR`
   d. Enter: `Object_Found 'file_path_of_object'`

      For example, enter:

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      Issuing the `Object\_Found` command notifies the grid of the object's location. It also triggers the active ILM policy, which makes additional copies as specified in the policy.

**Note**: If the Storage Node where you found the object is offline, you can copy the object to any Storage Node that is online. Place the object in any /var/local/rangedb directory of the online Storage Node. Then, issue the `Object\_Found` command using that file path to the object.

- If the object cannot be restored, the `Object\_Found` command fails. Contact technical support.
- If the object was successfully restored to StorageGRID, a success message appears. For example:

```
ade 12448208: /proc/STOR > Object_Found
'/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

ade 12448208: /proc/STOR > Object found succeeded.
First packet of file was valid. Extracted key: 38186FE53E3C49A5
Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
'/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
```

Continue with step Verify that new locations were created

1. If the object was successfully restored to StorageGRID, verify that new locations were created.
   a. Enter: `cd /proc/OBRP`
   b. Enter: `ObjectByUUID UUID_value`

The following example shows that there are two locations for the object with UUID 926026C4-00A4-449B-AC72-BCCA72DD1311.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
```

```
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.934425"
        }
    ]
}
```


a. Sign out of the LDR console. Enter: `exit`

   1. From an Admin Node, search the audit logs for the ORLM audit message for this object to confirm that information lifecycle management (ILM) has placed copies as required.

b. Log in to the grid node:

   i. Enter the following command: `ssh admin@grid_node_IP`

   ii. Enter the password listed in the `Passwords.txt` file.

   iii. Enter the following command to switch to root: `su -`

   iv. Enter the password listed in the `Passwords.txt` file. When you are logged in as root, the prompt changes from `$` to `#`.

c. Change to the directory where the audit logs are located: `cd /var/local/audit/export/`

d. Use grep to extract the audit messages associated with the object to an output file. Enter: `grep uuid-valueaudit_file_name > output_file_name`

   For example:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_restored_object.txt
```

e. Use grep to extract the Object Rules Met (ORLM) audit messages from this output file. Enter: `grep ORLM output_file_name`

   For example:

```
Admin: # grep ORLM messages_about_restored_object.txt
```

   An ORLM audit message looks like this sample message.

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

f. Find the LOCS field in the audit message.

   If present, the value of CLDI in LOCS is the node ID and the volume ID where an object copy has been created. This message shows that the ILM has been applied and that two object copies have been created in two locations in the grid. . Reset the count of lost objects in the Grid Manager.

**Related information**

Investigate lost objects

Reset lost and missing object counts

Review audit logs

### Reset lost and missing object counts

After investigating the StorageGRID 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.

**What you'll need**

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

**About this task**

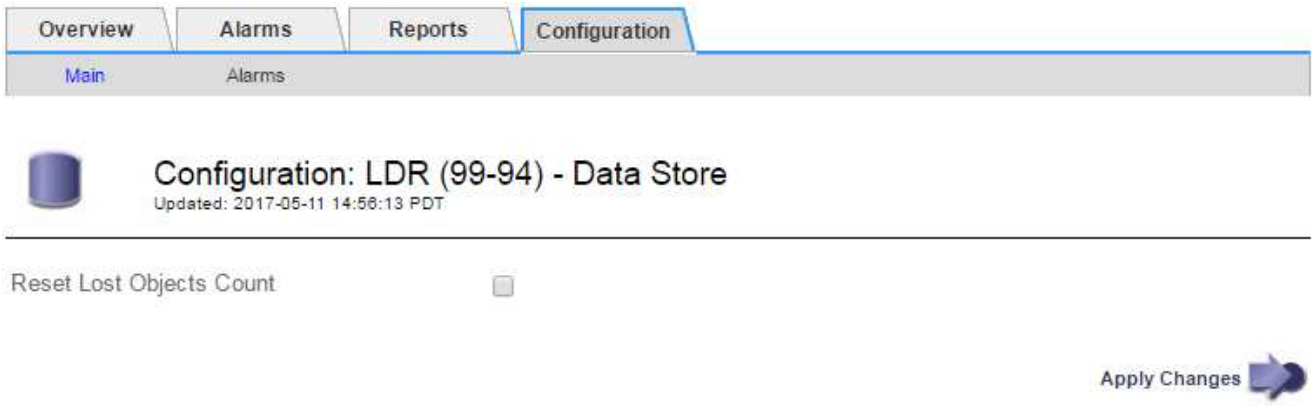
You can reset the Lost Objects counter from either of the following pages:

- **SUPPORT** > **Tools** > **Grid topology** > ***Site*** > ***Storage Node*** > **LDR** > **Data Store** > **Overview** > **Main**
- **SUPPORT** > **Tools** > **Grid topology** > ***Site*** > ***Storage Node*** > **DDS** > **Data Store** > **Overview** > **Main**

These instructions show resetting the counter from the **LDR** > **Data Store** page.

**Steps**

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Select ***Site*** > ***Storage Node*** > **LDR** > **Data Store** > **Configuration** for the Storage Node that has the **Objects lost** alert or the LOST alarm.
3. Select **Reset Lost Objects Count**.




4. Click **Apply Changes**.

   The Lost Objects attribute is reset to 0 and the **Objects lost** alert and the LOST alarm clear, which can take a few minutes.

5. Optionally, reset other related attribute values that might have been incremented in the process of identifying the lost object.

   a. Select ***Site*** > ***Storage Node*** > **LDR** > **Erasure Coding** > **Configuration**.
   b. Select **Reset Reads Failure Count** and **Reset Corrupt Copies Detected Count**.
   c. Click **Apply Changes**.
   d. Select ***Site*** > ***Storage Node*** > **LDR** > **Verification** > **Configuration**.
   e. Select **Reset Missing Objects Count** and **Reset Corrupt Objects Count**.
   f. If you are confident that quarantined objects are not required, you can select **Delete Quarantined Objects**.

      Quarantined objects are created when background verification identifies a corrupt replicated object copy. In most cases StorageGRID automatically replaces the corrupt object, and it is safe to delete the quarantined objects. However, if the **Objects lost** alert or the LOST alarm is triggered, technical support might want to access the quarantined objects.

g. Click **Apply Changes**.

It can take a few moments for the attributes to reset after you click **Apply Changes**.

#### Troubleshoot the Low object data storage alert

## The **Low object data storage** alert monitors how much space is available for storing object data on each Storage Node.

### What you'll need

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

### About this task

The **Low object data storage** alert is triggered when the total amount of replicated and erasure coded object data on a Storage Node meets one of the conditions configured in the alert rule.

By default, a major alert is triggered when this condition evaluates as true:

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

In this condition:

- `storagegrid_storage_utilization_data_bytes` is an estimate of the total size of replicated and erasure coded object data for a Storage Node.
- `storagegrid_storage_utilization_usable_space_bytes` is the total amount of object storage space remaining for a Storage Node.

If a major or minor **Low object data storage** alert is triggered, you should perform an expansion procedure as soon as possible.

### Steps

1. Select **ALERTS** > **Current**.

   The Alerts page appears.

2. From the table of alerts, expand the **Low object data storage** alert group, if required, and select the alert you want to view.

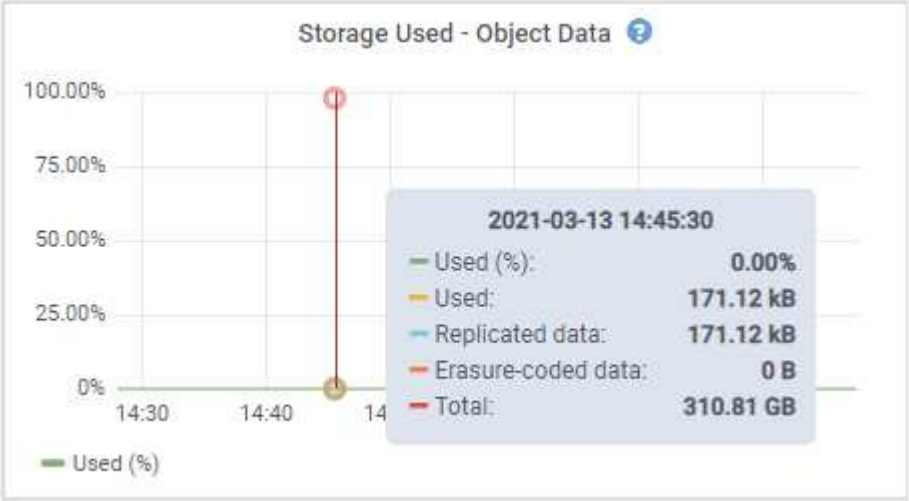
   Select the alert, not the heading for a group of alerts.

3. Review the details in the dialog box, and note the following:
   - Time triggered
   - The name of the site and node
   - The current values of the metrics for this alert
4. Select **NODES** > ***Storage Node or Site*** > **Storage**.

5. Hover your cursor over the Storage Used - Object Data graph.

   The following values are shown:

   - **Used (%)**: The percentage of the Total usable space that has been used for object data.
   - **Used**: The amount of the Total usable space that has been used for object data.
   - **Replicated data**: An estimate of the amount of replicated object data on this node, site, or grid.
   - **Erasure-coded data**: An estimate of the amount of erasure-coded object data on this node, site, or grid.
   - **Total**: The total amount of usable space on this node, site, or grid. The Used value is the `storagegrid_storage_utilization_data_bytes` metric.




6. Select the time controls above the graph to view storage use over different time periods.

   Looking at storage use over time can help you understand how much storage was used before and after the alert was triggered and can help you estimate how long it might take for the node's remaining space to become full.

7. As soon as possible, perform an expansion procedure to add storage capacity.

   You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes.

   To manage a full Storage Node, see the instructions for administering StorageGRID.

**Related information**

Troubleshoot the Storage Status (SSTS) alarm

Expand your grid

Administer StorageGRID

#### Troubleshoot Low read-only watermark override alerts

If you use custom values for storage volume watermarks, you might need to resolve the **Low read-only watermark override** alert. If possible, you should update your system to start using the optimized values.

In previous releases, the three storage volume watermarks were global settings — the same values applied to every storage volume on every Storage Node. Starting in StorageGRID 11.6, the software can optimize these watermarks for each storage volume, based on the size of the Storage Node and the relative capacity of the volume.

When you upgrade to StorageGRID 11.6, optimized read-only and read-write watermarks are automatically applied to all storage volumes, unless either of the following is true:

- Your system is close to capacity and would not be able to accept new data if optimized watermarks were applied. StorageGRID will not change watermark settings in this case.
- You previously set any of the storage volume watermarks to a custom value. StorageGRID will not override custom watermark settings with optimized values. However, StorageGRID might trigger the **Low read-only watermark override** alert if your custom value for the Storage Volume Soft Read-Only Watermark is too small.

### Understand the alert

If you use custom values for storage volume watermarks, the **Low read-only watermark override** alert might be triggered for one or more Storage Nodes.

Each instance of the alert indicates that the custom value of the **Storage Volume Soft Read-Only Watermark** is smaller than the minimum optimized value for that Storage Node. If you continue to use the custom setting, the Storage Node might run critically low on space before it can safely transition to the read-only state. Some storage volumes might become inaccessible (automatically unmounted) when the node reaches capacity.

For example, suppose you previously set the **Storage Volume Soft Read-Only Watermark** to 5 GB. Now suppose that StorageGRID has calculated the following optimized values for the four storage volumes in Storage Node A:

| | |
|---|---|
| Volume 0 | 12 GB |
| Volume 1 | 12 GB |
| Volume 2 | 11 GB |
| Volume 3 | 15 GB |

The **Low read-only watermark override** alert is triggered for Storage Node A because your custom watermark (5 GB) is smaller than the minimum optimized value for all volumes in that node (11 GB). If you continue using the custom setting, the node might run critically low on space before it can safely transition to the read-only state.

### Resolve the alert

Follow these steps if one or more **Low read-only watermark override** alerts have been triggered. You can also use these instructions if you currently use custom watermark settings and want to start using optimized settings even if no alerts have been triggered.

#### What you'll need

- You have completed the upgrade to StorageGRID 11.6.
- You are signed in to the Grid Manager using a supported web browser.

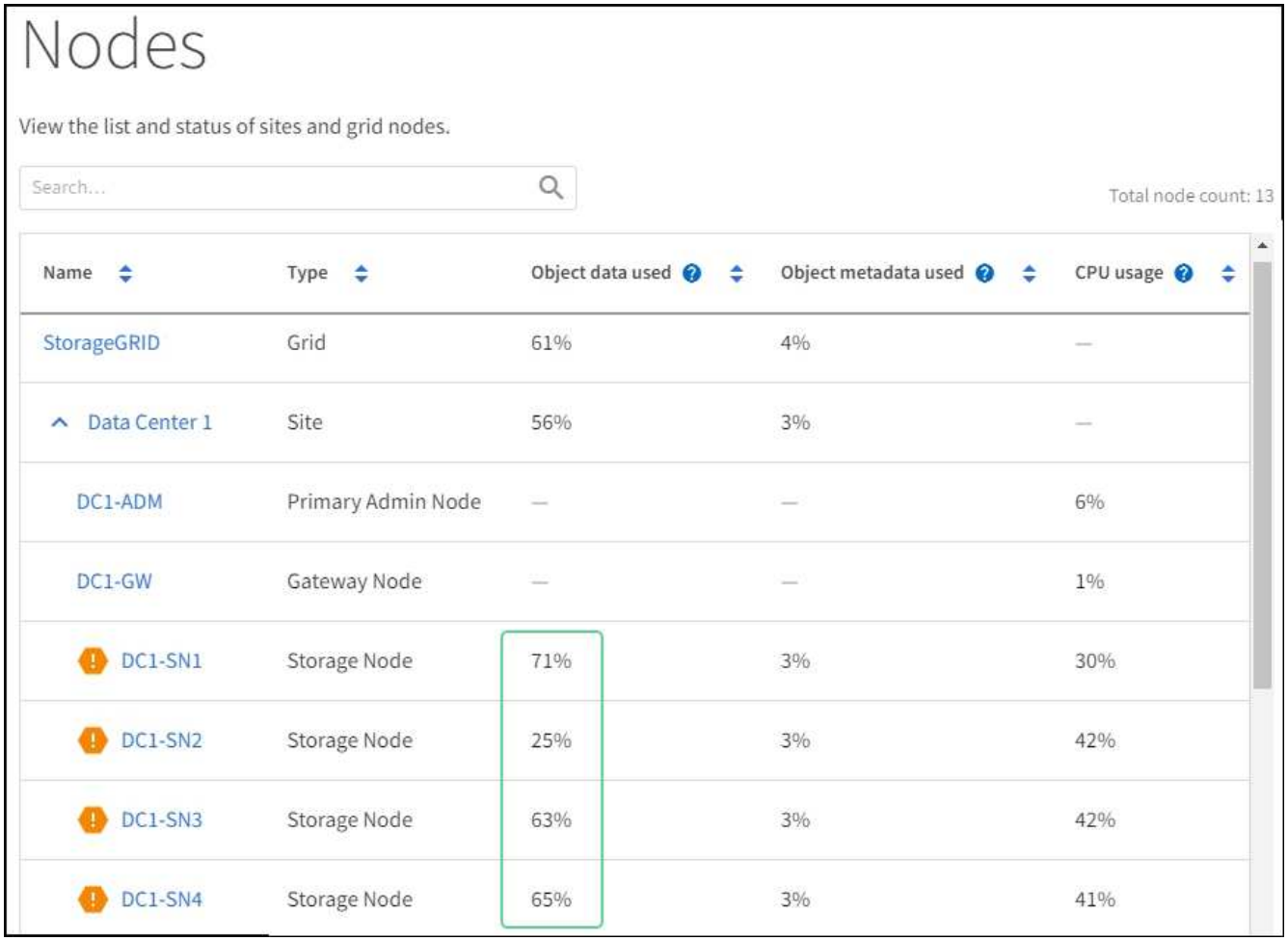
- You have the Root access permission.

### About this task

You can resolve the **Low read-only watermark override** alert by updating custom watermark settings to the new watermark overrides. However, if one or more Storage Nodes are close to full or you have special ILM requirements, you should first view the optimized storage watermarks and determine if it is safe to use them.

### Assess object data usage for entire grid

1. Select **NODES**.
2. For each site in the grid, expand the list of nodes.
3. Review the percentage values shown in the **Object data used** column for each Storage Node at every site.




4. If none of the Storage Nodes are close to full (for example, all **Object data used** values are less than 80%), you can start using the override settings. Go to Use optimized watermarks.

> There are some exceptions to this general rule. For example, if ILM rules use Strict ingest behavior or if specific storage pools are close to full, you should first perform the steps in View optimized storage watermarks and Determine if you can use optimized watermarks.

5. If one more more Storage Nodes are close to full, perform the steps in View optimized storage watermarks and Determine if you can use optimized watermarks.

### View optimized storage watermarks

StorageGRID uses two Prometheus metrics to show the optimized values it has calculated for the **Storage Volume Soft Read-Only Watermark**. You can view the minimum and maximum optimized values for each Storage Node in your grid.

1. Select **SUPPORT** > **Tools** > **Metrics**.
2. In the Prometheus section, select the link to access the Prometheus user interface.
3. To see the recommended minimum soft read-only watermark, enter the following Prometheus metric, and select **Execute**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   The last column shows the minimum optimized value of the Soft Read-Only Watermark for all storage volumes on each Storage Node. If this value is greater than the custom setting for the **Storage Volume Soft Read-Only Watermark**, the **Low read-only watermark override** alert is triggered for the Storage Node.

4. To see the recommended maximum soft read-only watermark, enter the following Prometheus metric, and select **Execute**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   The last column shows the maximum optimized value of the Soft Read-Only Watermark for all storage volumes on each Storage Node.

5. Note the maximum optimized value for each Storage Node.

### Determine if you can use optimized watermarks

1. Select **NODES**.
2. Repeat these steps for each online Storage Node:
   a. Select ***Storage Node*** > **Storage**.
   b. Scroll down to the Object Stores table.
   c. Compare the **Available** value for each object store (volume) to the maximum optimized watermark you noted for that Storage Node.
3. If at least one volume on every online Storage Node has more space available than maximum optimized watermark for that node, go to Use optimized watermarks to start using the optimized watermarks.

   Otherwise, expand your grid as soon as possible. Either add storage volumes to an existing node or add new Storage Nodes. Then, go to Use optimized watermarks to update watermark settings.

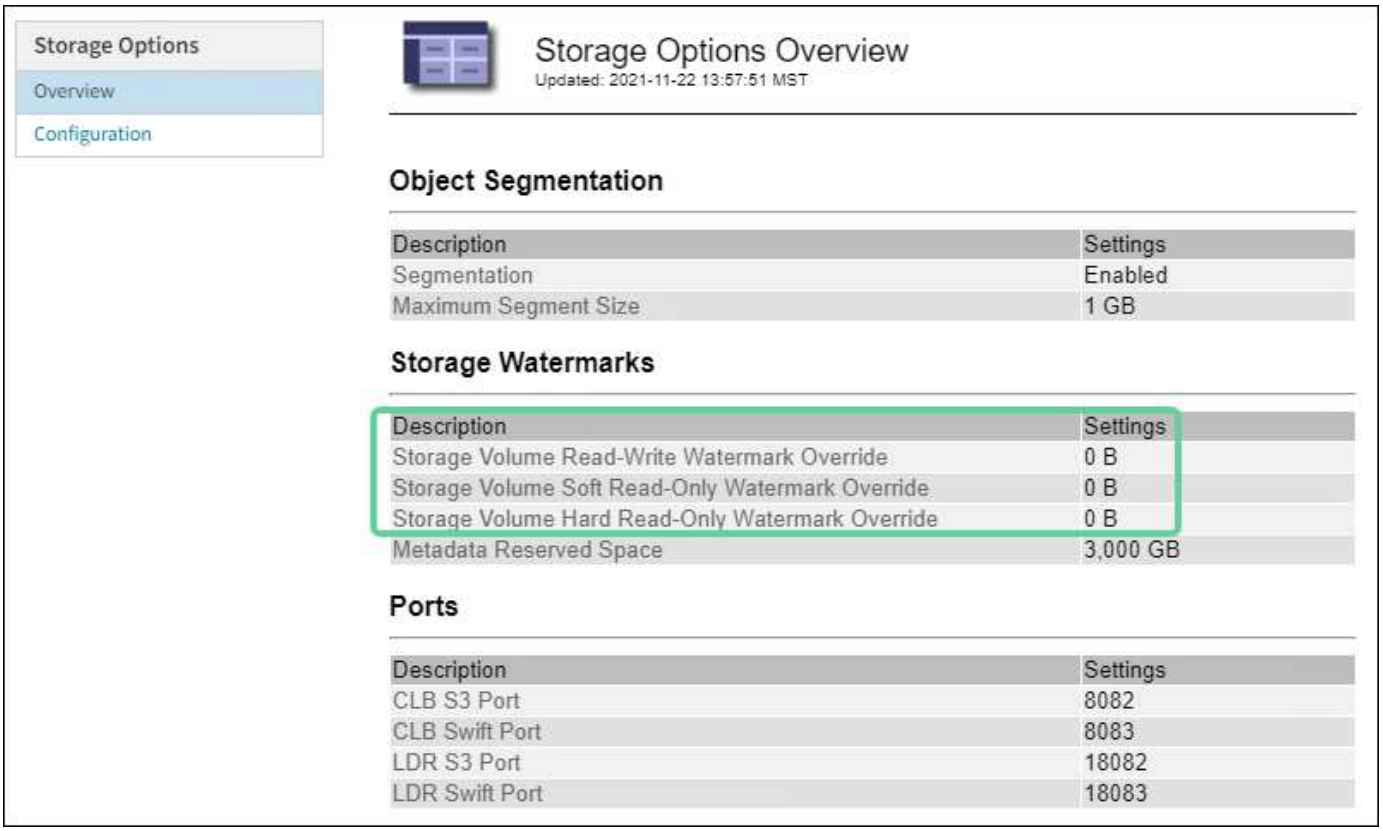
4. If you need to continue using custom values for the storage volume watermarks, silence or disable the **Low read-only watermark override** alert.

   > The same custom watermark values are applied to every storage volume on every Storage Node. Using smaller-than-recommended values for storage volume watermarks might cause some storage volumes to become inaccessible (automatically unmounted) when the node reaches capacity.

### Use optimized watermarks

1. Go to **CONFIGURATION** > **System** > **Storage options**.
2. Select **Configuration** from the Storage Options menu.
3. Change all three Watermark Overrides to 0.
4. Select **Apply Changes**.

Optimized storage volume watermark settings are now in effect for each storage volume, based on the size of the Storage Node and the relative capacity of the volume.




#### Troubleshoot the Storage Status (SSTS) alarm

## The Storage Status (SSTS) alarm is triggered if a Storage Node has insufficient free space remaining for object storage.

### What you'll need

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

### About this task

The SSTS (Storage Status) alarm is triggered at the Notice level when the amount of free space on every volume in a Storage Node falls below the value of the Storage Volume Soft Read Only Watermark (**CONFIGURATION** > **System** > **Storage options**).

Storage Options Overview
Updated: 2019-10-09 13:09:30 MDT

### Object Segmentation

| Description | Settings |
|---|---|
| Segmentation | Enabled |
| Maximum Segment Size | 1 GB |

### Storage Watermarks

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

For example, suppose the Storage Volume Soft Read-Only Watermark is set to 10 GB, which is its default value. The SSTS alarm is triggered if less than 10 GB of usable space remains on each storage volume in the Storage Node. If any of the volumes has 10 GB or more of available space, the alarm is not triggered.

If an SSTS alarm has been triggered, you can follow these steps to better understand the issue.

**Steps**

1. Select **SUPPORT** > **Alarms (legacy)** > **Current alarms**.
2. From the Service column, select the data center, node, and service that are associated with the SSTS alarm.

   The Grid Topology page appears. The Alarms tab shows the active alarms for the node and service you selected.

Overview | Alarms | Reports | Configuration
Main | History

Alarms: LDR (DC1-S3-101-195) - Storage
Updated: 2019-10-09 12:52:43 MDT

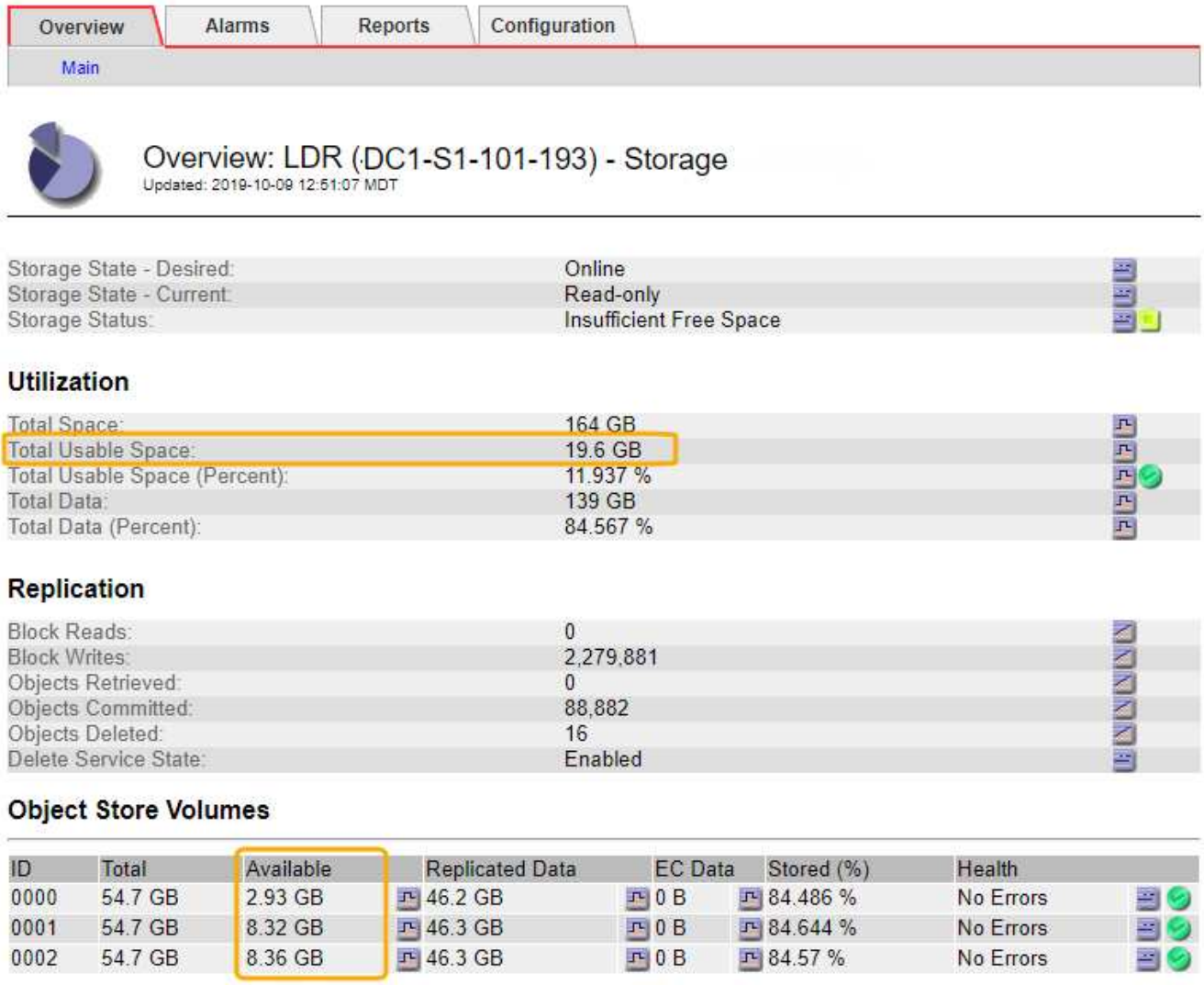
| Severity | Attribute | Description | Alarm Time | Trigger Value | Current Value | Acknowledge Time | Acknowledge |
|---|---|---|---|---|---|---|---|
| Notice | SSTS (Storage Status) | Insufficient Free Space | 2019-10-09 12:42:51 MDT | Insufficient Free Space | Insufficient Free Space | | |
| Notice | SAVP (Total Usable Space (Percent)) | Under 10 % | 2019-10-09 12:43:21 MDT | 7.95 % | 7.95 % | | |
| Normal | SHLH (Health) | | | | | | |

Apply Changes

   In this example, both the SSTS (Storage Status) and SAVP (Total Usable Space (Percent)) alarms have been triggered at the Notice level.

> Typically, both the SSTS alarm and the SAVP alarm are triggered at about the same time; however, whether both alarms are triggered depends on the the watermark setting in GB and the SAVP alarm setting in percent.

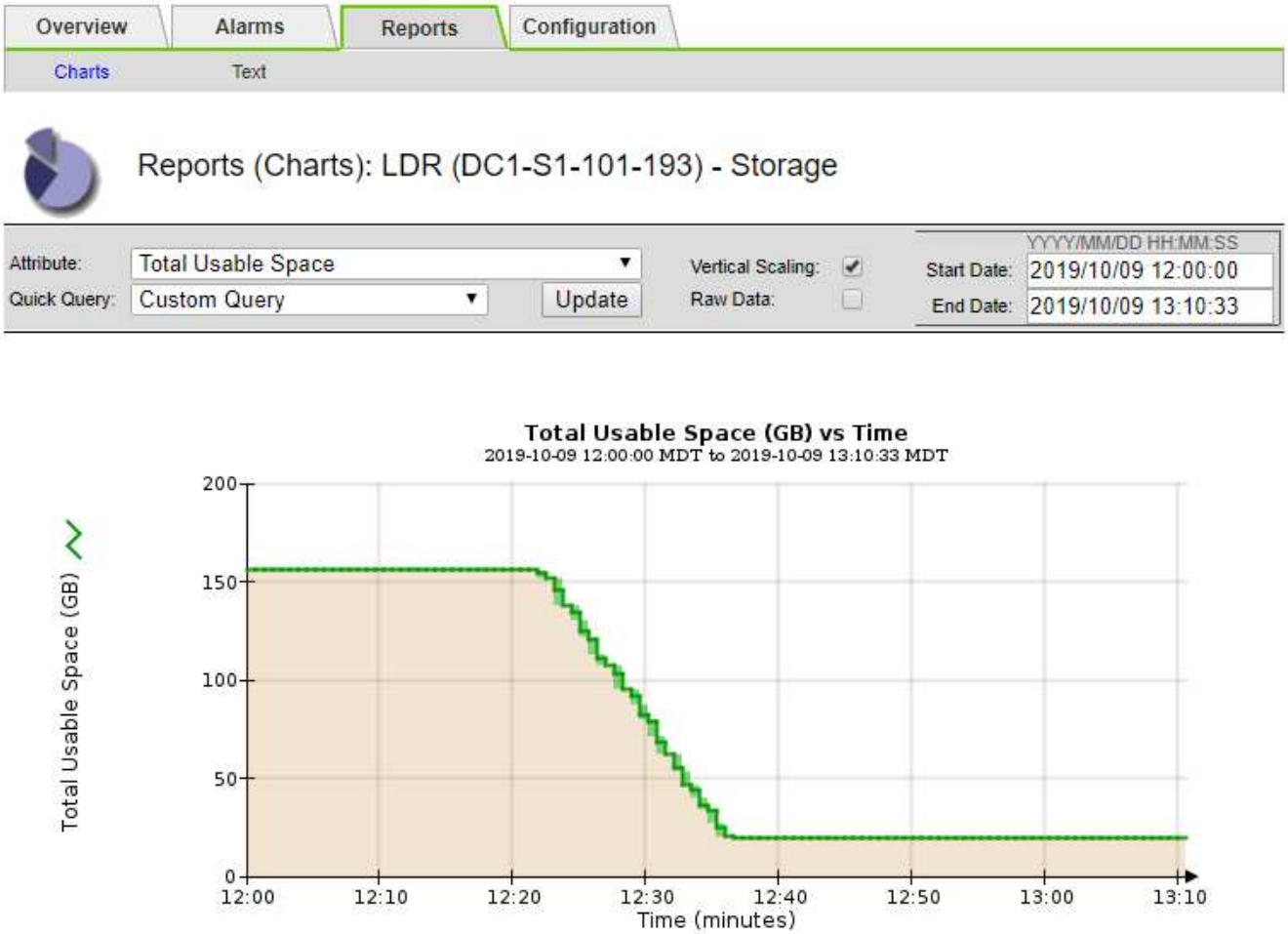
3. To determine how much usable space is actually available, select **LDR** > **Storage** > **Overview**, and find the Total Usable Space (STAS) attribute.




In this example, only 19.6 GB of the 164 GB of space on this Storage Node remains available. Note that the total value is the sum of the **Available** values for the three object store volumes. The SSTS alarm was triggered because each of the three storage volumes had less than 10 GB of available space.

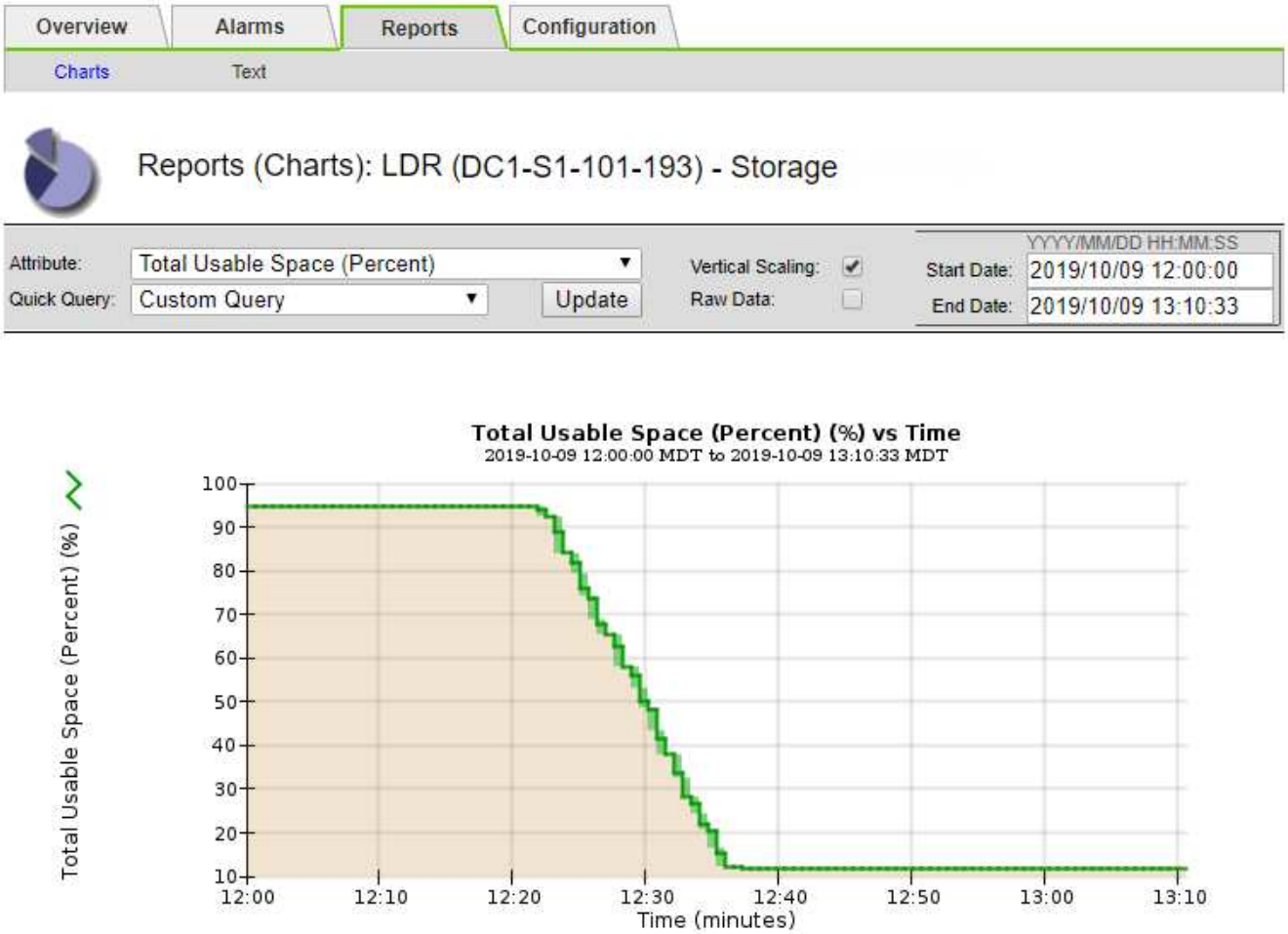
4. To understand how storage has been used over time, select the **Reports** tab, and plot Total Usable Space over the last few hours.

   In this example, Total Usable Space dropped from roughly 155 GB at 12:00 to 20 GB at 12:35, which corresponds to the time at which the SSTS alarm was triggered.




5. To understand how storage is being used as a percent of the total, plot Total Usable Space (Percent) over the last few hours.

   In this example, the total usable space dropped from 95% to just over 10% at approximately the same time.




6. As required, add storage capacity by expanding the StorageGRID system.

   For procedures on how to manage a full Storage Node, see the instructions for administering StorageGRID.

#### Troubleshoot delivery of platform services messages (SMTT alarm)

## The Total Events (SMTT) alarm is triggered in the Grid Manager if a platform service message is delivered to an destination that cannot accept the data.

### About this task

For example, an S3 multipart upload can succeed even though the associated replication or notification message cannot be delivered to the configured endpoint. Or, a message for CloudMirror replication can fail to be delivered if the metadata is too long.

The SMTT alarm contains a Last Event message that says, `Failed to publish notifications for` *`bucket-name object key`* for the last object whose notification failed.

Event messages are also listed in the `/var/local/log/bycast-err.log` log file. See the Log files reference.

For additional information about troubleshooting platform services, see the instructions for administering StorageGRID. You might need to access the tenant from the Tenant Manager to debug a platform service error.

### Steps

1. To view the alarm, select **NODES** > ***site*** > ***grid node*** > **Events**.
2. View Last Event at the top of the table.

   Event messages are also listed in `/var/local/log/bycast-err.log`.

3. Follow the guidance provided in the SMTT alarm contents to correct the issue.
4. Select **Reset event counts**.
5. Notify the tenant of the objects whose platform services messages have not been delivered.
6. Instruct the tenant to trigger the failed replication or notification by updating the object's metadata or tags.

### Troubleshoot metadata issues

You can perform several tasks to help determine the source of metadata problems.

#### Troubleshoot the Low metadata storage alert

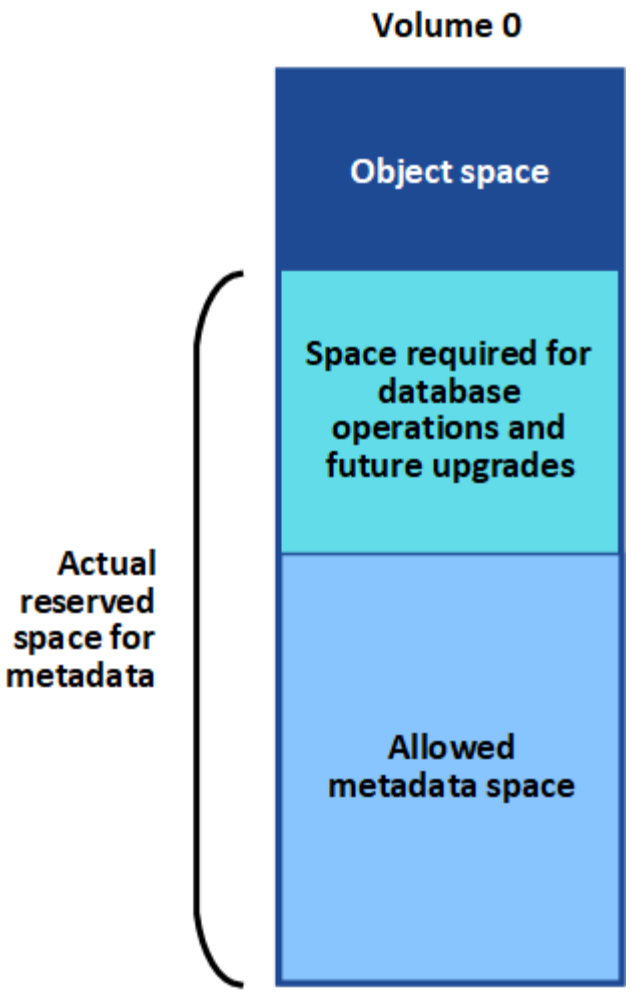
If the **Low metadata storage** alert is triggered, you must add new Storage Nodes.

**What you'll need**

- You must be signed in to the Grid Manager using a supported web browser.

**About this task**

StorageGRID reserves a certain amount of space on volume 0 of each Storage Node for object metadata. This space is known as the actual reserved space, and it is subdivided into the space allowed for object metadata (the allowed metadata space) and the space required for essential database operations, such as compaction and repair. The allowed metadata space governs overall object capacity.




If object metadata consumes more than 100% of the space allowed for metadata, database operations cannot run efficiently and errors will occur.

You can monitor object metadata capacity for each Storage Node to help you anticipate errors and correct them before they occur.

StorageGRID uses the following Prometheus metric to measure how full the allowed metadata space is:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

When this Prometheus expression reaches certain thresholds, the **Low metadata storage** alert is triggered.

- **Minor**: Object metadata is using 70% or more of the allowed metadata space. You should add new Storage Nodes as soon as possible.
- **Major**: Object metadata is using 90% or more of the allowed metadata space. You must add new Storage Nodes immediately.

> When object metadata is using 90% or more of the allowed metadata space, a warning appears on the Dashboard. If this warning appears, you must add new Storage Nodes immediately. You must never allow object metadata to use more than 100% of the allowed space.

- **Critical**: Object metadata is using 100% or more of the allowed metadata space and is starting to consume the space required for essential database operations. You must stop the ingest of new objects, and you must add new Storage Nodes immediately.

In the following example, object metadata is using more than 100% of the allowed metadata space. This is a critical situation, which will result in inefficient database operation and errors.

The following Storage Nodes are using more than 90% of the space allowed for object metadata:

| Node | % Used | Used | Allowed |
|---|---|---|---|
| DC1-S2-227 | 104.51% | 6.73 GB | 6.44 GB |
| DC1-S3-228 | 104.36% | 6.72 GB | 6.44 GB |
| DC2-S2-233 | 104.20% | 6.71 GB | 6.44 GB |
| DC1-S1-226 | 104.20% | 6.71 GB | 6.44 GB |
| DC2-S3-234 | 103.43% | 6.66 GB | 6.44 GB |

Undesirable results can occur if object metadata uses more than 100% of the allowed space. You must add new Storage Nodes immediately or contact support.

> If the size of volume 0 is smaller than the Metadata Reserved Space storage option (for example, in a non-production environment), the calculation for the **Low metadata storage** alert might be inaccurate.

**Steps**

1. Select **ALERTS** > **Current**.
2. From the table of alerts, expand the **Low metadata storage** alert group, if required, and select the specific alert you want to view.
3. Review the details in the alert dialog box.
4. If a major or critical **Low metadata storage** alert has been triggered, perform an expansion to add Storage Nodes immediately.

   > Because StorageGRID keeps complete copies of all object metadata at each site, the metadata capacity of the entire grid is limited by the metadata capacity of the smallest site. If you need to add metadata capacity to one site, you should also expand any other sites by the same number of Storage Nodes.

   After you perform the expansion, StorageGRID redistributes the existing object metadata to the new nodes, which increases the overall metadata capacity of the grid. No user action is required. The **Low metadata storage** alert is cleared.

#### Troubleshoot the Services: Status - Cassandra (SVST) alarm

The Services: Status - Cassandra (SVST) alarm indicates that you might need to rebuild the Cassandra database for a Storage Node. Cassandra is used as the metadata store for StorageGRID.

**What you'll need**

- You must be signed in to the Grid Manager using a supported web browser.
- You must have specific access permissions.
- You must have the `Passwords.txt` file.

**About this task**

If Cassandra is stopped for more than 15 days (for example, the Storage Node is powered off), Cassandra will not start when the node is brought back online. You must rebuild the Cassandra database for the affected DDS

service.

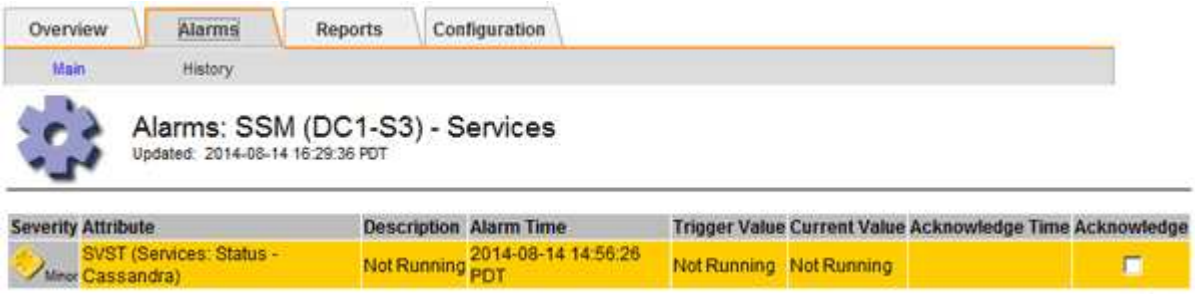
You can run diagnostics to obtain additional information on the current state of your grid.

> If two or more of the Cassandra database services are down for more than 15 days, contact technical support, and do not proceed with the steps below.

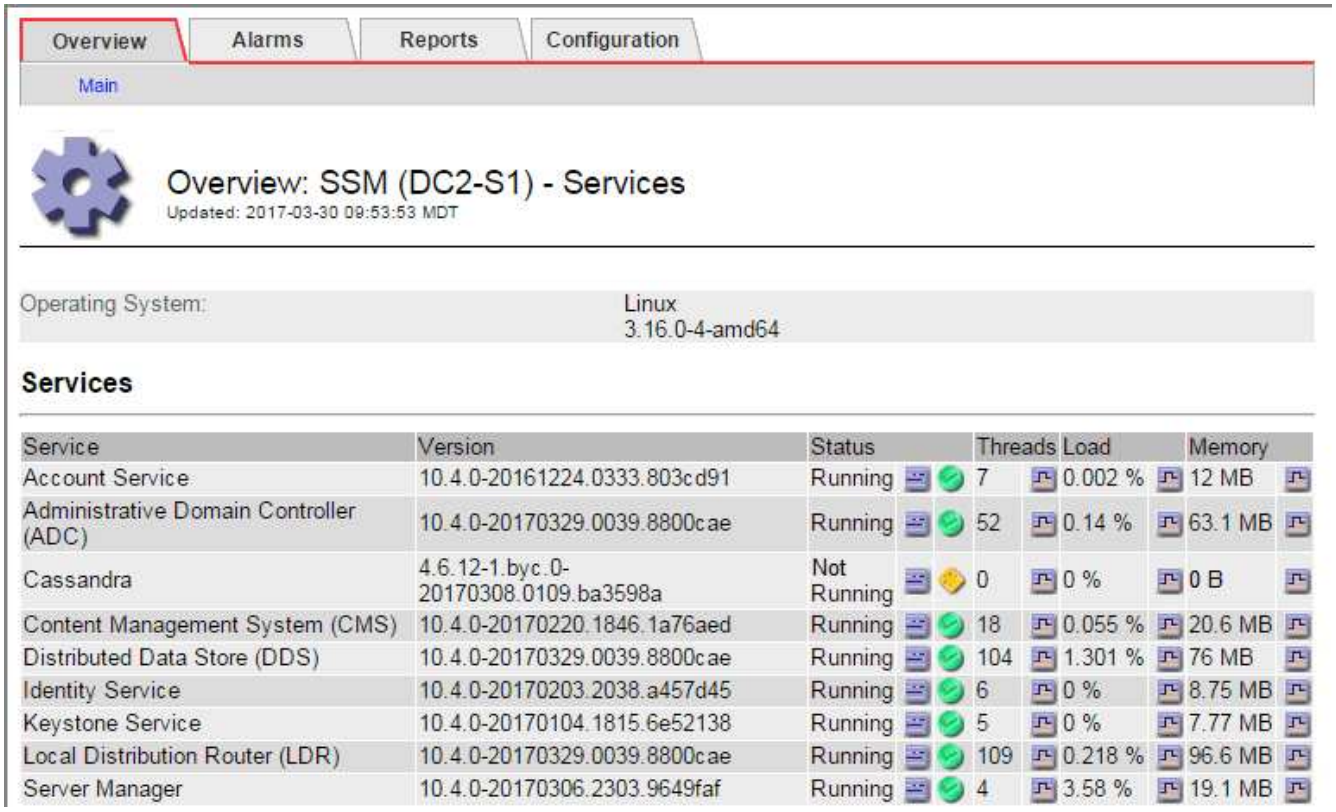
**Steps**

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Select ***Site*** > ***Storage Node*** > **SSM** > **Services** > **Alarms** > **Main** to display alarms.

   This example shows that the SVST alarm was triggered.




   The SSM Services Main page also indicates that Cassandra is not running.




3. Try restarting Cassandra from the Storage Node:
   a. Log in to the grid node:
      i. Enter the following command: `ssh admin@grid_node_IP`

ii. Enter the password listed in the `Passwords.txt` file.

iii. Enter the following command to switch to root: `su -`

iv. Enter the password listed in the `Passwords.txt` file. When you are logged in as root, the prompt changes from `$` to `#`.

b. Enter: `/etc/init.d/cassandra status`

c. If Cassandra is not running, restart it: `/etc/init.d/cassandra restart`

4. 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.

> If two or more of the Cassandra database services are down, contact technical support, and do not proceed with the steps below.

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

5. To chart Cassandra:

   a. Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***Site*** > ***Storage Node*** > **SSM** > **Services** > **Reports** > **Charts**.

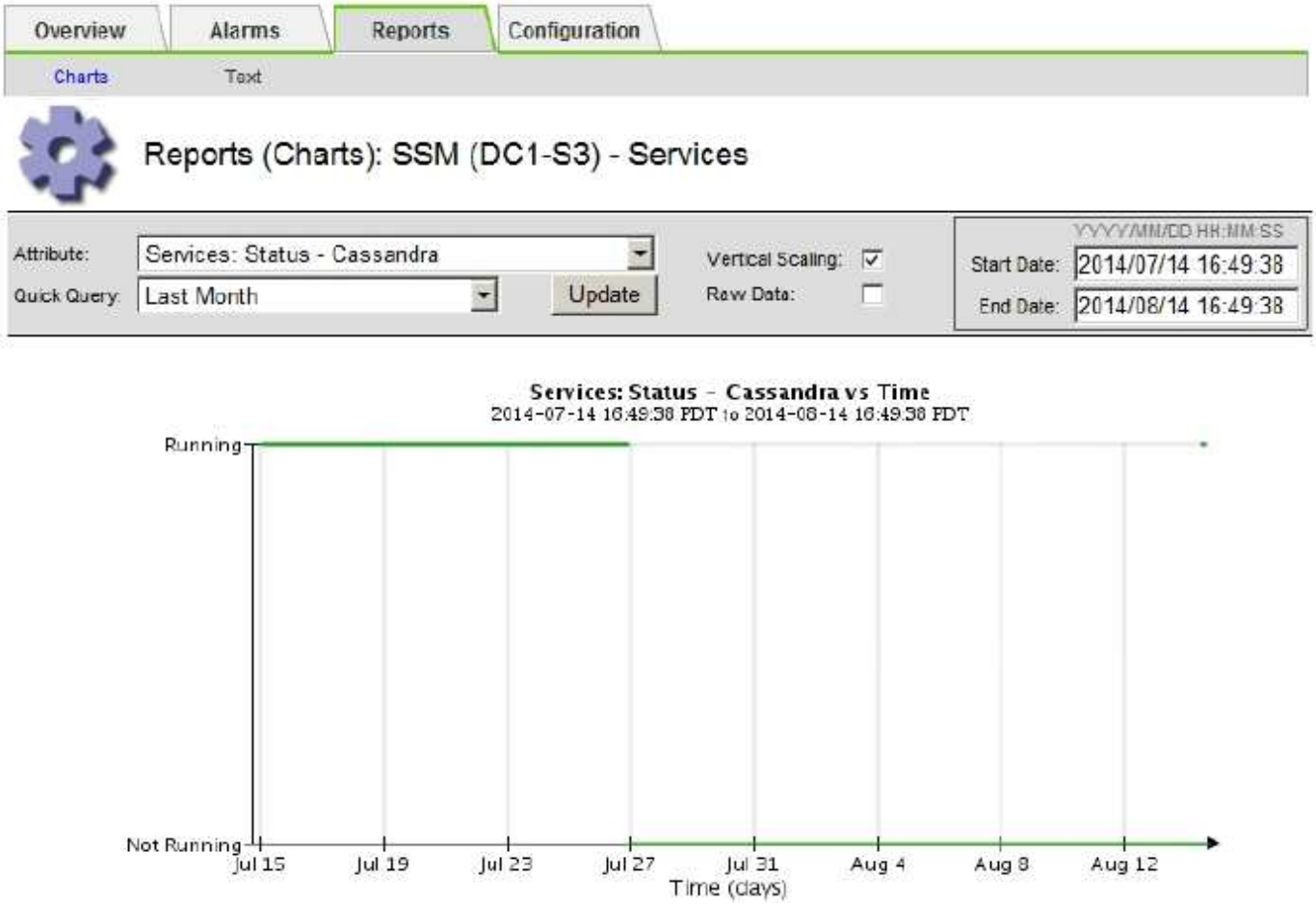
   b. Select **Attribute** > **Service: Status - Cassandra**.

   c. For **Start Date**, enter a date that is at least 16 days before the current date. For **End Date**, enter the current date.

   d. Click **Update**.

   e. 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.




6. To review the servermanager.log file on the Storage Node:
   a. Log in to the grid node:
      i. Enter the following command: `ssh admin@grid_node_IP`
      ii. Enter the password listed in the `Passwords.txt` file.
      iii. Enter the following command to switch to root: `su -`
      iv. Enter the password listed in the `Passwords.txt` file. When you are logged in as root, the prompt changes from `$` to `#`.
   b. Enter: `cat /var/local/log/servermanager.log`

      The contents of the servermanager.log file are displayed.

      If Cassandra has been down for longer than 15 days, the following message is displayed in the servermanager.log file:

      ```
      "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
      ```

   c. Make sure the timestamp of this message is the time when you attempted restarting Cassandra as instructed in step Restart Cassandra from the Storage Node.

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

d. If Cassandra has been down for longer than 15 days, you must rebuild the Cassandra database.

For instructions, see Recover Storage Node down more than 15 days.

e. Contact technical support if alarms do not clear after Cassandra is rebuilt.

#### Troubleshoot Cassandra Out of Memory errors (SMTT alarm)

A Total Events (SMTT) alarm is triggered when the Cassandra database has an out-of-memory error. If this error occurs, contact technical support to work through the issue.

**About this task**

If an out-of-memory error occurs for the Cassandra database, a heap dump is created, a Total Events (SMTT) alarm is triggered, and the Cassandra Heap Out Of Memory Errors count is incremented by one.

**Steps**

1. To view the event, select **SUPPORT** > **Tools** > **Grid topology** > **Configuration**.
2. Verify that the Cassandra Heap Out Of Memory Errors count is 1 or greater.

   You can run diagnostics to obtain additional information on the current state of your grid.

3. Go to `/var/local/core/`, compress the `Cassandra.hprof` file, and send it to technical support.
4. Make a backup of the `Cassandra.hprof` file, and delete it from the `/var/local/core/ directory`.

   This file can be as large as 24 GB, so you should remove it to free up space.

5. After the issue is resolved, select the **Reset** check box for the Cassandra Heap Out Of Memory Errors count. Then select **Apply Changes**.

   To reset event counts, you must have the Grid Topology Page Configuration permission.

### Troubleshoot certificate errors

If you see a security or certificate issue when you try to connect to StorageGRID using a web browser, an S3 or Swift client, or an external monitoring tool, you should check the certificate.

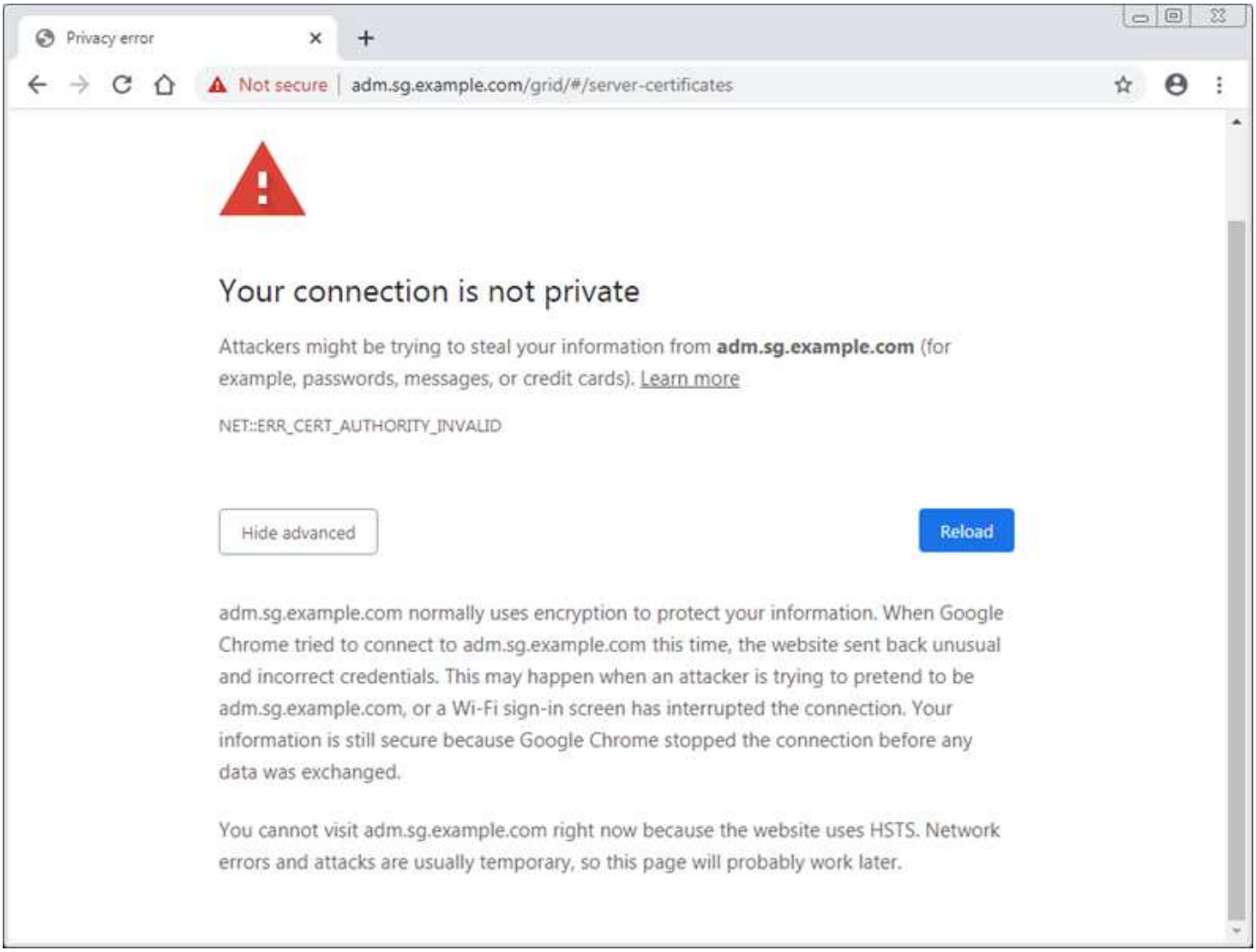
**About this task**

Certificate errors can cause problems when you try to connect to StorageGRID using the Grid Manager, Grid Management API, Tenant Manager, or the Tenant Management API. Certificate errors can also occur when you try to connect with an S3 or Swift client or external monitoring tool.

If you are accessing the Grid Manager or Tenant Manager using a domain name instead of an IP address, the browser shows a certificate error without an option to bypass if either of the following occurs:

- Your custom management interface certificate expires.
- You revert from a custom management interface certificate to the default server certificate.

The following example shows a certificate error when the custom management interface certificate expired:




To ensure that operations are not disrupted by a failed server certificate, the **Expiration of server certificate for Management Interface** alert is triggered when the server certificate is about to expire.

When you are using client certificates for external Prometheus integration, certificate errors can be caused by the StorageGRID management interface certificate or by client certificates. The **Expiration of client certificates configured on the Certificates page** alert is triggered when a client certificate is about to expire.

**Steps**

If you received an alert notification about an expired certificate, access the certificate details: . Select **CONFIGURATION** > **Security** > **Certificates** and then select the appropriate certificate tab.

1. Check the validity period of the certificate.
   Some web browsers and S3 or Swift clients do not accept certificates with a validity period greater than 398 days.
2. If the certificate has expired or will expire soon, upload or generate a new certificate.
   - For a server certificate, see the steps for configuring a custom server certificate for the Grid Manager and the Tenant Manager.
   - For a client certificate, see the steps for configuring a client certificate.
3. For server certificate errors, try either or both of the following options:
   - Ensure that the Subject Alternative Name (SAN) of the certificate is populated, and that the SAN matches the IP address or host name of the node that you are connecting to.

- If you are attempting to connect to StorageGRID using a domain name:
  i. Enter the IP address of the Admin Node instead of the domain name to bypass the connection error and access the Grid Manager.
  ii. From the Grid Manager, select **CONFIGURATION** > **Security** > **Certificates** and then select the appropriate certificate tab to install a new custom certificate or continue with the default certificate.
  iii. In the instructions for administering StorageGRID, see the steps for configuring a custom server certificate for the Grid Manager and the Tenant Manager.

### Troubleshoot Admin Node and user interface issues

There are several tasks you can perform to help determine the source of issues related to Admin Nodes and the StorageGRID user interface.

#### Troubleshoot sign-on errors

If you experience an error when you are signing in to a StorageGRID Admin Node, your system might have an issue with the identity federation configuration, a networking or hardware problem, an issue with Admin Node services, or an issue with the Cassandra database on connected Storage Nodes.

**What you'll need**

- You must have the `Passwords.txt` file.
- You must have specific access permissions.

**About this task**

Use these troubleshooting guidelines if you see any of the following error messages when attempting to sign in to an Admin Node:

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

**Steps**

1. Wait 10 minutes, and try signing in again.

   If the error is not resolved automatically, go to the next step.

2. If your StorageGRID system has more than one Admin Node, try signing in to the Grid Manager from another Admin Node.
   - If you are able to sign in, you can use the **Dashboard**, **NODES**, **Alerts**, and **SUPPORT** options to help determine the cause of the error.
   - If you have only one Admin Node or you still cannot sign in, go to the next step.
3. Determine if the node's hardware is offline.
4. If single sign-on (SSO) is enabled for your StorageGRID system, refer to the steps for configuring single sign-on, in the instructions for administering StorageGRID.

You might need to temporarily disable and re-enable SSO for a single Admin Node to resolve any issues.

> If SSO is enabled, you cannot sign on using a restricted port. You must use port 443.

5. Determine if the account you are using belongs to a federated user.

   If the federated user account is not working, try signing in to the Grid Manager as a local user, such as root.

   - If the local user can sign in:
     i. Review any displayed alarms.
     ii. Select **CONFIGURATION** > **Access Control** > **Identity federation**.
     iii. Click **Test Connection** to validate your connection settings for the LDAP server.
     iv. If the test fails, resolve any configuration errors.
   - If the local user cannot sign in and you are confident that the credentials are correct, go to the next step.

6. Use Secure Shell (ssh) to log in to the Admin Node:
   a. Enter the following command: `ssh admin@Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.

7. View the status of all services running on the grid node: `storagegrid-status`

   Make sure the nms, mi, nginx, and mgmt api services are all running.

   The output is updated immediately if the status of a service changes.

```
$ storagegrid-status
Host Name                       99-211
IP Address                      10.96.99.211
Operating System Kernel         4.19.0         Verified
Operating System Environment    Debian 10.1    Verified
StorageGRID Webscale Release    11.4.0         Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                 5.5.9999+default Running
Network Monitoring              11.4.0         Running
Time Synchronization            1:4.2.8p10+dfsg Running
ams                             11.4.0         Running
cmn                             11.4.0         Running
nms                             11.4.0         Running
ssm                             11.4.0         Running
mi                              11.4.0         Running
dynip                           11.4.0         Running
nginx                           1.10.3         Running
tomcat                          9.0.27         Running
grafana                         6.4.3          Running
mgmt api                        11.4.0         Running
prometheus                      11.4.0         Running
persistence                     11.4.0         Running
ade exporter                    11.4.0         Running
alertmanager                    11.4.0         Running
attrDownPurge                   11.4.0         Running
attrDownSamp1                   11.4.0         Running
attrDownSamp2                   11.4.0         Running
node exporter                   0.17.0+ds      Running
sg snmp agent                   11.4.0         Running
```

8. Confirm that the nginx-gw service is running `# service nginx-gw status`
9. Use Lumberjack to collect logs: `# /usr/local/sbin/lumberjack.rb`

   If the failed authentication happened in the past, you can use the --start and --end Lumberjack script options to specify the appropriate time range. Use lumberjack -h for details on these options.

   The output to the terminal indicates where the log archive has been copied.

10. Review the following logs:
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`
    - `**/*commands.txt`

11. If you could not identify any issues with the Admin Node, issue either of the following commands to determine the IP addresses of the three Storage Nodes that run the ADC service at your site. Typically, these are the first three Storage Nodes that were installed at the site.

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

Admin Nodes use the ADC service during the authentication process.

12. From the Admin Node, log in to each of the ADC Storage Nodes, using the IP addresses you identified.
    a. Enter the following command: `ssh admin@grid_node_IP`
    b. Enter the password listed in the `Passwords.txt` file.
    c. Enter the following command to switch to root: `su -`
    d. Enter the password listed in the `Passwords.txt` file.

    When you are logged in as root, the prompt changes from `$` to `#`.

13. View the status of all services running on the grid node: `storagegrid-status`

    Make sure the idnt, acct, nginx, and cassandra services are all running.

14. Repeat steps Use Lumberjack to collect logs and Review logs to review the logs on the Storage Nodes.
15. If you are unable to resolve the issue, contact technical support.

    Provide the logs you collected to technical support. See also Log files reference.

#### Troubleshoot user interface issues

You might see issues with the Grid Manager or the Tenant Manager after upgrading to a new version of StorageGRID software.

### Web interface does not respond as expected

The Grid Manager or the Tenant Manager might not respond as expected after StorageGRID software is upgraded.

If you experience issues with the web interface:

- Make sure you are using a supported web browser.

  > Browser support has changed for StorageGRID 11.5. Confirm you are using a supported version.

- Clear your web browser cache.

  Clearing the cache removes outdated resources used by the previous version of StorageGRID software,

and permits the user interface to operate correctly again. For instructions, see the documentation for your web browser.

#### Check the status of an unavailable Admin Node

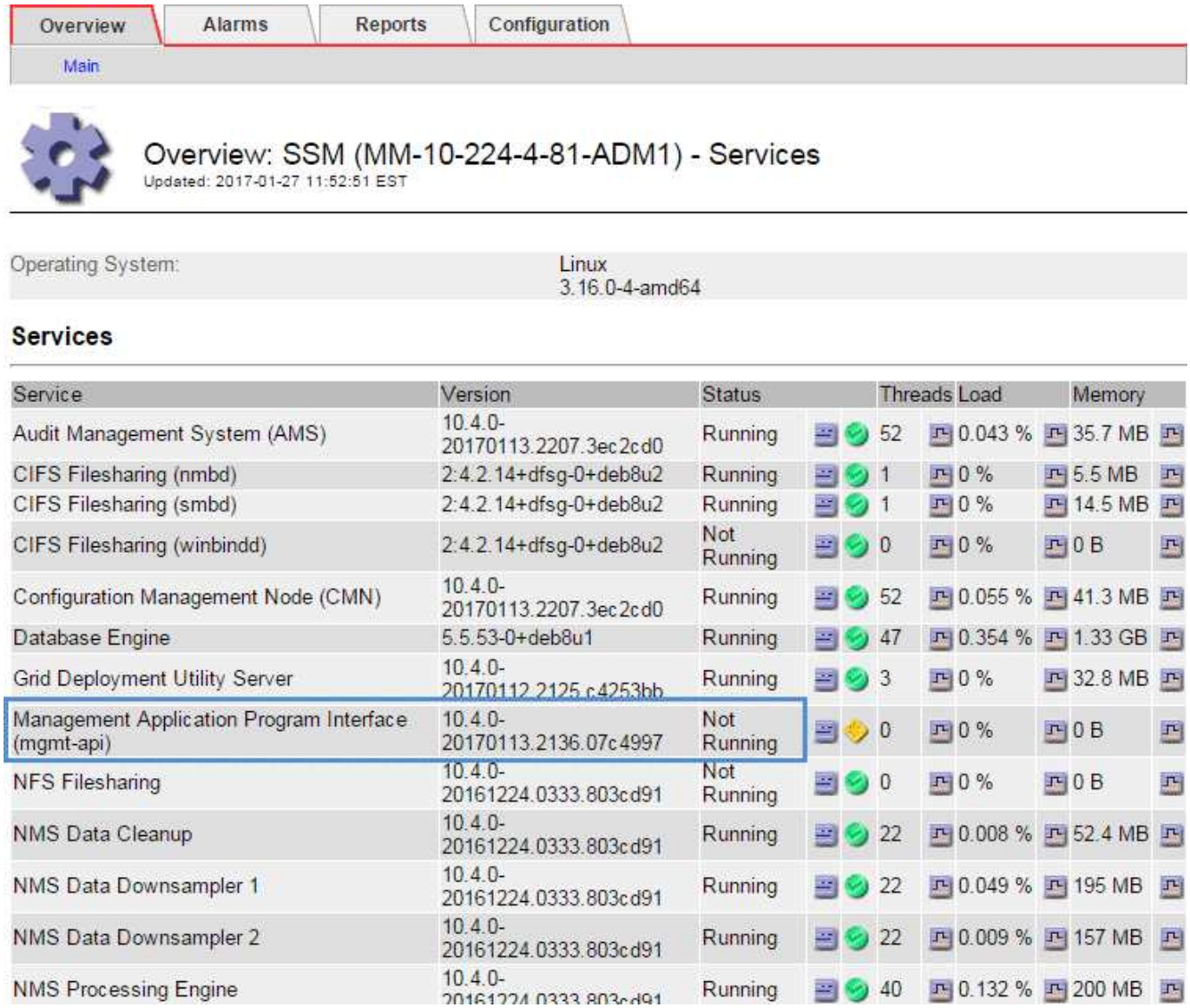
If the StorageGRID system includes multiple Admin Nodes, you can use another Admin Node to check the status of an unavailable Admin Node.

**What you'll need**

You must have specific access permissions.

**Steps**

1. From an available Admin Node, sign in to the Grid Manager using a supported web browser.
2. Select **SUPPORT** > **Tools** > **Grid topology**.
3. Select ***Site*** **> unavailable Admin Node** > **SSM** > **Services** > **Overview** > **Main**.
4. Look for services that have a status of Not Running and that might also be displayed in blue.




5. Determine if alarms have been triggered.

6. Take the appropriate actions to resolve the issue.

**Related information**

Administer StorageGRID

## Troubleshoot network, hardware, and platform issues

There are several tasks you can perform to help determine the source of issues related to StorageGRID network, hardware, and platform issues.

### Troubleshoot “422: Unprocessable Entity” errors

The error 422: Unprocessable Entity can occur in a number of circumstances. Check the error message to determine what caused your issue.

If you see one of the listed error messages, take the recommended action.

| Error message | Root cause and corrective action |
|---|---|
| `422: Unprocessable Entity`<br><br>`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839` | This message might occur if you select the **Do not use TLS** option for Transport Layer Security (TLS) when configuring identity federation using Windows Active Directory (AD).<br><br>Using the **Do not use TLS** option is not supported for use with AD servers that enforce LDAP signing. You must select either the **Use STARTTLS** option or the **Use LDAPS** option for TLS. |

| Error message | Root cause and corrective action |
| --- | --- |
| `422: Unprocessable Entity`<br><br>`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)` | This message appears if you try to use an unsupported cipher to make a Transport Layer Security (TLS) connection from StorageGRID to an external system used for identify federation or Cloud Storage Pools.<br><br>Check the ciphers that are offered by the external system. The system must use one of the ciphers supported by StorageGRID for outgoing TLS connections, as shown in the instructions for administering StorageGRID. |

**Related information**

Administer StorageGRID

#### Troubleshoot the Grid Network MTU mismatch alert

The **Grid Network MTU mismatch** alert is triggered when the maximum transmission unit (MTU) setting for the Grid Network interface (eth0) differs significantly across nodes in the grid.

**About this task**

The differences in MTU settings could indicate that some, but not all, eth0 networks are configured for jumbo frames. An MTU size mismatch of greater than 1000 might cause network performance problems.

**Steps**

1. List the MTU settings for eth0 on all nodes.
   - Use the query provided in the Grid Manager.
   - Navigate to *`primary Admin Node IP address`*`/metrics/graph` and enter the following query: `node_network_mtu_bytes{interface='eth0'}`
2. Modify the MTU settings as necessary to ensure they are the same for the Grid Network interface (eth0) on all nodes.
   - For appliance nodes, see the installation and maintenance instructions for your appliance.
   - For Linux- and VMware-based nodes, use the following command: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

     **Example**: `change-ip.py -n node 1500 grid admin`

     **Note**: On Linux-based nodes, if the desired MTU value for the network in the container exceeds the value already configured on the host interface, you must first configure the host interface to have the desired MTU value, and then use the `change-ip.py` script to change the MTU value of the network in the container.

Use the following arguments for modifying the MTU on Linux- or VMware-based nodes.

| Positional arguments | Description |
| --- | --- |
| `mtu` | The MTU to set. Must be in the range 1280 to 9216. |
| `network` | The networks to apply the MTU to. Include one or more of the following network types:<br>• grid<br>• admin<br>• client |

| Optional arguments | Description |
| --- | --- |
| `-h, - help` | Show the help message and exit. |
| `-n node, --node node` | The node. The default is the local node. |

**Related information**

SG100 and SG1000 services appliances

SG6000 storage appliances

SG5700 storage appliances

SG5600 storage appliances

#### Troubleshoot the Network Receive Error (NRER) alarm

Network Receive Error (NRER) alarms can be caused by connectivity issues between StorageGRID and your network hardware. In some cases, NRER errors can clear without manual intervention. If the errors do not clear, take the recommended actions.

**About this task**

NRER alarms can be caused by the following issues with networking hardware that connects to StorageGRID:

- Forward error correction (FEC) is required and not in use
- Switch port and NIC MTU mismatch
- High link error rates
- NIC ring buffer overrun

**Steps**

1. Follow the troubleshooting steps for all potential causes of the NRER alarm given your network configuration.
    - If the error is caused by FEC mismatch, perform the following steps:

**Note**: These steps are applicable only for NRER errors caused by FEC mismatch on StorageGRID appliances.

i. Check the FEC status of the port in the switch attached to your StorageGRID appliance.

ii. Check the physical integrity of the cables from the appliance to the switch.

iii. If you want to change FEC settings to try to resolve the NRER alarm, first ensure that the appliance is configured for **Auto** mode on the Link Configuration page of the StorageGRID Appliance Installer (see the installation and maintenance instructions for your appliance). Then, change the FEC settings on the switch ports. The StorageGRID appliance ports will adjust their FEC settings to match, if possible.

(You cannot configure FEC settings on StorageGRID appliances. Instead, the appliances attempt to discover and mirror the FEC settings on the switch ports they are connected to. If the links are forced to 25-GbE or 100-GbE network speeds, the switch and NIC might fail to negotiate a common FEC setting. Without a common FEC setting, the network will fall back to “no-FEC” mode. When FEC is not enabled, the connections are more susceptible to errors caused by electrical noise.)

**Note**: StorageGRID appliances support Firecode (FC) and Reed Solomon (RS) FEC, as well as no FEC.

- If the error is caused by a switch port and NIC MTU mismatch, check that the MTU size configured on the node is the same as the MTU setting for the switch port.

  The MTU size configured on the node might be smaller than the setting on the switch port the node is connected to. If a StorageGRID node receives an Ethernet frame larger than its MTU, which is possible with this configuration, the NRER alarm might be reported. If you believe this is what is happening, either change the MTU of the switch port to match the StorageGRID network interface MTU, or change the MTU of the StorageGRID network interface to match the switch port, depending on your end-to-end MTU goals or requirements.

  > For the best network performance, all nodes should be configured with similar MTU values on their Grid Network interfaces. The **Grid Network MTU mismatch** alert is triggered if there is a significant difference in MTU settings for the Grid Network on individual nodes. The MTU values do not have to be the same for all network types.

  > To change the MTU setting, see the installation and maintenance guide for your appliance.

- If the error is caused by high link error rates, perform the following steps:

  i. Enable FEC, if not already enabled.

  ii. Verify that your network cabling is of good quality and is not damaged or improperly connected.

  iii. If the cables do not appear to be the problem, contact technical support.

  > You might notice high error rates in an environment with high electrical noise.

- If the error is a NIC ring buffer overrun, contact technical support.

  The ring buffer can be overrun when the StorageGRID system is overloaded and unable to process network events in a timely manner.

2. After you resolve the underlying problem, reset the error counter.

a. Select **SUPPORT** > **Tools** > **Grid topology**.

b. Select ***site*** > ***grid node*** > **SSM** > **Resources** > **Configuration** > **Main**.

c. Select **Reset Receive Error Count** and click **Apply Changes**.

**Related information**

Troubleshoot the Grid Network MTU mismatch alert

Alarms reference (legacy system)

SG6000 storage appliances

SG5700 storage appliances

SG5600 storage appliances

SG100 and SG1000 services appliances

#### Troubleshoot time synchronization errors

You might see issues with time synchronization in your grid.

If you encounter time synchronization problems, verify that you have specified at least four external NTP sources, each providing a Stratum 3 or better reference, and that all external NTP sources are operating normally and are accessible by your StorageGRID nodes.

> When specifying the external NTP source for a production-level StorageGRID installation, do not use the Windows Time (W32Time) service on a version of Windows earlier than Windows Server 2016. The time service on earlier versions of Windows is not sufficiently accurate and is not supported by Microsoft for use in high-accuracy environments, such as StorageGRID.

**Related information**

Recover and maintain

#### Linux: Network connectivity issues

You might see issues with network connectivity for StorageGRID grid nodes hosted on Linux hosts.

### MAC address cloning

In some cases, network issues can be resolved by using MAC address cloning. If you are using virtual hosts, set the value of the MAC address cloning key for each of your networks to "true" in your node configuration file. This setting causes the MAC address of the StorageGRID container to use the MAC address of the host. To create node configuration files, see the instructions in the installation guide for your platform.

> Create separate virtual network interfaces for use by the Linux host OS. Using the same network interfaces for the Linux host OS and the StorageGRID container might cause the host OS to become unreachable if promiscuous mode has not been enabled on the hypervisor.

For more information on enabling MAC cloning, see the instructions in the installation guide for your platform.

### Promiscuous mode

If you do not want to use MAC address cloning and would rather allow all interfaces to receive and transmit data for MAC addresses other than the ones assigned by the hypervisor, ensure that the security properties at the virtual switch and port group levels are set to **Accept** for Promiscuous Mode, MAC Address Changes, and Forged Transmits. The values set on the virtual switch can be overridden by the values at the port group level, so ensure that settings are the same in both places.

### Related information

Install Red Hat Enterprise Linux or CentOS

Install Ubuntu or Debian

#### Linux: Node status is "orphaned"

A Linux node in an orphaned state usually indicates that either the storagegrid service or the StorageGRID node daemon controlling the node's container died unexpectedly.

### About this task

If a Linux node reports that it is in an orphaned state, you should:

- Check logs for errors and messages.
- Attempt to start the node again.
- If necessary, use container engine commands to stop the existing node container.
- Restart the node.

### Steps

1. Check logs for both the service daemon and the orphaned node for obvious errors or messages about exiting unexpectedly.
2. Log in to the host as root or using an account with sudo permission.
3. Attempt to start the node again by running the following command: `$ sudo storagegrid node start node-name`

   ```
   $ sudo storagegrid node start DC1-S1-172-16-1-172
   ```

   If the node is orphaned, the response is

   ```
   Not starting ORPHANED node DC1-S1-172-16-1-172
   ```

4. From Linux, stop the container engine and any controlling storagegrid-node processes. For example:`sudo docker stop --time secondscontainer-name`

   For `seconds`, enter the number of seconds you want to wait for the container to stop (typically 15 minutes or less). For example:

   ```
   sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
   ```

5. Restart the node: `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

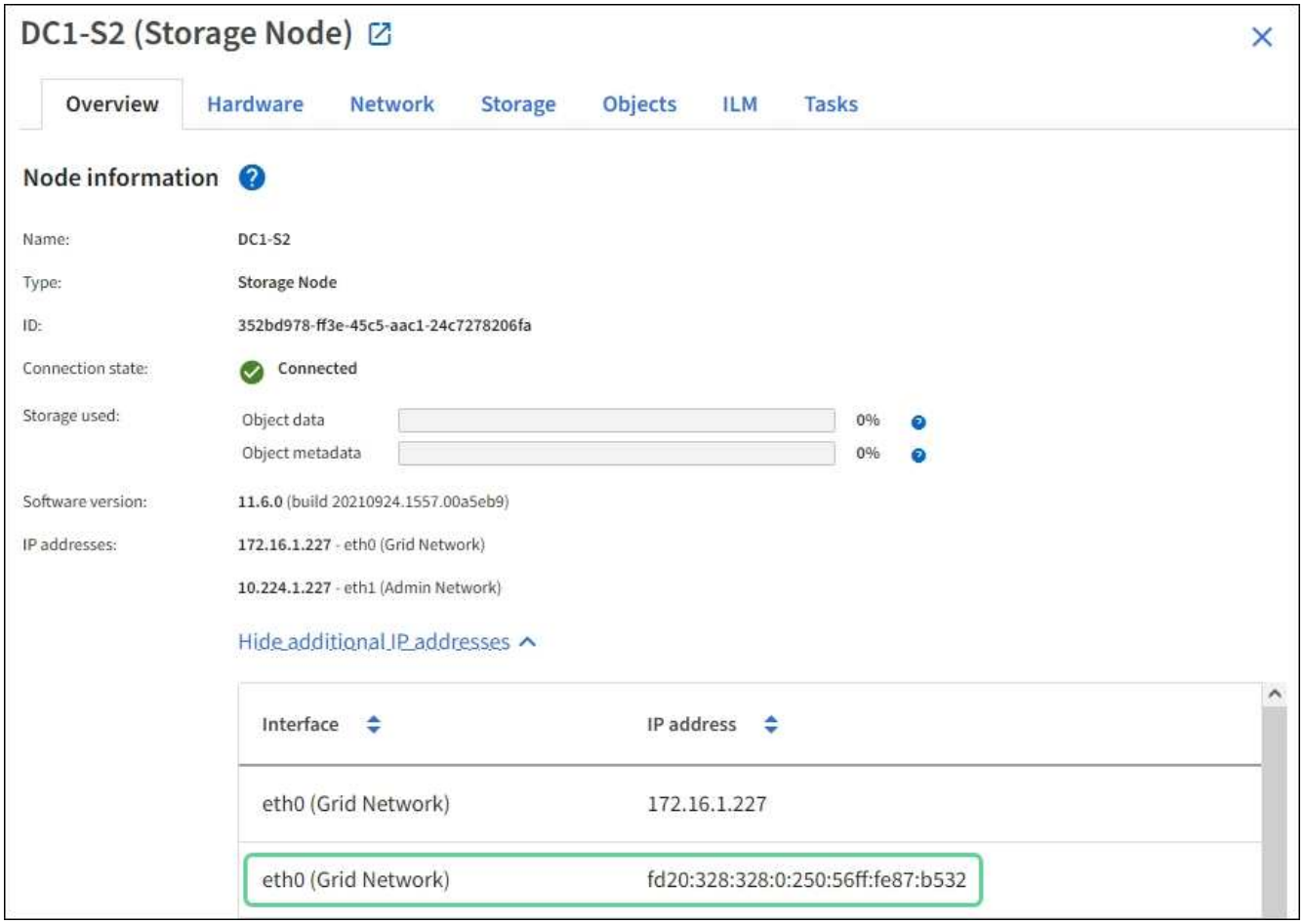
#### Linux: Troubleshoot IPv6 support

You might need to enable IPv6 support in the kernel if you have installed StorageGRID nodes on Linux hosts and you notice that IPv6 addresses have not been assigned to the node containers as expected.

**About this task**

You can see the IPv6 address that has been assigned to a grid node in the following locations in the Grid Manager:

- Select **NODES**, and select the node. Then, select **Show more** next to **IP Addresses** on the Overview tab.




- Select **SUPPORT** > **Tools** > **Grid topology**. Then, select ***node*** > **SSM** > **Resources**. If an IPv6 address has been assigned, it is listed below the IPv4 address in the **Network Addresses** section.

If the IPv6 address is not shown and the node is installed on a Linux host, follow these steps to enable IPv6 support in the kernel.

**Steps**

1. Log in to the host as root or using an account with sudo permission.

2. Run the following command: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

The result should be 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

> If the result is not 0, see the documentation for your operating system for changing `sysctl` settings. Then, change the value to 0 before continuing.

3. Enter the StorageGRID node container: `storagegrid node enter node-name`
4. Run the following command: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

The result should be 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```

> If the result is not 1, this procedure does not apply. Contact technical support.

5. Exit the container: `exit`

```
root@DC1-S1:~ # exit
```

6. As root, edit the following file: `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Locate the following two lines and remove the comment tags. Then, save and close the file.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Run these commands to restart the StorageGRID container:

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

#### Troubleshoot an external syslog server

The following table describes external syslog server error messages and lists corrective actions.

| Error message | Description and recommended actions |
|---|---|
| Cannot resolve hostname | The FQDN you entered for the syslog server could not be resolved to an IP address.<br>1. Check the hostname you entered. If you entered an IP address, make sure it is a valid IP address in W.X.Y.Z (“dotted decimal”) notation.<br>2. Check that the DNS servers are configured correctly.<br>3. Confirm that each node can access the IP addresses for the DNS server. |
| Connection refused | A TCP or TLS connection to the syslog server was refused. There might be no service listening on the TCP or TLS port for the host, or a firewall might be blocking access.<br>1. Check that you entered the correct FQDN or IP address, port, and protocol for the syslog server.<br>2. Confirm that the host for the syslog service is running a syslog daemon that is listening on the specified port.<br>3. Confirm that a firewall is not blocking access to TCP/TLS connections from the nodes to the IP and port of the syslog server. |
| Network unreachable | The syslog server is not on a directly attached subnet. A router returned an ICMP failure message to indicate it could not forward the test messages from the listed nodes to the syslog server.<br>1. Check that you entered the correct FQDN or IP address for the syslog server.<br>2. For each node listed, check the Grid Network Subnet List, the Admin Networks Subnet Lists, and the Client Network gateways. Confirm these are configured to route traffic to the syslog server over the expected network interface and gateway (Grid, Admin, or Client). |

| Error message | Description and recommended actions |
| --- | --- |
| Host unreachable | The syslog server is on a directly attached subnet (subnet used by the listed nodes for their Grid, Admin, or Client IP addresses). The nodes attempted to send test messages, but did not receive responses to ARP requests for the syslog server's MAC address.<br>1. Check that you entered the correct FQDN or IP address for the syslog server.<br>2. Check that the host running the syslog service is up. |
| Connection timed out | A TCP/TLS connection attempt was made, but no response was received from the syslog server for a long time. There might be a routing misconfiguration or a firewall might be dropping traffic without sending any response (a common configuration).<br>1. Check that you entered the correct FQDN or IP address for the syslog server.<br>2. For each node listed, check the Grid Network Subnet List, the Admin Networks Subnet Lists, and the Client Network gateways. Confirm these are configured to route traffic to the syslog server via the network interface and gateway (Grid, Admin, or Client) over which you expect the syslog server to be reached.<br>3. Confirm that a firewall is not blocking access to TCP/TLS connections from the nodes listed to the IP and port of the syslog server. |
| Connection closed by partner | A TCP connection to the syslog server was successfully established but was later closed. Reasons for this might include:<br>• The syslog server might have been restarted or rebooted.<br>• The node and the syslog server might have different TCP/TLS settings.<br>• An intermediate firewall might be closing idle TCP connections.<br>• A non-syslog server listening on the syslog server port might have closed the connection.<br>  1. Check that you entered the correct FQDN or IP address, port, and protocol for the syslog server.<br>  2. If you are using TLS, confirm the syslog server is also using TLS. If you are using TCP, confirm the syslog server is also using TCP.<br>  3. Check that an intermediate firewall is not configured to close idle TCP connections. |

| Error message | Description and recommended actions |
| --- | --- |
| TLS certificate error | The server certificate received from the syslog server was not compatible with the CA certificate bundle and client certificate you provided.<br>1. Confirm that the CA certificate bundle and client certificate (if any) are compatible with the server certificate on the syslog server.<br>2. Confirm that the identities in the server certificate from the syslog server include the expected IP or FQDN values. |
| Forwarding suspended | Syslog records are no longer being forwarded to the syslog server and StorageGRID is unable to detect the reason.<br>Review the debugging logs provided with this error to attempt to determine the root cause. |
| TLS session terminated | The syslog server terminated the TLS session and StorageGRID is unable to detect the reason.<br>1. Review the debugging logs provided with this error to attempt to determine the root cause.<br>2. Check that you entered the correct FQDN or IP address, port, and protocol for the syslog server.<br>3. If you are using TLS, confirm the syslog server is also using TLS. If you are using TCP, confirm the syslog server is also using TCP.<br>4. Confirm that the CA certificate bundle and client certificate (if any) are compatible with the server certificate from the syslog server.<br>5. Confirm that the identities in the server certificate from the syslog server include the expected IP or FQDN values. |
| Results query failed | The Admin Node used for syslog server configuration and testing is unable to request test results from the nodes listed. One or more nodes might be down.<br>1. Follow standard troubleshooting steps to ensure that the nodes are online and all expected services are running.<br>2. Restart the miscd service on the nodes listed. |

## Alerts reference

The following table lists all default StorageGRID alerts. As required, you can create custom alert rules to fit your system management approach.

See the information about commonly used Prometheus metrics to learn about the metrics used in some of these alerts.

| Alert name | Description and recommended actions |
| --- | --- |
| Appliance battery expired | The battery in the appliance's storage controller has expired.<br>1. Replace the battery. The steps to remove and replace a battery are included in the procedure for replacing a storage controller. See the instructions for your storage appliance:<br>◦ SG5600 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG6000 storage appliances<br>2. If this alert persists, contact technical support. |
| Appliance battery failed | The battery in the appliance's storage controller has failed.<br>1. Replace the battery. The steps to remove and replace a battery are included in the procedure for replacing a storage controller. See the instructions for your storage appliance:<br>◦ SG5600 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG6000 storage appliances<br>2. If this alert persists, contact technical support. |
| Appliance battery has insufficient learned capacity | The battery in the appliance's storage controller has insufficient learned capacity.<br>1. Replace the battery. The steps to remove and replace a battery are included in the procedure for replacing a storage controller. See the instructions for your storage appliance:<br>◦ SG5600 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG6000 storage appliances<br>2. If this alert persists, contact technical support. |
| Appliance battery near expiration | The battery in the appliance's storage controller is nearing expiration.<br>1. Replace the battery soon. The steps to remove and replace a battery are included in the procedure for replacing a storage controller. See the instructions for your storage appliance:<br>◦ SG5600 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG6000 storage appliances<br>2. If this alert persists, contact technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| Appliance battery removed | The battery in the appliance's storage controller is missing.<br><br>1. Install a battery. The steps to remove and replace a battery are included in the procedure for replacing a storage controller. See the instructions for your storage appliance:<br>◦ SG5600 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG6000 storage appliances<br>2. If this alert persists, contact technical support. |
| Appliance battery too hot | The battery in the appliance's storage controller is overheated.<br><br>1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert.<br>2. Investigate possible reasons for the temperature increase, such as a fan or HVAC failure.<br>3. If this alert persists, contact technical support. |
| Appliance BMC communication error | Communication with the baseboard management controller (BMC) has been lost.<br><br>1. Confirm that the BMC is operating normally. Select **NODES**, and then select the **Hardware** tab for the appliance node. Locate the Compute Controller BMC IP field, and browse to that IP.<br>2. Attempt to restore BMC communications by placing the node into maintenance mode and then powering the appliance off and back on. See the instructions for your appliance:<br>◦ SG100 and SG1000 services appliances<br>◦ SG6000 storage appliances<br>3. If this alert persists, contact technical support. |
| Appliance cache backup device failed | A persistent cache backup device has failed.<br><br>1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert.<br>2. Contact technical support. |
| Appliance cache backup device insufficient capacity | There is insufficient cache backup device capacity.<br><br>Contact technical support. |
| Appliance cache backup device write-protected | A cache backup device is write-protected.<br><br>Contact technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| Appliance cache memory size mismatch | The two controllers in the appliance have different cache sizes.<br><br>Contact technical support. |
| Appliance compute controller chassis temperature too high | The temperature of the compute controller in a StorageGRID appliance has exceeded a nominal threshold.<br><br>1. Check the hardware components for overheating conditions, and follow the recommended actions:<br>  ◦ If you have an SG100, SG1000, or SG6000, use the BMC.<br>  ◦ If you have an SG5600 or SG5700, use SANtricity System Manager.<br>2. If necessary, replace the component. See the instructions for your appliance:<br>  ◦ SG100 and SG1000 services appliances<br>  ◦ SG6000 storage appliances<br>  ◦ SG5700 storage appliances<br>  ◦ SG5600 storage appliances |
| Appliance compute controller CPU temperature too high | The temperature of the CPU in the compute controller in a StorageGRID appliance has exceeded a nominal threshold.<br><br>1. Check the hardware components for overheating conditions, and follow the recommended actions:<br>  ◦ If you have an SG100, SG1000, or SG6000, use the BMC.<br>  ◦ If you have an SG5600 or SG5700, use SANtricity System Manager.<br>2. If necessary, replace the component. See the instructions for your appliance:<br>  ◦ SG100 and SG1000 services appliances<br>  ◦ SG5600 storage appliances<br>  ◦ SG5700 storage appliances<br>  ◦ SG6000 storage appliances |

| Alert name | Description and recommended actions |
| --- | --- |
| Appliance compute controller needs attention | A hardware fault has been detected in the compute controller of a StorageGRID appliance.<br>1. Check the hardware components for errors, and follow the recommended actions:<br>◦ If you have an SG100, SG1000, or SG6000, use the BMC.<br>◦ If you have an SG5600 or SG5700, use SANtricity System Manager.<br>2. If necessary, replace the component. See the instructions for your appliance:<br>◦ SG100 and SG1000 services appliances<br>◦ SG5600 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG6000 storage appliances |
| Appliance compute controller power supply A has a problem | Power supply A in the compute controller has a problem.This alert might indicate that the power supply has failed or that it has a problem providing power.<br>1. Check the hardware components for errors, and follow the recommended actions:<br>◦ If you have an SG100, SG1000, or SG6000, use the BMC.<br>◦ If you have an SG5600 or SG5700, use SANtricity System Manager.<br>2. If necessary, replace the component. See the instructions for your appliance:<br>◦ SG100 and SG1000 services appliances<br>◦ SG5600 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG6000 storage appliances |

| Alert name | Description and recommended actions |
| --- | --- |
| Appliance compute controller power supply B has a problem | Power supply B in the compute controller has a problem.<br><br>This alert might indicate that the power supply has failed or that it has a problem providing power.<br><br>1. Check the hardware components for errors, and follow the recommended actions:<br>  ◦ If you have an SG100, SG1000, or SG6000, use the BMC.<br>  ◦ If you have an SG5600 or SG5700, use SANtricity System Manager.<br>2. If necessary, replace the component. See the instructions for your appliance:<br>  ◦ SG100 and SG1000 services appliances<br>  ◦ SG5600 storage appliances<br>  ◦ SG5700 storage appliances<br>  ◦ SG6000 storage appliances |
| Appliance compute hardware monitor service stalled | The service that monitors storage hardware status has stopped reporting data.<br><br>1. Check the status of the eos-system-status service in the base-os.<br>2. If the service is in a stopped or error state, restart the service.<br>3. If this alert persists, contact technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| Appliance Fibre Channel fault detected | A Fibre Channel link problem has been detected between the appliance storage controller and compute controller.<br><br>This alert might indicate that there is a problem with the Fibre Channel connection between the storage and compute controllers in the appliance.<br><br>1. Check the hardware components for errors (**NODES** > ***appliance node*** > **Hardware**). If the status of any of the components is not "Nominal," take these actions:<br>  a. Verify that the Fibre Channel cables between controllers are completely connected.<br>  b. Ensure that the Fibre Channel cables are free of excessive bends.<br>  c. Confirm that the SFP+ modules are properly seated.<br><br>  **Note:** If this problem persists, the StorageGRID system might take the problematic connection offline automatically.<br><br>2. If necessary, replace components. See the instructions for your appliance:<br>  ◦ SG5700 storage appliances<br>  ◦ SG6000 storage appliances |
| Appliance Fibre Channel HBA port failure | A Fibre Channel HBA port is failing or has failed.<br><br>Contact technical support. |
| Appliance flash cache drives non-optimal | The drives used for the SSD cache are non-optimal.<br><br>1. Replace the SSD cache drives. See the instructions for your appliance:<br>  ◦ SG5600 storage appliances<br>  ◦ SG5700 storage appliances<br>  ◦ SG6000 storage appliances<br>2. If this alert persists, contact technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| Appliance interconnect/battery canister removed | The interconnect/battery canister is missing.<br>1. Replace the battery. The steps to remove and replace a battery are included in the procedure for replacing a storage controller. See the instructions for your storage appliance.<br>◦ SG5600 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG6000 storage appliances<br>2. If this alert persists, contact technical support. |
| Appliance LACP port missing | A port on a StorageGRID appliance is not participating in the LACP bond.<br>1. Check the configuration for the switch. Ensure the interface is configured in the correct link aggregation group.<br>2. If this alert persists, contact technical support. |
| Appliance overall power supply degraded | The power of a StorageGRID appliance has deviated from the recommended operating voltage.<br>1. Check the status of power supply A and B to determine which power supply is operating abnormally, and follow the recommended actions:<br>◦ If you have an SG100, SG1000, or SG6000, use the BMC.<br>◦ If you have an SG5600 or SG5700, use SANtricity System Manager.<br>2. If necessary, replace the component. See the instructions for your appliance:<br>◦ SG6000 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG5600 storage appliances<br>◦ SG100 and SG1000 services appliances |
| Appliance storage controller A failure | Storage controller A in a StorageGRID appliance has failed.<br>1. Use SANtricity System Manager to check hardware components, and follow the recommended actions.<br>2. If necessary, replace the component. See the instructions for your appliance:<br>◦ SG6000 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG5600 storage appliances |

| Alert name | Description and recommended actions |
| --- | --- |
| Appliance storage controller B failure | Storage controller B in a StorageGRID appliance has failed.<br>1. Use SANtricity System Manager to check hardware components, and follow the recommended actions.<br>2. If necessary, replace the component. See the instructions for your appliance:<br>◦ SG6000 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG5600 storage appliances |
| Appliance storage controller drive failure | One or more drives in a StorageGRID appliance has failed or is not optimal.<br>1. Use SANtricity System Manager to check hardware components, and follow the recommended actions.<br>2. If necessary, replace the component. See the instructions for your appliance:<br>◦ SG6000 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG5600 storage appliances |
| Appliance storage controller hardware issue | SANtricity software is reporting "Needs attention" for a component in a StorageGRID appliance.<br>1. Use SANtricity System Manager to check hardware components, and follow the recommended actions.<br>2. If necessary, replace the component. See the instructions for your appliance:<br>◦ SG6000 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG5600 storage appliances |
| Appliance storage controller power supply A failure | Power supply A in a StorageGRID appliance has deviated from the recommended operating voltage.<br>1. Use SANtricity System Manager to check hardware components, and follow the recommended actions.<br>2. If necessary, replace the component. See the instructions for your appliance:<br>◦ SG6000 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG5600 storage appliances |

| Alert name | Description and recommended actions |
| --- | --- |
| Appliance storage controller power supply B failure | Power supply B in a StorageGRID appliance has deviated from the recommended operating voltage.<br>1. Use SANtricity System Manager to check hardware components, and follow the recommended actions.<br>2. If necessary, replace the component. See the instructions for your appliance:<br>◦ SG6000 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG5600 storage appliances |
| Appliance storage hardware monitor service stalled | The service that monitors storage hardware status has stopped reporting data.<br>1. Check the status of the eos-system-status service in the base-os.<br>2. If the service is in a stopped or error state, restart the service.<br>3. If this alert persists, contact technical support. |
| Appliance storage shelves degraded | The status of one of the components in the storage shelf for a storage appliance is degraded.<br>1. Use SANtricity System Manager to check hardware components, and follow the recommended actions.<br>2. If necessary, replace the component. See the instructions for your appliance:<br>◦ SG6000 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG5600 storage appliances |
| Appliance temperature exceeded | The nominal or maximum temperature for the appliance's storage controller has been exceeded.<br>1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert.<br>2. Investigate possible reasons for the temperature increase, such as a fan or HVAC failure.<br>3. If this alert persists, contact technical support. |
| Appliance temperature sensor removed | A temperature sensor has been removed. Contact technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| Cassandra auto-compactor error | The Cassandra auto-compactor has experienced an error.<br><br>The Cassandra auto-compactor exists on all Storage Nodes and manages the size of the Cassandra database for overwrite and delete heavy workloads. While this condition persists, certain workloads will experience unexpectedly high metadata consumption.<br><br>1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert.<br>2. Contact technical support. |
| Audit logs are being added to the in-memory queue | Node cannot send logs to the local syslog server and the in-memory queue is filling up.<br><br>1. Ensure that the rsyslog service is running on the node.<br>2. If necessary, restart the rsyslog service on the node using the command `service rsyslog restart`.<br>3. If the rsyslog service cannot be restarted and you do not save audit messages on Admin Nodes, contact technical support. Audit logs will be lost if this condition is not corrected. |
| Cassandra auto-compactor metrics out of date | The metrics that describe the Cassandra auto-compactor are out of date.<br><br>The Cassandra auto-compactor exists on all Storage Nodes and manages the size of the Cassandra database for overwrite and delete heavy workloads. While this alert persists, certain workloads will experience unexpectedly high metadata consumption.<br><br>1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert.<br>2. Contact technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| Cassandra communication error | The nodes that run the Cassandra service are having trouble communicating with each other.<br><br>This alert indicates that something is interfering with node-to-node communications. There might be a network issue or the Cassandra service might be down on one or more Storage Nodes.<br><br>1. Determine if there is another alert affecting one or more Storage Nodes. This alert might be resolved when you resolve the other alert.<br>2. Check for a network issue that might be affecting one or more Storage Nodes.<br>3. Select **SUPPORT** > **Tools** > **Grid topology**.<br>4. For each Storage Node in your system, select **SSM** > **Services**. Ensure that the status of the Cassandra service is "Running."<br>5. If Cassandra is not running, follow the steps for starting or restarting a service.<br>6. If all instances of the Cassandra service are now running and the alert is not resolved, contact technical support. |
| Cassandra compactions overloaded | The Cassandra compaction process is overloaded.<br><br>If the compaction process is overloaded, read performance might be degraded and RAM might be used up. The Cassandra service might also become unresponsive or crash.<br><br>1. Restart the Cassandra service by following the steps for restarting a service.<br>2. If this alert persists, contact technical support. |
| Cassandra repair metrics out of date | The metrics that describe Cassandra repair jobs are out of date. If this condition persists for more than 48 hours, client queries, such as bucket listings, might show deleted data.<br><br>1. Reboot the node. From the Grid Manager, go to **NODES**, select the node, and select the Tasks tab.<br>2. If this alert persists, contact technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| Cassandra repair progress slow | The progress of Cassandra database repairs is slow.<br><br>When database repairs are slow, Cassandra data consistency operations are impeded. If this condition persists for more than 48 hours, client queries, such as bucket listings, might show deleted data.<br><br>1. Confirm that all Storage Nodes are online and there are no networking-related alerts.<br>2. Monitor this alert for up to 2 days to see if the issue resolves on its own.<br>3. If database repairs continue to proceed slowly, contact technical support. |
| Cassandra repair service not available | The Cassandra repair service is not available.<br><br>The Cassandra repair service exists on all Storage Nodes and provides critical repair functions for the Cassandra database. If this condition persists for more than 48 hours, client queries, such as bucket listings, might show deleted data.<br><br>1. Select **SUPPORT** > **Tools** > **Grid topology**.<br>2. For each Storage Node in your system, select **SSM** > **Services**. Ensure that the status of the Cassandra Reaper service is "Running."<br>3. If Cassandra Reaper is not running, follow the steps for follow the steps for starting or restarting a service.<br>4. If all instances of the Cassandra Reaper service are now running and the alert is not resolved, contact technical support. |
| Cassandra table corruption | Cassandra has detected table corruption.<br><br>Cassandra automatically restarts if it detects table corruption.<br><br>Contact technical support. |
| Cloud Storage Pool connectivity error | The health check for Cloud Storage Pools detected one or more new errors.<br><br>1. Go to the Cloud Storage Pools section of the Storage Pools page.<br>2. Look at the Last Error column to determine which Cloud Storage Pool has an error.<br>3. See the instructions for managing objects with information lifecycle management. |

| Alert name | Description and recommended actions |
| --- | --- |
| DHCP lease expired | The DHCP lease on a network interface has expired. If the DHCP lease has expired, follow the recommended actions:<br><br>1. Ensure there is connectivity between this node and the DHCP server on the affected interface.<br>2. Ensure there are IP addresses available to assign in the affected subnet on the DHCP server.<br>3. Ensure there is a permanent reservation for the IP address configured in the DHCP server. Or, use the StorageGRID Change IP tool to assign a static IP address outside of the DHCP address pool. See the recovery and maintenance instructions. |
| DHCP lease expiring soon | The DHCP lease on a network interface is expiring soon.<br><br>To prevent the DHCP lease from expiring, follow the recommended actions:<br><br>1. Ensure there is connectivity between this node and the DHCP server on the affected interface.<br>2. Ensure there are IP addresses available to assign in the affected subnet on the DHCP server.<br>3. Ensure there is a permanent reservation for the IP address configured in the DHCP server. Or, use the StorageGRID Change IP tool to assign a static IP address outside of the DHCP address pool. See the recovery and maintenance instructions. |
| DHCP server unavailable | The DHCP server is unavailable.<br><br>The StorageGRID node is unable to contact your DHCP server. The DHCP lease for the node's IP address cannot be validated.<br><br>1. Ensure there is connectivity between this node and the DHCP server on the affected interface.<br>2. Ensure there are IP addresses available to assign in the affected subnet on the DHCP server.<br>3. Ensure there is a permanent reservation for the IP address configured in the DHCP server. Or, use the StorageGRID Change IP tool to assign a static IP address outside of the DHCP address pool. See the recovery and maintenance instructions. |

| Alert name | Description and recommended actions |
| --- | --- |
| Disk I/O is very slow | Very slow disk I/O might be impacting StorageGRID performance.<br><br>1. If the issue is related to a storage appliance node, use SANtricity System Manager to check for faulty drives, drives with predicted faults, or in-progress drive repairs. Also check the status of the Fibre Channel or SAS links between the appliance compute and storage controllers to see if any links are down or showing excessive error rates.<br>2. Examine the storage system that hosts this node's volumes to determine, and correct, the root cause of the slow I/O.<br>3. If this alert persists, contact technical support.<br><br>**Note:** Affected nodes might disable services and reboot themselves to avoid impacting overall grid performance. When the underlying condition is cleared and these nodes detect normal I/O performance, they will return to full service automatically. |
| EC rebalance failure | The job to rebalance erasure-coded data among Storage Nodes has failed or has been paused by the user.<br><br>1. Ensure that all Storage Nodes at the site being rebalanced are online and available.<br>2. Ensure that there are no volume failures at the site being rebalanced. If there are, terminate the EC rebalance job so that you can run a repair job.<br><br>`'rebalance-data terminate --job-id <ID>'`<br><br>3. Ensure that there are no service failures on the site being rebalanced. If a service is not running, follow the steps for starting or restarting a service in the recovery and maintenance instructions.<br>4. After resolving any issues, restart the job by running the following command on the primary Admin Node:<br><br>`'rebalance-data start --job-id <ID>'`<br><br>5. If you are unable to resolve the problem, contact technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| EC repair failure | A repair job for erasure-coded data has failed or has been stopped.<br><br>1. Ensure that there are sufficient available Storage Nodes or volumes to take the place of the failed Storage Node or volume.<br>2. Ensure that there are sufficient available Storage Nodes to satisfy the active ILM policy.<br>3. Ensure there are no network connectivity issues.<br>4. After resolving any issues, restart the job by running the following command on the primary Admin Node:<br><br>`'repair-data start-ec-node-repair --repair-id <ID>'`<br><br>5. If you are unable to resolve the problem, contact technical support. |
| EC repair stalled | A repair job for erasure-coded data has stalled.<br><br>1. Ensure that there are sufficient available Storage Nodes or volumes to take the place of the failed Storage Node or volume.<br>2. Ensure there are no network connectivity issues.<br>3. After resolving any issues, check if the alert is resolved. To see a more detailed report on the repair progress, run the following command on the primary Admin Node:<br><br>`'repair-data show-ec-repair-status --repair-id <ID>'`<br><br>4. If you are unable to resolve the problem, contact technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| Email notification failure | The email notification for an alert could not be sent.<br><br>This alert is triggered when an alert email notification fails or a test email (sent from the **ALERTS** > **Email setup** page) cannot be delivered.<br><br>1. Sign in to Grid Manager from the Admin Node listed in the **Site/Node** column of the alert.<br>2. Go to the **ALERTS** > **Email setup** page, check the settings, and change them if required.<br>3. Click **Send Test Email**, and check the inbox of a test recipient for the email. A new instance of this alert might be triggered if the test email cannot be sent.<br>4. If the test email could not be sent, confirm your email server is online.<br>5. If the server is working, select **SUPPORT** > **Tools** > **Logs**, and collect the log for the Admin Node. Specify a time period that is 15 minutes before and after the time of the alert.<br>6. Extract the downloaded archive, and review the contents of `prometheus.log` (`_/GID<gid><time_stamp>/<site_node>/<time_stamp>/metrics/prometheus.log`).<br>7. If you are unable to resolve the problem, contact technical support. |
| Expiration of client certificates configured on the Certificates page | One or more client certificates configured on the Certificates page are about to expire.<br><br>1. In the Grid Manager, select **CONFIGURATION** > **Security** > **Certificates** and then select the **Client** tab.<br>2. Select a certificate that will expire soon.<br>3. Select **Attach new certificate** to upload or generate a new certificate.<br>4. Repeat these steps for each certificate that will expire soon. |
| Expiration of load balancer endpoint certificate | One or more load balancer endpoint certificates are about to expire.<br><br>1. Select **CONFIGURATION** > **Network** > **Load balancer endpoints**.<br>2. Select an endpoint that has a certificate that will expire soon.<br>3. Select **Edit endpoint** to upload or generate a new certificate.<br>4. Repeat these steps for each endpoint that has an expired certificate or one that will expire soon.<br><br>For more information about managing load balancer endpoints, see the instructions for administering StorageGRID. |

| Alert name | Description and recommended actions |
| --- | --- |
| Expiration of server certificate for management interface | The server certificate used for the management interface is about to expire.<br>1. Select **CONFIGURATION** > **Security** > **Certificates**.<br>2. On the **Global** tab, select **Management interface certificate**.<br>3. Upload a new management interface certificate. |
| Expiration of global server certificate for S3 and Swift API | The server certificate used for accessing storage API endpoints is about to expire.<br>1. Select **CONFIGURATION** > **Security** > **Certificates**.<br>2. On the **Global** tab, select **S3 and Swift API certificate**.<br>3. Upload a new S3 and Swift API certificate. |
| External syslog CA certificate expiration | The certificate authority (CA) certificate used to sign the external syslog server certificate is about to expire.<br>1. Update the CA certificate on the external syslog server.<br>2. Obtain a copy of the updated CA certificate.<br>3. From the Grid Manager, go to **CONFIGURATION** > **Monitoring** > **Audit and syslog server**.<br>4. Select **Edit external syslog server**.<br>5. Select **Browse** to upload the new certificate.<br>6. Complete the Configuration wizard to save the new certificate and key. |
| External syslog client certificate expiration | The client certificate for an external syslog server is about to expire.<br>1. From the Grid Manager, go to **CONFIGURATION** > **Monitoring** > **Audit and syslog server**.<br>2. Select **Edit external syslog server**.<br>3. Select **Browse** to upload the new certificate.<br>4. Select **Browse** to upload the new private key.<br>5. Complete the Configuration wizard to save the new certificate and key. |
| External syslog server certificate expiration | The server certificate presented by the external syslog server is about to expire.<br>1. Update the server certificate on the external syslog server.<br>2. If you previously used the Grid Manager API to provide a server certificate for certificate validation, upload the updated server certificate using the API. |

| Alert name | Description and recommended actions |
| --- | --- |
| External syslog server forwarding error | Node cannot forward logs to the external syslog server.<br><br>1. From the Grid Manager, go to **CONFIGURATION** > **Monitoring** > **Audit and syslog server**.<br>2. Select **Edit external syslog server**.<br>3. Advance through the Configuration wizard until you are able to select **Send test messages**.<br>4. Select **Send test messages** to determine why logs cannot be forwarded to the external syslog server.<br>5. Resolve any reported issues. |
| Grid Network MTU mismatch | The maximum transmission unit (MTU) setting for the Grid Network interface (eth0) differs significantly across nodes in the grid.<br><br>The differences in MTU settings could indicate that some, but not all, eth0 networks are configured for jumbo frames. An MTU size mismatch of greater than 1000 might cause network performance problems.<br><br>See the instructions for the Grid Network MTU mismatch alert in Troubleshoot network, hardware, and platform issues. |
| High Java heap use | A high percentage of Java heap space is being used.<br><br>If the Java heap becomes full, metadata services can become unavailable and client requests can fail.<br><br>1. Review the ILM activity on the Dashboard. This alert might resolve on its own when the ILM workload decreases.<br>2. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert.<br>3. If this alert persists, contact technical support. |
| High latency for metadata queries | The average time for Cassandra metadata queries is too long.<br><br>An increase in query latency can be caused by a hardware change, such as replacing a disk; a workload change, such as a sudden increase in ingests; or a network change, such as a communication problem between nodes and sites.<br><br>1. Determine if there were any hardware, workload, or network changes around the time the query latency increased.<br>2. If you are unable to resolve the problem, contact technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| Identity federation synchronization failure | Unable to synchronize federated groups and users from the identity source.<br><br>1. Confirm that the configured LDAP server is online and available.<br>2. Review the settings on the Identity Federation page. Confirm that all values are current. See Use identity federation in the instructions for administering StorageGRID.<br>3. Click **Test Connection** to validate the settings for the LDAP server.<br>4. If you cannot resolve the issue, contact technical support. |
| Identity federation synchronization failure for a tenant | Unable to synchronize federated groups and users from the identity source configured by a tenant.<br><br>1. Sign in to the Tenant Manager.<br>2. Confirm that the LDAP server configured by the tenant is online and available.<br>3. Review the settings on the Identity Federation page. Confirm that all values are current. See Use identity federation in the instructions for using a tenant account.<br>4. Click **Test Connection** to validate the settings for the LDAP server.<br>5. If you cannot resolve the issue, contact technical support. |
| ILM placement unachievable | A placement instruction in an ILM rule cannot be achieved for certain objects.<br><br>This alert indicates that a node required by a placement instruction is unavailable or that an ILM rule is misconfigured. For example, a rule might specify more replicated copies than there are Storage Nodes.<br><br>1. Ensure that all nodes are online.<br>2. If all nodes are online, review the placement instructions in all ILM rules that are used the active ILM policy. Confirm that there are valid instructions for all objects. See the instructions for managing objects with information lifecycle management.<br>3. As required, update rule settings and activate a new policy.<br><br>**Note:** It might take up to 1 day for the alert to clear.<br><br>4. If the problem persists, contact technical support.<br><br>**Note:** This alert might appear during an upgrade and could persist for 1 day after the upgrade is completed successfully. When this alert is triggered by an upgrade, it will clear on its own. |

| Alert name | Description and recommended actions |
| --- | --- |
| ILM scan period too long | The time required to scan, evaluate objects, and apply ILM is too long.<br><br>If the estimated time to complete a full ILM scan of all objects is too long (see **Scan Period - Estimated** on the Dashboard), the active ILM policy might not be applied to newly ingested objects. Changes to the ILM policy might not be applied to existing objects.<br><br>1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert.<br>2. Confirm that all Storage Nodes are online.<br>3. Temporarily reduce the amount of client traffic. For example, from the Grid Manager, select **CONFIGURATION** > **Network** > **Traffic classification**, and create a policy that limits bandwidth or the number of requests.<br>4. If disk I/O or CPU are overloaded, try to reduce the load or increase the resource.<br>5. If necessary, update ILM rules to use synchronous placement (default for rules created after StorageGRID 11.3).<br>6. If this alert persists, contact technical support.<br><br>Administer StorageGRID |
| ILM scan rate low | The ILM scan rate is set to less than 100 objects/second.<br><br>This alert indicates that someone has changed the ILM scan rate for your system to less than 100 objects/second (default: 400 objects/second). The active ILM policy might not be applied to newly ingested objects. Subsequent changes to the ILM policy will not be applied to existing objects.<br><br>1. Determine if a temporary change was made to the ILM scan rate as part of an ongoing support investigation.<br>2. Contact technical support.<br><br>Never change the ILM scan rate without contacting technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| KMS CA certificate expiration | The certificate authority (CA) certificate used to sign the key management server (KMS) certificate is about to expire.<br>1. Using the KMS software, update the CA certificate for the key management server.<br>2. From the Grid Manager, select **CONFIGURATION** > **Security** > **Key management server**.<br>3. Select the KMS that has a certificate status warning.<br>4. Select **Edit**.<br>5. Select **Next** to go to Step 2 (Upload Server Certificate).<br>6. Select **Browse** to upload the new certificate.<br>7. Select **Save**.<br>Administer StorageGRID |
| KMS client certificate expiration | The client certificate for a key management server is about to expire.<br>1. From the Grid Manager, select **CONFIGURATION** > **Security** > **Key management server**.<br>2. Select the KMS that has a certificate status warning.<br>3. Select **Edit**.<br>4. Select **Next** to go to Step 3 (Upload Client Certificates).<br>5. Select **Browse** to upload the new certificate.<br>6. Select **Browse** to upload the new private key.<br>7. Select **Save**.<br>Administer StorageGRID |
| KMS configuration failed to load | The configuration for the key management server exists but failed to load.<br>1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert.<br>2. If this alert persists, contact technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| KMS connectivity error | An appliance node could not connect to the key management server for its site.<br>1. From the Grid Manager, select **CONFIGURATION** > **Security** > **Key management server**.<br>2. Confirm that the port and hostname entries are correct.<br>3. Confirm that the server certificate, client certificate, and the client certificate private key are correct and not expired.<br>4. Ensure that firewall settings allow the appliance node to communicate with the specified KMS.<br>5. Correct any networking or DNS issues.<br>6. If you need assistance or this alert persists, contact technical support. |
| KMS encryption key name not found | The configured key management server does not have an encryption key that matches the name provided.<br>1. Confirm that the KMS assigned to the site is using the correct name for the encryption key and any prior versions.<br>2. If you need assistance or this alert persists, contact technical support. |
| KMS encryption key rotation failed | All appliance volumes were decrypted, but one or more volumes could not rotate to the latest key.Contact technical support. |
| KMS is not configured | No key management server exists for this site.<br>1. From the Grid Manager, select **CONFIGURATION** > **Security** > **Key management server**.<br>2. Add a KMS for this site or add a default KMS.<br>Administer StorageGRID |
| KMS key failed to decrypt an appliance volume | One or more volumes on an appliance with node encryption enabled could not be decrypted with the current KMS key.<br>1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert.<br>2. Ensure that the key management server (KMS) has the configured encryption key and any previous key versions.<br>3. If you need assistance or this alert persists, contact technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| KMS server certificate expiration | The server certificate used by the key management server (KMS) is about to expire.<br><br>1. Using the KMS software, update the server certificate for the key management server.<br>2. If you need assistance or this alert persists, contact technical support.<br><br>Administer StorageGRID |
| Large audit queue | The disk queue for audit messages is full.<br><br>1. Check the load on the system—if there have been a significant number of transactions, the alert should resolve itself over time, and you can ignore the alert.<br>2. If the alert persists and increases in severity, view a chart of the queue size. If the number is steadily increasing over hours or days, the audit load has likely exceeded the audit capacity of the system.<br>3. Reduce the client operation rate or decrease the number of audit messages logged by changing the audit level for Client Writes and Client Reads to Error or Off (**CONFIGURATION** > **Monitoring** > **Audit and syslog server**).<br><br>Review audit logs |
| Legacy CLB load balancer activity detected | Some clients might be connecting to the deprecated CLB load balancer service using the default S3 and Swift API certificate.<br><br>1. To simplify future upgrades, install a custom S3 and Swift API certificate on the **Global** tab of the **Certificates** page. Then, ensure that all S3 or Swift clients who connect to the legacy CLB have the new certificate.<br>2. Create one or more load balancer endpoints. Then, direct all existing S3 and Swift clients to these endpoints. Contact technical support if you need to remap the client port.<br><br>Other activity might trigger this alert, including port scans. To determine if the deprecated CLB service is currently in use, view the `storagegrid_private_clb_http_connection_established_successful` Prometheus metric.<br><br>As required, silence or disable this alert rule if the CLB service is no longer in use. |

| Alert name | Description and recommended actions |
| --- | --- |
| Logs are being added to the on-disk queue | Node cannot forward logs to the external syslog server and the on-disk queue is filling up.<br>1. From the Grid Manager, go to **CONFIGURATION** > **Monitoring** > **Audit and syslog server**.<br>2. Select **Edit external syslog server**.<br>3. Advance through the Configuration wizard until you are able to select **Send test messages**.<br>4. Select **Send test messages** to determine why logs cannot be forwarded to the external syslog server.<br>5. Resolve any reported issues. |
| Low audit log disk capacity | The space available for audit logs is low.<br>1. Monitor this alert to see if the issue resolves on its own and the disk space becomes available again.<br>2. Contact technical support if the available space continues to decrease. |
| Low available node memory | The amount of RAM available on a node is low.<br>Low available RAM could indicate a change in the workload or a memory leak with one or more nodes.<br>1. Monitor this alert to see if the issue resolves on its own.<br>2. If the available memory falls below the major alert threshold, contact technical support. |
| Low free space for storage pool | The amount of space available to store object data in a storage pool is low.<br>1. Select **ILM** > **Storage pools**.<br>2. Select the storage pool listed in the alert, and select **View details**.<br>3. Determine where additional storage capacity is required. You can either add Storage Nodes to each site in the storage pool or add storage volumes (LUNs) to one or more existing Storage Nodes.<br>4. Perform an expansion procedure to increase storage capacity.<br>Expand your grid |

| Alert name | Description and recommended actions |
| --- | --- |
| Low installed node memory | The amount of installed memory on a node is low.<br><br>Increase the amount of RAM available to the virtual machine or Linux host. Check the threshold value for the major alert to determine the default minimum requirement for a StorageGRID node. See the installation instructions for your platform:<br><br>• Install Red Hat Enterprise Linux or CentOS<br>• Install Ubuntu or Debian<br>• Install VMware |
| Low metadata storage | The space available for storing object metadata is low.<br><br>**Critical alert**<br><br>1. Stop ingesting objects.<br>2. Immediately add Storage Nodes in an expansion procedure.<br><br>**Major alert**<br><br>Immediately add Storage Nodes in an expansion procedure.<br><br>**Minor alert**<br><br>1. Monitor the rate at which object metadata space is being used. Select **NODES** > ***Storage Node*** > **Storage**, and view the Storage Used - Object Metadata graph.<br>2. Add Storage Nodes in an expansion procedure as soon as possible.<br><br>Once new Storage Nodes are added, the system automatically rebalances object metadata across all Storage Nodes, and the alarm clears.<br><br>See the instructions for the Low metadata storage alert in Troubleshoot metadata issues. |
| Low metrics disk capacity | The space available for the metrics database is low.<br><br>1. Monitor this alert to see if the issue resolves on its own and the disk space becomes available again.<br>2. Contact technical support if the available space continues to decrease. |

| Alert name | Description and recommended actions |
| --- | --- |
| Low object data storage | The space available for storing object data is low.<br><br>Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes.<br><br>Troubleshoot the Low object data storage alert<br><br>Expand your grid |
| Low read-only watermark override | The Storage Volume Soft Read-Only Watermark Override is less than the minimum optimized watermark for a Storage Node.<br><br>To learn how to resolve this alert, go to Troubleshoot Low read-only watermark override alerts. |
| Low root disk capacity | The space available for the root disk is low.<br><br>1. Monitor this alert to see if the issue resolves on its own and the disk space becomes available again.<br>2. Contact technical support if the available space continues to decrease. |
| Low system data capacity | The space available for StorageGRID system data on the `/var/local` file system is low.<br><br>1. Monitor this alert to see if the issue resolves on its own and the disk space becomes available again.<br>2. Contact technical support if the available space continues to decrease. |
| Low tmp directory free space | The space available in the /tmp directory is low.<br><br>1. Monitor this alert to see if the issue resolves on its own and the disk space becomes available again.<br>2. Contact technical support if the available space continues to decrease. |
| Node network connectivity error | Errors have occurred while transferring data between nodes.<br><br>Network connectivity errors might clear without manual intervention. Contact technical support if the errors do not clear.<br><br>See the instructions for the Network Receive Error (NRER) alarm in Troubleshoot network, hardware, and platform issues. |

| Alert name | Description and recommended actions |
| --- | --- |
| Node network reception frame error | A high percentage of the network frames received by a node had errors.<br><br>This alert might indicate a hardware issue, such as a bad cable or a failed transceiver on either end of the Ethernet connection.<br><br>1. If you are using an appliance, try replacing each SFP+ or SFP28 transceiver and cable, one at a time, to see if the alert clears.<br>2. If this alert persists, contact technical support. |
| Node not in sync with NTP server | The node's time is not in sync with the network time protocol (NTP) server.<br><br>1. Verify that you have specified at least four external NTP servers, each providing a Stratum 3 or better reference.<br>2. Check that all NTP servers are operating normally.<br>3. Verify the connections to the NTP servers. Make sure they are not blocked by a firewall. |
| Node not locked with NTP server | The node is not locked to a network time protocol (NTP) server.<br><br>1. Verify that you have specified at least four external NTP servers, each providing a Stratum 3 or better reference.<br>2. Check that all NTP servers are operating normally.<br>3. Verify the connections to the NTP servers. Make sure they are not blocked by a firewall. |
| Non appliance node network down | One or more network devices are down or disconnected. This alert indicates that a network interface (eth) for a node installed on a virtual machine or Linux host is not accessible.<br><br>Contact technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| Object existence check failed | The object existence check job has failed.<br><br>1. Select **MAINTENANCE > Object existence check**.<br>2. Note the error message. Perform the appropriate corrective actions:<br><br>**Failed to start**, **Lost connection**, **Unknown error**<br><br>a. Ensure the Storage Nodes and volumes included in the job are online and available.<br>b. Ensure there are no service or volume failures on the Storage Nodes. If a service is not running, start or restart the service. See the recovery and maintenance instructions.<br>c. Ensure the selected consistency control can be satisfied.<br>d. After resolving any issues, select **Retry**. The job will resume from the last valid state.<br><br>**Critical storage error in volume**<br><br>a. Recover the failed volume. See the recovery and maintenance instructions.<br>b. Select **Retry**.<br>c. After the job completes, create another job for the remaining volumes on the node to check for additional errors.<br>3. If you are unable to resolve the issues, contact technical support. |
| Object existence check stalled | The object existence check job has stalled.<br><br>The object existence check job cannot continue. Either one or more Storage Nodes or volumes included in the job are offline or unresponsive, or the selected consistency control can no longer be satisfied because too many nodes are down or unavailable.<br><br>1. Ensure that all Storage Nodes and volumes being checked are online and available (select **NODES**).<br>2. Ensure that sufficient Storage Nodes are online and available to allow the current coordinator node to read object metadata using the selected consistency control. If necessary, start or restart a service. See the recovery and maintenance instructions.<br><br>When you resolve steps 1 and 2, the job will automatically start where it left off.<br><br>3. If the selected consistency control cannot be satisfied, cancel the job and start another job using a lower consistency control.<br>4. If you are unable to resolve the issues, contact technical support. |

| Alert name | Description and recommended actions |
| --- | --- |
| Objects lost | One or more objects have been lost from the grid.<br><br>This alert might indicate that data has been permanently lost and is not retrievable.<br><br>1. Investigate this alert immediately. You might need to take action to prevent further data loss. You also might be able to restore a lost object if you take prompt action.<br><br>Troubleshoot lost and missing object data<br><br>2. When the underlying problem is resolved, reset the counter:<br>a. Select **SUPPORT** > **Tools** > **Grid topology**.<br>b. For the Storage Node that raised the alert, select ***site*** > ***grid node*** > **LDR** > **Data Store** > **Configuration** > **Main**.<br>c. Select **Reset Lost Objects Count** and click **Apply Changes**. |
| Platform services unavailable | Too few Storage Nodes with the RSM service are running or available at a site.<br><br>Make sure that the majority of the Storage Nodes that have the RSM service at the affected site are running and in a non-error state.<br><br>See “Troubleshooting platform services” in the instructions for administering StorageGRID. |
| S3 PUT Object size too large | An S3 client is attempting to perform a PUT Object operation that exceeds the S3 size limits.<br><br>1. Use the tenant ID shown in the alert details to identify the tenant account.<br>2. Go to **Support** > **Tools** > **Logs**, and collect the Application Logs for the Storage Node shown in the alert details. Specify a time period that is 15 minutes before and after the time of the alert.<br>3. Extract the downloaded archive, and navigate to the location of `bycast.log` (`/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log`).<br>4. Search the contents of `bycast.log` for `"method=PUT"` and identify the IP address of the S3 client by looking at the `clientIP` field.<br>5. Inform all client users that the maximum PUT Object size is 5 GiB.<br>6. Use multipart uploads for objects larger than 5 GiB. |

| Alert name | Description and recommended actions |
| --- | --- |
| Services appliance link down on Admin Network port 1 | The Admin Network port 1 on the appliance is down or disconnected.<br>1. Check the cable and physical connection to Admin Network port 1.<br>2. Address any connection issues. See the installation and maintenance instructions for your appliance hardware.<br>3. If this port is disconnected on purpose, disable this rule. From the Grid Manager, select **ALERTS** > **Rules**, select the rule, and click **Edit rule**. Then, uncheck the **Enabled** check box.<br>◦ SG100 and SG1000 services appliances<br>◦ Disable alert rules |
| Services appliance link down on Admin Network (or Client Network) | The appliance interface to the Admin Network (eth1) or the Client Network (eth2) is down or disconnected.<br>1. Check the cables, SFPs, and physical connections to the StorageGRID network.<br>2. Address any connection issues. See the installation and maintenance instructions for your appliance hardware.<br>3. If this port is disconnected on purpose, disable this rule. From the Grid Manager, select **ALERTS** > **Rules**, select the rule, and click **Edit rule**. Then, uncheck the **Enabled** check box.<br>◦ SG100 and SG1000 services appliances<br>◦ Disable alert rules |
| Services appliance link down on network port 1, 2, 3, or 4 | Network port 1, 2, 3, or 4 on the appliance is down or disconnected.<br>1. Check the cables, SFPs, and physical connections to the StorageGRID network.<br>2. Address any connection issues. See the installation and maintenance instructions for your appliance hardware.<br>3. If this port is disconnected on purpose, disable this rule. From the Grid Manager, select **ALERTS** > **Rules**, select the rule, and click **Edit rule**. Then, uncheck the **Enabled** check box.<br>◦ SG100 and SG1000 services appliances<br>◦ Disable alert rules |

| Alert name | Description and recommended actions |
| --- | --- |
| Services appliance storage connectivity degraded | One of the two SSDs in a services appliance has failed or is out of synchronization with the other.<br><br>Appliance functionality is not impacted, but you should address the issue immediately. If both drives fail, the appliance will no longer function.<br><br>1. From the Grid Manager, select **NODES** > ***services appliance*, and then select the Hardware** tab.<br>2. Review the message in the **Storage RAID Mode** field.<br>3. If the message shows the progress of a resynchronization operation, wait for the operation to complete and then confirm that the alert is resolved. A resynchronization message means that SSD was replaced recently or that it is being resynchronized for another reason.<br>4. If the message indicates that one of the SSDs has failed, replace the failed drive as soon as possible.<br><br>For instructions on how to replace a drive in a services appliance, see the SG100 and SG1000 appliances installation and maintenance guide.<br><br>SG100 and SG1000 services appliances |
| Storage appliance link down on Admin Network port 1 | The Admin Network port 1 on the appliance is down or disconnected.<br><br>1. Check the cable and physical connection to Admin Network port 1.<br>2. Address any connection issues. See the installation and maintenance instructions for your appliance hardware.<br>3. If this port is disconnected on purpose, disable this rule. From the Grid Manager, select **ALERTS** > **Rules**, select the rule, and click **Edit rule**. Then, uncheck the **Enabled** check box.<br>◦ SG6000 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG5600 storage appliances<br>◦ Disable alert rules |

| Alert name | Description and recommended actions |
| --- | --- |
| Storage appliance link down on Admin Network (or Client Network) | The appliance interface to the Admin Network (eth1) or the Client Network (eth2) is down or disconnected.<br><br>1. Check the cables, SFPs, and physical connections to the StorageGRID network.<br>2. Address any connection issues. See the installation and maintenance instructions for your appliance hardware.<br>3. If this port is disconnected on purpose, disable this rule. From the Grid Manager, select **ALERTS** > **Rules**, select the rule, and click **Edit rule**. Then, uncheck the **Enabled** check box.<br>  ◦ SG6000 storage appliances<br>  ◦ SG5700 storage appliances<br>  ◦ SG5600 storage appliances<br>  ◦ Disable alert rules |
| Storage appliance link down on network port 1, 2, 3, or 4 | Network port 1, 2, 3, or 4 on the appliance is down or disconnected.<br><br>1. Check the cables, SFPs, and physical connections to the StorageGRID network.<br>2. Address any connection issues. See the installation and maintenance instructions for your appliance hardware.<br>3. If this port is disconnected on purpose, disable this rule. From the Grid Manager, select **ALERTS** > **Rules**, select the rule, and click **Edit rule**. Then, uncheck the **Enabled** check box.<br>  ◦ SG6000 storage appliances<br>  ◦ SG5700 storage appliances<br>  ◦ SG5600 storage appliances<br>  ◦ Disable alert rules |
| Storage appliance storage connectivity degraded | There is a problem with one or more connections between the compute controller and storage controller.<br><br>1. Go to the appliance to check the port indicator lights.<br>2. If a port's lights are off, confirm the cable is properly connected. As needed, replace the cable.<br>3. Wait up to five minutes.<br><br>  **Note:** If a second cable needs to be replaced, do not unplug it for at least 5 minutes. Otherwise, the root volume might become read-only, which requires a hardware restart.<br><br>4. From the Grid Manager, select **NODES**. Then, select the Hardware tab of the node that had the problem. Verify that the alert condition has resolved. |

| Alert name | Description and recommended actions |
| --- | --- |
| Storage device inaccessible | A storage device cannot be accessed.<br><br>This alert indicates that a volume cannot be mounted or accessed because of a problem with an underlying storage device.<br><br>1. Check the status of all storage devices used for the node:<br>◦ If the node is installed on a virtual machine or Linux host, follow the instructions for your operating system to run hardware diagnostics or perform a filesystem check.<br>▪ Install Red Hat Enterprise Linux or CentOS<br>▪ Install Ubuntu or Debian<br>▪ Install VMware<br>◦ If the node is installed on an SG100, SG1000 or SG6000 appliance, use the BMC.<br>◦ If the node is installed on a SG5600 or SG5700 appliance, use SANtricity System Manager.<br>2. If necessary, replace the component. See the instructions for your appliance:<br>◦ SG6000 storage appliances<br>◦ SG5700 storage appliances<br>◦ SG5600 storage appliances |
| Tenant quota usage high | A high percentage of tenant quota space is being used. If a tenant exceeds its quota, new ingests are rejected.<br><br>**Note:** This alert rule is disabled by default because it might generate a lot of notifications.<br><br>1. From the Grid Manager, select **TENANTS**.<br>2. Sort the table by **Quota Utilization**.<br>3. Select a tenant whose quota utilization is close to 100%.<br>4. Do either or both of the following:<br>◦ Select **Edit** to increase the storage quota for the tenant.<br>◦ Notify the tenant that their quota utilization is high. |

| Alert name | Description and recommended actions |
| --- | --- |
| Unable to communicate with node | One or more services are unresponsive, or the node cannot be reached.<br><br>This alert indicates that a node is disconnected for an unknown reason. For example, a service on the node might be stopped, or the node might have lost its network connection because of a power failure or unexpected outage.<br><br>Monitor this alert to see if the issue resolves on its own. If the issue persists:<br><br>1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert.<br>2. Confirm that all of the services on this node are running. If a service is stopped, try starting it. See the recovery and maintenance instructions.<br>3. Ensure that the host for the node is powered on. If it is not, start the host.<br><br>**Note:** If more than one host is powered off, see the recovery and maintenance instructions.<br><br>4. Determine if there is a network connectivity issue between this node and the Admin Node.<br>5. If you cannot resolve the alert, contact technical support. |
| Unexpected node reboot | A node rebooted unexpectedly within the last 24 hours.<br><br>1. Monitor this alert. The alert will be cleared after 24 hours. However, if the node reboots unexpectedly again, this alert will be triggered again.<br>2. If you cannot resolve the alert, there might be a hardware failure. Contact technical support. |
| Unidentified corrupt object detected | A file was found in replicated object storage that could not be identified as a replicated object.<br><br>1. Determine if there are any issues with the underlying storage on a Storage Node. For example, run hardware diagnostics or perform a filesystem check.<br>2. After resolving any storage issues, run object existence check to determine if any replicated copies, as defined by your ILM policy, are missing.<br>3. Monitor this alert. The alert will clear after 24 hours, but will be triggered again if the issue has not been fixed.<br>4. If you cannot resolve the alert, contact technical support. |

## Commonly used Prometheus metrics

The Prometheus service on Admin Nodes collects time series metrics from the services on all nodes. While Prometheus collects more than a thousand metrics, a relatively small number are required to monitor the most critical StorageGRID operations.

Metrics are stored on each Admin Node until the space reserved for Prometheus data is full. When the `/var/local/mysql_ibdata/` volume reaches capacity, the oldest metrics are deleted first.

To obtain the complete list of metrics, use the Grid Management API.

1. From the top of the Grid Manager, select the help icon and select **API Documentation**.
2. Locate the **metrics** operations.
3. Execute the `GET /grid/metric-names` operation.
4. Download the results.

The following table lists the most commonly used Prometheus metrics. You can refer to this list to better understand the conditions in the default alert rules or to construct the conditions for custom alert rules.

> Metrics that include *private* in their names are intended for internal use only and are subject to change between StorageGRID releases without notice.

| Prometheus metric | Description |
|---|---|
| alertmanager_notifications_failed_total | The total number of failed alert notifications. |
| node_filesystem_avail_bytes | The amount of filesystem space available to non-root users in bytes. |
| node_memory_MemAvailable_bytes | Memory information field MemAvailable_bytes. |
| node_network_carrier | Carrier value of /sys/class/net/<iface>. |
| node_network_receive_errs_total | Network device statistic receive_errs. |
| node_network_transmit_errs_total | Network device statistic transmit_errs. |
| storagegrid_administratively_down | The node is not connected to the grid for an expected reason. For example, the node, or services on the node, has been gracefully shut down, the node is rebooting, or the software is being upgraded. |
| storagegrid_appliance_compute_controller_hardware_status | The status of the compute controller hardware in an appliance. |
| storagegrid_appliance_failed_disks | For the storage controller in an appliance, the number of drives that are not optimal. |

| Prometheus metric | Description |
| --- | --- |
| storagegrid_appliance_storage_controller_hardware_status | The overall status of the storage controller hardware in an appliance. |
| storagegrid_content_buckets_and_containers | The total number of S3 buckets and Swift containers known by this Storage Node. |
| storagegrid_content_objects | The total number of S3 and Swift data objects known by this Storage Node. Count is valid only for data objects created by client applications that interface with the system through S3 or Swift. |
| storagegrid_content_objects_lost | The total number of objects this service detects as missing from the StorageGRID system. Action should be taken to determine the cause of the loss and if recovery is possible.<br><br>Troubleshoot lost and missing object data |
| storagegrid_http_sessions_incoming_attempted | The total number of HTTP sessions that have been attempted to a Storage Node. |
| storagegrid_http_sessions_incoming_currently_established | The number of HTTP sessions that are currently active (open) on the Storage Node. |
| storagegrid_http_sessions_incoming_failed | The total number of HTTP sessions that failed to complete successfully, either due to a malformed HTTP request or a failure while processing an operation. |
| storagegrid_http_sessions_incoming_successful | The total number of HTTP sessions that have completed successfully. |
| storagegrid_ilm_awaiting_background_objects | The total number of objects on this node awaiting ILM evaluation from the scan. |
| storagegrid_ilm_awaiting_client_evaluation_objects_per_second | The current rate at which objects are evaluated against the ILM policy on this node. |
| storagegrid_ilm_awaiting_client_objects | The total number of objects on this node awaiting ILM evaluation from client operations (for example, ingest). |
| storagegrid_ilm_awaiting_total_objects | The total number of objects awaiting ILM evaluation. |
| storagegrid_ilm_scan_objects_per_second | The rate at which objects owned by this node are scanned and queued for ILM. |

| Prometheus metric | Description |
| --- | --- |
| storagegrid_ilm_scan_period_estimated_minutes | The estimated time to complete a full ILM scan on this node.<br><br>**Note:** A full scan does not guarantee that ILM has been applied to all objects owned by this node. |
| storagegrid_load_balancer_endpoint_cert_expiry_time | The expiration time of the load balancer endpoint certificate in seconds since the epoch. |
| storagegrid_metadata_queries_average_latency_milliseconds | The average time required to run a query against the metadata store through this service. |
| storagegrid_network_received_bytes | The total amount of data received since installation. |
| storagegrid_network_transmitted_bytes | The total amount of data sent since installation. |
| storagegrid_node_cpu_utilization_percentage | The percentage of available CPU time currently being used by this service. Indicates how busy the service is. The amount of available CPU time depends on the number of CPUs for the server. |
| storagegrid_ntp_chosen_time_source_offset_milliseconds | Systematic offset of time provided by a chosen time source. Offset is introduced when the delay to reach a time source is not equal to the time required for the time source to reach the NTP client. |
| storagegrid_ntp_locked | The node is not locked to a network time protocol (NTP) server. |
| storagegrid_s3_data_transfers_bytes_ingested | The total amount of data ingested from S3 clients to this Storage Node since the attribute was last reset. |
| storagegrid_s3_data_transfers_bytes_retrieved | The total amount of data retrieved by S3 clients from this Storage Node since the attribute was last reset. |
| storagegrid_s3_operations_failed | The total number of failed S3 operations (HTTP status codes 4xx and 5xx), excluding those caused by S3 authorization failure. |
| storagegrid_s3_operations_successful | The total number of successful S3 operations (HTTP status code 2xx). |
| storagegrid_s3_operations_unauthorized | The total number of failed S3 operations that are the result of an authorization failure. |

| Prometheus metric | Description |
| --- | --- |
| storagegrid_servercertificate_management_interface_cert_expiry_days | The number of days before the Management Interface certificate expires. |
| storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days | The number of days before the Object Storage API certificate expires. |
| storagegrid_service_cpu_seconds | The cumulative amount of time that the CPU has been used by this service since installation. |
| storagegrid_service_memory_usage_bytes | The amount of memory (RAM) currently in use by this service. This value is identical to that displayed by the Linux top utility as RES. |
| storagegrid_service_network_received_bytes | The total amount of data received by this service since installation. |
| storagegrid_service_network_transmitted_bytes | The total amount of data sent by this service. |
| storagegrid_service_restarts | The total number of times the service has been restarted. |
| storagegrid_service_runtime_seconds | The total amount of time that the service has been running since installation. |
| storagegrid_service_uptime_seconds | The total amount of time the service has been running since it was last restarted. |
| storagegrid_storage_state_current | The current state of the storage services. Attribute values are:<br>• 10 = Offline<br>• 15 = Maintenance<br>• 20 = Read-only<br>• 30 = Online |
| storagegrid_storage_status | The current status of the storage services. Attribute values are:<br>• 0 = No Errors<br>• 10 = In Transition<br>• 20 = Insufficient Free Space<br>• 30 = Volume(s) Unavailable<br>• 40 = Error |

| Prometheus metric | Description |
| --- | --- |
| storagegrid_storage_utilization_bytes | An estimate of the total size of replicated and erasure coded object data on the Storage Node. |
| storagegrid_storage_utilization_metadata_allowed_bytes | The total space on volume 0 of each Storage Node that is allowed for object metadata. This value is always less than the actual space reserved for metadata on a node, because a portion of the reserved space is required for essential database operations (such as compaction and repair) and future hardware and software upgrades.The allowed space for object metadata controls overall object capacity. |
| storagegrid_storage_utilization_metadata_bytes | The amount of object metadata on storage volume 0, in bytes. |
| storagegrid_storage_utilization_total_space_bytes | The total amount of storage space allocated to all object stores. |
| storagegrid_storage_utilization_usable_space_bytes | The total amount of object storage space remaining. Calculated by adding together the amount of available space for all object stores on the Storage Node. |
| storagegrid_swift_data_transfers_bytes_ingested | The total amount of data ingested from Swift clients to this Storage Node since the attribute was last reset. |
| storagegrid_swift_data_transfers_bytes_retrieved | The total amount of data retrieved by Swift clients from this Storage Node since the attribute was last reset. |
| storagegrid_swift_operations_failed | The total number of failed Swift operations (HTTP status codes 4xx and 5xx), excluding those caused by Swift authorization failure. |
| storagegrid_swift_operations_successful | The total number of successful Swift operations (HTTP status code 2xx). |
| storagegrid_swift_operations_unauthorized | The total number of failed Swift operations that are the result of an authorization failure (HTTP status codes 401, 403, 405). |
| storagegrid_tenant_usage_data_bytes | The logical size of all objects for the tenant. |
| storagegrid_tenant_usage_object_count | The number of objects for the tenant. |

| Prometheus metric | Description |
| --- | --- |
| storagegrid_tenant_usage_quota_bytes | The maximum amount of logical space available for the tenant's objects. If a quota metric is not provided, an unlimited amount of space is available. |

## Alarms reference (legacy system)

The following table lists all of the legacy Default alarms. If an alarm is triggered, you can look up the alarm code in this table to find the recommended actions.

> While the legacy alarm system continues to be supported, the alert system offers significant benefits and is easier to use.

| Code | Name | Service | Recommended action |
| --- | --- | --- | --- |
| ABRL | Available Attribute Relays | BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS | 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.<br><br>If the problem persists, contact technical support. |
| ACMS | Available Metadata Services | BARC, BLDR, BCMN | 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.<br><br>Check and restore connections to a DDS service to clear this alarm and return the service to full functionality. |
| ACTS | Cloud Tiering Service Status | ARC | Only available for Archive Nodes with a Target Type of Cloud Tiering - Simple Storage Service (S3).<br><br>If the ACTS attribute for the Archive Node is set to Read-Only Enabled or Read-Write Disabled, you must set the attribute to Read-Write Enabled.<br><br>If a major alarm is triggered due to an authentication failure, verify the credentials associated with destination bucket and update values, if necessary.<br><br>If a major alarm is triggered due to any other reason, contact technical support. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| ADCA | ADC Status | ADC | If an alarm is triggered, select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **ADC** > **Overview** > **Main** and **ADC** > **Alarms** > **Main** to determine the cause of the alarm.<br><br>If the problem persists, contact technical support. |
| ADCE | ADC State | ADC | If the value of ADC State is Standby, continue monitoring the service and if the problem persists, contact technical support.<br><br>If the value of ADC State is Offline, restart the service. If the problem persists, contact technical support. |
| AITE | Retrieve State | BARC | Only available for Archive Node's with a Target Type of Tivoli Storage Manager (TSM).<br><br>If the value of Retrieve State is Waiting for Target, check the TSM middleware server and ensure that it is operating correctly. If the Archive Node has just been added to the StorageGRID system, ensure that the Archive Node's connection to the targeted external archival storage system is configured correctly.<br><br>If the value of Archive Retrieve State is Offline, attempt to update the state to Online. Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **Main**, select **Archive Retrieve State** > **Online**, and click **Apply Changes**.<br><br>If the problem persists, contact technical support. |
| AITU | Retrieve Status | BARC | If the value of Retrieve Status is Target Error, check the targeted external archival storage system for errors.<br><br>If the value of Archive Retrieve Status is Session Lost, check the targeted external archival storage system to ensure it is online and operating correctly. Check the network connection with the target.<br><br>If the value of Archive Retrieve Status is Unknown Error, contact technical support. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| ALIS | Inbound Attribute Sessions | ADC | If the number of inbound attribute sessions on an attribute relay grows too large, it can be an indication that the StorageGRID system has become unbalanced. Under normal conditions, attribute sessions should be evenly distributed amongst ADC services. An imbalance can lead to performance issues.<br><br>If the problem persists, contact technical support. |
| ALOS | Outbound Attribute Sessions | ADC | The ADC service has a high number of attribute sessions, and is becoming overloaded. If this alarm is triggered, contact technical support. |
| ALUR | Unreachable Attribute Repositories | ADC | Check network connectivity with the NMS service to ensure that the service can contact the attribute repository.<br><br>If this alarm is triggered and network connectivity is good, contact technical support. |
| AMQS | Audit Messages Queued | BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS | If audit messages cannot be immediately forwarded to an audit relay or repository, the messages are stored in a disk queue. If the disk queue becomes full, outages can occur.<br><br>To allow you to respond in time to prevent an outage, AMQS alarms are triggered when the number of messages in the disk queue reaches the following thresholds:<br><br>• Notice: More than 100,000 messages<br>• Minor: At least 500,000 messages<br>• Major: At least 2,000,000 messages<br>• Critical: At least 5,000,000 messages<br><br>If an AMQS alarm is triggered, check the load on the system—if there have been a significant number of transactions, the alarm should resolve itself over time. In this case, you can ignore the alarm.<br><br>If the alarm persists and increases in severity, view a chart of the queue size. If the number is steadily increasing over hours or days, the audit load has likely exceeded the audit capacity of the system. Reduce the client operation rate or decrease the number of audit messages logged by changing the audit level to Error or Off. See Configure audit messages and log destinations. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| AOTE | Store State | BARC | Only available for Archive Node's with a Target Type of Tivoli Storage Manager (TSM).<br><br>If the value of Store State is Waiting for Target, check the external archival storage system and ensure that it is operating correctly. If the Archive Node has just been added to the StorageGRID system, ensure that the Archive Node's connection to the targeted external archival storage system is configured correctly.<br><br>If the value of Store State is Offline, check the value of Store Status. Correct any problems before moving the Store State back to Online. |
| AOTU | Store Status | BARC | If the value of Store Status is Session Lost check that the external archival storage system is connected and online.<br><br>If the value of Target Error, check the external archival storage system for errors.<br><br>If the value of Store Status is Unknown Error, contact technical support. |
| APMS | Storage Multipath Connectivity | SSM | If the multipath state alarm appears as "Degraded" (select **SUPPORT** > **Tools** > **Grid topology**, then select ***site*** > ***grid node*** > **SSM** > **Events**), do the following:<br><br>1. Plug in or replace the cable that does not display any indicator lights.<br>2. Wait one to five minutes.<br><br>Do not unplug the other cable until at least five minutes after you plug in the first one. Unplugging too early can cause the root volume to become read-only, which requires that the hardware be restarted.<br><br>3. Return to the **SSM** > **Resources** page, and verify that the "Degraded" Multipath status has changed to "Nominal" in the Storage Hardware section. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| ARCE | ARC State | ARC | The ARC service has a state of Standby until all ARC components (Replication, Store, Retrieve, Target) have started. It then transitions to Online.<br><br>If the value of ARC State does not transition from Standby to Online, check the status of the ARC components.<br><br>If the value of ARC State is Offline, restart the service. If the problem persists, contact technical support. |
| AROQ | Objects Queued | ARC | This alarm can be triggered if the removable storage device is running slowly due to problems with the targeted external archival storage system, or if it encounters multiple read errors. Check the external archival storage system for errors, and ensure that it is operating correctly.<br><br>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. |
| ARRF | Request Failures | ARC | If a retrieval from the targeted external archival storage system fails, the Archive Node retries the retrieval as the failure can be due to a transient issue. However, if the object data is corrupt or has been marked as being permanently unavailable, the retrieval does not fail. Instead, the Archive Node continuously retries the retrieval and the value for Request Failures continues to increase.<br><br>This alarm can indicate that the storage media holding the requested data is corrupt. Check the external archival storage system to further diagnose the problem.<br><br>If you determine that the object data is no longer in the archive, the object will have to be removed from the StorageGRID system. For more information, contact technical support.<br><br>Once the problem that triggered this alarm is addressed, reset the failures count. Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **Main**, select **Reset Request Failure Count** and click **Apply Changes**. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| ARRV | Verification Failures | ARC | To diagnose and correct this problem, contact technical support.<br><br>Once the problem that triggered this alarm is addressed, reset the failures count. Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **Main**, select **Reset Verification Failure Count** and click **Apply Changes**. |
| ARVF | Store Failures | ARC | This alarm can occur as a result of errors with the targeted external archival storage system. Check the external archival storage system for errors, and ensure that it is operating correctly.<br><br>Once the problem that triggered this alarm is addressed, reset the failures count. Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **Main**, select **Reset Store Failure Count**, and click **Apply Changes**. |
| ASXP | Audit Shares | AMS | 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.<br><br>If the problem persists, contact technical support. |
| AUMA | AMS Status | AMS | If the value of AMS Status is DB Connectivity Error, restart the grid node.<br><br>If the problem persists, contact technical support. |
| AUME | AMS State | AMS | If the value of AMS State is Standby, continue monitoring the StorageGRID system. If the problem persists, contact technical support.<br><br>If the value of AMS State is Offline, restart the service. If the problem persists, contact technical support. |
| AUXS | Audit Export Status | AMS | If an alarm is triggered, correct the underlying problem, and then restart the AMS service.<br><br>If the problem persists, contact technical support. |
| BADD | Storage Controller Failed Drive Count | SSM | This alarm is triggered when one or more drives in a StorageGRID appliance has failed or is not optimal. Replace the drives as required. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| BASF | Available Object Identifiers | CMN | When a StorageGRID system is provisioned, the CMN service is allocated a fixed number of object identifiers. This alarm is triggered when the StorageGRID system begins to exhaust its supply of object identifiers.<br><br>To allocate more identifiers, contact technical support. |
| BASS | Identifier Block Allocation Status | CMN | By default, an alarm is triggered when object identifiers cannot be allocated because ADC quorum cannot be reached.<br><br>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 system (clients can still ingest and retrieve content), as approximately one month's supply of identifiers are cached elsewhere in the grid; however, if the condition continues, the StorageGRID system will lose the ability to ingest new content.<br><br>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.<br><br>If the problem persists, contact technical support. |
| BRDT | Compute Controller Chassis Temperature | SSM | An alarm is triggered if the temperature of the compute controller in a StorageGRID appliance exceeds a nominal threshold.<br><br>Check hardware components and environmental issues for overheated condition. If necessary, replace the component. |
| BTOF | Offset | BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC | 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 system's time source is correct.<br><br>If the problem persists, contact technical support. |

| Code | Name | Service | Recommended action |
| --- | --- | --- | --- |
| BTSE | Clock State | BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC | 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 system's time source is correct.<br><br>If the problem persists, contact technical support. |
| CAHP | Java Heap Usage Percent | DDS | An alarm is triggered if Java is unable to perform garbage collection at a rate that allows enough heap space for the system to properly function. An alarm might indicate a user workload that exceeds the resources available across the system for the DDS metadata store. Check the ILM Activity in the Dashboard, or select **SUPPORT** > **Tools** > **Grid topology**, then select ***site*** > ***grid node*** > **DDS** > **Resources** > **Overview** > **Main**.<br><br>If the problem persists, contact technical support. |
| CAIH | Number Available Ingest Destinations | CLB | This alarm is deprecated. |
| CAQH | Number Available Destinations | CLB | 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.<br><br>If the problem persists, contact technical support. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| CASA | Data Store Status | DDS | An alarm is raised if the Cassandra metadata store becomes unavailable.<br><br>Check the status of Cassandra:<br><br>1. At the Storage Node, log in as admin and `su` to root using the password listed in the Passwords.txt file.<br>2. Enter: `service cassandra status`<br>3. If Cassandra is not running, restart it: `service cassandra restart`<br><br>This alarm might also indicate that the metadata store (Cassandra database) for a Storage Node requires rebuilding.<br><br>See information about troubleshooting the Services: Status - Cassandra (SVST) alarm in Troubleshoot metadata issues.<br><br>If the problem persists, contact technical support. |
| CASE | Data Store State | DDS | This alarm is triggered during installation or expansion to indicate a new data store is joining the grid. |
| CCES | Incoming Sessions - Established | CLB | This alarm is triggered if there are 20,000 or more HTTP sessions currently active (open) on the Gateway Node. If a client has too many connections, you might see connection failures. You should reduce the workload. |
| CCNA | Compute Hardware | SSM | This alarm is triggered if the status of the compute controller hardware in a StorageGRID appliance is Needs Attention. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| CDLP | Metadata Used Space (Percent) | DDS | This alarm is triggered when the Metadata Effective Space (CEMS) reaches 70% full (minor alarm), 90% full (major alarm), and 100% full (critical alarm).<br><br>If this alarm reaches the 90% threshold, a warning appears on the Dashboard in the Grid Manager. You must perform an expansion procedure to add new Storage Nodes as soon as possible. See Expand your grid.<br><br>If this alarm reaches the 100% threshold, you must stop ingesting objects and add Storage Nodes immediately. Cassandra requires a certain amount of space to perform essential operations such as compaction and repair. These operations will be impacted if object metadata uses more than 100% of the allowed space. Undesirable results can occur.<br><br>**Note**: Contact technical support if you are unable to add Storage Nodes.<br><br>After new Storage Nodes are added, the system automatically rebalances object metadata across all Storage Nodes, and the alarm clears.<br><br>Also see information about troubleshooting the Low metadata storage alert in Troubleshoot metadata issues. |
| CLBA | CLB Status | CLB | If an alarm is triggered, select **SUPPORT** > **Tools** > **Grid topology**, then select ***site*** > ***grid node*** > **CLB** > **Overview** > **Main** and **CLB** > **Alarms** > **Main** to determine the cause of the alarm and to troubleshoot the problem.<br><br>If the problem persists, contact technical support. |
| CLBE | CLB State | CLB | If the value of CLB State is Standby, continue monitoring the situation and if the problem persists, contact technical support.<br><br>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 technical support. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| CMNA | CMN Status | CMN | If the value of CMN Status is Error, select **SUPPORT** > **Tools** > **Grid topology**, then select ***site*** > ***grid node*** > **CMN** > **Overview** > **Main** and **CMN** > **Alarms** > **Main** to determine the cause of the error and to troubleshoot the problem.<br><br>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).<br><br>If the problem persists, contact technical support. |
| CPRC | Remaining Capacity | NMS | 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.<br><br>If an alarm is triggered, contact technical support. |
| CPSA | Compute Controller Power Supply A | SSM | An alarm is triggered if there is an issue with power supply A in the compute controller for a StorageGRID appliance.<br><br>If necessary, replace the component. |
| CPSB | Compute Controller Power Supply B | SSM | An alarm is triggered if there is an issue with power supply B in the compute controller for a StorageGRID appliance.<br><br>If necessary, replace the component. |
| CPUT | Compute Controller CPU Temperature | SSM | An alarm is triggered if the temperature of the CPU in the compute controller in a StorageGRID appliance exceeds a nominal threshold.<br><br>If the Storage Node is a StorageGRID appliance, the StorageGRID system indicates that the controller needs attention.<br><br>Check hardware components and environment issues for overheated condition. If necessary, replace the component. |
| DNST | DNS Status | SSM | 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. |

| Code | Name | Service | Recommended action |
| --- | --- | --- | --- |
| ECCD | Corrupt Fragments Detected | LDR | An alarm is triggered when the background verification process detects a corrupt erasure coded fragment. If a corrupt fragment is detected, an attempt is made to rebuild the fragment. Reset the Corrupt Fragments Detected and Copies Lost attributes to zero and monitor them to see if counts go up again. If counts do go up, there may be a problem with the Storage Node's underlying storage. A copy of erasure coded object data is not considered missing until such time that the number of lost or corrupt fragments breaches the erasure code's fault tolerance; therefore, it is possible to have corrupt fragment and to still be able to retrieve the object.<br><br>If the problem persists, contact technical support. |
| ECST | Verification Status | LDR | This alarm indicates the current status of the background verification process for erasure coded object data on this Storage Node.<br><br>A major alarm is triggered if there is an error in the background verification process. |
| FOPN | Open File Descriptors | BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS | FOPN can become large during peak activity. If it does not diminish during periods of slow activity, contact technical support. |
| HSTE | HTTP State | BLDR | See recommended actions for HSTU. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| HSTU | HTTP Status | BLDR | HSTE and HSTU are related to the HTTP protocol for all LDR traffic, including S3, Swift, and other internal StorageGRID traffic. An alarm indicates that one of the following situations has occurred:<br><br>• The HTTP protocol has been taken offline manually.<br>• The Auto-Start HTTP attribute has been disabled.<br>• The LDR service is shutting down.<br><br>The Auto-Start HTTP attribute is enabled by default. If this setting is changed, HTTP could remain offline after a restart.<br><br>If necessary, wait for the LDR service to restart.<br><br>Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***Storage Node*** > **LDR** > **Configuration**. If the HTTP protocol is offline, place it online. Verify that the Auto-Start HTTP attribute is enabled.<br><br>If the HTTP protocol remains offline, contact technical support. |
| HTAS | Auto-Start HTTP | LDR | Specifies whether to start HTTP services automatically on start-up. This is a user-specified configuration option. |
| IRSU | Inbound Replication Status | BLDR, BARC | An alarm indicates that inbound replication has been disabled. Confirm configuration settings: Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration** > **Main**. |
| LATA | Average Latency | NMS | Check for connectivity issues.<br><br>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.<br><br>Check for multiple alarms. An increase in average latency times can be indicated by an excessive number of triggered alarms.<br><br>If the problem persists, contact technical support. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| LDRE | LDR State | LDR | If the value of LDR State is Standby, continue monitoring the situation and if the problem persists, contact technical support.<br><br>If the value of LDR State is Offline, restart the service. If the problem persists, contact technical support. |
| LOST | Lost Objects | DDS, LDR | Triggered when the StorageGRID system fails to retrieve a copy of the requested object from anywhere in the system. Before a LOST (Lost Objects) alarm is triggered, the system attempts to retrieve and replace a missing object from elsewhere in the system.<br><br>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 DDS service purposely purging the content to satisfy the ILM policy.<br><br>Investigate LOST (LOST Object) alarms immediately. If the problem persists, contact technical support.<br><br>Troubleshoot lost and missing object data |
| MCEP | Management Interface Certificate Expiry | CMN | Triggered when the certificate used for accessing the management interface is about to expire.<br><br>1. From the Grid Manager, select **CONFIGURATION** > **Security** > **Certificates**.<br>2. On the **Global** tab, select **Management interface certificate**.<br>3. Upload a new management interface certificate. |
| MINQ | E-mail Notifications Queued | NMS | Check the network connections of the servers hosting the NMS service and the external mail server. Also confirm that the email server configuration is correct.<br><br>Configure email server settings for alarms (legacy system) |
| MINS | E-mail Notifications Status | BNMS | 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 email server configuration is correct.<br><br>Configure email server settings for alarms (legacy system) |

| Code | Name | Service | Recommended action |
| --- | --- | --- | --- |
| MISS | NMS Interface Engine Status | BNMS | 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. |
| NANG | Network Auto Negotiate Setting | SSM | Check the network adapter configuration. The setting must match preferences of your network routers and switches.<br><br>An incorrect setting can have a severe impact on system performance. |
| NDUP | Network Duplex Setting | SSM | Check the network adapter configuration. The setting must match preferences of your network routers and switches.<br><br>An incorrect setting can have a severe impact on system performance. |
| NLNK | Network Link Detect | SSM | Check the network cable connections on the port and at the switch.<br><br>Check the network router, switch, and adapter configurations.<br><br>Restart the server.<br><br>If the problem persists, contact technical support. |
| NRER | Receive Errors | SSM | The following can be causes of NRER alarms:<br><br>• Forward error correction (FEC) mismatch<br>• Switch port and NIC MTU mismatch<br>• High link error rates<br>• NIC ring buffer overrun<br><br>See information about troubleshooting the Network Receive Error (NRER) alarm in Troubleshoot network, hardware, and platform issues. |

| Code | Name | Service | Recommended action |
| --- | --- | --- | --- |
| NRLY | Available Audit Relays | BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS | 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.<br><br>Restore connectivity to an ADC service as soon as possible.<br><br>If the problem persists, contact technical support. |
| NSCA | NMS Status | NMS | If the value of NMS Status is DB Connectivity Error, restart the service. If the problem persists, contact technical support. |
| NSCE | NMS State | NMS | If the value of NMS State is Standby, continue monitoring and if the problem persists, contact technical support.<br><br>If the value of NMS State is Offline, restart the service. If the problem persists, contact technical support. |
| NSPD | Speed | SSM | This can be caused by network connectivity or driver compatibility issues. If the problem persists, contact technical support. |
| NTBR | Free Tablespace | NMS | 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 technical support.<br><br>Adjusting the alarm threshold allows you to proactively manage when additional storage needs to be allocated.<br><br>If the available space reaches a low threshold (see alarm threshold), contact technical support to change the database allocation. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| NTER | Transmit Errors | SSM | 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.<br><br>When the underlying problem is resolved, reset the counter. Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **SSM** > **Resources** > **Configuration** > **Main**, select **Reset Transmit Error Count**, and click **Apply Changes**. |
| NTFQ | NTP Frequency Offset | SSM | If the frequency offset exceeds the configured threshold, there is likely a hardware problem with the local clock. If the problem persists, contact technical support to arrange a replacement. |
| NTLK | NTP Lock | SSM | 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. |
| NTOF | NTP Time Offset | SSM | 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 technical support to arrange a replacement. |
| NTSJ | Chosen Time Source Jitter | SSM | This value indicates the reliability and stability of the time source that NTP on the local server is using as its reference.<br><br>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. |
| NTSU | NTP Status | SSM | If the value of NTP Status is Not Running, contact technical support. |
| OPST | Overall Power Status | SSM | An alarm is triggered if the power of a StorageGRID appliance deviates from the recommended operating voltage.<br><br>Check the status of Power Supply A or B to determine which power supply is operating abnormally.<br><br>If necessary, replace the power supply. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| OQRT | Objects Quarantined | LDR | After the objects are automatically restored by the StorageGRID system, the quarantined objects can be removed from the quarantine directory.<br><br>1. Select **SUPPORT** > **Tools** > **Grid topology**.<br>2. Select **site** > **Storage Node** > **LDR** > **Verification** > **Configuration** > **Main**.<br>3. Select **Delete Quarantined Objects**.<br>4. Click **Apply Changes**.<br><br>The quarantined objects are removed, and the count is reset to zero. |
| ORSU | Outbound Replication Status | BLDR, BARC | 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. Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration**.<br><br>An alarm is triggered if the LDR service is unavailable for replication. Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **LDR** > **Storage**. |
| OSLF | Shelf Status | SSM | An alarm is triggered if the status of one of the components in the storage shelf for a storage appliance is degraded. Storage shelf components include the IOMs, fans, power supplies, and drive drawers.If this alarm is triggered, see the maintenance instructions for your appliance. |
| PMEM | Service Memory Usage (Percent) | BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS | Can have a value of Over Y% RAM, where Y represents the percentage of memory being used by the server.<br><br>Figures under 80% are normal. Over 90% is considered a problem.<br><br>If memory usage is high for a single service, monitor the situation and investigate.<br><br>If the problem persists, contact technical support. |
| PSAS | Power Supply A Status | SSM | An alarm is triggered if power supply A in a StorageGRID appliance deviates from the recommended operating voltage.<br><br>If necessary, replace power supply A. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| PSBS | Power Supply B Status | SSM | An alarm is triggered if power supply B in a StorageGRID appliance deviates from the recommended operating voltage.<br><br>If necessary, replace the power supply B. |
| RDTE | Tivoli Storage Manager State | BARC | Only available for Archive Nodes with a Target Type of Tivoli Storage Manager (TSM).<br><br>If the value of Tivoli Storage Manager State is Offline, check Tivoli Storage Manager Status and resolve any problems.<br><br>Bring the component back online. Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **ARC** > **Target** > **Configuration** > **Main**, select **Tivoli Storage Manager State** > **Online**, and click **Apply Changes**. |
| RDTU | Tivoli Storage Manager Status | BARC | Only available for Archive Nodes with a Target Type of Tivoli Storage Manager (TSM).<br><br>If the value of Tivoli Storage Manager Status is Configuration Error and the Archive Node has just been added to the StorageGRID system, ensure that the TSM middleware server is correctly configured.<br><br>If the value of Tivoli Storage Manager Status is Connection Failure, or Connection Failure, Retrying, check the network configuration on the TSM middleware server, and the network connection between the TSM middleware server and the StorageGRID system.<br><br>If the value of Tivoli Storage Manager Status is Authentication Failure, or Authentication Failure, Reconnecting, the StorageGRID system can connect to the TSM middleware server, but cannot authenticate the connection. Check that the TSM middleware server is configured with the correct user, password, and permissions, and restart the service.<br><br>If the value of Tivoli Storage Manager Status is Session Failure, an established session has been lost unexpectedly. Check the network connection between the TSM middleware server and the StorageGRID system. Check the middleware server for errors.<br><br>If the value of Tivoli Storage Manager Status is Unknown Error, contact technical support. |

| Code | Name | Service | Recommended action |
| --- | --- | --- | --- |
| RIRF | Inbound Replications — Failed | BLDR, BARC | An Inbound Replications — Failed alarm can occur during periods of high load or temporary network disruptions. After system activity reduces, this alarm 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.<br><br>To reset the count, select **SUPPORT** > **Tools** > **Grid topology**, then select ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration** > **Main**. Select **Reset Inbound Replication Failure Count**, and click **Apply Changes**. |
| RIRQ | Inbound Replications — Queued | BLDR, BARC | 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. |
| RORQ | Outbound Replications — Queued | BLDR, BARC | The outbound replication queue contains object data being copied to satisfy ILM rules and objects requested by clients.<br><br>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. |
| SAVP | Total Usable Space (Percent) | LDR | If usable space reaches a low threshold, options include expanding the StorageGRID system or move object data to archive through an Archive Node. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| SCAS | Status | CMN | If the value of Status for the active grid task is Error, look up the grid task message. Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **CMN** > **Grid Tasks** > **Overview** > **Main**. The grid task message displays information about the error (for example, “check failed on node 12130011”).<br><br>After you have investigated and corrected the problem, restart the grid task. Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **CMN** > **Grid Tasks** > **Configuration** > **Main**, and select **Actions** > **Run**.<br><br>If the value of Status for a grid task being aborted is Error, retry aborting the grid task.<br><br>If the problem persists, contact technical support. |
| SCEP | Storage API Service Endpoints Certificate Expiry | CMN | Triggered when the certificate used for accessing storage API endpoints is about to expire.<br><br>1. Select **CONFIGURATION** > **Security** > **Certificates**.<br>2. On the **Global** tab, select **S3 and Swift API certificate**.<br>3. Upload a new S3 and Swift API certificate. |
| SCHR | Status | CMN | If the value of Status for the historical grid task is Aborted, investigate the reason and run the task again if required.<br><br>If the problem persists, contact technical support. |
| SCSA | Storage Controller A | SSM | An alarm is triggered if there is an issue with storage controller A in a StorageGRID appliance.<br><br>If necessary, replace the component. |
| SCSB | Storage Controller B | SSM | An alarm is triggered if there is an issue with storage controller B in a StorageGRID appliance.<br><br>If necessary, replace the component.<br><br>Some appliance models do not have a storage controller B. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| SHLH | Health | LDR | If the value of Health for an object store is Error, check and correct:<br>• problems with the volume being mounted<br>• file system errors |
| SLSA | CPU Load Average | SSM | The higher the value the busier the system.<br><br>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: Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **SSM** > **Resources** > **Reports** > **Charts**.<br><br>If the load on the system is not heavy and the problem persists, contact technical support. |
| SMST | Log Monitor State | SSM | If the value of Log Monitor State is not Connected for a persistent period of time, contact technical support. |
| SMTT | Total Events | SSM | 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.<br><br>When an issue is resolved, reset the counter to clear the alarm. Select **NODES** > ***site*** > ***grid node*** > **Events** > **Reset event counts**.<br><br>To reset event counts, you must have the Grid Topology Page Configuration permission.<br><br>If the value of Total Events is zero, or the number increases and the problem persists, contact technical support. |
| SNST | Status | CMN | 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 system (50 percent plus one) and then wait a few minutes.<br><br>If the problem persists, contact technical support. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| SOSS | Storage Operating System Status | SSM | An alarm is triggered if SANtricity software indicates that there is a “Needs attention” issue with a component in a StorageGRID appliance.<br><br>Select **NODES**. Then select **appliance Storage Node** > **Hardware**. Scroll down to view the status of each component. In SANtricity software, check other appliance components to isolate the issue. |
| SSMA | SSM Status | SSM | If the value of SSM Status is Error, select **SUPPORT** > **Tools** > **Grid topology**, then select ***site*** > ***grid node*** > **SSM** > **Overview** > **Main** and **SSM** > **Overview** > **Alarms** to determine the cause of the alarm.<br><br>If the problem persists, contact technical support. |
| SSME | SSM State | SSM | If the value of SSM State is Standby, continue monitoring, and if the problem persists, contact technical support.<br><br>If the value of SSM State is Offline, restart the service. If the problem persists, contact technical support. |
| SSTS | Storage Status | BLDR | 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.<br><br>Additional storage should be added. It is not impacting end user functionality, but the alarm persists until additional storage is added.<br><br>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: Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **LDR** > **Storage** > **Overview** > **Main**. The volume’s Health is listed under Object Stores.<br><br>If the value of Storage Status is Error, contact technical support.<br><br>Troubleshoot the Storage Status (SSTS) alarm |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| SVST | Status | SSM | This alarm clears when other alarms related to a non-running service are resolved. Track the source service alarms to restore operation.<br><br>Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **SSM** > **Services** > **Overview** > **Main**. When the status of a service is shown as Not Running, its state is Administratively Down. The service's status can be listed as Not Running for the following reasons:<br><br>• The service has been manually stopped (`/etc/init.d/<service\> stop`).<br>• There is an issue with the MySQL database and Server Manager shuts down the MI service.<br>• A grid node has been added, but not started.<br>• During installation, a grid node has not yet connected to the Admin Node.<br><br>If a service is listed as Not Running, restart the service (`/etc/init.d/<service\> restart`).<br><br>This alarm might also indicate that the metadata store (Cassandra database) for a Storage Node requires rebuilding.<br><br>If the problem persists, contact technical support.<br><br>Troubleshoot the Services: Status - Cassandra (SVST) alarm |
| TMEM | Installed Memory | SSM | Nodes running with less than 24 GiB of installed memory can lead to performance problems and system instability. The amount of memory installed on the system should be increased to at least 24 GiB. |
| TPOP | Pending Operations | ADC | A queue of messages can indicate that the ADC service is overloaded. Too few ADC services can be connected to the StorageGRID system. In a large deployment, the ADC service can require adding computational resources, or the system can require additional ADC services. |
| UMEM | Available Memory | SSM | If the available RAM gets low, determine whether this is a hardware or software issue. If it is not a hardware issue, or if available memory falls below 50 MB (the default alarm threshold), contact technical support. |

| Code | Name | Service | Recommended action |
|---|---|---|---|
| VMFI | Entries Available | SSM | This is an indication that additional storage is required. Contact technical support. |
| VMFR | Space Available | SSM | 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.<br><br>If the problem persists, contact technical support. |
| VMST | Status | SSM | 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 | BLDR, BARC | 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 | BLDR | Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***site*** > ***grid node*** > **LDR** > **Storage** > **Overview** > **Main**.<br><br>Check the operating system for any signs of block-device or file system errors.<br><br>If the value of Object Verification Status is Unknown Error, it usually indicates a low-level file system or hardware problem (I/O error) that prevents the Storage Verification task from accessing stored content. Contact technical support. |
| XAMS | Unreachable Audit Repositories | BADC, BARC, BCLB, BCMN, BLDR, BNMS | Check network connectivity to the server hosting the Admin Node.<br><br>If the problem persists, contact technical support. |

#### Alarms that generate SNMP notifications (legacy system)

The following table lists the legacy alarms that generate SNMP notifications. Unlike alerts, not all alarms generate SNMP notifications. Only the alarms listed generate SNMP notifications and only at the indicated severity or higher.

> While the legacy alarm system continues to be supported, the alert system offers significant benefits and is easier to use.

| Code | Name | Severity |
| --- | --- | --- |
| ACMS | Available Metadata Services | Critical |
| AITE | Retrieve State | Minor |
| AITU | Retrieve Status | Major |
| AMQS | Audit Messages Queued | Notice |
| AOTE | Store State | Minor |
| AOTU | Store Status | Major |
| AROQ | Objects Queued | Minor |
| ARRF | Request Failures | Major |
| ARRV | Verification Failures | Major |
| ARVF | Store Failures | Major |
| ASXP | Audit Shares | Minor |
| AUMA | AMS Status | Minor |
| AUXS | Audit Export Status | Minor |
| BTOF | Offset | Notice |
| CAHP | Java Heap Usage Percent | Major |
| CAQH | Number Available Destinations | Notice |
| CASA | Data Store Status | Major |
| CDLP | Metadata Used Space (Percent) | Major |
| CLBE | CLB State | Critical |
| DNST | DNS Status | Critical |
| ECST | Verification Status | Major |
| HSTE | HTTP State | Major |

| Code | Name | Severity |
| --- | --- | --- |
| HTAS | Auto-Start HTTP | Notice |
| LOST | Lost Objects | Major |
| MINQ | E-mail Notifications Queued | Notice |
| MINS | E-mail Notifications Status | Minor |
| NANG | Network Auto Negotiate Setting | Notice |
| NDUP | Network Duplex Setting | Minor |
| NLNK | Network Link Detect | Minor |
| NRER | Receive Errors | Notice |
| NSPD | Speed | Notice |
| NTER | Transmit Errors | Notice |
| NTFQ | NTP Frequency Offset | Minor |
| NTLK | NTP Lock | Minor |
| NTOF | NTP Time Offset | Minor |
| NTSJ | Chosen Time Source Jitter | Minor |
| NTSU | NTP Status | Major |
| OPST | Overall Power Status | Major |
| ORSU | Outbound Replication Status | Notice |
| PSAS | Power Supply A Status | Major |
| PSBS | Power Supply B Status | Major |
| RDTE | Tivoli Storage Manager State | Notice |
| RDTU | Tivoli Storage Manager Status | Major |
| SAVP | Total Usable Space (Percent) | Notice |

| Code | Name | Severity |
|---|---|---|
| SHLH | Health | Notice |
| SLSA | CPU Load Average | Notice |
| SMTT | Total Events | Notice |
| SNST | Status | |
| SOSS | Storage Operating System Status | Notice |
| SSTS | Storage Status | Notice |
| SVST | Status | Notice |
| TMEM | Installed Memory | Minor |
| UMEM | Available Memory | Minor |
| VMST | Status | Minor |
| VPRI | Verification Priority | Notice |
| VSTU | Object Verification Status | Notice |

## Log files reference

StorageGRID provides logs that are used to capture events, diagnostic messages, and error conditions. You might be asked to collect log files and forward them to technical support to assist with troubleshooting.

The logs are categorized as follows:

- StorageGRID software logs
- Deployment and maintenance logs
- Logs for third-party software
- About the bycast.log

> The details provided for each log type are for reference only. The logs are intended for advanced troubleshooting by technical support. Advanced techniques that involve reconstructing the problem history using the audit logs and the application log files are beyond the scope of these instructions.

To access the logs, you can collect log files and system data from one or more nodes as a single log file archive (**SUPPORT** > **Tools** > **Logs**). Or, if the primary Admin Node is unavailable or unable to reach a specific

node, you can access individual log files for each grid node as follows:

1. Enter the following command: `ssh admin@grid_node_IP`
2. Enter the password listed in the `Passwords.txt` file.
3. Enter the following command to switch to root: `su -`
4. Enter the password listed in the `Passwords.txt` file.

The StorageGRID log file archive contains the logs described for each category and additional files that contain metrics and debug command output.

| Archive location | Description |
|---|---|
| `audit` | Audit messages generated during normal system operation. |
| `base-os-logs` | Base operating system information, including StorageGRID image versions. |
| `bundles` | Global configuration information (bundles). |
| `cassandra` | Cassandra database information and Reaper repair logs. |
| `ec` | VCSs information on the current node and EC group information by profile ID. |
| `grid` | General grid logs including debug (`bycast.log`) and `servermanager` logs. |
| `grid.xml` | Grid configuration file shared across all nodes. |
| `hagroups` | High availability groups metrics and logs. |
| `install` | `Gdu-server` and install logs. |
| `lumberjack.log` | Debug messages related to log collection. |
| `Lambda-arbitrator` | Logs related to the S3 Select proxy request. |
| `Metrics` | Service logs for Grafana, Jaeger, node exporter, and Prometheus. |
| `miscd` | Miscd access and error logs. |
| `mysql` | The mariaDB database configuration and related logs. |
| `net` | Logs generated by networking-related scripts and the Dynip service. |
| `nginx` | Load balancer configuration files and logs. Also includes Grid Manager and Tenant Manager traffic logs. |

| Archive location | Description |
| --- | --- |
| `nginx-gw` | Load balancer configuration files and logs. |
| `ntp` | NTP configuration file and logs. |
| `os` | Node and grid state file, including services `pid`. |
| `other` | Log files under `/var/local/log` that are not collected in other folders. |
| `perf` | Peformance information for CPU, networking, and disk I/O. |
| `prometheus-data` | Current Prometheus metrics, if the log collection includes Prometheus data. |
| `provisioning` | Logs related to grid provisioning process. |
| `raft` | Logs from Raft cluster used in platform services. |
| `snmp` | SNMP agent configuration and alarm allow/deny lists used for sending SNMP notifications. |
| `sockets-data` | Sockets data for network debug. |
| `system-commands.txt` | Output of StorageGRID container commands. Contains system information, such as networking and disk usage. |

**Related information**

Collect log files and system data

### StorageGRID software logs

You can use StorageGRID logs to troubleshoot issues.

> If you want to send your logs to an external syslog server or change the destination of audit information such as the `bycast.log` and `nms.log`, see Configure audit messages and log destinations.

#### General StorageGRID logs

| File name | Notes | Found on |
| --- | --- | --- |
| `/var/local/log/bycast.log` | The primary StorageGRID troubleshooting file. Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***Site*** > ***Node*** > **SSM** > **Events**. | All nodes |

| File name | Notes | Found on |
| --- | --- | --- |
| `/var/local/log/bycast-err.log` | Contains a subset of `bycast.log` (messages with severity ERROR and CRITICAL). CRITICAL messages are also displayed in the system. Select **SUPPORT** > **Tools** > **Grid topology**. Then select ***Site*** > ***Node*** > **SSM** > **Events**. | All nodes |
| `/var/local/core/` | Contains any core dump files created if the program terminates abnormally. Possible causes include assertion failures, violations, or thread timeouts.<br>The file `` `/var/local/core/kexec_cmd `` usually exists on appliance nodes and does not indicate an error. | All nodes |

#### Server Manager logs

| File name | Notes | Found on |
| --- | --- | --- |
| `/var/local/log/servermanager.log` | Log file for the Server Manager application running on the server. | All nodes |
| `/var/local/log/GridstatBackend.errlog` | Log file for the Server Manager GUI backend application. | All nodes |
| `/var/local/log/gridstat.errlog` | Log file for the Server Manager GUI. | All nodes |

#### Logs for StorageGRID services

| File name | Notes | Found on |
| --- | --- | --- |
| `/var/local/log/acct.errlog` | | Storage Nodes running the ADC service |
| `/var/local/log/adc.errlog` | 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. | Storage Nodes running the ADC service |
| `/var/local/log/ams.errlog` | | Admin Nodes |
| `/var/local/log/arc.errlog` | | Archive Nodes |

| File name | Notes | Found on |
| --- | --- | --- |
| `/var/local/log/cassandra/system.log` | Information for the metadata store (Cassandra database) that can be used if problems occur when adding new Storage Nodes, or if the nodetool repair task stalls. | Storage Nodes |
| `/var/local/log/cassandra-reaper.log` | Information for the Cassandra Reaper service, which performs repairs of the data in the Cassandra database. | Storage Nodes |
| `/var/local/log/cassandra-reaper.errlog` | Error information for the Cassandra Reaper service. | Storage Nodes |
| `/var/local/log/chunk.errlog` | | Storage Nodes |
| `/var/local/log/clb.errlog` | Error information for the CLB service.<br><br>**Note:** The CLB service is deprecated. | Gateway Nodes |
| `/var/local/log/cmn.errlog` | | Admin Nodes |
| `/var/local/log/cms.errlog` | This log file might be present on systems that have been upgraded from an older version of StorageGRID. It contains legacy information. | Storage Nodes |
| `/var/local/log/cts.errlog` | This log file is only created if the Target Type is **Cloud Tiering - Simple Storage Service (S3).** | Archive Nodes |
| `/var/local/log/dds.errlog` | | Storage Nodes |
| `/var/local/log/dmv.errlog` | | Storage Nodes |
| `/var/local/log/dynip*` | Contains logs related to the dynip service, which monitors the grid for dynamic IP changes and updates local configuration. | All nodes |
| `/var/local/log/grafana.log` | The log associated with the Grafana service, which is used for metrics visualization in the Grid Manager. | Admin Nodes |
| `/var/local/log/hagroups.log` | The log associated with high availability groups. | Admin Nodes and Gateway Nodes |

| File name | Notes | Found on |
| --- | --- | --- |
| `/var/local/log/hagroups_events.log` | Tracks state changes, such as transition from BACKUP to MASTER or FAULT. | Admin Nodes and Gateway Nodes |
| `/var/local/log/idnt.errlog` | | Storage Nodes running the ADC service |
| `/var/local/log/jaeger.log` | The log associated with the jaeger service, which is used for trace collection. | All nodes |
| `/var/local/log/kstn.errlog` | | Storage Nodes running the ADC service |
| `/var/local/log/lambda*` | Contains logs for the S3 Select service. | Admin and Gateway Nodes<br><br>Only certain Admin and Gateway Nodes contain this log. See the S3 Select requirements and limitations for Admin and Gateway Nodes. |
| `/var/local/log/ldr.errlog` | | Storage Nodes |
| `/var/local/log/miscd/*.log` | Contains logs for the MISCd service (Information Service Control Daemon), which provides an interface for querying and managing services on other nodes and for managing environmental configurations on the node such as querying the state of services running on other nodes. | All nodes |
| `/var/local/log/nginx/*.log` | Contains logs for the nginx service, which acts as an authentication and secure communication mechanism for various grid services (such as Prometheus and Dynip) to be able to talk to services on other nodes over HTTPS APIs. | All nodes |
| `/var/local/log/nginx-gw/*.log` | Contains logs for the restricted admin ports on Admin Nodes and for the Load Balancer service, which provides load balancing of S3 and Swift traffic from clients to Storage Nodes. | Admin Nodes and Gateway Nodes |

| File name | Notes | Found on |
| --- | --- | --- |
| `/var/local/log/persistence*` | Contains logs for the Persistence service, which manages files on the root disk that need to persist across a reboot. | All nodes |
| `/var/local/log/prometheus.log` | For all nodes, contains the node exporter service log and the ade-exporter metrics service log.<br><br>For Admin Nodes, also contains logs for the Prometheus and Alert Manager services. | All nodes |
| `/var/local/log/raft.log` | Contains the output of the library used by the RSM service for the Raft protocol. | Storage Nodes with RSM service |
| `/var/local/log/rms.errlog` | Contains logs for the Replicated State Machine Service (RSM) service, which is used for S3 platform services. | Storage Nodes with RSM service |
| `/var/local/log/ssm.errlog` | | All nodes |
| `/var/local/log/update-s3vs-domains.log` | Contains logs related to processing updates for the S3 virtual hosted domain names configuration.See the instructions for implementing S3 client applications. | Admin and Gateway Nodes |
| `/var/local/log/update-snmp-firewall.*` | Contain logs related to the firewall ports being managed for SNMP. | All nodes |
| `/var/local/log/update-sysl.log` | Contains logs related to changes made to the system syslog configuration. | All nodes |
| `/var/local/log/update-traffic-classes.log` | Contains logs related to changes to the traffic classifiers configuration. | Admin and Gateway Nodes |
| `/var/local/log/update-utcn.log` | Contains logs related to Untrusted Client Network mode on this node. | All nodes |

**NMS logs**

| File name | Notes | Found on |
| --- | --- | --- |
| `/var/local/log/nms.log` | • Captures notifications from the Grid Manager and the Tenant Manager.<br>• Captures events related to the operation of the NMS service, for example, alarm processing, email notifications, and configuration changes.<br>• Contains XML bundle updates resulting from configuration changes made in the system.<br>• Contains error messages related to the attribute downsampling done once a day.<br>• Contains Java web server error messages, for example, page generation errors and HTTP Status 500 errors. | Admin Nodes |
| `/var/local/log/nms.errlog` | Contains error messages related to MySQL database upgrades.<br><br>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. | Admin Nodes |
| `/var/local/log/nms.requestlog` | Contains information about outgoing connections from the Management API to internal StorageGRID services. | Admin Nodes |

**Related information**

About the bycast.log

Use S3

**Deployment and maintenance logs**

You can use the deployment and maintenance logs to troubleshoot issues.

| File name | Notes | Found on |
| --- | --- | --- |
| `/var/local/log/install.log` | Created during software installation. Contains a record of the installation events. | All nodes |
| `/var/local/log/expansion-progress.log` | Created during expansion operations. Contains a record of the expansion events. | Storage Nodes |

| File name | Notes | Found on |
| --- | --- | --- |
| `/var/local/log/gdu-server.log` | Created by the GDU service. Contains events related to provisioning and maintenance procedures managed by the primary Admin Node. | Primary Admin Node |
| `/var/local/log/send_admin_hw.log` | Created during installation. Contains debugging information related to a node's communications with the primary Admin Node. | All nodes |
| `/var/local/log/upgrade.log` | Created during software upgrade. Contains a record of the software update events. | All nodes |

#### Logs for third-party software

You can use the third-party software logs to troubleshoot issues.

| Category | File name | Notes | Found on |
| --- | --- | --- | --- |
| Archiving | `/var/local/log/dsierror.log` | Error information for TSM Client APIs. | Archive Nodes |
| MySQL | `/var/local/log/mysql.err`<br>`/var/local/log/mysql-slow.log` | Log files generated by MySQL.<br><br>The file `mysql.err` captures database errors and events such as startups and shutdowns.<br><br>The file `mysql-slow.log` (the slow query log) captures the SQL statements that took more than 10 seconds to execute. | Admin Nodes |
| Operating system | `/var/local/log/messages` | This directory contains log files for the operating system. The errors contained in these logs are also displayed in the Grid Manager. Select **SUPPORT** > **Tools** > **Grid topology**. Then select **Topology** > ***Site*** > ***Node*** > **SSM** > **Events**. | All nodes |

| Category | File name | Notes | Found on |
|---|---|---|---|
| NTP | `/var/local/log/ntp.log`<br>`/var/lib/ntp/var/log/ntpstats/` | `/var/local/log/ntp.log` contains the log file for NTP error messages.<br><br>The `/var/lib/ntp/var/log/ntpstats/` directory contains NTP timing statistics.<br><br>`loopstats` records loop filter statistics information.<br><br>`peerstats` records peer statistics information. | All nodes |
| Samba | `/var/local/log/samba/` | The Samba log directory includes a log file for each Samba process (smb, nmb, and winbind) and every client hostname/IP. | Admin Node configured to export the audit share over CIFS |

### About the bycast.log

The file `/var/local/log/bycast.log` is the primary troubleshooting file for the StorageGRID 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.

Optionally, you can change the destination of audit logs and send audit information to an external syslog server. Local logs of audit records continue to be generated and stored when an external syslog server is configured. See Configure audit messages and log destinations.

#### File rotation for bycast.log

When the `bycast.log` file reaches 1 GB, the existing file is saved, and a new log file is started.

The saved file is renamed `bycast.log.1`, and the new file is named `bycast.log`. When the new `bycast.log` reaches 1 GB, `bycast.log.1` is renamed and compressed to become `bycast.log.2.gz`, and `bycast.log` is renamed `bycast.log.1`.

The rotation limit for `bycast.log` is 21 files. When the 22nd version of the `bycast.log` file is created, the oldest file is deleted.

The rotation limit for `bycast-err.log` is seven files.

> If a log file has been compressed, you must not uncompress it to the same location in which it was written. Uncompressing the file to the same location can interfere with the log rotation scripts.

Optionally, you can change the destination of audit logs and send audit information to an external syslog

server. Local logs of audit records continue to be generated and stored when an external syslog server is configured. See Configure audit messages and log destinations.

**Related information**

Collect log files and system data

#### Messages in bycast.log

Messages in `bycast.log` are written by the ADE (Asynchronous Distributed Environment). ADE is the runtime environment used by each grid node's services.

Example ADE message:

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

ADE messages contain the following information:

| Message segment | Value in example |
|---|---|
| Node ID | `12455685` |
| ADE process ID | `0357819531` |
| Module name | `SVMR` |
| Message identifier | `EVHR` |
| UTC system time | `2019-05-05T27T17:10:29.784677 (YYYY-MM-DDTHH:MM:SS.uuuuuu)` |
| Severity level | `ERROR` |
| Internal tracking number | `0906` |
| Message | `SVMR: Health check on volume 3 has failed with reason 'TOUT'` |

#### Message severities in bycast.log

The 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** — An abnormal condition has occurred that has stopped normal operations. You should address

the underlying condition immediately. Critical messages are also displayed in the Grid Manager. Select **SUPPORT** > **Tools** > **Grid topology**. Then select **Site** > **Node** > **SSM** > **Events**.

#### Error codes in `bycast.log`

Most of the error messages in `bycast.log` contain error codes.

The following table lists common non-numerical codes in `bycast.log`. The exact meaning of a non-numerical code depends on the context in which it is reported.

| Error code | Meaning |
|---|---|
| SUCS | No error |
| GERR | Unknown |
| CANC | Canceled |
| ABRT | Aborted |
| TOUT | Timeout |
| INVL | Invalid |
| NFND | Not found |
| VERS | Version |
| CONF | Configuration |
| FAIL | Failed |
| ICPL | Incomplete |
| DONE | Done |
| SUNV | Service unavailable |

The following table lists the numerical error codes in `bycast.log`.

| Error number | Error code | Meaning |
|---|---|---|
| 001 | EPERM | Operation not permitted |
| 002 | ENOENT | No such file or directory |
| 003 | ESRCH | No such process |

| Error number | Error code | Meaning |
|---|---|---|
| 004 | EINTR | Interrupted system call |
| 005 | EIO | I/O error |
| 006 | ENXIO | No such device or address |
| 007 | E2BIG | Argument list too long |
| 008 | ENOEXEC | Exec format error |
| 009 | EBADF | Bad file number |
| 010 | ECHILD | No child processes |
| 011 | EAGAIN | Try again |
| 012 | ENOMEM | Out of memory |
| 013 | EACCES | Permission denied |
| 014 | EFAULT | Bad address |
| 015 | ENOTBLK | Block device required |
| 016 | EBUSY | Device or resource busy |
| 017 | EEXIST | File exists |
| 018 | EXDEV | Cross-device link |
| 019 | ENODEV | No such device |
| 020 | ENOTDIR | Not a directory |
| 021 | EISDIR | Is a directory |
| 022 | EINVAL | Invalid argument |
| 023 | ENFILE | File table overflow |
| 024 | EMFILE | Too many open files |
| 025 | ENOTTY | Not a typewriter |

| Error number | Error code | Meaning |
|---|---|---|
| 026 | ETXTBSY | Text file busy |
| 027 | EFBIG | File too large |
| 028 | ENOSPC | No space left on device |
| 029 | ESPIPE | Illegal seek |
| 030 | EROFS | Read-only file system |
| 031 | EMLINK | Too many links |
| 032 | EPIPE | Broken pipe |
| 033 | EDOM | Math argument out of domain of func |
| 034 | ERANGE | Math result not representable |
| 035 | EDEADLK | Resource deadlock would occur |
| 036 | ENAMETOOLONG | File name too long |
| 037 | ENOLCK | No record locks available |
| 038 | ENOSYS | Function not implemented |
| 039 | ENOTEMPTY | Directory not empty |
| 040 | ELOOP | Too many symbolic links encountered |
| 041 | | |
| 042 | ENOMSG | No message of desired type |
| 043 | EIDRM | Identifier removed |
| 044 | ECHRNG | Channel number out of range |
| 045 | EL2NSYNC | Level 2 not synchronized |
| 046 | EL3HLT | Level 3 halted |
| 047 | EL3RST | Level 3 reset |

| Error number | Error code | Meaning |
|---|---|---|
| 048 | ELNRNG | Link number out of range |
| 049 | EUNATCH | Protocol driver not attached |
| 050 | ENOCSI | No CSI structure available |
| 051 | EL2HLT | Level 2 halted |
| 052 | EBADE | Invalid exchange |
| 053 | EBADR | Invalid request descriptor |
| 054 | EXFULL | Exchange full |
| 055 | ENOANO | No anode |
| 056 | EBADRQC | Invalid request code |
| 057 | EBADSLT | Invalid slot |
| 058 | | |
| 059 | EBFONT | Bad font file format |
| 060 | ENOSTR | Device not a stream |
| 061 | ENODATA | No data available |
| 062 | ETIME | Timer expired |
| 063 | ENOSR | Out of streams resources |
| 064 | ENONET | Machine is not on the network |
| 065 | ENOPKG | Package not installed |
| 066 | EREMOTE | Object is remote |
| 067 | ENOLINK | Link has been severed |
| 068 | EADV | Advertise error |
| 069 | ESRMNT | Srmount error |

| Error number | Error code | Meaning |
|---|---|---|
| 070 | ECOMM | Communication error on send |
| 071 | EPROTO | Protocol error |
| 072 | EMULTIHOP | Multihop attempted |
| 073 | EDOTDOT | RFS specific error |
| 074 | EBADMSG | Not a data message |
| 075 | EOVERFLOW | Value too large for defined data type |
| 076 | ENOTUNIQ | Name not unique on network |
| 077 | EBADFD | File descriptor in bad state |
| 078 | EREMCHG | Remote address changed |
| 079 | ELIBACC | Cannot access a needed shared library |
| 080 | ELIBBAD | Accessing a corrupted shared library |
| 081 | ELIBSCN | |
| 082 | ELIBMAX | Attempting to link in too many shared libraries |
| 083 | ELIBEXEC | Cannot exec a shared library directly |
| 084 | EILSEQ | Illegal byte sequence |
| 085 | ERESTART | Interrupted system call should be restarted |
| 086 | ESTRPIPE | Streams pipe error |
| 087 | EUSERS | Too many users |
| 088 | ENOTSOCK | Socket operation on non-socket |
| 089 | EDESTADDRREQ | Destination address required |
| 090 | EMSGSIZE | Message too long |
| 091 | EPROTOTYPE | Protocol wrong type for socket |

| Error number | Error code | Meaning |
|---|---|---|
| 092 | ENOPROTOOPT | Protocol not available |
| 093 | EPROTONOSUPPORT | Protocol not supported |
| 094 | ESOCKTNOSUPPORT | Socket type not supported |
| 095 | EOPNOTSUPP | Operation not supported on transport endpoint |
| 096 | EPFNOSUPPORT | Protocol family not supported |
| 097 | EAFNOSUPPORT | Address family not supported by protocol |
| 098 | EADDRINUSE | Address already in use |
| 099 | EADDRNOTAVAIL | Cannot assign requested address |
| 100 | ENETDOWN | Network is down |
| 101 | ENETUNREACH | Network is unreachable |
| 102 | ENETRESET | Network dropped connection because of reset |
| 103 | ECONNABORTED | Software caused connection abort |
| 104 | ECONNRESET | Connection reset by peer |
| 105 | ENOBUFS | No buffer space available |
| 106 | EISCONN | Transport endpoint is already connected |
| 107 | ENOTCONN | Transport endpoint is not connected |
| 108 | ESHUTDOWN | Cannot send after transport endpoint shutdown |
| 109 | ETOOMANYREFS | Too many references: cannot splice |
| 110 | ETIMEDOUT | Connection timed out |
| 111 | ECONNREFUSED | Connection refused |
| 112 | EHOSTDOWN | Host is down |
| 113 | EHOSTUNREACH | No route to host |

| Error number | Error code | Meaning |
|---|---|---|
| 114 | EALREADY | Operation already in progress |
| 115 | EINPROGRESS | Operation now in progress |
| 116 | | |
| 117 | EUCLEAN | Structure needs cleaning |
| 118 | ENOTNAM | Not a XENIX named type file |
| 119 | ENAVAIL | No XENIX semaphores available |
| 120 | EISNAM | Is a named type file |
| 121 | EREMOTEIO | Remote I/O error |
| 122 | EDQUOT | Quota exceeded |
| 123 | ENOMEDIUM | No medium found |
| 124 | EMEDIUMTYPE | Wrong medium type |
| 125 | ECANCELED | Operation Canceled |
| 126 | ENOKEY | Required key not available |
| 127 | EKEYEXPIRED | Key has expired |
| 128 | EKEYREVOKED | Key has been revoked |
| 129 | EKEYREJECTED | Key was rejected by service |
| 130 | EOWNERDEAD | For robust mutexes: Owner died |
| 131 | ENOTRECOVERABLE | For robust mutexes: State not recoverable |

# Expand your grid

## Expand your grid: Overview

Use these instructions to expand the capacity or capabilities of your StorageGRID system without interrupting system operations.

### About these instructions

These instructions describe how to perform a StorageGRID expansion to add storage volumes to Storage Nodes, new grid nodes to an existing site, or an entire new site.

These instructions are for technical personnel who are responsible for configuring and supporting the StorageGRID system after it has been installed.

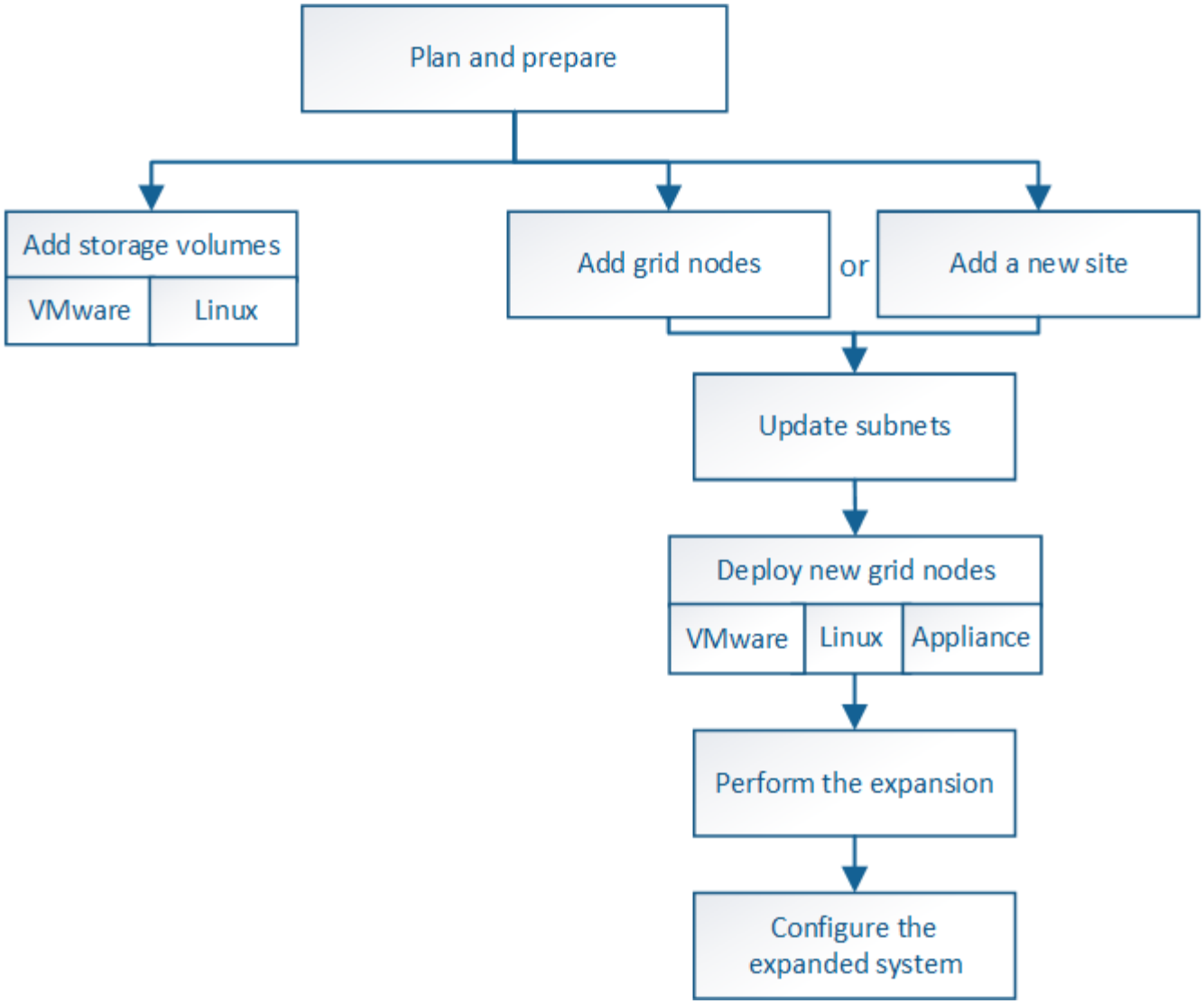
### Overview of expansion procedure

The reason you are performing the expansion determines how many new nodes of each type you must add and the location of those new nodes. For example, there are different node requirements if you are performing an expansion to increase storage capacity, add metadata capacity, or add redundancy or new capabilities.

As shown in the workflow diagram, the steps for performing an expansion depend on whether you are adding storage volumes to a Storage Node, adding new nodes to an existing site, or adding a new site. In all cases, you can perform the expansion without interrupting the operation of your current system.

The steps for adding nodes also depend on whether you are adding StorageGRID appliances or hosts running VMware or Linux.

> “Linux” refers to a Red Hat® Enterprise Linux®, Ubuntu®, CentOS, or Debian® deployment. Use the NetApp Interoperability Matrix Tool (IMT) to get a list of supported versions.




## Plan StorageGRID expansion

### Add storage capacity

#### Guidelines for adding object capacity

You can expand the object storage capacity of your StorageGRID system by adding storage volumes to existing Storage Nodes or by adding new Storage Nodes to existing sites. You must add storage capacity in a way that meets the requirements of your information lifecycle management (ILM) policy.

#### Guidelines for adding storage volumes

Before adding storage volumes to existing Storage Nodes, review the following guidelines and limitations:

- You must examine your current ILM rules to determine where and when to add storage volumes to increase the storage available for replicated or erasure-coded objects. See the instructions for managing objects with information lifecycle management.
- You cannot increase the metadata capacity of your system by adding storage volumes because object metadata is stored only on volume 0.

- Each software-based Storage Node can support a maximum of 16 storage volumes. If you need to add capacity beyond that, you must add new Storage Nodes.
- You can add one or two expansion shelves to each SG6060 or SG6060X appliance. Each expansion shelf adds 16 storage volumes. With both expansion shelves installed, the SG6060 and SG6060X can each support a total of 48 storage volumes.
- You cannot add storage volumes to any other storage appliance.
- You cannot increase the size of an existing storage volume.
- You cannot add storage volumes to a Storage Node at the same time you are performing a system upgrade, recovery operation, or another expansion.

After you have decided to add storage volumes and have determined which Storage Nodes you must expand to satisfy your ILM policy, follow the instructions for your type of Storage Node:

- To add one or two expansion shelves to an SG6060 or SG6060X storage appliance, go to Add expansion shelf to deployed SG6060 or SG6060X.
- For a software-based node, follow the instructions for adding storage volumes to Storage Nodes.

### Guidelines for adding Storage Nodes

Before adding Storage Nodes to existing sites, review the following guidelines and limitations:

- You must examine your current ILM rules to determine where and when to add Storage Nodes to increase the storage available for replicated or erasure-coded objects. See the instructions for managing objects with information lifecycle management.
- You should not add more than 10 Storage Nodes in a single expansion procedure.
- You can add Storage Nodes to more than one site in a single expansion procedure.
- You can add Storage Nodes and other types of nodes in a single expansion procedure.
- Before starting the expansion procedure, you must confirm that all data-repair operations performed as part of a recovery are complete. See Check data repair jobs.
- If you need to remove Storage Nodes before or after performing an expansion, you should not decommission more than 10 Storage Nodes in a single Decommission Node procedure.

### Guidelines for ADC service on Storage Nodes

When configuring the expansion, you must choose whether to include the Administrative Domain Controller (ADC) service on each new Storage Node. The ADC service keeps track of the location and availability of grid services.

- The StorageGRID system requires a quorum of ADC services to be available at each site and at all times.
- At least three Storage Nodes at each site must include the ADC service.
- Adding the ADC service to every Storage Node is not recommended. Including too many ADC services can cause slowdowns due to the increased amount of communication between nodes.
- A single grid should not have more than 48 Storage Nodes with the ADC service. This is equivalent to 16 sites with three ADC services at each site.
- In general, when you select the **ADC Service** setting for a new node, you should select **Automatic**. Select **Yes** only if the new node will replace another Storage Node that includes the ADC service. Because you cannot decommission a Storage Node if too few ADC services would remain, this ensures that a new ADC service is available before the old service is removed.

- You cannot add the ADC service to a node after it is deployed.

#### Add storage capacity for replicated objects

If the information lifecycle management (ILM) policy for your deployment includes a rule that creates replicated copies of objects, you must consider how much storage to add and where to add the new storage volumes or Storage Nodes.

For guidance on where to add additional storage, examine the ILM rules that create replicated copies. If ILM rules create two or more object copies, plan to add storage in each location where object copies are made. As a simple example, if you have a two-site grid and an ILM rule that creates one object copy at each site, you must add storage to each site to increase the overall object capacity of the grid. See the instructions for managing objects with information lifecycle management.

For performance reasons, you should attempt to keep storage capacity and compute power balanced across sites. So, for this example, you should add the same number of Storage Nodes to each site or additional storage volumes at each site.

If you have a more complex ILM policy that includes rules that place objects in different locations based on criteria such as bucket name, or rules that change object locations over time, your analysis of where storage is required for the expansion will be similar, but more complex.

Charting how quickly overall storage capacity is being consumed can help you understand how much storage to add in the expansion, and when the additional storage space will be required. You can use the Grid Manager to monitor and chart storage capacity as described in the instructions for monitoring and troubleshooting StorageGRID.

When planning the timing of an expansion, remember to consider how long it might take to procure and install additional storage.

#### Add storage capacity for erasure-coded objects

If your ILM policy includes a rule that makes erasure-coded copies, you must plan where to add new storage and when to add new storage. The amount of storage you add and the timing of the addition can affect the grid's usable storage capacity.

The first step in planning a storage expansion is to examine the rules in your ILM policy that create erasure-coded objects. Because StorageGRID creates *k+m* fragments for every erasure-coded object and stores each fragment on a different Storage Node, you must ensure that at least *k+m* Storage Nodes have space for new erasure-coded data after the expansion. If the erasure-coding profile provides site-loss protection, you must add storage to each site. See Manage objects with ILM.

The number of nodes you need to add also depends on how full the existing nodes are when you perform the expansion.

**General recommendation for adding storage capacity for erasure-coded objects**

If you want to avoid detailed calculations, you can add two Storage Nodes per site when existing Storage Nodes reach 70% capacity.

This general recommendation provides reasonable results across a wide range of erasure-coding schemes for both single-site grids and for grids where erasure coding provides site-loss protection.

To better understand the factors that lead to this recommendation or to develop a more precise plan for your

site, review the next section. For a custom recommendation optimized for your situation, contact your NetApp account representative.

### Calculate number of expansion Storage Nodes to add for erasure-coded objects

To optimize how you expand a deployment that stores erasure-coded objects, you must consider many factors:

- Erasure-coding scheme in use
- Characteristics of the storage pool used for erasure coding, including the number of nodes at each site and the amount of free space on each node
- Whether the grid was previously expanded (because the amount of free space per Storage Node might not be approximately the same on all nodes)
- Exact nature of the ILM policy, such as whether ILM rules make both replicated and erasure-coded objects

The following examples can help you understand the impact of the erasure-coding scheme, the number of nodes in the storage pool, and the amount of free space on each node.

Similar considerations affect the calculations for an ILM policy that stores both replicated and erasure-coded data and the calculations for a grid that has been previously expanded.

> The examples in this section represent the best practices for adding storage capacity to a StorageGRID system. If you are unable to add the recommended number of nodes, you might need to run the EC rebalance procedure to allow additional erasure-coded objects to be stored. See Rebalance erasure-coded data.

### Example 1: Expand one-site grid that uses 2+1 erasure coding

This example shows how to expand a simple grid that includes only three Storage Nodes.

> This example uses only three Storage Nodes for simplicity. However, using only three Storage Nodes is not recommended: an actual production grid should use a minimum of $k+m+1$ Storage Nodes for redundancy, which equals four Storage Nodes (2+1+1) for this example.

Assume the following:

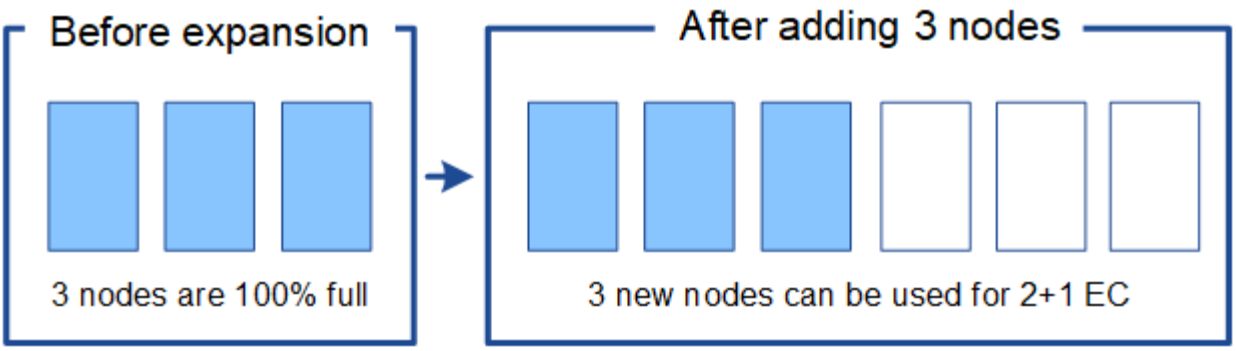
- All data is stored using the 2+1 erasure-coding scheme. With the 2+1 erasure coding scheme, every object is stored as three fragments, and each fragment is saved on a different Storage Node.
- You have one site with three Storage Nodes. Each Storage Node has a total capacity of 100 TB.
- You want to expand by adding new 100 TB Storage Nodes.
- You want to eventually balance erasure-coded data across the old and new nodes.

You have a number of options, based on how full the Storage Nodes are when you perform the expansion.

- **Add three 100 TB Storage Nodes when the existing nodes are 100% full**

  In this example, the existing nodes are 100% full. Because there is no free capacity, you must immediately add three nodes to continue 2+1 erasure coding.

  After the expansion is complete, when objects are erasure-coded, all fragments will be placed on the new nodes.

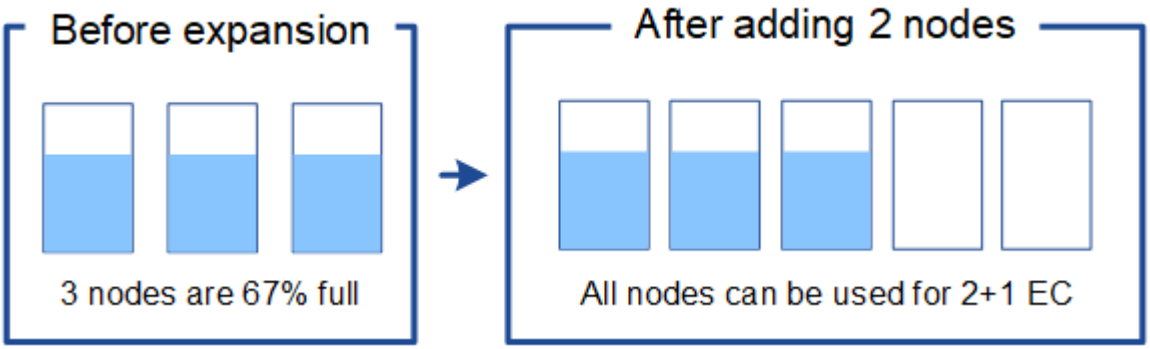



> This expansion adds *k+m* nodes. Adding four nodes is recommended for redundancy. If you add only *k+m* expansion Storage Nodes when existing nodes are 100% full, all new objects are stored on the expansion nodes. If any of the new nodes become unavailable, even temporarily, StorageGRID cannot meet ILM requirements.

- **Add two 100 TB Storage Nodes, when the existing Storage Nodes are 67% full**

  In this example, the existing nodes are 67% full. Because there are 100 TB of free capacity on the existing nodes (33 TB per node), you only need to add two nodes if you perform the expansion now.

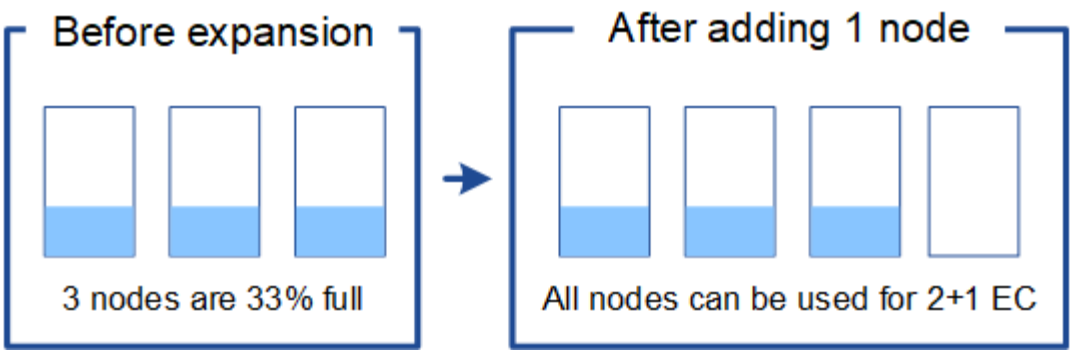
  Adding 200 TB of additional capacity will allow you to continue 2+1 erasure coding and to eventually balance erasure-coded data across all nodes.




- **Add one 100 TB Storage Node when the existing Storage Nodes are 33% full**

  In this example, the existing nodes are 33% full. Because there are 200 TB of free capacity on the existing nodes (67 TB per node), you only need to add one node if you perform the expansion now.

  Adding 100 TB of additional capacity will allow you to continue 2+1 erasure coding and to eventually balance erasure-coded data across all nodes.




**Example 2: Expand three-site grid that uses 6+3 erasure coding**

This example shows how to develop an expansion plan for a multi-site grid that has an erasure-coding scheme with a larger number of fragments. Despite the differences between these examples, the recommended expansion plan is very similar.

Assume the following:

- All data is stored using the 6+3 erasure coding scheme. With the 6+3 erasure coding scheme, every object is stored as 9 fragments, and each fragment is saved to a different Storage Node.
- You have three sites, and each site has four Storage Nodes (12 nodes in total). Each node has a total capacity of 100 TB.
- You want to expand by adding new 100 TB Storage Nodes.
- You want to eventually balance erasure-coded data across the old and new nodes.

You have a number of options, based on how full the Storage Nodes are when you perform the expansion.

- **Add nine 100 TB Storage Nodes (three per site), when existing nodes are 100% full**

  In this example, the 12 existing nodes are 100% full. Because there is no free capacity, you must immediately add nine nodes (900 TB of additional capacity) to continue 6+3 erasure coding.

  After the expansion is complete, when objects are erasure-coded, all fragments will be placed on the new nodes.

  > This expansion adds *k+m* nodes. Adding 12 nodes (four per site) is recommended for redundancy. If you add only *k+m* expansion Storage Nodes when existing nodes are 100% full, all new objects are stored on the expansion nodes. If any of the new nodes become unavailable, even temporarily, StorageGRID cannot meet ILM requirements.

- **Add six 100 TB Storage Nodes (two per site), when existing nodes are 75% full**

  In this example, the 12 existing nodes are 75% full. Because there are 300 TB of free capacity (25 TB per node), you only need to add six nodes if you perform the expansion now. You would add two nodes to each of the three sites.

  Adding 600 TB of storage capacity will allow you to continue 6+3 erasure coding and to eventually balance erasure-coded data across all nodes.

- **Add three 100 TB Storage Nodes (one per site), when existing nodes are 50% full**

In this example, the 12 existing nodes are 50% full. Because there are 600 TB of free capacity (50 TB per node), you only need to add three nodes if you perform the expansion now. You would add one node to each of the three sites.

Adding 300 TB of storage capacity will allow you to continue 6+3 erasure coding and to eventually balance erasure-coded data across all nodes.

#### Considerations for rebalancing erasure-coded data

If you are performing an expansion to add Storage Nodes and your ILM policy includes one or more ILM rules to erasure code data, you might need to perform the EC rebalance procedure after the expansion is complete.

For example, if you cannot add the recommended number of Storage Nodes for the erasure-coding scheme you are using, you might need to run the EC rebalance procedure to allow additional erasure-coded objects to be stored.

After reviewing these considerations, perform the expansion, and then go to Rebalance erasure-coded data after adding Storage Nodes to run the procedure.

### What is EC rebalancing?

EC rebalancing is a StorageGRID procedure that might be required after a Storage Node expansion. The procedure is run as a command-line script from the primary Admin Node. When you run the EC rebalance procedure, StorageGRID redistributes erasure-coded fragments among the existing and the newly expanded Storage Nodes at a site.

The EC rebalance procedure:

- Only moves erasure-coded object data. It does not move replicated object data.
- Redistributes the data within a site. It does not move data between sites.
- Redistributes data among all Storage Nodes at a site. It does not redistribute data within storage volumes.
- Does not consider the replicated data usage on each Storage Node when determining where to move erasure-coded data

When the EC rebalance procedure is complete:

- Erasure-coded data is moved from Storage Nodes with less available space to Storage Nodes with more available space.
- Used (%) values might remain different between Storage Nodes because the EC rebalance procedure does not move replicated object copies.
- The data protection of erasure-coded objects will be unchanged.

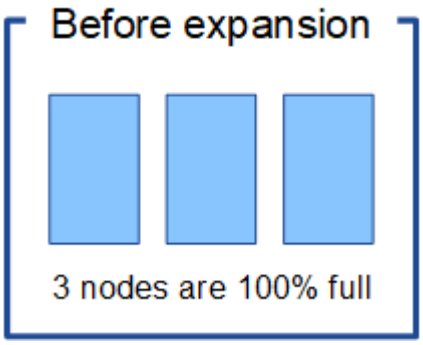
When the EC rebalance procedure is running, the performance of ILM operations and S3 and Swift client operations are likely to be impacted. For this reason, you should only perform this procedure in limited cases.

### When not to perform EC rebalance

As an example of when you do not need to perform an EC rebalance, consider the following:

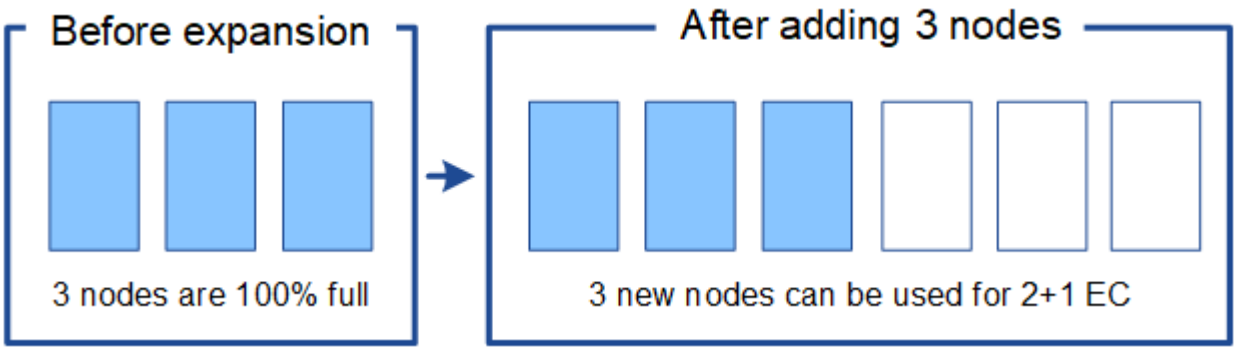
- StorageGRID is running at a single site, which contains three Storage Nodes.

- The ILM policy uses a 2+1 erasure-coding rule for all objects larger than 1.0 MB and a 2-copy replication rule for smaller objects.
- All Storage Nodes have become completely full, and the **Low Object Storage** alert has been triggered at the major severity level. The recommended action is to perform an expansion procedure to add Storage Nodes.



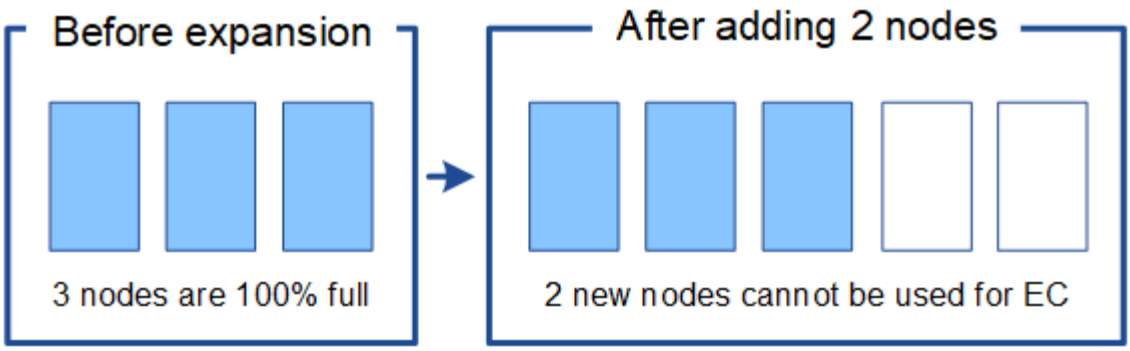

To expand the site in this example, it is recommended that you add three or more new Storage Nodes. StorageGRID requires three Storage Nodes for 2+1 erasure coding so that it can place the two data fragments and the one parity fragment on different nodes.

After you add the three Storage Nodes, the original Storage Nodes remain full, but objects can continue to be ingested into the 2+1 erasure coding scheme on the new nodes. Running the EC rebalance procedure is not recommended for this case: running the procedure will temporarily decrease performance, which might impact client operations.

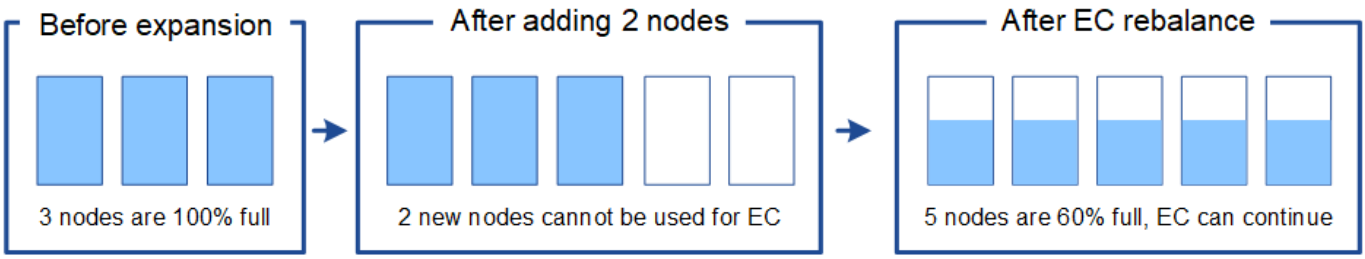



**When to perform EC rebalance**

As an example of when you should perform the EC rebalance procedure, consider the same example, but assume that you can only add two Storage Nodes. Because 2+1 erasure coding requires at least three Storage Nodes, the new nodes cannot be used for erasure-coded data.




To resolve this issue and make use of the new Storage Nodes, you can run the EC rebalance procedure. When this procedure runs, StorageGRID redistributes erasure-coded data and parity fragments among all Storage Nodes at the site. In this example, when the EC rebalance procedure is complete, all five nodes are now only 60% full, and objects can continue to be ingested into the 2+1 erasure coding scheme on all Storage Nodes.




### Requirements for EC rebalancing

In general, you should only run the EC rebalance procedure in limited cases. Specifically, you should perform EC rebalancing only if all of the following statements are true:

- You use erasure coding for your object data.
- The **Low Object Storage** alert has been triggered for one or more Storage Nodes at a site, indicating that the nodes are 80% or more full.
- You are unable to add the recommended number of new Storage Nodes for the erasure-coding scheme in use. See Add storage capacity for erasure-coded objects.
- Your S3 and Swift clients can tolerate lower performance for their write and read operations while the EC rebalance procedure is running.

### How EC rebalance procedure interacts with other maintenance tasks

You cannot perform certain maintenance procedures at the same time you are running the EC rebalance procedure.

| Procedure | Allowed during EC rebalance procedure? |
|---|---|
| Additional EC rebalance procedures | No.<br><br>You can only run one EC rebalance procedure at a time. |

| Procedure | Allowed during EC rebalance procedure? |
| --- | --- |
| Decommission procedure<br><br>EC data repair job | No.<br><br>• You are prevented from starting a decommission procedure or an EC data repair while the EC rebalance procedure is running.<br>• You are prevented from starting the EC rebalance procedure while a Storage Node decommission procedure or an EC data repair is running. |
| Expansion procedure | No.<br><br>If you need to add new Storage Nodes in an expansion, you should wait to run the EC rebalance procedure until after you have added all new nodes. If an EC rebalance procedure is in progress when you add new Storage Nodes, data will not be moved to those nodes. |
| Upgrade procedure | No.<br><br>If you need to upgrade StorageGRID software, you should perform the upgrade procedure before or after running the EC rebalance procedure. As required, you can terminate the EC rebalance procedure to perform a software upgrade. |
| Appliance node clone procedure | No.<br><br>If you need to clone an appliance Storage Node, you should wait to run the EC rebalance procedure until after you have added the new node. If an EC rebalance procedure is in progress when you add new Storage Nodes, data will not be moved to those nodes. |
| Hotfix procedure | Yes.<br><br>You can apply a StorageGRID hotfix while the EC rebalance procedure is running. |
| Other maintenance procedures | No.<br><br>You must terminate the EC rebalance procedure before running other maintenance procedures. |

#### How EC rebalance procedure interacts with ILM

While the EC rebalance procedure is running, avoid making ILM changes that might change the location of existing erasure-coded objects. For example, do not start using an ILM rule that has a different Erasure Coding profile. If you need to make such ILM changes, you should abort the EC rebalance procedure.

#### Add metadata capacity

To ensure that adequate space is available for object metadata, you might need to perform an expansion procedure to add new Storage Nodes at each site.

StorageGRID reserves space for object metadata on volume 0 of each Storage Node. Three copies of all object metadata are maintained at each site, evenly distributed across all Storage Nodes.

You can use the Grid Manager to monitor the metadata capacity of Storage Nodes and to estimate how quickly metadata capacity is being consumed. In addition, the **Low metadata storage** alert is triggered for a Storage Node when the used metadata space reaches certain thresholds.

Note that a grid's object metadata capacity might be consumed faster than its object storage capacity, depending on how you use the grid. For example, if you typically ingest large numbers of small objects or add large quantities of user metadata or tags to objects, you might need to add Storage Nodes to increase metadata capacity even though sufficient object storage capacity remains.

For more information, see the following:

- Manage object metadata storage
- Monitor object metadata capacity for each Storage Node

#### Guidelines for increasing metadata capacity

Before adding Storage Nodes to increase metadata capacity, review the following guidelines and limitations:

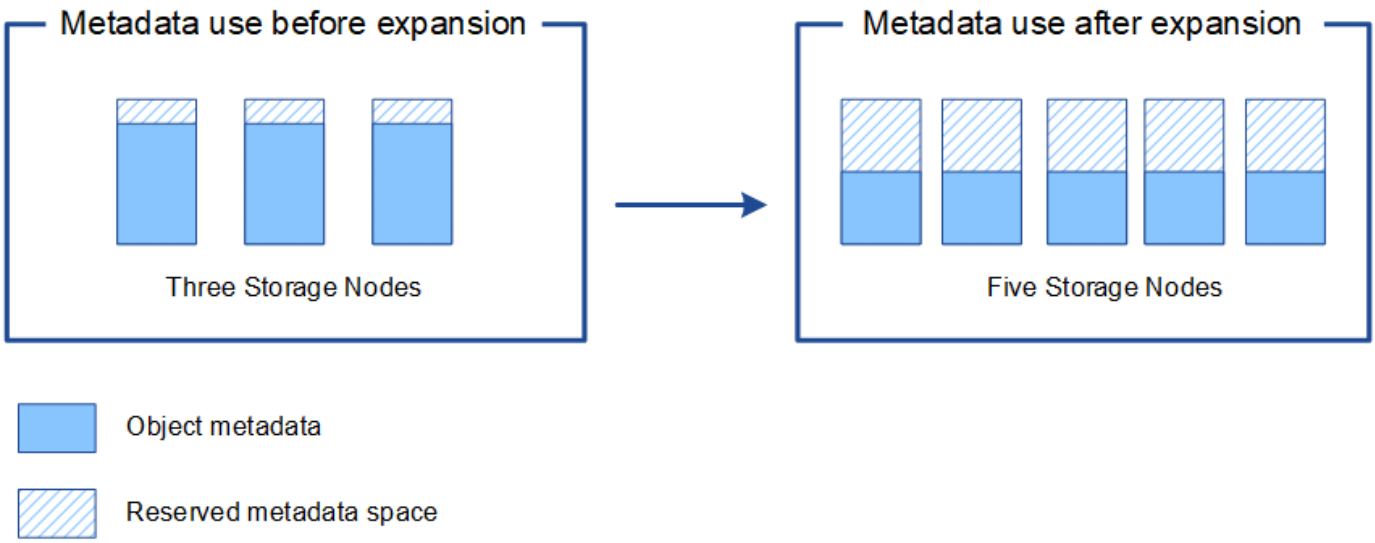
- Assuming sufficient object storage capacity is available, having more space available for object metadata increases the number of objects you can store in your StorageGRID system.
- You can increase a grid's metadata capacity by adding one or more Storage Nodes to each site.
- The actual space reserved for object metadata on any given Storage Node depends on the Metadata Reserved Space storage option (system-wide setting), the amount of RAM allocated to the node, and the size of the node's volume 0. See the instructions for administering StorageGRID.
- You cannot increase metadata capacity by adding storage volumes to existing Storage Nodes, because metadata is stored only on volume 0.
- You cannot increase metadata capacity by adding a new site.
- StorageGRID keeps three copies of all object metadata at every site. For this reason, the metadata capacity for your system is limited by the metadata capacity of your smallest site.
- When adding metadata capacity, you should add the same number of Storage Nodes to each site.

#### How metadata is redistributed when you add Storage Nodes

When you add Storage Nodes in an expansion, StorageGRID redistributes the existing object metadata to the new nodes at each site, which increases the overall metadata capacity of the grid. No user action is required.

The following figure shows how StorageGRID redistributes object metadata when you add Storage Nodes in an expansion. The left side of the figure represents volume 0 of three Storage Nodes before an expansion. Metadata is consuming a relatively large portion of each node's available metadata space, and the **Low metadata storage** alert has been triggered.

The right side of the figure shows how the existing metadata is redistributed after two Storage Nodes are added to the site. The amount of metadata on each node has decreased, the **Low metadata storage** alert is no longer triggered, and the space available for metadata has increased.




**Add grid nodes to add capabilities to your system**

You can add redundancy or additional capabilities to a StorageGRID system by adding new grid nodes to existing sites.

For example, you might choose to add additional Gateway Nodes to support the creation of High Availability groups of Gateway Nodes, or you might add an Admin Node at a remote site to permit monitoring using a local node.

You can add one or more of the following types of nodes to one or more existing sites in a single expansion operation:

- Non-primary Admin Nodes
- Storage Nodes
- Gateway Nodes
- Archive Nodes

When preparing to add grid nodes, be aware of the following limitations:

- The primary Admin Node is deployed during the initial installation. You cannot add a primary Admin Node during an expansion.
- You can add Storage Nodes and other types of nodes in the same expansion.
- When adding Storage Nodes, you must carefully plan the number and location of the new nodes. See Guidelines for adding object capacity.
- If you are adding Archive Nodes, note that each Archive Node only supports tape through Tivoli Storage Manager (TSM) middleware.
- If the **New Node Client Network Default** option is set to **Untrusted** on the Untrusted Client Networks page, client applications that connect to expansion nodes using the Client Network must connect using a load balancer endpoint port (**CONFIGURATION** > **Network** > **Untrusted Client Networks**). See the instructions for administering StorageGRID to change the setting for the new node and to configure load balancer endpoints.

### Add a new site

You can expand your StorageGRID system by adding a new site.

#### Guidelines for adding a site

Before adding a site, review the following requirements and limitations:

- You can only add one site per expansion operation.
- You cannot add grid nodes to an existing site as part of the same expansion.
- All sites must include at least three Storage Nodes.
- Adding a new site does not automatically increase the number of objects you can store. The total object capacity of a grid depends on the amount of available storage, the ILM policy, and the metadata capacity at each site.
- When sizing a new site, you must ensure that it includes enough metadata capacity.

  StorageGRID keeps a copy of all object metadata at every site. When you add a new site, you must ensure that it includes enough metadata capacity for the existing object metadata and enough metadata capacity for growth.

  For more information, see the following:

  - Manage object metadata storage
  - Monitor object metadata capacity for each Storage Node
- You must consider the available network bandwidth between sites, and the level of network latency. Metadata updates are continually replicated between sites even if all objects are stored only at the site where they are ingested.
- Because your StorageGRID system remains operational during the expansion, you must review ILM rules before starting the expansion procedure. You must ensure that object copies are not stored to the new site until the expansion procedure is complete.

  For example, before you begin the expansion, determine if any rules use the default storage pool (All Storage Nodes). If they do, you must create a new storage pool that contains the existing Storage Nodes and update your ILM rules to use the new storage pool. Otherwise, objects will be copied to the new site as soon as the first node at that site becomes active.

  For more information about changing ILM when adding a new site, see the example for changing an ILM policy in the instructions for managing objects with ILM.

## Gather required materials

Before performing an expansion operation, gather the materials and install and configure any new hardware and networks.

| Item | Notes |
| --- | --- |
| StorageGRID installation archive | If you are adding new grid nodes or a new site, you must download and extract the StorageGRID installation archive. You must use the same version that is currently running on the grid.<br><br>For details, see the instructions for downloading and extracting the StorageGRID installation files.<br><br>**Note:** You do not need to download files if you are adding new storage volumes to existing Storage Nodes or installing a new StorageGRID appliance. |
| Service laptop | The service laptop has the following:<br><br>• Network port<br>• SSH client (for example, PuTTY)<br>• Supported web browser |
| `Passwords.txt` file | Contains the passwords required to access grid nodes on the command line. Included in the Recovery Package. |
| Provisioning passphrase | The passphrase is created and documented when the StorageGRID system is first installed. The provisioning passphrase is not in the `Passwords.txt` file. |
| StorageGRID documentation | • Administer StorageGRID<br>• Release notes<br>• Installation instructions for your platform<br>  ◦ Install Red Hat Enterprise Linux or CentOS<br>  ◦ Install Ubuntu or Debian<br>  ◦ Install VMware |
| Current documentation for your platform | For supported versions, see the Interoperability Matrix. |

### Download and extract the StorageGRID installation files

Before you can add new grid nodes or a new site, you must download the appropriate StorageGRID installation archive and extract the files.

#### About this task

You must perform expansion operations using the version of StorageGRID that is currently running on the grid.

#### Steps

1. Go to the NetApp Downloads page for StorageGRID.

NetApp Downloads: StorageGRID

2. Select the version of StorageGRID that is currently running on the grid.
3. Sign in with the username and password for your NetApp account.
4. Read the End User License Agreement, select the check box, and then select **Accept & Continue**.
5. In the **Install StorageGRID** column of the download page, select the `.tgz` or `.zip` file for your platform.

   The version shown in the installation archive file must match the version of the software that is currently installed.

   Use the `.zip` file if you are running Windows on the service laptop.

| Platform | Installation archive |
|---|---|
| Red Hat Enterprise Linux or CentOS | `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`<br><br>`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz` |
| Ubuntu or Debian or Appliances | `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip`<br><br>`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz` |
| VMware | `StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip`<br><br>`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz` |
| OpenStack/other Hypervisor | To expand an existing deployment on OpenStack, you must deploy a virtual machine running one of the supported Linux distributions listed above and follow the appropriate instructions for Linux. |

6. Download and extract the archive file.
7. Follow the appropriate step for your platform to choose the files you need, based on your platform, planned grid topology, and how you will expand your StorageGRID system.

   The paths listed in the step for each platform are relative to the top-level directory installed by the archive file.

8. If you are expanding a Red Hat Enterprise Linux or CentOS system, select the appropriate files.

| Path and file name | Description |
|---|---|
| `./rpms/README` | A text file that describes all of the files contained in the StorageGRID download file. |
| `./rpms/NLF000000.txt` | A free license that does not provide any support entitlement for the product. |
| `./rpms/StorageGRID-Webscale-Images-`*`version`*`-SHA.rpm` | RPM package for installing the StorageGRID node images on your RHEL or CentOS hosts. |

| Path and file name | Description |
| --- | --- |
| `./rpms/StorageGRID-Webscale-Service-`*`version`*`-SHA.rpm` | RPM package for installing the StorageGRID host service on your RHEL or CentOS hosts. |
| **Deployment scripting tool** | **Description** |
| `./rpms/configure-storagegrid.py` | A Python script used to automate the configuration of a StorageGRID system. |
| `./rpms/configure-sga.py` | A Python script used to automate the configuration of StorageGRID appliances. |
| `./rpms/configure-storagegrid.sample.json` | An example configuration file for use with the `configure-storagegrid.py` script. |
| `./rpms/storagegrid-ssoauth.py` | An example Python script that you can use to sign in to the Grid Management API when single sign-on is enabled. |
| `./rpms/configure-storagegrid.blank.json` | A blank configuration file for use with the `configure-storagegrid.py` script. |
| `./rpms/extras/ansible` | Example Ansible role and playbook for configuring RHEL or CentOS hosts for StorageGRID container deployment. You can customize the role or playbook as necessary. |
| `./rpms/extras/api-schemas` | API schemas for StorageGRID.<br><br>**Note**: Before you perform an upgrade, you can use these schemas to confirm that any code you have written to use StorageGRID management APIs will be compatible with the new StorageGRID release if you do not have a non-production StorageGRID environment for upgrade compatibility testing. |

9. If you are expanding an Ubuntu or Debian system, select the appropriate files.

| Path and file name | Description |
| --- | --- |
| `./debs/README` | A text file that describes all of the files contained in the StorageGRID download file. |
| `./debs/NLF000000.txt` | A non-production NetApp License File that you can use for testing and proof of concept deployments. |
| `./debs/storagegrid-webscale-images-version-SHA.deb` | DEB package for installing the StorageGRID node images on Ubuntu or Debian hosts. |

| Path and file name | Description |
| --- | --- |
| `./debs/storagegrid-webscale-images-version-SHA.deb.md5` | MD5 checksum for the file `/debs/storagegrid-webscale-images-version-SHA.deb`. |
| `./debs/storagegrid-webscale-service-version-SHA.deb` | DEB package for installing the StorageGRID host service on Ubuntu or Debian hosts. |
| **Deployment scripting tool** | **Description** |
| `./debs/configure-storagegrid.py` | A Python script used to automate the configuration of a StorageGRID system. |
| `./debs/configure-sga.py` | A Python script used to automate the configuration of StorageGRID appliances. |
| `./debs/storagegrid-ssoauth.py` | An example Python script that you can use to sign in to the Grid Management API when single sign-on is enabled. |
| `./debs/configure-storagegrid.sample.json` | An example configuration file for use with the `configure-storagegrid.py` script. |
| `./debs/configure-storagegrid.blank.json` | A blank configuration file for use with the `configure-storagegrid.py` script. |
| `./debs/extras/ansible` | Example Ansible role and playbook for configuring Ubuntu or Debian hosts for StorageGRID container deployment. You can customize the role or playbook as necessary. |
| `./debs/extras/api-schemas` | API schemas for StorageGRID.<br><br>**Note**: Before you perform an upgrade, you can use these schemas to confirm that any code you have written to use StorageGRID management APIs will be compatible with the new StorageGRID release if you do not have a non-production StorageGRID environment for upgrade compatibility testing. |

10. If you are expanding a VMware system, select the appropriate files.

| Path and file name | Description |
| --- | --- |
| `./vsphere/README` | A text file that describes all of the files contained in the StorageGRID download file. |
| `./vsphere/NLF000000.txt` | A free license that does not provide any support entitlement for the product. |

| Path and file name | Description |
| --- | --- |
| `./vsphere/NetApp-SG-version-SHA.vmdk` | The virtual machine disk file that is used as a template for creating grid node virtual machines. |
| `./vsphere/vsphere-primary-admin.ovf`<br><br>`./vsphere/vsphere-primary-admin.mf` | The Open Virtualization Format template file (`.ovf`) and manifest file (`.mf`) for deploying the primary Admin Node. |
| `./vsphere/vsphere-non-primary-admin.ovf`<br><br>`./vsphere/vsphere-non-primary-admin.mf` | The template file (`.ovf`) and manifest file (`.mf`) for deploying non-primary Admin Nodes. |
| `./vsphere/vsphere-archive.ovf`<br><br>`./vsphere/vsphere-archive.mf` | The template file (`.ovf`) and manifest file (`.mf`) for deploying Archive Nodes. |
| `./vsphere/vsphere-gateway.ovf`<br><br>`./vsphere/vsphere-gateway.mf` | The template file (`.ovf`) and manifest file (`.mf`) for deploying Gateway Nodes. |
| `./vsphere/vsphere-storage.ovf`<br><br>`./vsphere/vsphere-storage.mf` | The template file (`.ovf`) and manifest file (`.mf`) for deploying virtual machine-based Storage Nodes. |
| **Deployment scripting tool** | **Description** |
| `./vsphere/deploy-vsphere-ovftool.sh` | A Bash shell script used to automate the deployment of virtual grid nodes. |
| `./vsphere/deploy-vsphere-ovftool-sample.ini` | An example configuration file for use with the `deploy-vsphere-ovftool.sh` script. |
| `./vsphere/configure-storagegrid.py` | A Python script used to automate the configuration of a StorageGRID system. |
| `./vsphere/configure-sga.py` | A Python script used to automate the configuration of StorageGRID appliances. |
| `./vsphere/storagegrid-ssoauth.py` | An example Python script that you can use to sign in to the Grid Management API when single sign-on is enabled. |
| `./vsphere/configure-storagegrid.sample.json` | An example configuration file for use with the `configure-storagegrid.py` script. |
| `./vsphere/configure-storagegrid.blank.json` | A blank configuration file for use with the `configure-storagegrid.py` script. |

| Path and file name | Description |
| --- | --- |
| `./vsphere/extras/api-schemas` | API schemas for StorageGRID.<br><br>**Note**: Before you perform an upgrade, you can use these schemas to confirm that any code you have written to use StorageGRID management APIs will be compatible with the new StorageGRID release if you do not have a non-production StorageGRID environment for upgrade compatibility testing. |

11. If you are expanding a StorageGRID appliance-based system, select the appropriate files.

| Path and file name | Description |
| --- | --- |
| `./debs/storagegrid-webscale-images-version-SHA.deb` | DEB package for installing the StorageGRID node images on your appliances. |
| `./debs/storagegrid-webscale-images-version-SHA.deb.md5` | Checksum of the DEB installation package used by the StorageGRID Appliance Installer to validate that the package is intact after upload. |

> For appliance installation, these files are only required if you need to avoid network traffic. The appliance can download the required files from the primary Admin Node.

#### Verify hardware and networking

Before beginning the expansion of your StorageGRID system, ensure the following:

- The hardware needed to support the new grid nodes or new site has been installed and configured.
- All new nodes have bidirectional communication paths to all existing and new nodes (a requirement for the Grid Network).
- The primary Admin Node can communicate with all expansion servers that are intended to host the StorageGRID system.
- If any of the new nodes has a Grid Network IP address on a subnet not previously used, you have already added the new subnet to the Grid Network subnet list. Otherwise, you will have to cancel the expansion, add the new subnet, and start the procedure again.
- You are not using network address translation (NAT) on the Grid Network between grid nodes or between StorageGRID sites. When you use private IPv4 addresses for the Grid Network, those addresses must be directly routable from every grid node at every site. Using NAT to bridge the Grid Network across a public network segment is supported only if you use a tunneling application that is transparent to all nodes in the grid, meaning the grid nodes require no knowledge of public IP addresses.

  This NAT restriction is specific to grid nodes and the Grid Network. As required, you can use NAT between external clients and grid nodes, such as to provide a public IP address for a Gateway Node.

## Add storage volumes

### Add storage volumes to Storage Nodes

You can expand the storage capacity of Storage Nodes that have 16 or fewer storage volumes by adding additional storage volumes. You might need to add storage volumes to more than one Storage Node to satisfy ILM requirements for replicated or erasure-coded copies.

#### What you'll need

Before adding storage volumes, review the guidelines for adding object capacity to ensure that you know where to add volumes to meet the requirements of your ILM policy.

> These instructions apply to software-based Storage Nodes only. See Add expansion shelf to deployed SG6060 or SG6060X to learn how to add storage volumes to the SG6060 or SG6060X by installing expansion shelves. Other appliance Storage Nodes cannot be expanded.

#### About this task

The underlying storage of a Storage Node is divided into a number of storage volumes. Storage volumes are block-based storage devices that are formatted by the StorageGRID system and mounted to store objects. Each Storage Node can support up to 16 storage volumes, which are called *object stores* in the Grid Manager.

> Object metadata is always stored in object store 0.

Each object store is mounted on a volume that corresponds to its ID. For example, the object store with an ID of 0000 corresponds to the `/var/local/rangedb/0` mount point.

Before adding new storage volumes, use the Grid Manager to view the current object stores for each Storage Node as well as the corresponding mount points. You can use this information when adding storage volumes.

#### Steps

1. Select **NODES** > ***site*** > ***Storage Node*** > **Storage**.
2. Scroll down to view the amounts of available storage for each volume and object store.

   For appliance Storage Nodes, the Worldwide Name for each disk matches the volume world-wide identifier (WWID) that appears when you view standard volume properties in SANtricity software (the management software connected to the appliance's storage controller).

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

## Disk devices

| Name | World Wide Name | I/O load | Read rate | Write rate |
|---|---|---|---|---|
| sdc(8:16,sdb) | N/A | 0.05% | 0 bytes/s | 4 KB/s |
| sde(8:48,sdd) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |
| sdf(8:64,sde) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |
| sdg(8:80,sdf) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |
| sdd(8:32,sdc) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |
| croot(8:1,sda1) | N/A | 0.04% | 0 bytes/s | 4 KB/s |
| cvloc(8:2,sda2) | N/A | 0.95% | 0 bytes/s | 52 KB/s |

## Volumes

| Mount point | Device | Status | Size | Available | Write cache status |
|---|---|---|---|---|---|
| / | croot | Online | 21.00 GB | 14.73 GB | Unknown |
| /var/local | cvloc | Online | 85.86 GB | 80.94 GB | Unknown |
| /var/local/rangedb/0 | sdc | Online | 107.32 GB | 107.17 GB | Enabled |
| /var/local/rangedb/1 | sdd | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/2 | sde | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/3 | sdf | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/4 | sdg | Online | 107.32 GB | 107.18 GB | Enabled |

## Object stores

| ID | Size | Available | Replicated data | EC data | Object data (%) | Health |
|---|---|---|---|---|---|---|
| 0000 | 107.32 GB | 96.44 GB | 1.55 MB | 0 bytes | 0.00% | No Errors |
| 0001 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0002 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0003 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0004 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |

3. Follow the instructions for your platform to add new storage volumes to the Storage Node.
   - VMware: Add storage volumes to Storage Node
   - Linux: Add direct-attached or SAN volumes to Storage Node

### VMware: Add storage volumes to Storage Node

If a Storage Node includes fewer than 16 storage volumes, you can increase its capacity by using VMware vSphere to add volumes.

#### What you'll need

- You have access to the instructions for installing StorageGRID for VMware deployments.
  - Install VMware
- You have the `Passwords.txt` file.
- You have specific access permissions.

> Do not attempt to add storage volumes to a Storage Node while a software upgrade, recovery procedure, or another expansion procedure is active.

#### About this task

The Storage Node is unavailable for a brief time when you add storage volumes. You should perform this procedure on one Storage Node at a time to avoid impacting client-facing grid services.

#### Steps

1. If necessary, install new storage hardware and create new VMware datastores.
2. Add one or more hard disks to the virtual machine for use as storage (object stores).
   a. Open VMware vSphere Client.
   b. Edit the virtual machine settings to add one or more additional hard disks.

   The hard disks are typically configured as Virtual Machine Disks (VMDKs). VMDKs are more commonly used and are easier to manage, while RDMs may provide better performance for workloads that use larger object sizes (for example, greater than 100 MB). For more information about adding hard disks to virtual machines, see the VMware vSphere documentation.
3. Restart the virtual machine by using the **Restart Guest OS** option in the VMware vSphere Client, or by entering the following command in an ssh session to the virtual machine:`sudo reboot`

   > Do not use **Power Off** or **Reset** to restart the virtual machine.
4. Configure the new storage for use by the Storage Node:
   a. Log in to the grid node:
      i. Enter the following command: `ssh admin@grid_node_IP`
      ii. Enter the password listed in the `Passwords.txt` file.
      iii. Enter the following command to switch to root: `su -`
      iv. Enter the password listed in the `Passwords.txt` file. When you are logged in as root, the prompt changes from `$` to `#`.

b. Configure the new storage volumes:

```
sudo add_rangedbs.rb
```

This script finds any new storage volumes and prompts you to format them.

c. Enter **y** to accept the formatting.

d. If any of the volumes have previously been formatted, decide if you want to reformat them.

- Enter **y** to reformat.
- Enter **n** to skip reformatting.

e. When asked, enter **y** to stop storage services.

The storage services are stopped, and the `setup_rangedbs.sh` script runs automatically. After the volumes are ready for use as rangedbs, the services start again.

5. Check that the services start correctly:

a. View a listing of the status of all services on the server:

```
sudo storagegrid-status
```

The status is updated automatically.

b. Wait until all services are Running or Verified.

c. Exit the status screen:

```
Ctrl+C
```

6. Verify that the Storage Node is online:

a. Sign in to the Grid Manager using a supported web browser.

b. Select **SUPPORT** > **Tools** > **Grid topology**.

c. Select ***site*** > ***Storage Node*** > **LDR** > **Storage**.

d. Select the **Configuration** tab and then the **Main** tab.

e. If the **Storage State - Desired** drop-down list is set to Read-only or Offline, select **Online**.

f. Select **Apply Changes**.

7. To see the new object stores:

a. Select **NODES** > ***site*** > ***Storage Node*** > **Storage**.

b. View the details in the **Object Stores** table.

**Result**

You can use the expanded capacity of the Storage Nodes to save object data.

**Linux: Add direct-attached or SAN volumes to Storage Node**

If a Storage Node includes fewer than 16 storage volumes, you can increase its capacity by adding new block storage devices, making them visible to the Linux hosts, and adding the new block device mappings to the StorageGRID configuration file used for the

Storage Node.

**What you'll need**

- You have access to the instructions for installing StorageGRID for your Linux platform.
  - Install Red Hat Enterprise Linux or CentOS
  - Install Ubuntu or Debian
- You have the `Passwords.txt` file.
- You have specific access permissions.

> Do not attempt to add storage volumes to a Storage Node while a software upgrade, recovery procedure, or another expansion procedure is active.

**About this task**

The Storage Node is unavailable for a brief time when you add storage volumes. You should perform this procedure on one Storage Node at a time to avoid impacting client-facing grid services.

**Steps**

1. Install the new storage hardware.

   For more information, see the documentation provided by your hardware vendor.

2. Create new block storage volumes of the desired sizes.
   - Attach the new disk drives and update the RAID controller configuration as needed, or allocate the new SAN LUNs on the shared storage arrays and allow the Linux host to access them.
   - Use the same persistent naming scheme you used for the storage volumes on the existing Storage Node.
   - If you use the StorageGRID node migration feature, make the new volumes visible to other Linux hosts that are migration targets for this Storage Node. For more information, see the instructions for installing StorageGRID for your Linux platform.
3. Log into the Linux host supporting the Storage Node as root or with an account that has sudo permission.
4. Confirm that the new storage volumes are visible on the Linux host.

   You might have to rescan for devices.

5. Run the following command to temporarily disable the Storage Node:

   ```
   sudo storagegrid node stop <node-name>
   ```

6. Using a text editor such as vim or pico, edit the node configuration file for the Storage Node, which can be found at `/etc/storagegrid/nodes/<node-name>.conf`.
7. Locate the section of the node configuration file that contains the existing object storage block device mappings.

   In the example, `BLOCK_DEVICE_RANGEDB_00` to `BLOCK_DEVICE_RANGEDB_03` are the existing object storage block device mappings.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

8. Add new object storage block device mappings corresponding to the block storage volumes you added for this Storage Node.

   Make sure to start at the next `BLOCK_DEVICE_RANGEDB_nn`. Do not leave a gap.

   - Based on the example above, start at `BLOCK_DEVICE_RANGEDB_04`.
   - In the example below, four new block storage volumes have been added to the node: `BLOCK_DEVICE_RANGEDB_04` to `BLOCK_DEVICE_RANGEDB_07`.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

9. Run the following command to validate your changes to the node configuration file for the Storage Node:

   ```
   sudo storagegrid node validate <node-name>
   ```

   Address any errors or warnings before proceeding to the next step.

If you observe an error similar to the following, it means that the node configuration file is attempting to map the block device used by `<node-name>` for `<PURPOSE>` to the given `<path-name>` in the Linux file system, but there is not a valid block device special file (or softlink to a block device special file) at that location.

```
Checking configuration file for node <node-name>…
ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
<path-name> is not a valid block device
```

Verify that you entered the correct `<path-name>`.

10. Run the following command to restart the node with the new block device mappings in place:

    ```
    sudo storagegrid node start <node-name>
    ```

11. Log in to the Storage Node as admin using the password listed in the `Passwords.txt` file.
12. Check that the services start correctly:
    a. View a listing of the status of all services on the server:
       `sudo storagegrid-status`

       The status is updated automatically.

    b. Wait until all services are Running or Verified.
    c. Exit the status screen:

       `Ctrl+C`

13. Configure the new storage for use by the Storage Node:
    a. Configure the new storage volumes:

       `sudo add_rangedbs.rb`

       This script finds any new storage volumes and prompts you to format them.

    b. Enter **y** to format the storage volumes.
    c. If any of the volumes have previously been formatted, decide if you want to reformat them.
       - Enter **y** to reformat.
       - Enter **n** to skip reformatting.
    d. When asked, enter **y** to stop storage services.

       The storage services are stopped, and the `setup_rangedbs.sh` script runs automatically. After the volumes are ready for use as rangedbs, the services start again.

14. Check that the services start correctly:
    a. View a listing of the status of all services on the server:

       `sudo storagegrid-status`

The status is updated automatically.

b. Wait until all services are Running or Verified.

c. Exit the status screen:

```
Ctrl+C
```

15. Verify that the Storage Node is online:
    a. Sign in to the Grid Manager using a supported web browser.
    b. Select **SUPPORT** > **Tools** > **Grid topology**.
    c. Select ***site*** > ***Storage Node*** > **LDR** > **Storage**.
    d. Select the **Configuration** tab and then the **Main** tab.
    e. If the **Storage State - Desired** drop-down list is set to Read-only or Offline, select **Online**.
    f. Click **Apply Changes**.
16. To see the new object stores:
    a. Select **NODES** > ***site*** > ***Storage Node*** > **Storage**.
    b. View the details in the **Object Stores** table.

#### Result

You can now use the expanded capacity of the Storage Nodes to save object data.

## Add grid nodes or site

### Add grid nodes to existing site or add new site

You can follow this procedure to add grid nodes to existing sites or to add a new site, but you cannot perform both types of expansion at the same time.

#### What you'll need

- You have the Root access or Maintenance permission.
- All existing nodes in the grid are up and running across all sites.
- Any previous expansion, upgrade, decommissioning, or recovery procedures are complete.

> You are prevented from starting an expansion while another expansion, upgrade, recovery, or active decommission procedure is in progress. However, if necessary, you can pause a decommission procedure to start an expansion.

#### Steps

1. Update subnets for Grid Network.
2. Deploy new grid nodes.
3. Perform expansion.

### Update subnets for Grid Network

When you add grid nodes or a new site in an expansion, you might need to update or add

subnets to the Grid Network.

StorageGRID maintains a list of the network subnets used to communicate between grid nodes on the Grid Network (eth0). These entries include the subnets used for the Grid Network by each site in your StorageGRID system as well as any subnets used for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

**What you'll need**

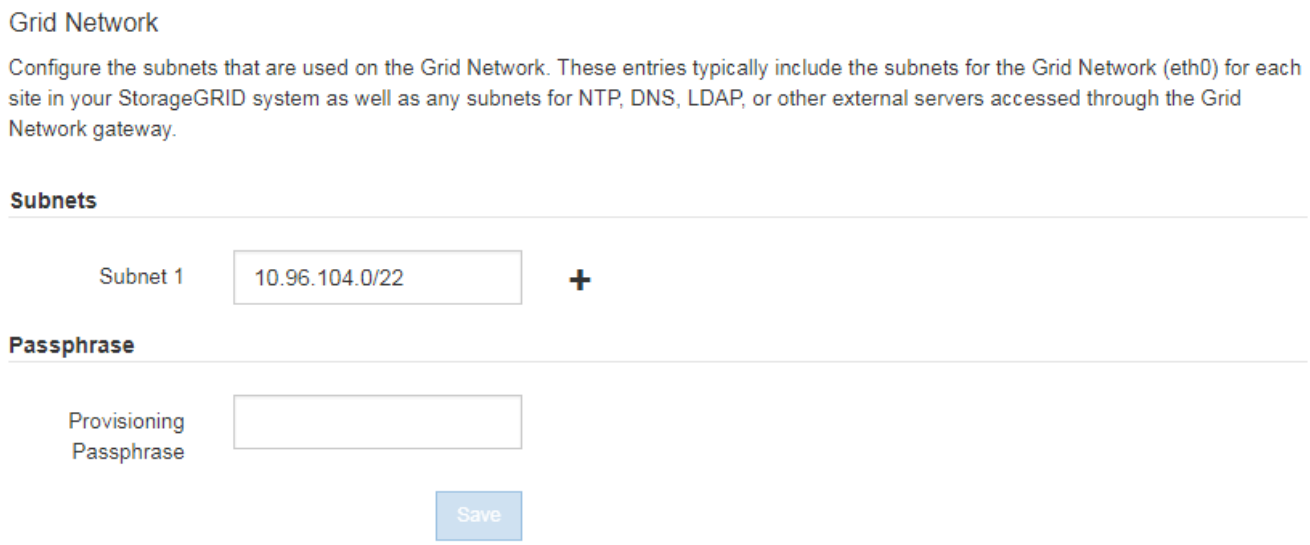
- You are signed in to the Grid Manager using a supported web browser.
- You have the Maintenance or Root access permission.
- You have the provisioning passphrase.
- You have the network addresses, in CIDR notation, of the subnets you want to configure.

**About this task**

If any of the new nodes has a Grid Network IP address on a subnet not previously used, you must add the new subnet to the Grid Network subnet list before starting the expansion. Otherwise, you will have to cancel the expansion, add the new subnet, and start the procedure again.

**Steps**

1. Select **MAINTENANCE** > **Network** > **Grid Network**.




2. In the Subnets list, select the plus sign to add a new subnet in CIDR notation.

   For example, enter 10.96.104.0/22.

3. Enter the provisioning passphrase, and select **Save**.

   The subnets you have specified are configured automatically for your StorageGRID system.

**Deploy new grid nodes**

The steps for deploying new grid nodes in an expansion are the same as the steps used when the grid was first installed. You must deploy all new grid nodes before you can perform the expansion.

When you expand the grid, the nodes you add do not have to match the existing node types. You can add VMware nodes, Linux container-based nodes, or appliance nodes.

#### VMware: Deploy grid nodes

You must deploy a virtual machine in VMware vSphere for each VMware node you want to add in the expansion.

**Steps**

1. Deploy the new node as virtual machine and connect it to one or more StorageGRID networks.

   When you deploy the node, you can optionally remap node ports or increase CPU or memory settings.

2. After you have deployed all new VMware nodes, perform the expansion procedure.

#### Linux: Deploy grid nodes

You can deploy grid nodes on new Linux hosts or on existing Linux hosts. If you need additional Linux hosts to support the CPU, RAM, and storage requirements of the StorageGRID nodes you want to add to your grid, you prepare them in the same way you prepared the hosts when you first installed them. Then, you deploy the expansion nodes in the same way you deployed grid nodes during installation.

**What you'll need**

- You have the instructions for installing StorageGRID for your version of Linux, and you have reviewed the hardware and storage requirements.
  - Install Red Hat Enterprise Linux or CentOS
  - Install Ubuntu or Debian
- If you plan to deploy new grid nodes on existing hosts, you have confirmed the existing hosts have enough CPU, RAM, and storage capacity for the additional nodes.
- You have a plan to minimize failure domains. For example, you should not deploy all Gateway Nodes on a single physical host.

  > In a production deployment, do not run more than one Storage Node on a single physical or virtual host. Using a dedicated host for each Storage Node provides an isolated failure domain.

- If the StorageGRID node uses storage assigned from a NetApp ONTAP system, confirm that the volume does not have a FabricPool tiering policy enabled. Disabling FabricPool tiering for volumes used with StorageGRID nodes simplifies troubleshooting and storage operations.

**Steps**

1. If you are adding new hosts, access the installation instructions for deploying StorageGRID nodes.
2. To deploy the new hosts, follow the instructions for preparing the hosts.
3. To create node configuration files and to validate the StorageGRID configuration, follow the instructions for deploying grid nodes.
4. If you are adding nodes to a new Linux host, start the StorageGRID host service.
5. If you are adding nodes to an existing Linux host, start the new nodes using the storagegrid host service CLI:`sudo storagegrid node start [<node name\>]`

**After you finish**

After deploying all new grid nodes, you can perform the expansion.

#### Appliances: Deploying Storage, Gateway, or non-primary Admin Nodes

To install the StorageGRID software on an appliance node, you use the StorageGRID Appliance Installer, which is included on the appliance. In an expansion, each storage appliance functions as a single Storage Node, and each services appliance functions as a single Gateway Node or non-primary Admin Node. Any appliance can connect to the Grid Network, the Admin Network, and the Client Network.

**What you'll need**

- The appliance has been installed in a rack or cabinet, connected to your networks, and powered on.
- You have used the StorageGRID Appliance Installer to complete all of the "configure hardware" steps in the appliance installation and maintenance instructions.
  - SG100 and SG1000 services appliances
  - Configure hardware (SG5600)
  - Configure hardware (SG5700)
  - Configure hardware (SG6000)

  Configuring appliance hardware includes the required steps for configuring StorageGRID connections (network links and IP addresses) as well the optional steps for enabling node encryption, changing the RAID mode, and remapping network ports.
- All Grid Network subnets listed on the IP Configuration page of the StorageGRID Appliance Installer have been defined in the Grid Network Subnet List on the primary Admin Node.
- The StorageGRID Appliance Installer firmware on the replacement appliance is compatible with the StorageGRID software version currently running on your grid. For example, version 3.6 of the StorageGRID Appliance Installer is compatible with version 11.6 of StorageGRID. (If the versions are not compatible, you must upgrade the StorageGRID Appliance Installer firmware.)
- You have a service laptop with a supported web browser.
- You know one of the IP addresses assigned to the appliance's compute controller. You can use the IP address for any attached StorageGRID network.

**About this task**

The process of installing StorageGRID on an appliance node has the following phases:

- You specify or confirm the IP address of the primary Admin Node and the name of the appliance node.
- You start the installation and wait as volumes are configured and the software is installed.

  Partway through appliance installation tasks, the installation pauses. To resume the installation, you sign into the Grid Manager, approve all grid nodes, and complete the StorageGRID installation process.

> If you need to deploy multiple appliance nodes at one time, you can automate the installation process by using the `configure-sga.py` Appliance Installation Script.

**Steps**

1. Open a browser, and enter one of the IP addresses for the appliance's compute controller.

   `https://Controller_IP:8443`

The StorageGRID Appliance Installer Home page appears.

2. In the **Primary Admin Node** connection section, determine whether you need to specify the IP address for the primary Admin Node.

   If you have previously installed other nodes in this data center, the StorageGRID Appliance Installer can discover this IP address automatically, assuming the primary Admin Node, or at least one other grid node with ADMIN_IP configured, is present on the same subnet.

3. If this IP address is not shown or you need to change it, specify the address:

| Option | Description |
|---|---|
| Manual IP entry | a. Unselect the **Enable Admin Node discovery** check box.<br>b. Enter the IP address manually.<br>c. Click **Save**.<br>d. Wait for the connection state for the new IP address to become ready. |
| Automatic discovery of all connected primary Admin Nodes | a. Select the **Enable Admin Node discovery** check box.<br>b. Wait for the list of discovered IP addresses to be displayed.<br>c. Select the primary Admin Node for the grid where this appliance Storage Node will be deployed.<br>d. Click **Save**.<br>e. Wait for the connection state for the new IP address to become ready. |

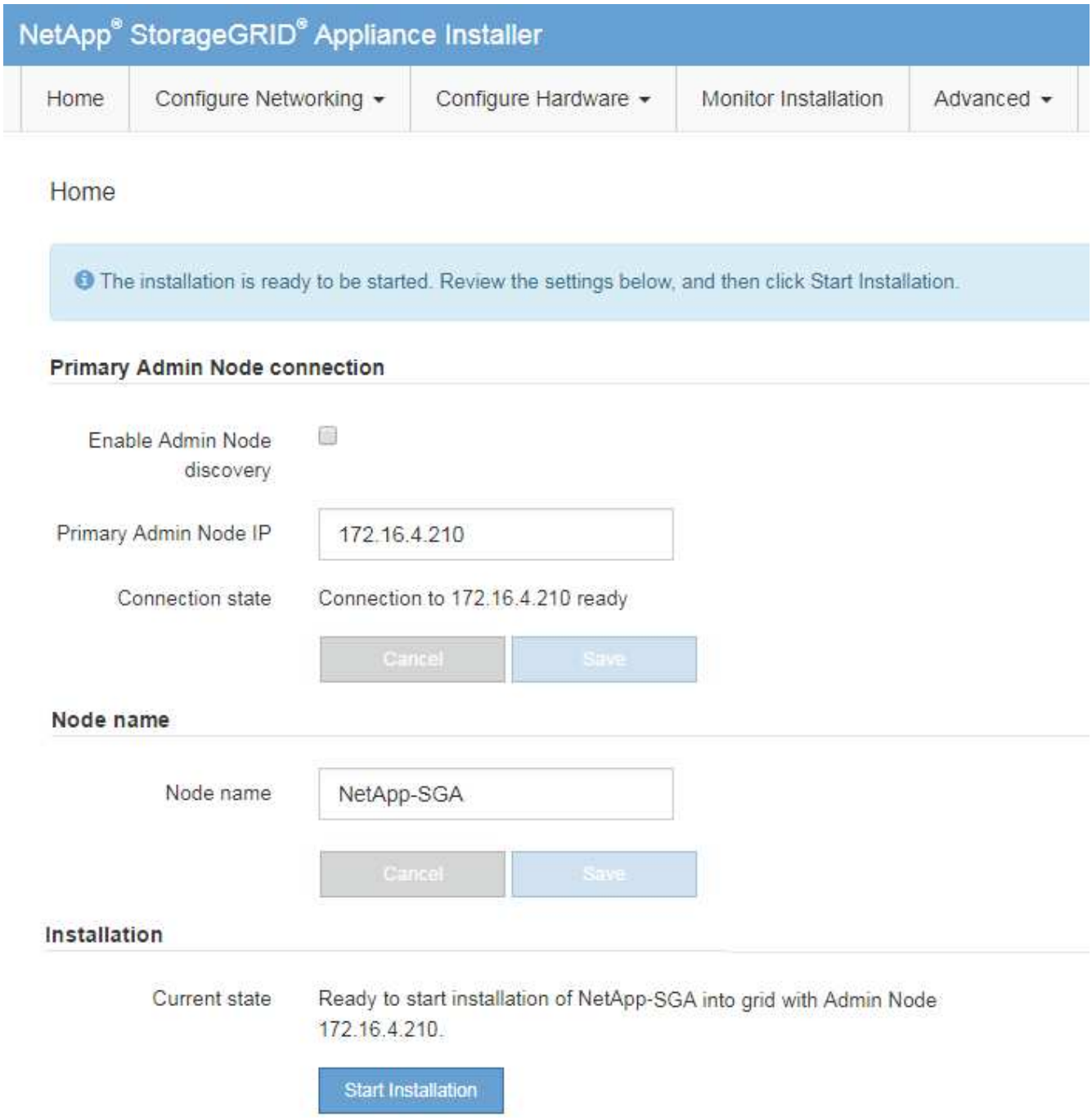
4. In the **Node name** field, enter the name you want to use for this appliance node, and select **Save**.

   The node name is assigned to this appliance node in the StorageGRID system. It is shown on the Nodes page (Overview tab) in the Grid Manager. If required, you can change the name when you approve the node.

5. In the **Installation** section, confirm that the current state is “Ready to start installation of *node name* into grid with primary Admin Node *admin_ip*” and that the **Start Installation** button is enabled.

   If the **Start Installation** button is not enabled, you might need to change the network configuration or port settings. For instructions, see the installation and maintenance instructions for your appliance.

6. From the StorageGRID Appliance Installer home page, select **Start Installation**.



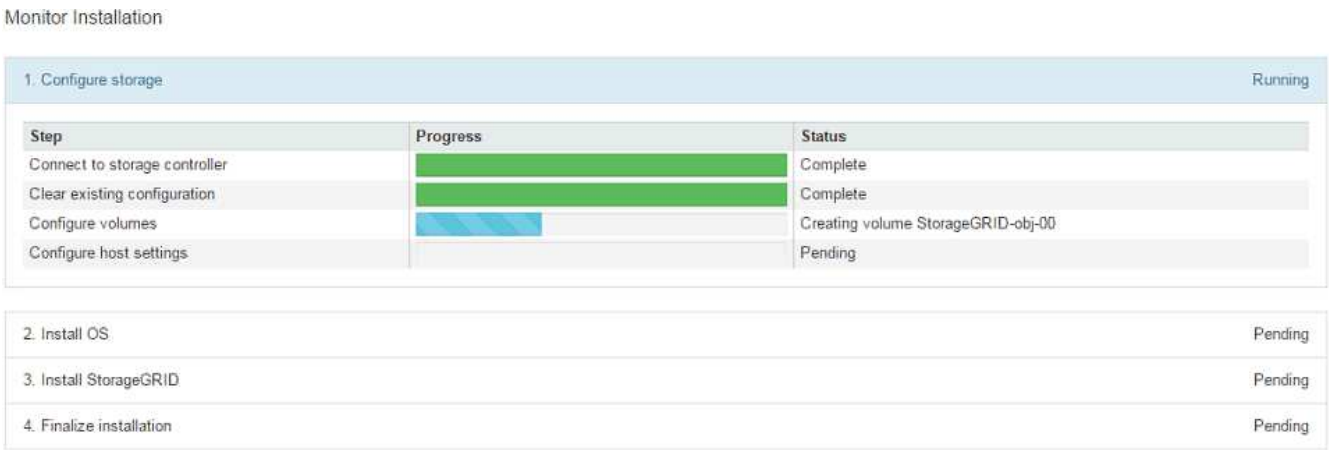

The Current state changes to “Installation is in progress,” and the Monitor Installation page is displayed.

7. If your expansion includes multiple appliance nodes, repeat the previous steps for each appliance.

> If you need to deploy multiple appliance Storage Nodes at one time, you can automate the installation process by using the configure-sga.py appliance installation script.

8. If you need to manually access the Monitor Installation page, select **Monitor Installation** from the menu bar.

   The Monitor Installation page shows the installation progress.




The blue status bar indicates which task is currently in progress. Green status bars indicate tasks that have completed successfully.

> The installer ensures that tasks completed in a previous install are not re-run. If you are re-running an installation, any tasks that do not need to be re-run are shown with a green status bar and a status of “Skipped.”

9. Review the progress of first two installation stages.

   **1. Configure appliance**

   During this stage, one of the following processes occurs:

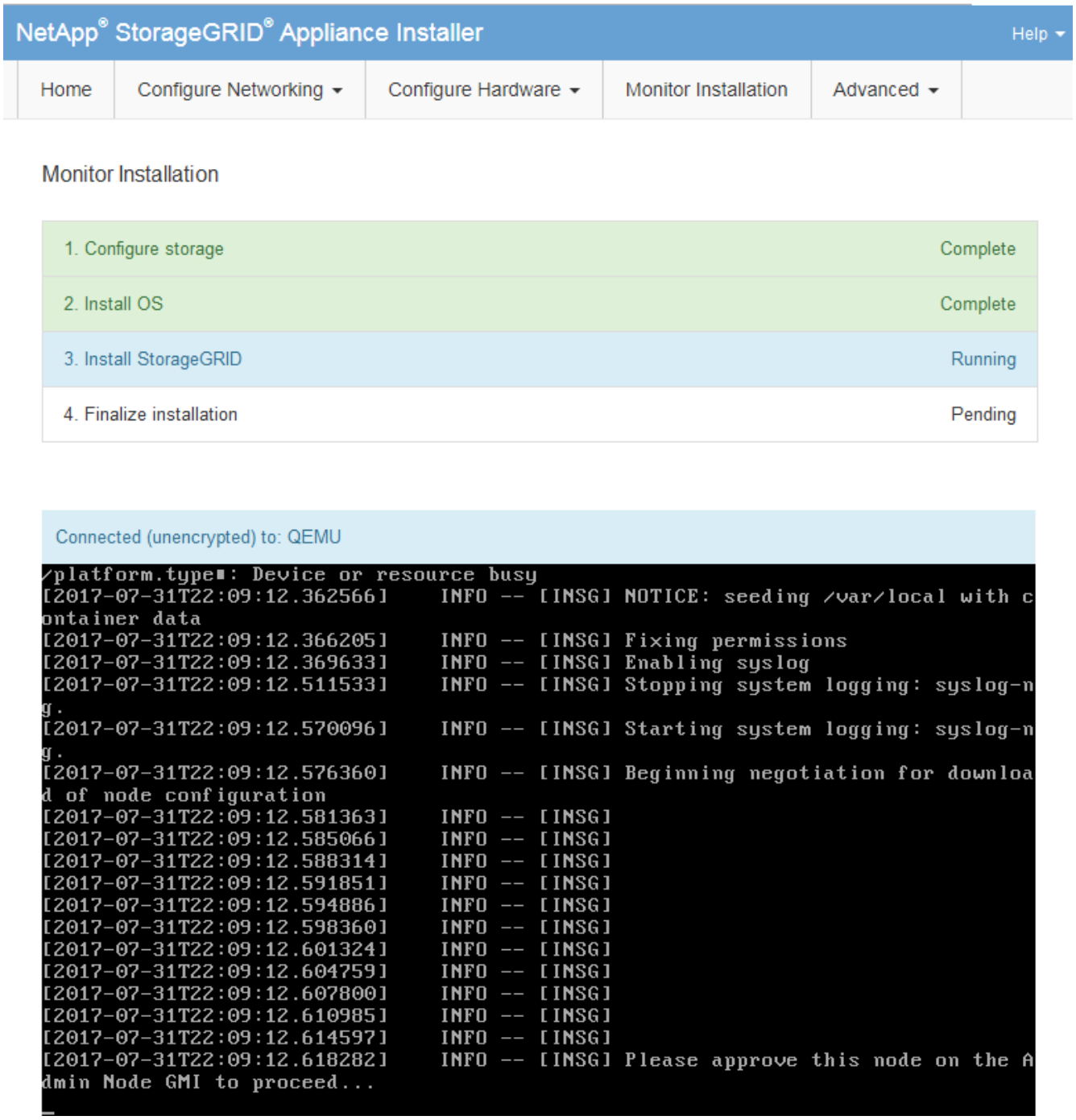
   - For a storage appliance, the installer connects to the storage controller, clears any existing configuration, communicates with SANtricity software to configure volumes, and configures host settings.
   - For a services appliance, the installer clears any existing configuration from the drives in the compute controller, and configures host settings.

   **2. Install OS**

   During this stage, the installer copies the base operating system image for StorageGRID to the appliance.

10. Continue monitoring the installation progress until a message appears in the console window, prompting you to use the Grid Manager to approve the node.

> Wait until all nodes you added in this expansion are ready for approval before going to the Grid Manager to approve the nodes.




### Perform expansion

When you perform the expansion, the new grid nodes are added to your existing StorageGRID deployment.

#### What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have the Maintenance or Root access permission.
- You have the provisioning passphrase.
- You have deployed all of the grid nodes that are being added in this expansion.

- If you are adding Storage Nodes, you have confirmed that all data-repair operations performed as part of a recovery are complete. See Check data repair jobs.
- If you are adding a new site, you must review and update ILM rules before starting the expansion procedure to ensure that object copies are not stored to the new site until after the expansion is complete. For example, if a rule uses the default storage pool (All Storage Nodes), you must create a new storage pool that contains only the existing Storage Nodes and update the ILM rule to use the new storage pool. Otherwise, objects will be copied to the new site as soon as the first node at that site becomes active. See the instructions for managing objects with ILM.

### About this task

Performing the expansion includes these phases:

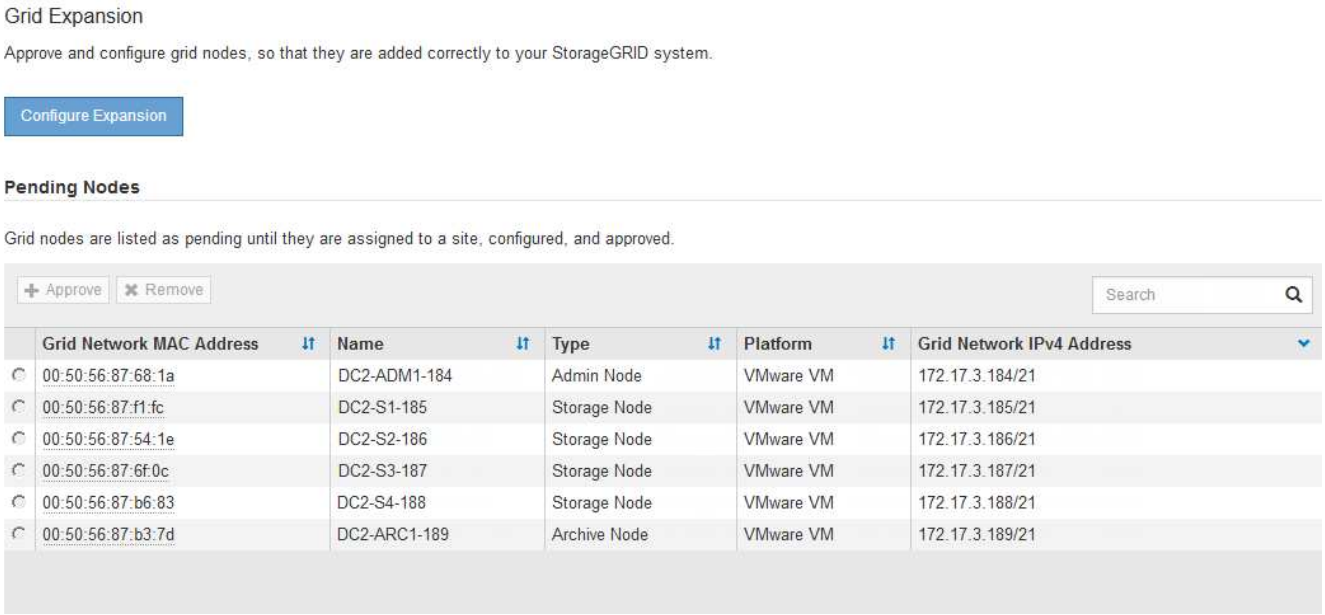
1. You configure the expansion by specifying whether you are adding new grid nodes or a new site and approving the grid nodes you want to add.
2. You start the expansion.
3. While the expansion process is running, you download a new Recovery Package file.
4. You monitor the status of the grid configuration stages, which run automatically. The set of stages depends on what types of grid nodes are being added and on whether a new site is being added.

> Some stages might take a significant amount of time to run on a large grid. For example, streaming Cassandra to a new Storage Node might take only a few minutes if the Cassandra database is empty. However, if the Cassandra database includes a large amount of object metadata, this stage might take several hours or longer. Do not reboot any Storage Nodes during the either the "Expanding the Cassandra cluster" or "Starting Cassandra and streaming data" stages.

### Steps

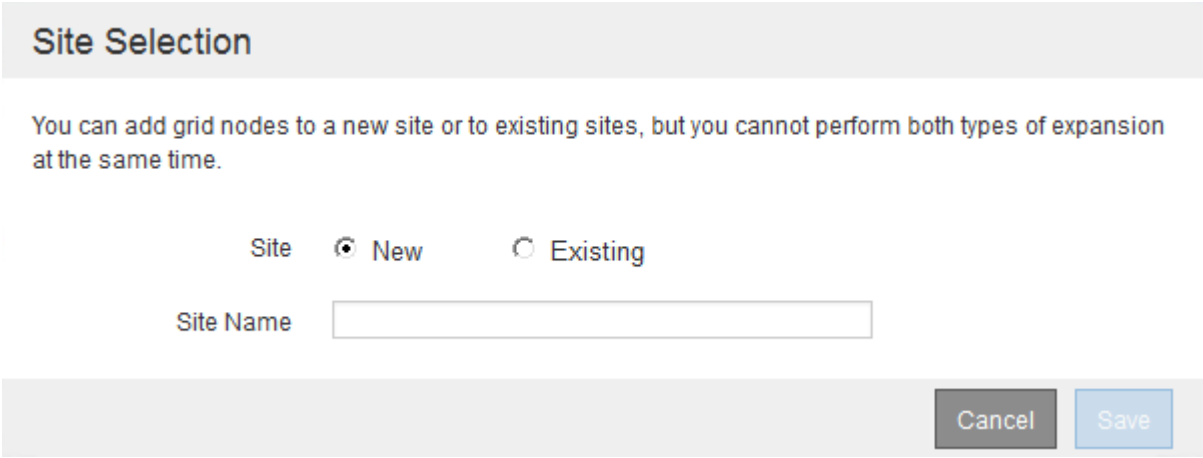
1. Select **MAINTENANCE** > **Tasks** > **Expansion**.

   The Grid Expansion page appears. The Pending Nodes section lists all nodes that are ready to be added.



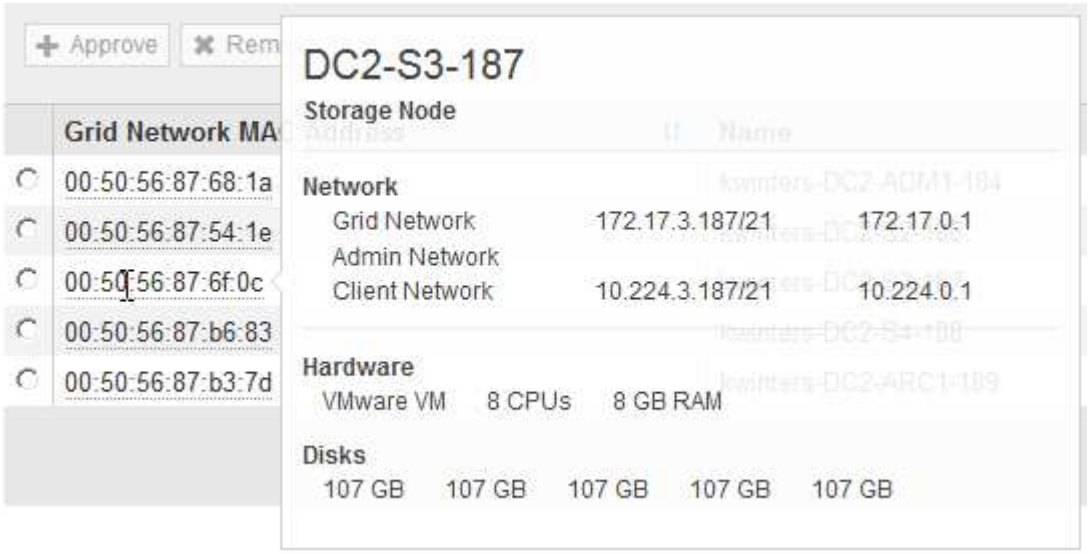

2. Select **Configure Expansion**.

The Site Selection dialog box appears.




3. Select the type of expansion you are starting:
   - If you are adding a new site, select **New**, and enter the name of the new site.
   - If you are adding grid nodes to an existing site, select **Existing**.
4. Select **Save**.
5. Review the **Pending Nodes** list, and confirm that it shows all of the grid nodes you deployed.

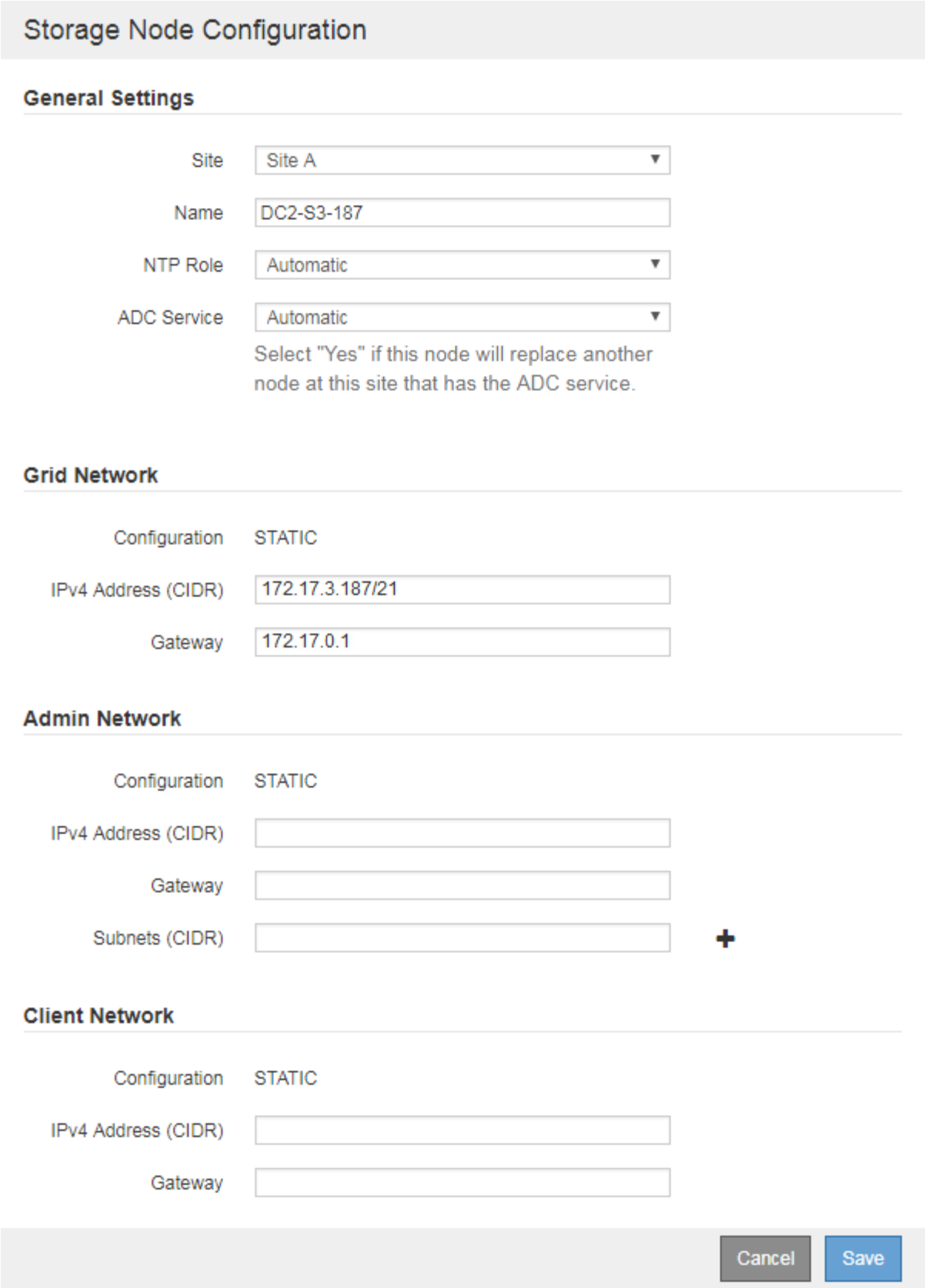
   As required, you can hover your cursor over a node's **Grid Network MAC Address** to see details about that node.




> If a grid node is missing, confirm that it was deployed successfully.

6. From the list of pending nodes, approve the grid nodes for this expansion.
   a. Select the radio button next to the first pending grid node you want to approve.
   b. Select **Approve**.

      The grid node configuration form appears.




c. As required, modify the general settings:

- **Site**: The name of the site the grid node will be associated with. If you are adding multiple nodes, be sure to select the correct site for each node. If you are adding a new site, all nodes are added to the new site.

- **Name**: The hostname that will be assigned to the node, and the name that will be displayed in the Grid Manager.
- **NTP Role**: The Network Time Protocol (NTP) role of the grid node. The options are **Automatic**, **Primary**, and **Client**. Selecting **Automatic** assigns the Primary role to Admin Nodes, Storage Nodes with ADC services, Gateway Nodes, and any grid nodes that have non-static IP addresses. All other grid nodes are assigned the Client role.

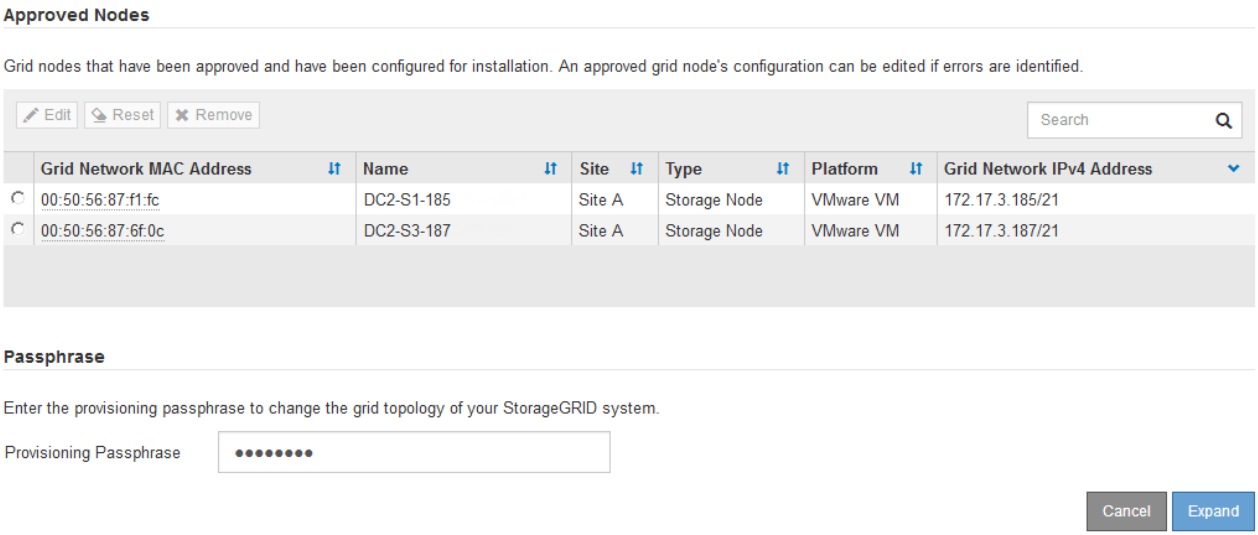
  > Assign the Primary NTP role to at least two nodes at each site. This provides redundant system access to external timing sources.

- **ADC Service** (Storage Nodes only): Whether this Storage Node will run the Administrative Domain Controller (ADC) service. The ADC service keeps track of the location and availability of grid services. At least three Storage Nodes at each site must include the ADC service. You cannot add the ADC service to a node after it is deployed.
  - If you are adding this node to replace a Storage Node, select **Yes** if the node you are replacing includes the ADC service. Because you cannot decommission a Storage Node if too few ADC services would remain, this ensures that a new ADC service is available before the old service is removed.
  - Otherwise, select **Automatic** to let the system determine whether this node requires the ADC service. Learn about the ADC quorum here.

d. As required, modify the settings for the Grid Network, Admin Network, and Client Network.
   - **IPv4 Address (CIDR)**: The CIDR network address for the network interface. For example: 172.16.10.100/24
   - **Gateway**: The default gateway of the grid node. For example: 172.16.10.1
   - **Subnets (CIDR)**: One or more subnetworks for the Admin Network.

e. Select **Save**.

   The approved grid node moves to the Approved Nodes list.




   - To modify the properties of an approved grid node, select its radio button, and select **Edit**.
   - To move an approved grid node back to the Pending Nodes list, select its radio button, and select **Reset**.

- To permanently remove an approved grid node, power the node off. Then, select its radio button, and select **Remove**.

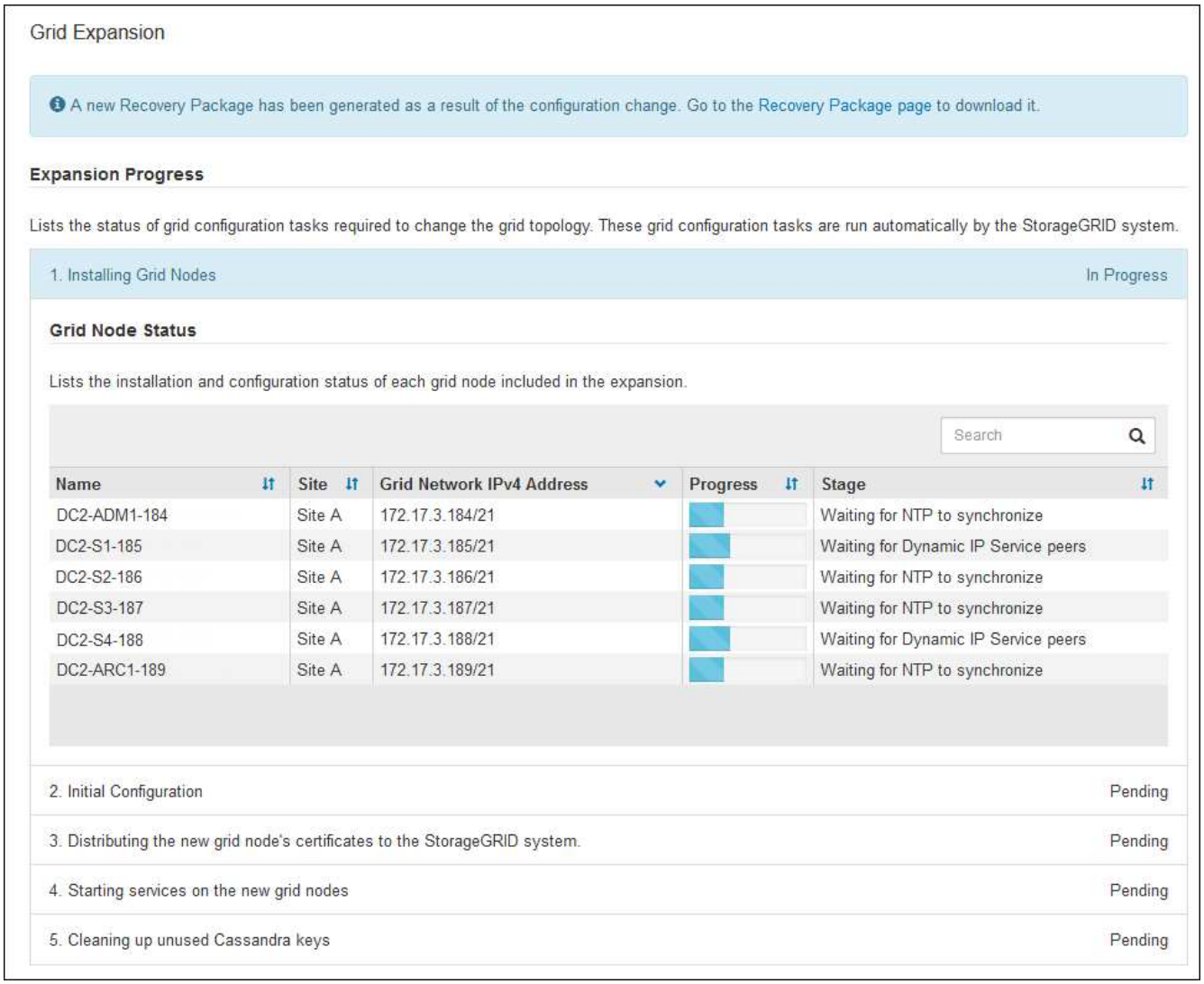
f. Repeat these steps for each pending grid node you want to approve.

> If possible, you should approve all pending grid notes and perform a single expansion. More time will be required if you perform multiple small expansions.

7. When you have approved all grid nodes, enter the **Provisioning Passphrase**, and select **Expand**.

   After a few minutes, this page updates to display the status of the expansion procedure. When tasks that affect individual grid node are in progress, the Grid Node Status section lists the current status for each grid node.

> During this process, for appliances the StorageGRID Appliance Installer shows installation moving from Stage 3 to Stage 4, Finalize Installation. When Stage 4 completes, the controller is rebooted.




> A site expansion includes an additional task to configure Cassandra for the new site.

8. As soon as the **Download Recovery Package** link appears, download the Recovery Package file.

You must download an updated copy of the Recovery Package file as soon as possible after making grid topology changes to the StorageGRID system. The Recovery Package file allows you to restore the system if a failure occurs.

a. Select the download link.

b. Enter the provisioning passphrase, and select **Start Download**.

c. When the download completes, open the `.zip` file and confirm it includes a `gpt-backup` directory and a `_SAID.zip` file. Then, extract the `_SAID.zip` file, go to the `/GID*_REV*` directory, and confirm you can open the `passwords.txt` file.

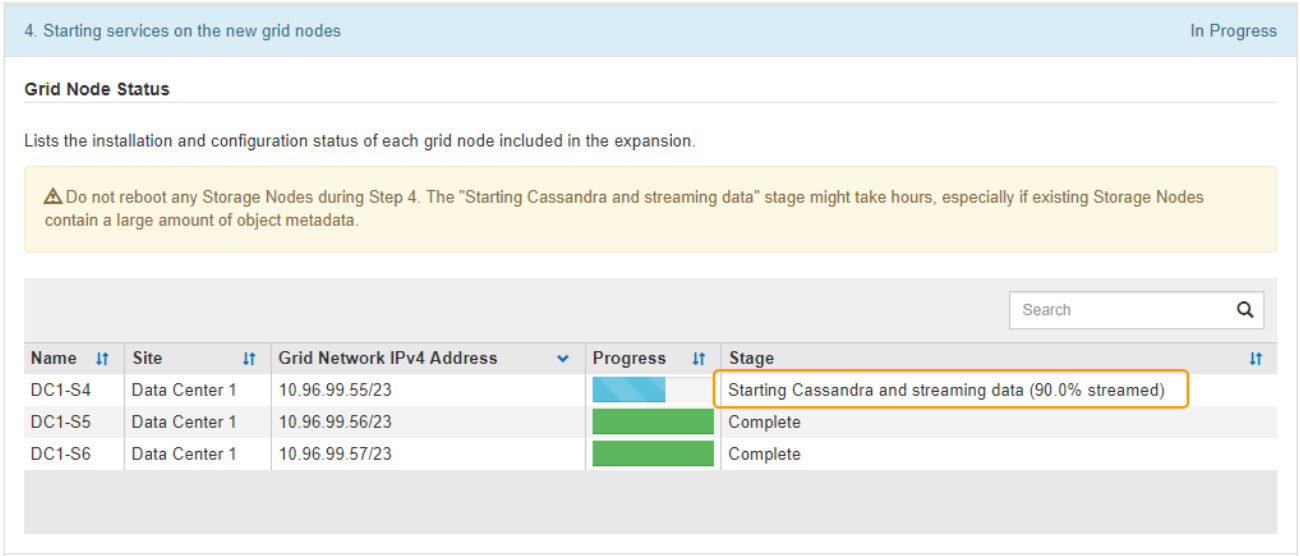
d. Copy the downloaded Recovery Package file (.zip) to two safe, secure, and separate locations.

> The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

9. Follow the instructions for adding a Storage Node to an existing site or adding a new site.

#### Add Storage Node to existing site

If you are adding one or more Storage Nodes to an existing site, monitor the progress of the "Starting Cassandra and streaming data" stage by reviewing the percentage shown in the status message.




This percentage estimates how complete the Cassandra streaming operation is, based on the total amount of Cassandra data available and the amount that has already been written to the new node.

> Do not reboot any Storage Nodes during either the "Expanding the Cassandra cluster" or "Starting Cassandra and streaming data" stages. These stages might take many hours to complete for each new Storage Node, especially if existing Storage Nodes contain a large amount of object metadata.

#### Add new site

If you are adding a new site, use `nodetool status` to monitor the progress of Cassandra streaming and to see how much metadata has been copied to the new site during the "Expanding the Cassandra cluster" stage. The total Data Load on the new site should be within about 20% of the total of a current site.

> Do not reboot any Storage Nodes during either the "Expanding the Cassandra cluster" or "Starting Cassandra and streaming data" stages. These stages might take many hours to complete for each new Storage Node, especially if existing Storage Nodes contain a large amount of object metadata.

10. Continue monitoring the expansion until all tasks are complete and the **Configure Expansion** button reappears.

#### After you finish

Depending on which types of grid nodes you added, you must perform additional integration and configuration steps. See Configuration steps after expansion.

## Configure expanded system

### Configuration steps after expansion

After completing an expansion, you must perform additional integration and configuration steps.

#### About this task

You must complete the configuration tasks listed below for the grid nodes you are adding in your expansion. Some tasks might be optional, depending on the options selected when installing and administering your system, and how you want to configure the grid nodes added during the expansion.

#### Steps

1. If you added a Storage Node, complete the following configuration tasks:
   a. Review the storage pools used in your ILM rules to ensure the new storage will be used. See Manage objects with ILM.
      - If you added a site, create a storage pool for the site and update ILM rules to use the new storage pool.
      - If you added a Storage Node to an existing site, confirm that the new node uses the correct storage grade.

      > By default, a new Storage Node is assigned to the All Storage Nodes storage grade and added to storage pools that use that grade for the site. If you want a new node to use a custom storage grade, you must assign it to the custom grade manually (**ILM** > **Storage grades**).

   b. Verify that the Storage Node is ingesting objects. See Verify that the Storage Node is active.
   c. Rebalance erasure-coded data (only if you were unable to add the recommended number of Storage Nodes). See Rebalance erasure-coded data after adding Storage Nodes.
2. If you added a Gateway Node, complete the following configuration task:
   - If high availability (HA) groups are used for client connections, optionally add the Gateway Node to an HA group. Select **CONFIGURATION** > **Network** > **High availability groups** to review the list of existing HA groups and to add the new node. See Administer StorageGRID.
3. If you added an Admin Node, complete the following configuration tasks:
   a. If single sign-on (SSO) is enabled for your StorageGRID system, create a relying party trust for the new Admin Node. You cannot sign in to the node until you create this relying party trust. See Configure single sign-on.
   b. If you plan to use the Load Balancer service on Admin Nodes, optionally add the new Admin Node to an HA group. Select **CONFIGURATION** > **Network** > **High availability groups** to review the list of existing HA groups and to add the new node. See Administer StorageGRID.
   c. Optionally, copy the Admin Node database from the primary Admin Node to the expansion Admin Node if you want to keep the attribute and audit information consistent on each Admin Node. See Copy the Admin Node database.
   d. Optionally, copy the Prometheus database from the primary Admin Node to the expansion Admin Node if you want to keep the historical metrics consistent on each Admin Node. See Copy Prometheus metrics.
   e. Optionally, copy the existing audit logs from the primary Admin Node to the expansion Admin Node if you want to keep the historical log information consistent on each Admin Node. See Copy audit logs.
   f. Optionally, configure access to the system for auditing purposes through an NFS or a CIFS file share.

See Administer StorageGRID.

> Audit export through CIFS/Samba has been deprecated and will be removed in a future StorageGRID release.

g. Optionally, change the preferred sender for notifications. You can make the expansion Admin Node the preferred sender. Otherwise, an existing Admin Node configured as the preferred sender continues to send notifications, including AutoSupport messages, SNMP notifications, alert emails, and alarm emails (legacy system). See Administer StorageGRID.

4. If you added an Archive Node, complete the following configuration tasks.
   a. Configure the Archive Node's connection to the targeted external archival storage system. When you complete the expansion, Archive Nodes are in an alarm state until you configure connection information through the **ARC** > **Target** component. See Administer StorageGRID.
   b. Update the ILM policy to archive object data through the new Archive Node. See Manage objects with ILM.
   c. Configure custom alarms for the attributes that are used to monitor the speed and efficiency of object data retrieval from Archive Nodes. See Administer StorageGRID.
5. To check if expansion nodes were added with an untrusted Client Network or to change whether a node's Client Network is untrusted or trusted, go to **CONFIGURATION** > **Network** > **Untrusted Client Network**.

   If the Client Network on the expansion node is untrusted, then connections to the node on the Client Network must be made using a load balancer endpoint. See Administer StorageGRID.

6. Configure the Domain Name System (DNS).

   If you have been specifying DNS settings separately for each grid node, you must add custom per-node DNS settings for the new nodes. See Modify DNS configuration for single grid node.

   The best practice is for the grid-wide DNS server list to contain some DNS servers that are accessible locally from each site. If you just added a new site, add new DNS servers for the site to the grid-wide DNS configuration.

   > Provide two to six IPv4 addresses for DNS servers. You should select DNS servers that each site can access locally in the event of network islanding. This is to ensure an islanded site continues to have access to the DNS service. After configuring the grid-wide DNS server list, you can further customize the DNS server list for each node. For details, see Modify DNS configuration for single grid node..

7. If you added a new site, confirm that Network Time Protocol (NTP) servers are accessible from that site. See Configure NTP servers.

   > Make sure that at least two nodes at each site can access at least four external NTP sources. If only one node at a site can reach the NTP sources, timing issues will occur if that node goes down. In addition, designating two nodes per site as primary NTP sources ensures accurate timing if a site is isolated from the rest of the grid.

#### Verify that Storage Node is active

After an expansion operation that adds new Storage Nodes completes, the StorageGRID system should automatically start using the new Storage Nodes. You must use the

StorageGRID system to verify that the new Storage Node is active.

#### Steps

1. Sign in to the Grid Manager using a supported web browser.
2. Select **NODES** > ***Expansion Storage Node*** > **Storage**.
3. Hover your cursor over the **Storage Used - Object Data** graph to view the value for **Used**, which is the amount of the Total usable space that has been used for object data.
4. Verify that the value of **Used** is increasing as you move your cursor to the right on the graph.

### Copy Admin Node database

When adding Admin Nodes through an expansion procedure, you can optionally copy the database from the primary Admin Node to the new Admin Node. Copying the database allows you to retain historical information about attributes, alerts, and alerts.

#### What you'll need

- You have completed the required expansion steps to add an Admin Node.
- You have the `Passwords.txt` file.
- You have the provisioning passphrase.

#### About this task

The StorageGRID software activation process creates an empty database for the NMS service on the expansion Admin Node. When the NMS service starts on the expansion Admin Node, it records information for servers and services that are currently part of the system or added later. This Admin Node database includes the following information:

- Alert history
- Alarm history
- Historical attribute data, which is used in the charts and text reports available from the **SUPPORT** > **Tools** > **Grid topology** page

To ensure that the Admin Node database is consistent between nodes, you can copy the database from the primary Admin Node to the expansion Admin Node.

> Copying the database from the primary Admin Node (the*source Admin Node*) to an expansion Admin Node can take up to several hours to complete. During this period, the Grid Manager is inaccessible.

Use these steps to stop the MI service and the Management API service on both the primary Admin Node and the expansion Admin Node before copying the database.

#### Steps

1. Complete the following steps on the primary Admin Node:
   a. Log in to the Admin Node:
      i. Enter the following command: `ssh admin@grid_node_IP`
      ii. Enter the password listed in the `Passwords.txt` file.
      iii. Enter the following command to switch to root: `su -`

    iv. Enter the password listed in the `Passwords.txt` file.

  b. Run the following command: `recover-access-points`

  c. Enter the provisioning passphrase.

  d. Stop the MI service: `service mi stop`

  e. Stop the Management Application Program Interface (mgmt-api) service: `service mgmt-api stop`

2. Complete the following steps on the expansion Admin Node:

  a. Log in to the expansion Admin Node:

    i. Enter the following command: `ssh admin@`*`grid_node_IP`*

    ii. Enter the password listed in the `Passwords.txt` file.

    iii. Enter the following command to switch to root: `su -`

    iv. Enter the password listed in the `Passwords.txt` file.

  b. Stop the MI service: `service mi stop`

  c. Stop the mgmt-api service: `service mgmt-api stop`

  d. Add the SSH private key to the SSH agent. Enter:`ssh-add`

  e. Enter the SSH Access Password listed in the `Passwords.txt` file.

  f. Copy the database from the source Admin Node to the expansion Admin Node: `/usr/local/mi/bin/mi-clone-db.sh` *`Source_Admin_Node_IP`*

  g. When prompted, confirm that you want to overwrite the MI database on the expansion Admin Node.

     The database and its historical data are copied to the expansion Admin Node. When the copy operation is done, the script starts the expansion Admin Node.

  h. When you no longer require passwordless access to other servers, remove the private key from the SSH agent. Enter:`ssh-add -D`

3. Restart the services on the primary Admin Node: `service servermanager start`

### Copy Prometheus metrics

After adding a new Admin Node, you can optionally copy the historical metrics maintained by Prometheus from the primary Admin Node to the new Admin Node. Copying the metrics ensures that historical metrics are consistent between Admin Nodes.

#### What you'll need

- The new Admin Node is installed and running.
- You have the `Passwords.txt` file.
- You have the provisioning passphrase.

#### About this task

When you add an Admin Node, the software installation process creates a new Prometheus database. You can keep the historical metrics consistent between nodes by copying the Prometheus database from the primary Admin Node (the *source Admin Node*) to the new Admin Node.

> Copying the Prometheus database might take an hour or more. Some Grid Manager features will be unavailable while services are stopped on the source Admin Node.

**Steps**

1. Log in to the source Admin Node:
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.
2. From the source Admin Node, stop the Prometheus service: `service prometheus stop`
3. Complete the following steps on the new Admin Node:
   a. Log in to the new Admin Node:
      i. Enter the following command: `ssh admin@grid_node_IP`
      ii. Enter the password listed in the `Passwords.txt` file.
      iii. Enter the following command to switch to root: `su -`
      iv. Enter the password listed in the `Passwords.txt` file.
   b. Stop the Prometheus service: `service prometheus stop`
   c. Add the SSH private key to the SSH agent. Enter:`ssh-add`
   d. Enter the SSH Access Password listed in the `Passwords.txt` file.
   e. Copy the Prometheus database from the source Admin Node to the new Admin Node: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. When prompted, press **Enter** to confirm that you want to destroy the new Prometheus database on the new Admin Node.

      The original Prometheus database and its historical data are copied to the new Admin Node. When the copy operation is done, the script starts the new Admin Node. The following status appears:

      ```
      Database cloned, starting services
      ```

   g. When you no longer require passwordless access to other servers, remove the private key from the SSH agent. Enter:

      ```
      ssh-add -D
      ```

4. Restart the Prometheus service on the source Admin Node.

   ```
   service prometheus start
   ```

**Copy audit logs**

When you add a new Admin Node through an expansion procedure, its AMS service only logs events and actions that occur after it joins the system. As required, you can copy audit logs from a previously installed Admin Node to the new expansion Admin Node so

that it is in sync with the rest of the StorageGRID system.

**What you'll need**

- You have completed the required expansion steps to add an Admin Node.
- You have the `Passwords.txt` file.

**About this task**

To make historical audit messages available on a new Admin Node, you must copy the audit log files manually from an existing Admin Node to the expansion Admin Node.

> By default, audit information is sent to the audit log on Admin Nodes. You can skip these steps if either of the following applies:
>
> - You configured an external syslog server and audit logs are now being sent to the syslog server instead of to Admin Nodes.
> - You explicitly specified that audit messages should be saved only on the local nodes that generated them.
>
> See Configure audit messages and log destinations for details.

**Steps**

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@_primary_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.
2. Stop the AMS service to prevent it from creating a new file: `service ams stop`
3. Rename the `audit.log` file to ensure that it does not overwrite the file on the expansion Admin Node you are copying it to:

   ```
   cd /var/local/audit/export
   ls -l
   mv audit.log new_name.txt
   ```
4. Copy all audit log files to the expansion Admin Node:

   ```
   scp -p * IP_address:/var/local/audit/export
   ```
5. If prompted for the passphrase for `/root/.ssh/id_rsa`, enter the SSH Access Password for the Primary Admin Node listed in the `Passwords.txt` file.
6. Restore the original `audit.log` file:

   ```
   mv new_name.txt audit.log
   ```
7. Start the AMS service:

```
service ams start
```

8. Log out from the server:

```
exit
```

9. Log in to the expansion Admin Node:
   a. Enter the following command: `ssh admin@expansion_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.

10. Update the user and group settings for the audit log files:

```
cd /var/local/audit/export
chown ams-user:bycast *
```

11. Log out from the server:

```
exit
```

### Rebalance erasure-coded data after adding Storage Nodes

In some cases, you might need to rebalance erasure-coded data after you add new Storage Nodes.

#### What you'll need

- You have completed the expansion steps to add the new Storage Nodes.
- You have reviewed the considerations for rebalancing erasure-coded data.

> Only perform this procedure if the **Low Object Storage** alert has been triggered for one or more Storage Nodes at a site and you were unable to add the recommended number of new Storage Nodes.

- You understand that replicated object data will not be moved by this procedure and that the EC rebalance procedure does not consider the replicated data usage on each Storage Node when determining where to move erasure-coded data.
- You have the `Passwords.txt` file.

#### About this task

When the EC rebalance procedure is running, the performance of ILM operations and S3 and Swift client operations are likely to be impacted. For this reason, you should only perform this procedure in limited cases.

> The EC rebalance procedure temporarily reserves a large amount of storage. Storage alerts might be triggered, but will resolve when the rebalance is complete. If there is not enough storage for the reservation, the EC rebalance procedure will fail. Storage reservations are released when the EC rebalance procedure completes, whether the procedure failed or succeeded.

> S3 and Swift API operations to upload objects (or object parts) might fail during the EC rebalancing procedure if they require more than 24 hours to complete. Long-duration PUT operations will fail if the applicable ILM rule uses Strict or Balanced placement on ingest. The following error will be reported:
>
> `500 Internal Server Error`

**Steps**

1. Review the current object storage details for the site you plan to rebalance.
   a. Select **NODES**.
   b. Select the first Storage Node at the site.
   c. Select the **Storage** tab.
   d. Hover your cursor over the Storage Used - Object Data chart to see the current amount of replicated data and erasure-coded data on the Storage Node.
   e. Repeat these steps to view the other Storage Nodes at the site.
2. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.
3. Enter the following command:

   ```
   rebalance-data start --site "site-name"
   ```

   For `"`*`site-name`*`"`, specify the first site where you added new Storage Node or nodes. Enclose `site-name` in quotes.

   The EC rebalance procedure starts, and a job ID is returned.
4. Copy the job ID.
5. Monitor the status of the EC rebalance procedure.
   - To view the status of a single EC rebalance procedure:

     ```
     rebalance-data status --job-id job-id
     ```

     For *`job-id`*, specify the ID that was returned when you started the procedure.

- To view the status of the current EC rebalance procedure and any previously completed procedures:

  ```
  rebalance-data status
  ```

  > To get help on the rebalance-data command:
  >
  > ```
  > rebalance-data --help
  > ```

- To view the estimated time to completion and the completion percentage for the current job, select **SUPPORT** > **Tools** > **Metrics**. Then, select **EC Overview** in the Grafana section. Look at the **Grid EC Job Estimated Time to Completion** and **Grid EC Job Percentage Completed** dashboards.

6. Perform additional steps, based on the status returned:
   - If the status is `In progress`, the EC rebalance operation is still running. You should periodically monitor the procedure until it completes.
   - If the status is `Failure`, perform the failure steps.
   - If the status is `Success`, perform the success step.
7. If the EC rebalance procedure is generating too much load (for example, ingest operations are affected), pause the procedure.

   ```
   rebalance-data pause --job-id job-id
   ```

8. If you need to terminate the EC rebalance procedure (for example, so you can perform a StorageGRID software upgrade), enter the following:

   ```
   rebalance-data terminate --job-id job-id
   ```

   > When you terminate an EC rebalance procedure, any data fragments that have already been moved remain in the new location. Data is not moved back to the original location.

9. If the status of the EC rebalance procedure is `Failure`, follow these steps:
   a. Confirm that all Storage Nodes at the site are connected to the grid.
   b. Check for and resolve any alerts that might be affecting these Storage Nodes.

      For information about specific alerts, see the monitoring and troubleshooting instructions.

   c. Restart the EC rebalance procedure:
      `rebalance-data start --job-id job-id`
   d. If the status of the EC rebalance procedure is still `Failure`, contact technical support.
10. If the status of the EC rebalance procedure is `Success`, optionally review object storage to see the updated details for the site.

    Erasure-coded data should now be more balanced among the Storage Nodes at the site.

11. If you are using erasure coding at more than one site, run this procedure for all other affected sites.

## Contact technical support

If you encounter errors during the grid expansion process that you are unable to resolve,

or if a grid task fails, contact technical support.

#### About this task

When you contact technical support, you must provide the required log files to assist in troubleshooting the errors you are encountering.

#### Steps

1. Connect to the expansion node that has experienced failures:

   a. Enter the following command:`ssh -p 8022 admin@grid_node_IP`

   > Port 8022 is the SSH port of the base OS, while port 22 is the SSH port of the container engine running StorageGRID.

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

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

2. Depending on the stage the installation reached, retrieve any of the following logs that are available on the grid node:

| Platform | Logs |
|---|---|
| VMware | • `/var/log/daemon.log`<br>• `/var/log/storagegrid/daemon.log`<br>• `/var/log/storagegrid/nodes/<node-name>.log` |
| Linux | • `/var/log/storagegrid/daemon.log`<br>• `/etc/storagegrid/nodes/<node-name>.conf` (for each failed node)<br>• `/var/log/storagegrid/nodes/<node-name>.log` (for each failed node; might not exist) |

# Recover and maintain

## Recover and maintain: Overview

Use these instructions to maintain your StorageGRID system and to recover from failures.

#### About these instructions

These instructions describe how to apply a software hotfix, recover grid nodes, recover a failed site, decommission grid nodes or an entire site, perform network maintenance, perform host-level and middleware maintenance procedures, and perform grid node procedures.

In these instructions, “Linux” refers to a Red Hat® Enterprise Linux®, Ubuntu®, CentOS, or Debian® deployment. Use the NetApp Interoperability Matrix Tool to get a list of supported versions.

### Before you begin

- You have a broad understanding of the StorageGRID system.
- You have reviewed your StorageGRID system’s topology and you understand the grid configuration.
- You understand that you must follow all instructions exactly and heed all warnings.
- You understand that maintenance procedures not described are not supported or require a services engagement.

### Maintenance procedures for appliances

For hardware procedures, see the installation and maintenance instructions for your StorageGRID appliance.

- SG100 and SG1000 services appliances
- SG6000 storage appliances
- SG5700 storage appliances
- SG5600 storage appliances

### Download Recovery Package

The Recovery Package file allows you to restore the StorageGRID system if a failure occurs.

#### What you’ll need

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

Download the current Recovery Package file before making grid topology changes to the StorageGRID system or before upgrading software. Then, download a new copy of the Recovery Package after making grid topology changes or after upgrading software.

#### Steps

1. Select **MAINTENANCE** > **System** > **Recovery package**.
2. Enter the provisioning passphrase, and select **Start Download**.

   The download starts immediately.

3. When the download completes:
   a. Open the `.zip` file.
   b. Confirm it includes a gpt-backup directory and an inner `.zip` file.
   c. Extract the inner `.zip` file.
   d. Confirm you can open the `Passwords.txt` file.

4. Copy the downloaded Recovery Package file (`.zip`) to two safe, secure, and separate locations.

> The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

**Related information**

Administer StorageGRID

## StorageGRID hotfix procedure

You might need to apply a hotfix to your StorageGRID system if issues with the software are detected and resolved between feature releases.

StorageGRID hotfixes contain software changes that are made available outside of a feature or patch release. The same changes are included in a future release. In addition, each hotfix release contains a roll-up of all previous hotfixes within the feature or patch release.

### Considerations for applying a hotfix

When you apply a hotfix, a cumulative series of software updates is applied to the nodes in your StorageGRID system.

You cannot apply a StorageGRID hotfix when another maintenance procedure is running. For example, you cannot apply a hotfix while a decommission, expansion, or recovery procedure is running.

> If a node or site decommission procedure is paused, you can safely apply a hotfix. In addition, you might be able to apply a hotfix during the final stages of a StorageGRID upgrade procedure. See the instructions for upgrading StorageGRID software for details.

After you upload the hotfix in the Grid Manager, the hotfix is applied automatically to the primary Admin Node. Then, you can approve the application of the hotfix to the rest of the nodes in your StorageGRID system.

If a hotfix fails to be applied to one or more nodes, the reason for the failure appears in the Details column of the hotfix progress table. You must resolve whatever issues caused the failures and then retry the entire process. Nodes with a previously successful application of the hotfix will be skipped in subsequent applications. You can safely retry the hotfix process as many times as required until all nodes have been updated. The hotfix must be successfully installed on all grid nodes in order for the application to be complete.

While grid nodes are updated with the new hotfix version, the actual changes in a hotfix might only affect specific services on specific types of nodes. For example, a hotfix might only affect the LDR service on Storage Nodes.

#### How hotfixes are applied for recovery and expansion

After a hotfix has been applied to your grid, the primary Admin Node automatically installs the same hotfix version to any nodes restored by recovery operations or added in an expansion.

However, if you need to recover the primary Admin Node, you must manually install the correct StorageGRID release and then apply the hotfix. The final StorageGRID version of the primary Admin Node must match the version of the other nodes in the grid.

The following example illustrates how to apply a hotfix when recovering the primary Admin Node:

1. Assume the grid is running a StorageGRID 11.*A.B* version with the latest hotfix. The “grid version” is 11.*A.B.y*.
2. The primary Admin Node fails.
3. You redeploy the primary Admin Node using StorageGRID 11.*A.B*, and perform the recovery procedure.

> As required to match the grid version, you can use a minor release when deploying the node; you do not need to deploy the major release first.

4. You then apply hotfix 11.*A.B.y* to the primary Admin Node.

**Related information**

Configure replacement primary Admin Node

### Plan and prepare for a hotfix

You must plan before applying a hotfix to ensure minimal disruption to your StorageGRID system.

**Steps**

- How your system is affected when you apply a hotfix
- Obtaining the required materials for a hotfix
- Downloading the hotfix file
- Checking the system’s condition before applying a hotfix

### How your system is affected when you apply a hotfix

You must understand how your StorageGRID system will be affected when you apply a hotfix.

#### Client applications might experience short-term disruptions

The StorageGRID system can ingest and retrieve data from client applications throughout the hotfix process; however, client connections to individual Gateway Nodes or Storage Nodes might be disrupted temporarily if the hotfix needs to restart services on those nodes. Connectivity will be restored after the hotfix process completes and services resume on the individual nodes.

You might need to schedule downtime to apply a hotfix if loss of connectivity for a short period is not acceptable. You can use selective approval to schedule when certain nodes are updated.

> You can use multiple gateways and high availability (HA) groups to provide automatic failover during the hotfix process. See the instructions for configuring high availability groups.

#### Alerts and SNMP notifications might be triggered

Alerts and SNMP notifications might be triggered when services are restarted and when the StorageGRID system is operating as a mixed-version environment (some grid nodes running an earlier version, while others have been upgraded to a later version). In general, these alerts and notifications will clear when the hotfix completes.

#### Configuration changes are restricted

When applying a hotfix to StorageGRID:

- Do not make any grid configuration changes (for example, specifying Grid Network subnets or approving pending grid nodes) until the hotfix has been applied to all nodes.
- Do not update the ILM configuration until the hotfix has been applied to all nodes.

### Obtain required materials for hotfix

Before applying a hotfix, you must obtain all required materials.

| Item | Notes |
|---|---|
| StorageGRID hotfix file | You must download the StorageGRID hotfix file. |
| • Network port<br>• Supported web browser<br>• SSH client (for example, PuTTY) | |
| Recovery Package (`.zip`) file | Before applying a hotfix, download the most recent Recovery Package file in case any problems occur during the hotfix.Then, after the hotfix has been applied, download a new copy of the Recovery Package file and save it in a safe location. The updated Recovery Package file allows you to restore the system if a failure occurs. |
| `Passwords.txt file` | Optional and used only if you are applying a hotfix manually using the SSH client. The `Passwords.txt` file is included in the SAID package, which is part of the Recovery Package `.zip` file. |
| Provisioning passphrase | The passphrase is created and documented when the StorageGRID system is first installed. The provisioning passphrase is not listed in the `Passwords.txt` file. |
| Related documentation | `readme.txt` file for the hotfix. This file is included on the hotfix download page. Be sure to review the `readme` file carefully before applying the hotfix. |

#### Related information

Download hotfix file

### Download hotfix file

You must download the hotfix file before you can apply the hotfix.

#### Steps

1. Go to the NetApp Downloads page for StorageGRID.

NetApp Downloads: StorageGRID

2. Select the down arrow under **Available Software** to see a list of hotfixes that are available to download.

   Hotfix file versions have the form: 11.4.*x.y*.

3. Review the changes that are included in the update.

   If you have just recovered the primary Admin Node and you need to apply a hotfix, select the same hotfix version that is installed on the other grid nodes.

   a. Select the hotfix version you want to download, and select **Go**.
   b. Sign in using the username and password for your NetApp account.
   c. Read and accept the End User License Agreement.

      The download page for the version you selected appears.

   d. Download the hotfix `readme.txt` file to view a summary of the changes included in the hotfix.

4. Select the download button for the hotfix, and save the file.

   Do not change the name of this file.

   If you are using a macOS device, the hotfix file might be automatically saved as a `.txt` file. If it is, you must rename the file without the `.txt` extension.

5. Select a location for the download, and select **Save**.

**Related information**

Configure replacement primary Admin Node

### Check system's condition before applying hotfix

You must verify the system is ready to accommodate the hotfix.

1. Sign in to the Grid Manager using a supported web browser.
2. If possible, ensure that the system is running normally and that all grid nodes are connected to the grid.

   Connected nodes have green check marks on the Nodes page.

3. Check for and resolve any current alerts, if possible.

   For information about specific alerts, see the instructions for monitoring and troubleshooting StorageGRID.

4. Ensure no other maintenance procedures are in progress, such as an upgrade, recovery, expansion, or decommission procedure.

   You should wait for any active maintenance procedures to complete before applying a hotfix.

   You cannot apply a StorageGRID hotfix when another maintenance procedure is running. For example, you cannot apply a hotfix while a decommission, expansion, or recovery procedure is running.

If a node or site decommission procedure is paused, you can safely apply a hotfix. In addition, you might be able to apply a hotfix during the final stages of a StorageGRID upgrade procedure. See the instructions for upgrading StorageGRID software for details.

**Related information**

Monitor and troubleshoot

Pause and resume decommission process for Storage Nodes

### Apply hotfix

The hotfix is first applied automatically to the primary Admin Node. Then, you must approve the application of the hotfix to other grid nodes until all nodes are running the same software version. You can customize the approval sequence by selecting to approve individual grid nodes, groups of grid nodes, or all grid nodes.

**What you'll need**

- You have reviewed the considerations and completed the steps in Plan and prepare for a hotfix.
- You have the provisioning passphrase.
- You have Root Access or the Maintenance permission.

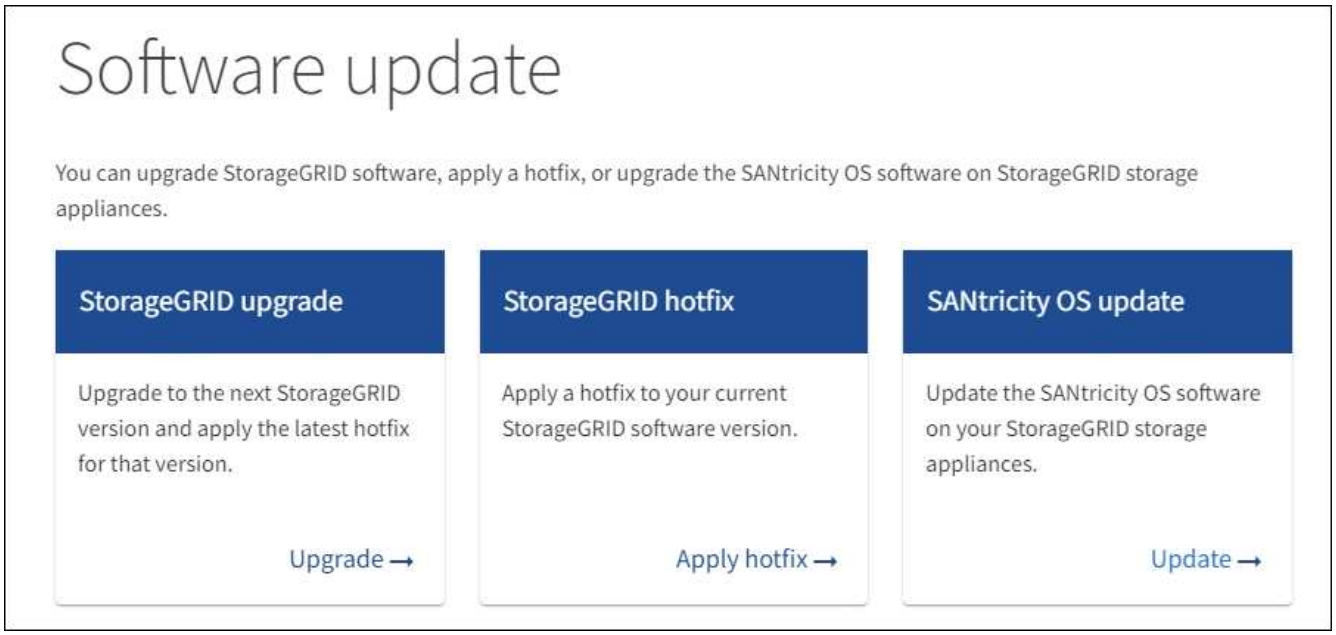
**About this task**

- You can delay applying a hotfix to a node, but the hotfix process is not complete until you apply the hotfix to all nodes.
- You cannot perform a StorageGRID software upgrade or a SANtricity OS upgrade until you have completed the hotfix process.

**Steps**

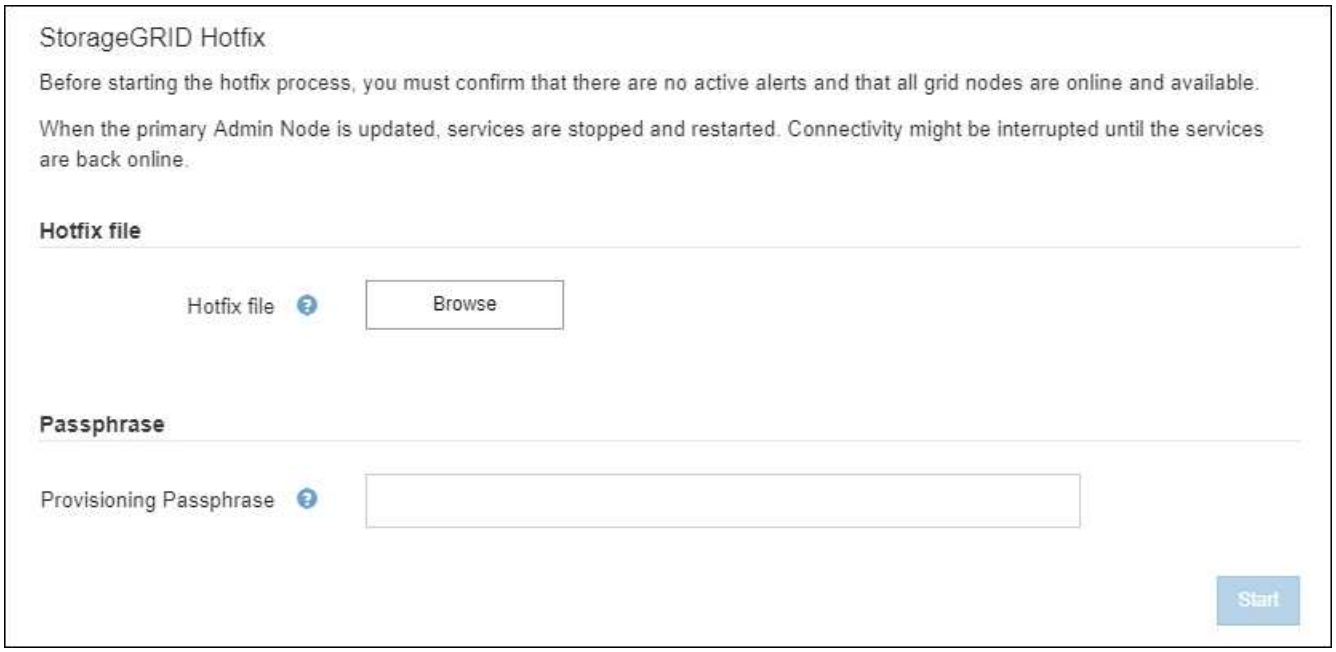
1. Sign in to the Grid Manager using a supported web browser.
2. Select **MAINTENANCE** > **System** > **Software update**.

   The Software Update page appears.




3. Select **Apply hotfix**.

   The StorageGRID Hotfix page appears.




4. Select the hotfix file you downloaded from the NetApp support site.
   a. Select **Browse**.
   b. Locate and select the file.

      `hotfix-install-`*`version`*

   c. Select **Open**.

      The file is uploaded. When the upload is finished, the file name is shown in the Details field.

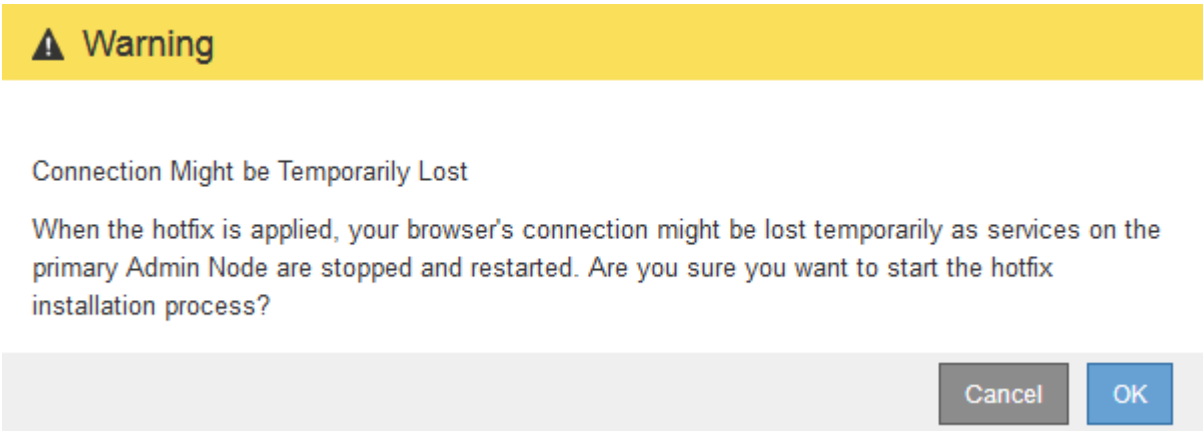
> Do not change the file name since it is part of the verification process.

5. Enter the provisioning passphrase in the text box.

   The **Start** button becomes enabled.

6. Select **Start**.

   A warning appears stating that your browser's connection might be lost temporarily as services on the primary Admin Node are restarted.




7. Select **OK** to start applying the hotfix to the primary Admin Node.

   When the hotfix starts:

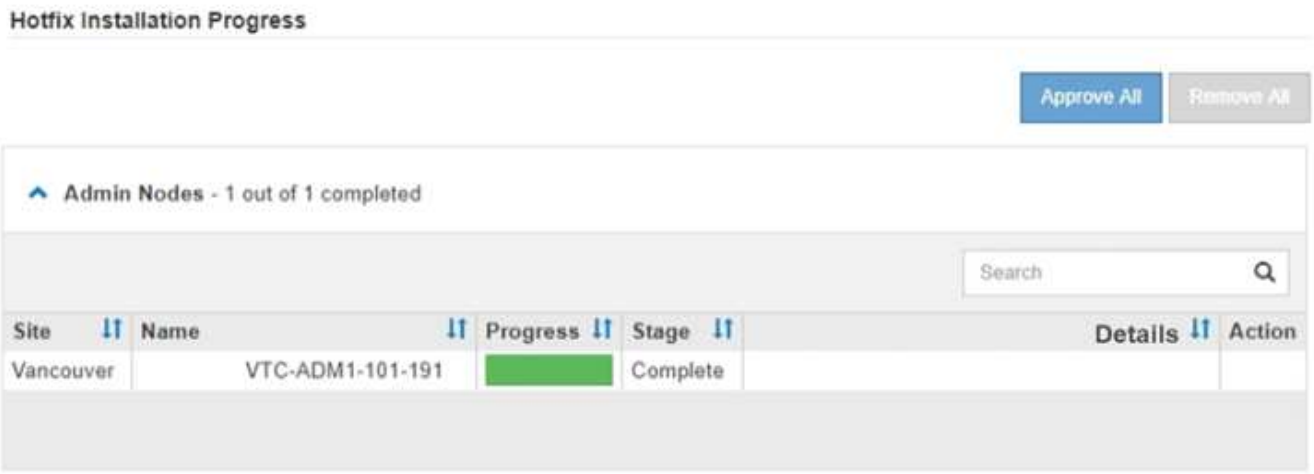
   a. The hotfix validations are run.

      > If any errors are reported, resolve them, re-upload the hotfix file, and select **Start** again.

   b. The hotfix installation progress table appears. This table shows all nodes in your grid and the current stage of the hotfix installation for each node. The nodes in the table are grouped by type:

      - Admin Nodes
      - Gateway Nodes
      - Storage Nodes
      - Archive Nodes

      > The progress bar reaches completion, and then the primary Admin Node is shown first with stage "Complete."




8. Optionally, sort the lists of nodes in each grouping in ascending or descending order by **Site**, **Name**, **Progress**, **Stage**, or **Details**. Or, enter a term in the **Search** box to search for specific nodes.
9. Approve the grid nodes that are ready to be updated. Approved nodes of the same type are upgraded one at a time.

> Do not approve the hotfix for a node unless you are sure the node is ready to be updated.When the hotfix is applied to a grid node, some services on that node might be restarted. These operations might cause service interruptions for clients that are communicating with the node.

- Select one or more **Approve** buttons to add one or more individual nodes to the hotfix queue.
- Select the **Approve All** button within each grouping to add all nodes of the same type to the hotfix queue. If you have entered search criteria in the **Search** box, the **Approve All** button applies to all the nodes selected by the search criteria.

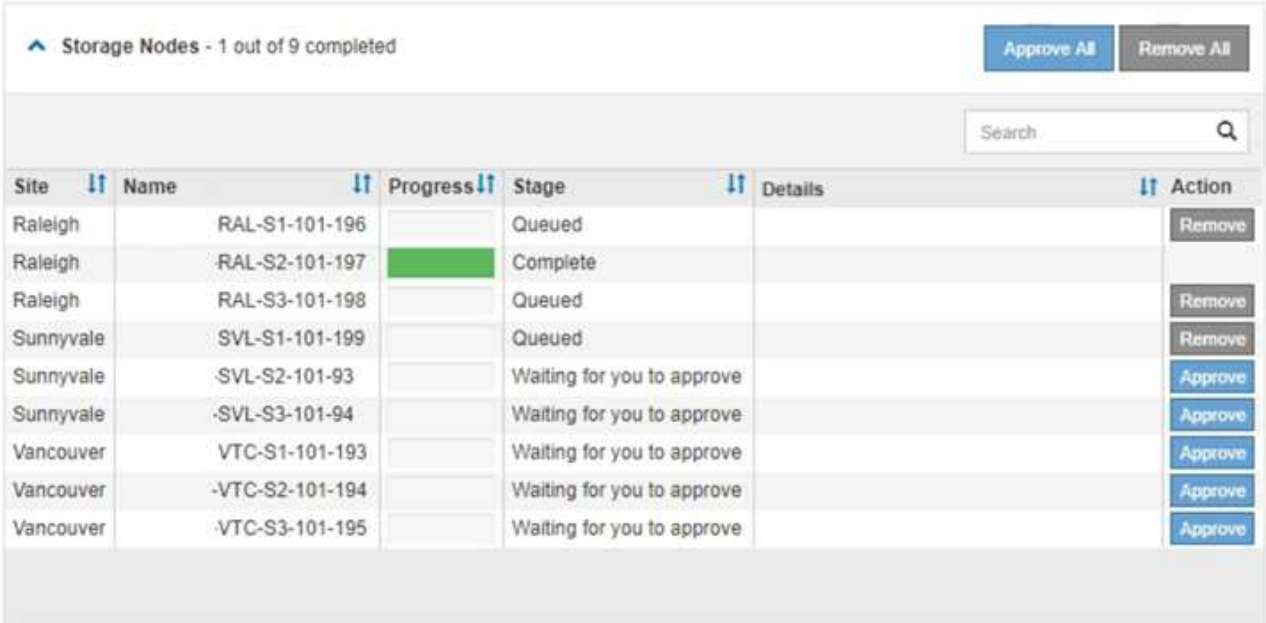
> The **Approve All** button at the top of the page approves all nodes listed on the page, while the **Approve All** button at the top of a table grouping only approves all nodes in that group. If the order in which nodes are upgraded is important, approve nodes or groups of nodes one at a time and wait until the upgrade is complete on each node before approving the next node(s).

- Select the top-level **Approve All** button at the top of the page to add all nodes in the grid to the hotfix queue.

> You must complete the StorageGRID hotfix before you can start a different software update. If you are unable to complete the hotfix, contact technical support.

- Select **Remove** or **Remove All** to remove a node or all nodes from the hotfix queue.

  When the Stage progresses beyond “Queued,” the **Remove** button is hidden and you can no longer remove the node from the hotfix process.




10. Wait while the hotfix is applied to each approved grid node.

    When the hotfix has been successfully installed on all nodes, the Hotfix Installation Progress table closes. A green banner shows the date and time the hotfix was completed.

11. If the hotfix could not be applied to any nodes, review the error for each node, resolve the issue, and repeat these steps.

    The procedure is not complete until the hotfix is successfully applied to all nodes. You can safely retry the hotfix process as many times as required until it is complete.

**Related information**

Administer StorageGRID

Monitor and troubleshoot

## Grid node recovery procedures

If a grid node fails, you can recover it by replacing the failed physical or virtual server, reinstalling StorageGRID software, and restoring recoverable data.

Grid nodes can fail if a hardware, virtualization, operating system, or software fault renders the node inoperable or unreliable. There are many kinds of failure that can trigger the need to recover a grid node.

The steps to recover a grid node vary, depending on the platform where the grid node is hosted and on the type of grid node. Each type of grid node has a specific recovery procedure, which you must follow exactly.

Generally, you try to preserve data from the failed grid node where possible, repair or replace the failed node, use the Grid Manager to configure the replacement node, and restore the node's data.

> If an entire StorageGRID site has failed, contact technical support. Technical support will work with you to develop and execute a site recovery plan that maximizes the amount of data that is recovered, and meets your business objectives.

**Related information**

How site recovery is performed by technical support

### Warnings and considerations for grid node recovery

If a grid node fails, you must recover it as soon as possible. You must review all warnings and considerations for node recovery before you begin.

> StorageGRID is a distributed system composed of multiple nodes working with each other. Do not use disk snapshots to restore grid nodes. Instead, refer to the recovery and maintenance procedures for each type of node.

Some of the reasons for recovering a failed grid node as soon as possible include the following:

- A failed grid node can reduce the redundancy of system and object data, leaving you vulnerable to the risk of permanent data loss if another node fails.
- A failed grid node can impact the efficiency of day-to-day operations.
- A failed grid node can reduce your ability to monitor system operations.
- A failed grid node can cause a 500 internal server error if strict ILM rules are in place.
- If a grid node is not recovered promptly, recovery times might increase. For example, queues might develop that need to be cleared before recovery is complete.

Always follow the recovery procedure for the specific type of grid node you are recovering. Recovery procedures vary for primary or non-primary Admin Nodes, Gateway Nodes, Archive Nodes, appliance nodes, and Storage Nodes.

#### Preconditions for recovering grid nodes

All of the following conditions are assumed when recovering grid nodes:

- The failed physical or virtual hardware has been replaced and configured.
- The StorageGRID Appliance Installer version on the replacement appliance matches the software version of your StorageGRID system, as described in hardware installation and maintenance for verifying and upgrading the StorageGRID Appliance Installer version.
  - SG100 and SG1000 services appliances
  - SG5600 storage appliances
  - SG5700 storage appliances
  - SG6000 storage appliances
- If you are recovering a grid node other than the primary Admin Node, there is connectivity between the grid node being recovered and the primary Admin Node.

#### Order of node recovery if a server hosting more than one grid node fails

If a server that is hosting more than one grid node fails, you can recover the nodes in any order. However, if the failed server is hosting the primary Admin Node, you must recover that node first. Recovering the primary Admin Node first prevents other node recoveries from halting as they wait to contact the primary Admin Node.

#### IP addresses for recovered nodes

Do not attempt to recover a node using an IP address that is currently assigned to any other node. When you deploy the new node, use the failed node's current IP address or an unused IP address.

If you use a new IP address to deploy the new node and then recover the node, the new IP address will continue to be used for the recovered node. If you want to revert to the original IP address, use the Change IP tool after the recovery is complete.

### Gather required materials for grid node recovery

Before performing maintenance procedures, you must ensure you have the necessary materials to recover a failed grid node.

| Item | Notes |
|---|---|
| StorageGRID installation archive | If you need to recover a grid node, you need to download the StorageGRID installation files for your platform.<br><br>**Note:** You do not need to download files if you are recovering failed storage volumes on a Storage Node. |
| Service laptop | The service laptop must have the following:<br><br>• Network port<br>• SSH client (for example, PuTTY)<br>• Supported web browser |
| Recovery Package `.zip` file | Obtain a copy of the most recent Recovery Package `.zip` file: `sgws-recovery-package-`*`id-revision`*`.zip`<br><br>The contents of the `.zip` file are updated each time the system is modified. You are directed to store the most recent version of the Recovery Package in a secure location after making such changes. Use the most recent copy to recover from grid failures.<br><br>If the primary Admin Node is operating normally, you can download the Recovery Package from the Grid Manager. Select **MAINTENANCE** > **System** > **Recovery package**.<br><br>If you cannot access the Grid Manager, you can find encrypted copies of the Recovery Package on some Storage Nodes that contain the ADC service. On each Storage Node, examine this location for the Recovery Package: `/var/local/install/sgws-recovery-package-`*`grid-id-revision`*`.zip.gpg` Use the Recovery Package with the highest revision number. |
| `Passwords.txt` file | Contains the passwords required to access grid nodes on the command line. Included in the Recovery Package. |

| Item | Notes |
| --- | --- |
| Provisioning passphrase | The passphrase is created and documented when the StorageGRID system is first installed. The provisioning passphrase is not in the `Passwords.txt` file. |
| Current documentation for your platform | Go to the platform vendor's website for documentation.<br><br>For the current supported versions of your platform, see the NetApp Interoperability Matrix Tool. |

#### Download and extract StorageGRID installation files

Download the software and extract the files, unless you are recovering failed storage volumes on a Storage Node.

You must use the version of StorageGRID that is currently running on the grid.

**Steps**

1. Determine which version of the software is currently installed. From the top of the Grid Manager, select the help icon and select **About**.
2. Go to the NetApp Downloads page for StorageGRID.
3. Select the version of StorageGRID that is currently running on the grid.

   StorageGRID software versions have this format: `11.x.y`.

4. Sign in with the username and password for your NetApp account.
5. Read the End User License Agreement, select the check box, and then select **Accept & Continue**.
6. In the **Install StorageGRID** column of the download page, select the `.tgz` or `.zip` file for your platform.

   The version shown in the installation archive file must match the version of the software that is currently installed.

   Use the `.zip` file if you are running Windows.

   | Platform | Installation archive |
   | --- | --- |
   | Red Hat Enterprise Linux or CentOS | `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`<br><br>`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz` |
   | Ubuntu or Debian or Appliances | `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip`<br><br>`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz` |
   | VMware | `StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip`<br><br>`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz` |

7. Download and extract the archive file.
8. Follow the appropriate step for your platform to choose the files you need, based on your platform and

which grid nodes you need to recover.

The paths listed in the step for each platform are relative to the top-level directory installed by the archive file.

9. If you are recovering a Red Hat Enterprise Linux or CentOS system, select the appropriate files.

| Path and file name | Description |
|---|---|
| `./rpms/README` | A text file that describes all of the files contained in the StorageGRID download file. |
| `./rpms/NLF000000.txt` | A free license that does not provide any support entitlement for the product. |
| `./rpms/StorageGRID-Webscale-Images-`*`version`*`-SHA.rpm` | RPM package for installing the StorageGRID node images on your RHEL or CentOS hosts. |
| `./rpms/StorageGRID-Webscale-Service-`*`version`*`-SHA.rpm` | RPM package for installing the StorageGRID host service on your RHEL or CentOS hosts. |
| **Deployment scripting tool** | **Description** |
| `./rpms/configure-storagegrid.py` | A Python script used to automate the configuration of a StorageGRID system. |
| `./rpms/configure-sga.py` | A Python script used to automate the configuration of StorageGRID appliances. |
| `./rpms/configure-storagegrid.sample.json` | An example configuration file for use with the `configure-storagegrid.py` script. |
| `./rpms/storagegrid-ssoauth.py` | An example Python script that you can use to sign in to the Grid Management API when single sign-on is enabled. |
| `./rpms/configure-storagegrid.blank.json` | A blank configuration file for use with the `configure-storagegrid.py` script. |
| `./rpms/extras/ansible` | Example Ansible role and playbook for configuring RHEL or CentOS hosts for StorageGRID container deployment. You can customize the role or playbook as necessary. |

| Path and file name | Description |
| --- | --- |
| `./rpms/extras/api-schemas` | API schemas for StorageGRID.<br><br>**Note**: Before you perform an upgrade, you can use these schemas to confirm that any code you have written to use StorageGRID management APIs will be compatible with the new StorageGRID release if you do not have a non-production StorageGRID environment for upgrade compatibility testing. |

10. If you are recovering an Ubuntu or Debian system, select the appropriate files.

| Path and file name | Description |
| --- | --- |
| `./debs/README` | A text file that describes all of the files contained in the StorageGRID download file. |
| `./debs/NLF000000.txt` | A non-production NetApp License File that you can use for testing and proof of concept deployments. |
| `./debs/storagegrid-webscale-images-version-SHA.deb` | DEB package for installing the StorageGRID node images on Ubuntu or Debian hosts. |
| `./debs/storagegrid-webscale-images-version-SHA.deb.md5` | MD5 checksum for the file `/debs/storagegrid-webscale-images-version-SHA.deb`. |
| `./debs/storagegrid-webscale-service-version-SHA.deb` | DEB package for installing the StorageGRID host service on Ubuntu or Debian hosts. |
| **Deployment scripting tool** | **Description** |
| `./debs/configure-storagegrid.py` | A Python script used to automate the configuration of a StorageGRID system. |
| `./debs/configure-sga.py` | A Python script used to automate the configuration of StorageGRID appliances. |
| `./debs/storagegrid-ssoauth.py` | An example Python script that you can use to sign in to the Grid Management API when single sign-on is enabled. |
| `./debs/configure-storagegrid.sample.json` | An example configuration file for use with the `configure-storagegrid.py` script. |
| `./debs/configure-storagegrid.blank.json` | A blank configuration file for use with the `configure-storagegrid.py` script. |

| Path and file name | Description |
| --- | --- |
| `./debs/extras/ansible` | Example Ansible role and playbook for configuring Ubuntu or Debian hosts for StorageGRID container deployment. You can customize the role or playbook as necessary. |
| `./debs/extras/api-schemas` | API schemas for StorageGRID.<br><br>**Note**: Before you perform an upgrade, you can use these schemas to confirm that any code you have written to use StorageGRID management APIs will be compatible with the new StorageGRID release if you do not have a non-production StorageGRID environment for upgrade compatibility testing. |

11. If you are recovering a VMware system, select the appropriate files.

| Path and file name | Description |
| --- | --- |
| `./vsphere/README` | A text file that describes all of the files contained in the StorageGRID download file. |
| `./vsphere/NLF000000.txt` | A free license that does not provide any support entitlement for the product. |
| `./vsphere/NetApp-SG-version-SHA.vmdk` | The virtual machine disk file that is used as a template for creating grid node virtual machines. |
| `./vsphere/vsphere-primary-admin.ovf`<br><br>`./vsphere/vsphere-primary-admin.mf` | The Open Virtualization Format template file (`.ovf`) and manifest file (`.mf`) for deploying the primary Admin Node. |
| `./vsphere/vsphere-non-primary-admin.ovf`<br><br>`./vsphere/vsphere-non-primary-admin.mf` | The template file (`.ovf`) and manifest file (`.mf`) for deploying non-primary Admin Nodes. |
| `./vsphere/vsphere-archive.ovf`<br><br>`./vsphere/vsphere-archive.mf` | The template file (`.ovf`) and manifest file (`.mf`) for deploying Archive Nodes. |
| `./vsphere/vsphere-gateway.ovf`<br><br>`./vsphere/vsphere-gateway.mf` | The template file (`.ovf`) and manifest file (`.mf`) for deploying Gateway Nodes. |
| `./vsphere/vsphere-storage.ovf`<br><br>`./vsphere/vsphere-storage.mf` | The template file (`.ovf`) and manifest file (`.mf`) for deploying virtual machine-based Storage Nodes. |
| **Deployment scripting tool** | **Description** |
| `./vsphere/deploy-vsphere-ovftool.sh` | A Bash shell script used to automate the deployment of virtual grid nodes. |

| Path and file name | Description |
| --- | --- |
| `./vsphere/deploy-vsphere-ovftool-sample.ini` | An example configuration file for use with the `deploy-vsphere-ovftool.sh` script. |
| `./vsphere/configure-storagegrid.py` | A Python script used to automate the configuration of a StorageGRID system. |
| `./vsphere/configure-sga.py` | A Python script used to automate the configuration of StorageGRID appliances. |
| `./vsphere/storagegrid-ssoauth.py` | An example Python script that you can use to sign in to the Grid Management API when single sign-on is enabled. |
| `./vsphere/configure-storagegrid.sample.json` | An example configuration file for use with the `configure-storagegrid.py` script. |
| `./vsphere/configure-storagegrid.blank.json` | A blank configuration file for use with the `configure-storagegrid.py` script. |
| `./vsphere/extras/api-schemas` | API schemas for StorageGRID.<br><br>**Note**: Before you perform an upgrade, you can use these schemas to confirm that any code you have written to use StorageGRID management APIs will be compatible with the new StorageGRID release if you do not have a non-production StorageGRID environment for upgrade compatibility testing. |

12. If you are recovering a StorageGRID appliance-based system, select the appropriate files.

| Path and file name | Description |
| --- | --- |
| `./debs/storagegrid-webscale-images-version-SHA.deb` | DEB package for installing the StorageGRID node images on your appliances. |
| `./debs/storagegrid-webscale-images-version-SHA.deb.md5` | Checksum of the DEB installation package used by the StorageGRID Appliance Installer to validate that the package is intact after upload. |

> For appliance installation, these files are only required if you need to avoid network traffic. The appliance can download the required files from the primary Admin Node.

#### Select node recovery procedure

You must select the correct recovery procedure for the type of node that has failed.

| Grid node | Recovery procedure |
| --- | --- |
| More than one Storage Node | Contact technical support. If more than one Storage Node has failed, technical support must assist with recovery to prevent database inconsistencies that could lead to data loss. A site recovery procedure might be required.<br><br>How site recovery is performed by technical support |
| A single Storage Node | The Storage Node recovery procedure depends on the type and duration of the failure.<br><br>Recover from Storage Node failures |
| Admin Node | The Admin Node procedure depends on whether you need to recover the primary Admin Node or a non-primary Admin Node.<br><br>Recover from Admin Node failures |
| Gateway Node | Recover from Gateway Node failures. |
| Archive Node | Recover from Archive Node failures. |

> If a server that is hosting more than one grid node fails, you can recover the nodes in any order. However, if the failed server is hosting the primary Admin Node, you must recover that node first. Recovering the primary Admin Node first prevents other node recoveries from halting as they wait to contact the primary Admin Node.

#### Recover from Storage Node failures

The procedure for recovering a failed Storage Node depends on the type of failure and the type of Storage Node that has failed.

Use this table to select the recovery procedure for a failed Storage Node.

| Issue | Action | Notes |
| --- | --- | --- |
| • More than one Storage Node has failed.<br>• A second Storage Node has failed less than 15 days after a Storage Node failure or recovery.<br><br>This includes the case where a Storage Node fails while recovery of another Storage Node is still in progress. | You must contact technical support. | If all failed Storage Nodes are at the same site, it might be necessary to perform a site recovery procedure.<br><br>Technical support will assess your situation and develop a recovery plan.<br><br>How site recovery is performed by technical support<br><br>Recovering more than one Storage Node (or more than one Storage Node within 15 days) might affect the integrity of the Cassandra database, which can cause data loss.<br><br>Technical support can determine when it is safe to begin recovery of a second Storage Node.<br><br>**Note**: If more than one Storage Node that contains the ADC service fails at a site, you lose any pending platform service requests for that site. |
| A Storage Node has been offline for more than 15 days. | Recover Storage Node down more than 15 days | This procedure is required to ensure Cassandra database integrity. |
| An appliance Storage Node has failed. | Recover appliance Storage Node | The recovery procedure for appliance Storage Nodes is the same for all failures. |
| One or more storage volumes have failed, but the system drive is intact | Recover from storage volume failure where system drive is intact | This procedure is used for software-based Storage Nodes. |
| The system drive has failed. | Recover from system drive failure | The node replacement procedure depends on the deployment platform and on whether any storage volumes have also failed. |

Some StorageGRID recovery procedures use Reaper to handle Cassandra repairs. Repairs occur automatically as soon as the related or required services have started. You might notice script output that mentions “reaper” or “Cassandra repair.” If you see an error message indicating the repair has failed, run the command indicated in the error message.

#### Recover Storage Node down more than 15 days

## If a single Storage Node has been offline and not connected to other Storage Nodes for more than 15 days, you must rebuild Cassandra on the node.

### What you'll need

- You have checked that a Storage Node decommissioning is not in progress, or you have paused the node decommission procedure. (In the Grid Manager, select **MAINTENANCE** > **Tasks** > **Decommission**.)
- You have checked that an expansion is not in progress. (In the Grid Manager, select **MAINTENANCE** > **Tasks** > **Expansion**.)

### About this task

Storage Nodes have a Cassandra database that includes object metadata. If a Storage Node has not been able to communicate with other Storage Nodes for more than 15 days, StorageGRID assumes that node's Cassandra database is stale. The Storage Node cannot rejoin the grid until Cassandra has been rebuilt using information from other Storage Nodes.

Use this procedure to rebuild Cassandra only if a single Storage Node is down. Contact technical support if additional Storage Nodes are offline or if Cassandra has been rebuilt on another Storage Node within the last 15 days; for example, Cassandra might have been rebuilt as part of the procedures to recover failed storage volumes or to recover a failed Storage Node.

> If more than one Storage Node has failed (or is offline), contact technical support. Do not perform the following recovery procedure. Data loss could occur.

> If this is the second Storage Node failure in less than 15 days after a Storage Node failure or recovery, contact technical support. Do not perform the following recovery procedure. Data loss could occur.

> If more than one Storage Node at a site has failed, a site recovery procedure might be required. Contact technical support.

How site recovery is performed by technical support

### Steps

1. If necessary, power on the Storage Node that needs to be recovered.
2. Log in to the grid node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.+

> If you are unable to log in to the grid node, the system disk might not be intact. Go to the procedure for recovering from system drive failure.

3. Perform the following checks on the Storage Node:
   a. Issue this command: `nodetool status`

      The output should be `Connection refused`

   b. In the Grid Manager, select **SUPPORT** > **Tools** > **Grid topology**.
   c. Select ***Site*** > **Storage Node** > **SSM** > **Services**. Verify that the Cassandra service displays `Not Running`.
   d. Select **Storage Node** > **SSM** > **Resources**. Verify that there is no error status in the Volumes section.
   e. Issue this command: `grep -i Cassandra /var/local/log/servermanager.log`

      You should see the following message in the output:

      ```
      Cassandra not started because it has been offline for more than 15
      day grace period - rebuild Cassandra
      ```

4. Issue this command, and monitor the script output: `check-cassandra-rebuild`
   - If storage services are running, you will be prompted to stop them. Enter: **y**
   - Review the warnings in the script. If none of them apply, confirm that you want to rebuild Cassandra. Enter: **y**

   > Some StorageGRID recovery procedures use Reaper to handle Cassandra repairs. Repairs occur automatically as soon as the related or required services have started. You might notice script output that mentions “reaper” or “Cassandra repair.” If you see an error message indicating the repair has failed, run the command indicated in the error message.

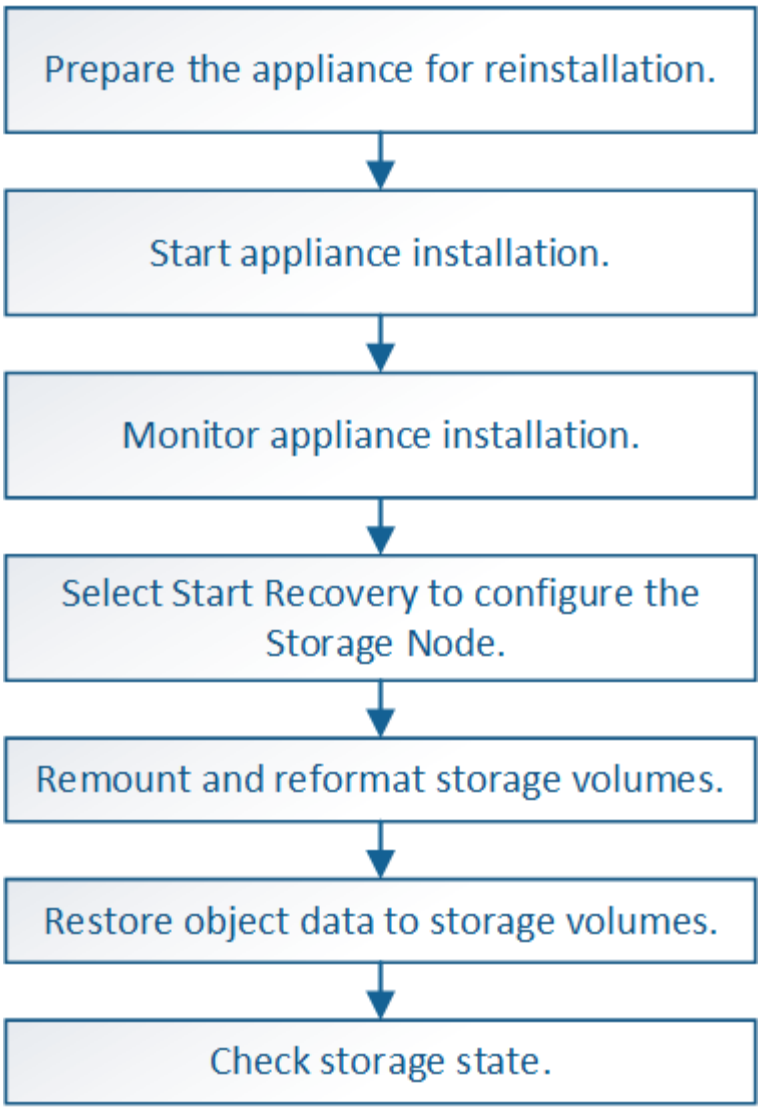
5. After the rebuild completes, perform the following checks:
   a. In the Grid Manager, select **SUPPORT** > **Tools** > **Grid topology**.
   b. Select ***Site*** > **recovered Storage Node** > **SSM** > **Services**.
   c. Confirm that all services are running.
   d. Select **DDS** > **Data Store**.
   e. Confirm that the **Data Store Status** is “Up” and the **Data Store State** is “Normal.”

#### Recover appliance Storage Node

## The procedure for recovering a failed StorageGRID appliance Storage Node is the same whether you are recovering from the loss of the system drive or from the loss of storage volumes only.

### About this task

You must prepare the appliance and reinstall software, configure the node to rejoin the grid, reformat storage, and restore object data.




If more than one Storage Node has failed (or is offline), contact technical support. Do not perform the following recovery procedure. Data loss could occur.

If this is the second Storage Node failure in less than 15 days after a Storage Node failure or recovery, contact technical support. Rebuilding Cassandra on two or more Storage Nodes within 15 days can result in data loss.

If more than one Storage Node at a site has failed, a site recovery procedure might be required. Contact technical support.

### How site recovery is performed by technical support

If ILM rules are configured to store only one replicated copy and the copy exists on a storage volume that has failed, you will not be able to recover the object.

If you encounter a Services: Status - Cassandra (SVST) alarm during recovery, see the monitoring and troubleshooting instructions to recover from the alarm by rebuilding Cassandra. After Cassandra is rebuilt, alarms should clear. If alarms do not clear, contact technical support.

For hardware maintenance procedures, such as instructions for replacing a controller or reinstalling SANtricity OS, see the installation and maintenance instructions for your storage appliance.

**Related information**

Monitor and troubleshoot

SG6000 storage appliances

SG5700 storage appliances

SG5600 storage appliances

### Prepare appliance Storage Node for reinstallation

When recovering an appliance Storage Node, you must first prepare the appliance for reinstallation of StorageGRID software.

1. Log in to the failed Storage Node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Prepare the appliance Storage Node for the installation of StorageGRID software. `sgareinstall`

3. When prompted to continue, enter: `y`

   The appliance reboots, and your SSH session ends. It usually takes about 5 minutes for the StorageGRID Appliance Installer to become available, although in some cases you might need to wait up to 30 minutes.

   The StorageGRID appliance Storage Node is reset, and data on the Storage Node is no longer accessible. IP addresses configured during the original installation process should remain intact; however, it is recommended that you confirm this when the procedure completes.

   After executing the `sgareinstall` command, all StorageGRID-provisioned accounts, passwords, and SSH keys are removed, and new host keys are generated.

### Start StorageGRID appliance installation

To install StorageGRID on an appliance Storage Node, you use the StorageGRID Appliance Installer, which is included on the appliance.

**What you'll need**

- The appliance has been installed in a rack, connected to your networks, and powered on.
- Network links and IP addresses have been configured for the appliance using the StorageGRID Appliance Installer.

- You know the IP address of the primary Admin Node for the StorageGRID grid.
- All Grid Network subnets listed on the IP Configuration page of the StorageGRID Appliance Installer have been defined in the Grid Network Subnet List on the primary Admin Node.
- You have completed these prerequisite tasks by following the installation and maintenance instructions for your storage appliance:
  - SG5600 storage appliances
  - SG5700 storage appliances
  - SG6000 storage appliances
- You are using a supported web browser.
- You know one of the IP addresses assigned to the compute controller in the appliance. You can use the IP address for the Admin Network (management port 1 on the controller), the Grid Network, or the Client Network.

**About this task**

To install StorageGRID on an appliance Storage Node:

- You specify or confirm the IP address of the primary Admin Node and the name of the node.
- You start the installation and wait as volumes are configured and the software is installed.
- Partway through the process, the installation pauses. To resume the installation, you must sign into the Grid Manager and configure the pending Storage Node as a replacement for the failed node.
- After you have configured the node, the appliance installation process completes, and the appliance is rebooted.

**Steps**

1. Open a browser and enter one of the IP addresses for the compute controller in the appliance.

   ```
   https://Controller_IP:8443
   ```

   The StorageGRID Appliance Installer Home page appears.

2. In the Primary Admin Node connection section, determine whether you need to specify the IP address for the primary Admin Node.

   The StorageGRID Appliance Installer can discover this IP address automatically, assuming the primary Admin Node, or at least one other grid node with ADMIN_IP configured, is present on the same subnet.

3. If this IP address is not shown or you need to change it, specify the address:

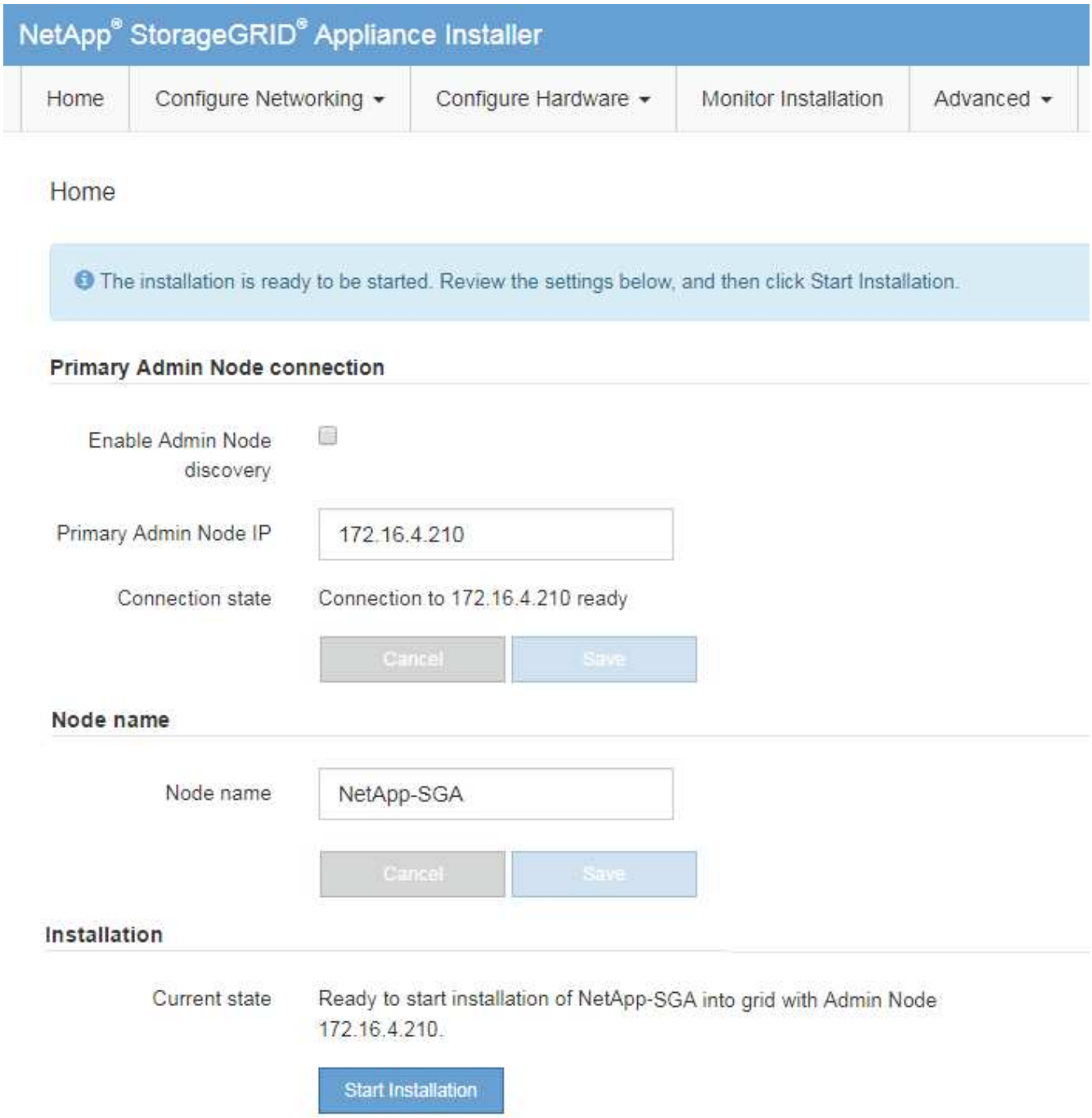
| Option | Steps |
|---|---|
| Manual IP entry | a. Unselect the **Enable Admin Node discovery** check box.<br>b. Enter the IP address manually.<br>c. Click **Save**.<br>d. Wait while the connection state for the new IP address becomes “ready.” |

| Option | Steps |
| --- | --- |
| Automatic discovery of all connected primary Admin Nodes | a. Select the **Enable Admin Node discovery** check box.<br>b. From the list of discovered IP addresses, select the primary Admin Node for the grid where this appliance Storage Node will be deployed.<br>c. Click **Save**.<br>d. Wait while the connection state for the new IP address becomes “ready.” |

4. In the **Node Name** field, enter the same name that was used for the node you are recovering, and click **Save**.
5. In the Installation section, confirm that the current state is “Ready to start installation of node name into grid with Primary Admin Node admin_ip” and that the **Start Installation** button is enabled.

   If the **Start Installation** button is not enabled, you might need to change the network configuration or port settings. For instructions, see the installation and maintenance instructions for your appliance.

6. From the StorageGRID Appliance Installer home page, click **Start Installation**.




The Current state changes to “Installation is in progress,” and the Monitor Installation page is displayed.

> If you need to access the Monitor Installation page manually, click **Monitor Installation** from the menu bar.

**Related information**

SG100 and SG1000 services appliances

SG6000 storage appliances

SG5700 storage appliances

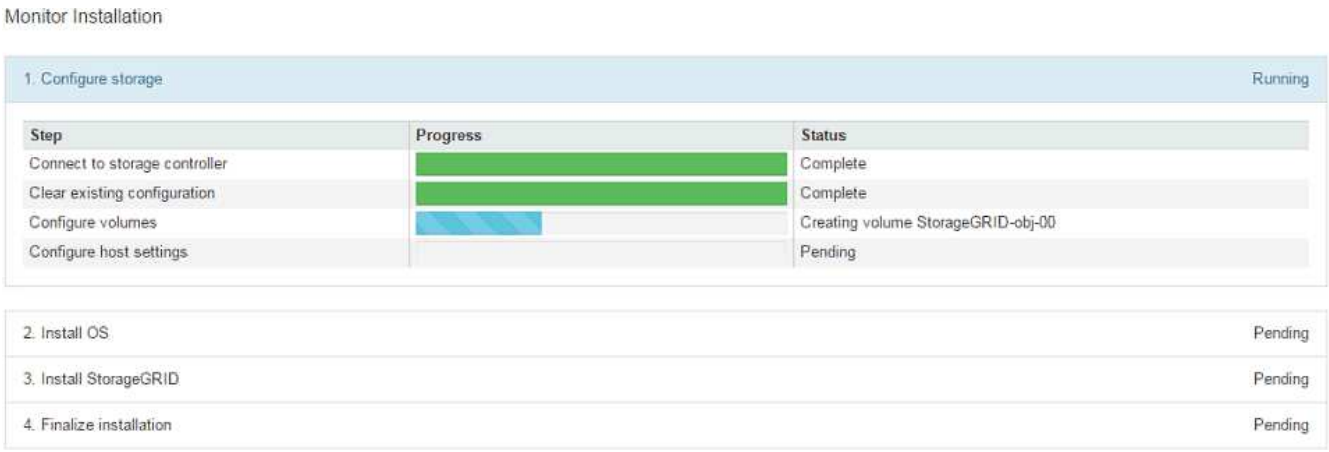
SG5600 storage appliances

### Monitor StorageGRID appliance installation

The StorageGRID Appliance Installer provides status until installation is complete. When the software installation is complete, the appliance is rebooted.

1. To monitor the installation progress, click **Monitor Installation** from the menu bar.

   The Monitor Installation page shows the installation progress.

   The blue status bar indicates which task is currently in progress. Green status bars indicate tasks that have completed successfully.

   > The installer ensures that tasks completed in a previous install are not re-run. If you are re-running an installation, any tasks that do not need to be re-run are shown with a green status bar and a status of “Skipped.”

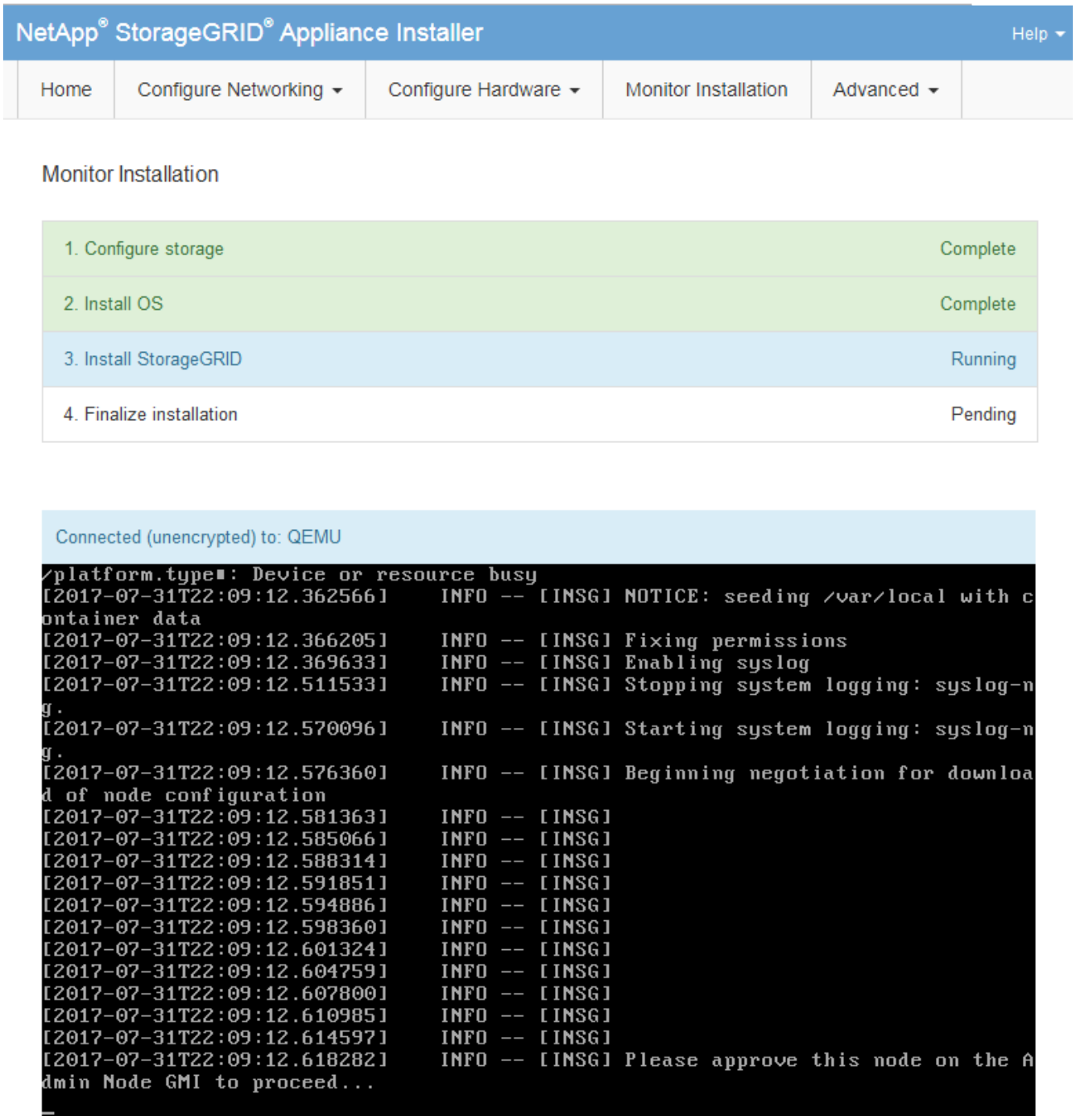
2. Review the progress of first two installation stages.
   - **1. Configure storage**

     During this stage, the installer connects to the storage controller, clears any existing configuration, communicates with SANtricity software to configure volumes, and configures host settings.

   - **2. Install OS**

     During this stage, the installer copies the base operating system image for StorageGRID to the appliance.

3. Continue monitoring the installation progress until the **Install StorageGRID** stage pauses and a message appears on the embedded console prompting you to approve this node on the Admin Node using the Grid Manager.




4. Go to the procedure to configure the appliance Storage Node.

### Select Start Recovery to configure appliance Storage Node

You must select Start Recovery in the Grid Manager to configure an appliance Storage Node as a replacement for the failed node.

#### What you'll need

- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Maintenance or Root Access permission.
- You must have the provisioning passphrase.

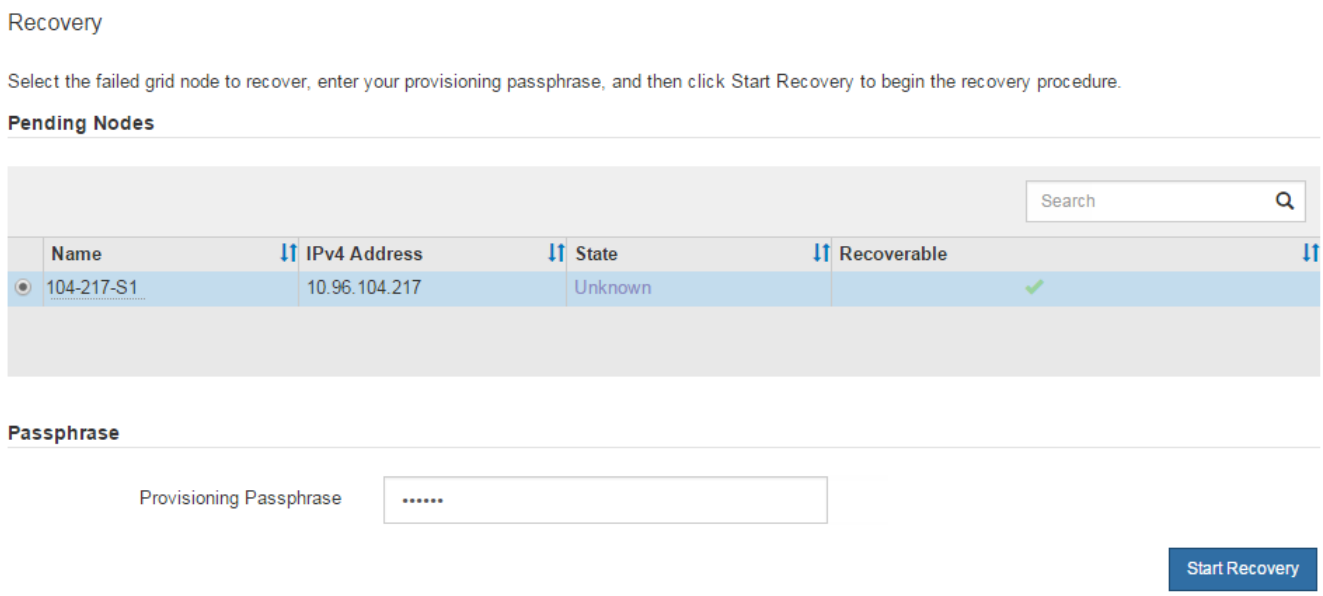
- You must have deployed a recovery appliance Storage Node.
- You must know the start date of any repair jobs for erasure-coded data.
- You must have verified that the Storage Node has not been rebuilt within the last 15 days.

**Steps**

1. From the Grid Manager, select **MAINTENANCE** > **Tasks** > **Recovery**.
2. Select the grid node you want to recover in the Pending Nodes list.

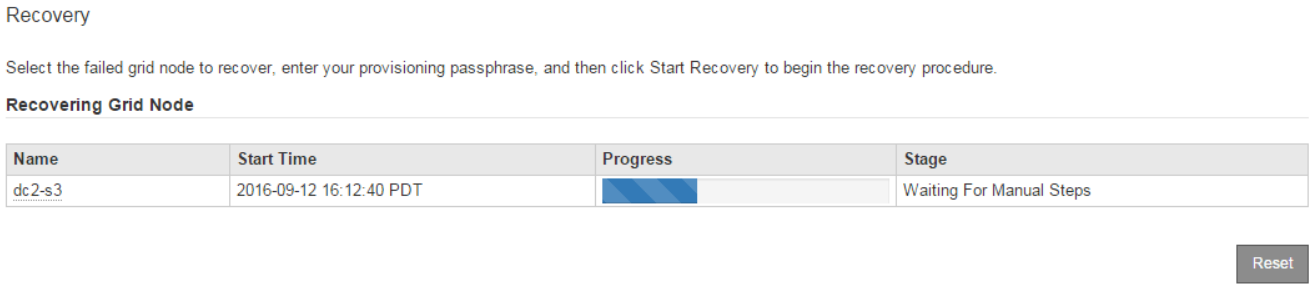
   Nodes appear in the list after they fail, but you cannot select a node until it has been reinstalled and is ready for recovery.

3. Enter the **Provisioning Passphrase**.
4. Click **Start Recovery**.

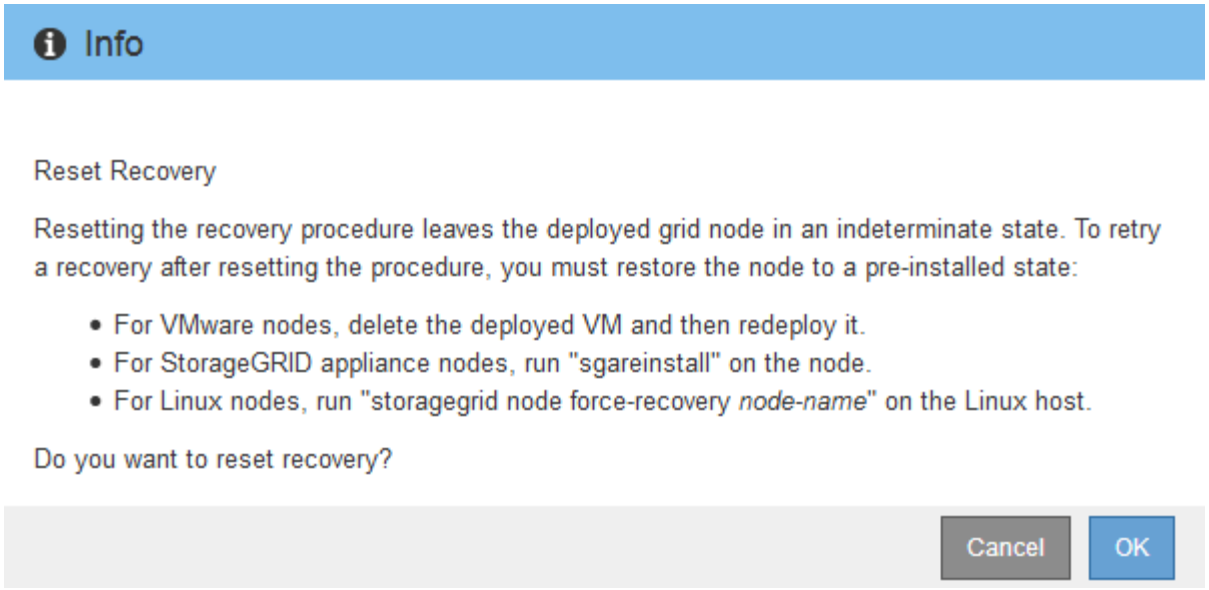



5. Monitor the progress of the recovery in the Recovering Grid Node table.

   When the grid node reaches the “Waiting for Manual Steps” stage, go to the next topic and perform the manual steps to remount and reformat appliance storage volumes.




> At any point during the recovery, you can click **Reset** to start a new recovery. An Info dialog box appears, indicating that the node will be left in an indeterminate state if you reset the procedure.




If you want to retry the recovery after resetting the procedure, you must restore the appliance node to a pre-installed state by running `sgareinstall` on the node.

### Remount and reformat appliance storage volumes (“Manual Steps”)

You must manually run two scripts to remount preserved storage volumes and reformat any failed storage volumes. The first script remounts volumes that are properly formatted as StorageGRID storage volumes. The second script reformats any unmounted volumes, rebuilds the Cassandra database, if needed, and starts services.

#### What you’ll need

- You have already replaced the hardware for any failed storage volumes that you know require replacement.

  Running the `sn-remount-volumes` script might help you identify additional failed storage volumes.

- You have checked that a Storage Node decommissioning is not in progress, or you have paused the node decommission procedure. (In the Grid Manager, select **MAINTENANCE** > **Tasks** > **Decommission**.)
- You have checked that an expansion is not in progress. (In the Grid Manager, select **MAINTENANCE** > **Tasks** > **Expansion**.)

> Contact technical support if more than one Storage Node is offline or if a Storage Node in this grid has been rebuilt in the last 15 days. Do not run the `sn-recovery-postinstall.sh` script. Rebuilding Cassandra on two or more Storage Nodes within 15 days of each other might result in data loss.

#### About this task

To complete this procedure, you perform these high-level tasks:

- Log in to the recovered Storage Node.
- Run the `sn-remount-volumes` script to remount properly formatted storage volumes. When this script runs, it does the following:

- Mounts and unmounts each storage volume to replay the XFS journal.
- Performs an XFS file consistency check.
- If the file system is consistent, determines if the storage volume is a properly formatted StorageGRID storage volume.
- If the storage volume is properly formatted, remounts the storage volume. Any existing data on the volume remains intact.

- Review the script output and resolve any issues.
- Run the `sn-recovery-postinstall.sh` script. When this script runs, it does the following.

> Do not reboot a Storage Node during recovery before running `sn-recovery-postinstall.sh` (step 4) to reformat the failed storage volumes and restore object metadata. Rebooting the Storage Node before `sn-recovery-postinstall.sh` completes causes errors for services that attempt to start and causes StorageGRID appliance nodes to exit maintenance mode.

  - Reformats any storage volumes that the `sn-remount-volumes` script could not mount or that were found to be improperly formatted.

    > If a storage volume is reformatted, any data on that volume is lost. You must perform an additional procedure to restore object data from other locations in the grid, assuming that ILM rules were configured to store more than one object copy.

  - Rebuilds the Cassandra database on the node, if needed.
  - Starts the services on the Storage Node.

**Steps**

1. Log in to the recovered Storage Node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Run the first script to remount any properly formatted storage volumes.

   > If all storage volumes are new and need to be formatted, or if all storage volumes have failed, you can skip this step and run the second script to reformat all unmounted storage volumes.

   a. Run the script: `sn-remount-volumes`

      This script might take hours to run on storage volumes that contain data.

   b. As the script runs, review the output and answer any prompts.

As required, you can use the `tail -f` command to monitor the contents of the script's log file (`/var/local/log/sn-remount-volumes.log`) . The log file contains more detailed information than the command line output.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
```

```
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

In the example output, one storage volume was remounted successfully and three storage volumes had errors.

- `/dev/sdb` passed the XFS file system consistency check and had a valid volume structure, so it was remounted successfully. Data on devices that are remounted by the script is preserved.
- `/dev/sdc` failed the XFS file system consistency check because the storage volume was new or corrupt.
- `/dev/sdd` could not be mounted because the disk was uninitialized or the disk's superblock was corrupted. When the script cannot mount a storage volume, it asks if you want to run the file system consistency check.
  - If the storage volume is attached to a new disk, answer **N** to the prompt. You do not need check the file system on a new disk.
  - If the storage volume is attached to an existing disk, answer **Y** to the prompt. You can use the results of the file system check to determine the source of the corruption. The results are saved in the `/var/local/log/sn-remount-volumes.log` log file.

- `/dev/sde` passed the XFS file system consistency check and had a valid volume structure; however, the LDR node ID in the `volID` file did not match the ID for this Storage Node (the `configured LDR noid` displayed at the top). This message indicates that this volume belongs to another Storage Node.

3. Review the script output and resolve any issues.

> If a storage volume failed the XFS file system consistency check or could not be mounted, carefully review the error messages in the output. You must understand the implications of running the `sn-recovery-postinstall.sh` script on these volumes.

a. Check to make sure that the results include an entry for all of the volumes you expected. If any volumes are not listed, rerun the script.

b. Review the messages for all mounted devices. Make sure there are no errors indicating that a storage volume does not belong to this Storage Node.

   In the example, the output for /dev/sde includes the following error message:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> If a storage volume is reported as belonging to another Storage Node, contact technical support. If you run the `sn-recovery-postinstall.sh` script, the storage volume will be reformatted, which might cause data loss.

c. If any storage devices could not be mounted, make a note of the device name, and repair or replace the device.

> You must repair or replace any storage devices that could not be mounted.

   You will use the device name to look up the volume ID, which is required input when you run the `repair-data` script to restore object data to the volume (the next procedure).

d. After repairing or replacing all unmountable devices, run the `sn-remount-volumes` script again to confirm that all storage volumes that can be remounted have been remounted.

> If a storage volume cannot be mounted or is improperly formatted, and you continue to the next step, the volume and any data on the volume will be deleted. If you had two copies of object data, you will have only a single copy until you complete the next procedure (restoring object data).

> Do not run the `sn-recovery-postinstall.sh` script if you believe that the data remaining on a failed storage volume cannot be rebuilt from elsewhere in the grid (for example, if your ILM policy uses a rule that makes only one copy or if volumes have failed on multiple nodes). Instead, contact technical support to determine how to recover your data.

4. Run the `sn-recovery-postinstall.sh` script: `sn-recovery-postinstall.sh`

This script reformats any storage volumes that could not be mounted or that were found to be improperly formatted; rebuilds the Cassandra database on the node, if needed; and starts the services on the Storage Node.

Be aware of the following:

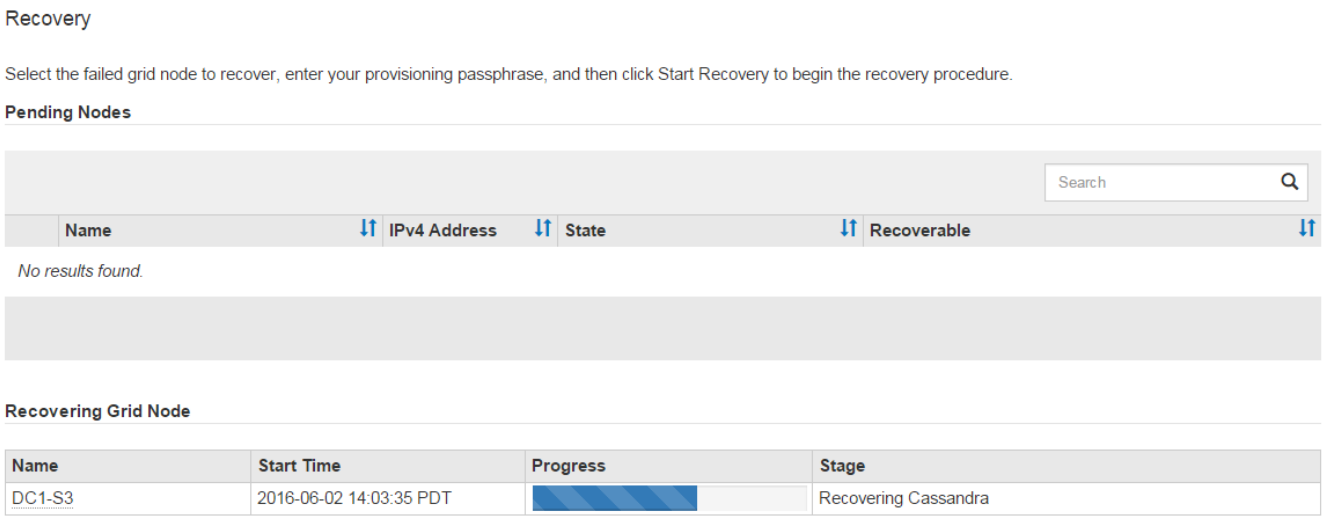
- The script might take hours to run.
- In general, you should leave the SSH session alone while the script is running.
- Do not press **Ctrl+C** while the SSH session is active.
- The script will run in the background if a network disruption occurs and terminates the SSH session, but you can view the progress from the Recovery page.
- If the Storage Node uses the RSM service, the script might appear to stall for 5 minutes as node services are restarted. This 5-minute delay is expected whenever the RSM service boots for the first time.

> The RSM service is present on Storage Nodes that include the ADC service.

> Some StorageGRID recovery procedures use Reaper to handle Cassandra repairs. Repairs occur automatically as soon as the related or required services have started. You might notice script output that mentions “reaper” or “Cassandra repair.” If you see an error message indicating the repair has failed, run the command indicated in the error message.

5. As the `sn-recovery-postinstall.sh` script runs, monitor the Recovery page in the Grid Manager.

   The Progress bar and the Stage column on the Recovery page provide a high-level status of the `sn-recovery-postinstall.sh` script.




After the `sn-recovery-postinstall.sh` script has started services on the node, you can restore object data to any storage volumes that were formatted by the script, as described in the next procedure.

**Related information**

Review warnings for Storage Node system drive recovery

Restore object data to storage volume for appliance

### Restore object data to storage volume for appliance

After recovering storage volumes for the appliance Storage Node, you can restore the object data that was lost when the Storage Node failed.

#### What you'll need

- You must have confirmed that the recovered Storage Node has a Connection State of **Connected** on the **NODES** > **Overview** tab in the Grid Manager.

#### About this task

Object data can be restored from other Storage Nodes, an Archive Node, or a Cloud Storage Pool, assuming that the grid's ILM rules were configured such that object copies are available.

Note the following:

- If an ILM rule was configured to store only one replicated copy and that copy existed on a storage volume that failed, you will not be able to recover the object.
- If the only remaining copy of an object is in a Cloud Storage Pool, StorageGRID must issue multiple requests to the Cloud Storage Pool endpoint to restore object data. Before performing this procedure, contact technical support for help in estimating the recovery time frame and the associated costs.
- If the only remaining copy of an object is on an Archive Node, object data is retrieved from the Archive Node. Restoring object data to a Storage Node from an Archive Node takes longer than restoring copies from other Storage Nodes because of the latency associated with retrievals from external archival storage systems.

#### About the `repair-data` script

To restore object data, you run the `repair-data` script. This script begins the process of restoring object data and works with ILM scanning to ensure that ILM rules are met.

Select **Replicated data** or **Erasure-coded (EC) data** below to learn the different options for the `repair-data` script, based on whether you are restoring replicated data or erasure-coded data. If you need to restore both types of data, you must run both sets of commands.

> For more information about the `repair-data` script, enter `repair-data --help` from the command line of the primary Admin Node.

**Replicated data**

Two commands are available for restoring replicated data, based on whether you need to repair the entire node or only certain volumes on the node:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

You can track repairs of replicated data with this command:

```
repair-data show-replicated-repair-status
```

> The `show-replicated-repair-status` option is available for technical preview in StorageGRID 11.6. This feature is under development, and the value returned might be incorrect or delayed. To determine if a repair is complete, use **Awaiting – All**, **Repairs Attempted (XRPA)**, and **Scan Period — Estimated (XSCM)** as described in Monitor repairs.

**Erasure coded (EC) data**

Two commands are available for restoring erasure-coded data, based on whether you need to repair the entire node or only certain volumes on the node:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Repairs of erasure-coded data can begin while some Storage Nodes are offline. Repair will complete after all nodes are available.

You can track repairs of erasure-coded data with this command:

```
repair-data show-ec-repair-status
```

> The EC repair job temporarily reserves a large amount of storage. Storage alerts might be triggered, but will resolve when the repair is complete. If there is not enough storage for the reservation, the EC repair job will fail. Storage reservations are released when the EC repair job completes, whether the job failed or succeeded.

### Find hostname for Storage Node

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.

2. Use the `/etc/hosts` file to find the hostname of the Storage Node for the restored storage volumes. To see a list of all nodes in the grid, enter the following: `cat /etc/hosts`.

### Repair data if all volumes have failed

If all storage volumes have failed, repair the entire node. Follow the instructions for **replicated data**, **erasure-coded (EC) data**, or both, based on whether you use replicated data, erasure-coded (EC) data, or both.

If only some volumes have failed, go to Repair data if only some volumes have failed.

> You cannot run `repair-data` operations for more than one node at the same time. To recover multiple nodes, contact technical support.

#### Replicated data

If your grid includes replicated data, use the `repair-data start-replicated-node-repair` command with the `--nodes` option to repair the entire Storage Node.

This command repairs the replicated data on a Storage Node named SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> As object data is restored, the **Objects Lost** alert is triggered if the StorageGRID system cannot locate replicated object data. Alerts might be triggered on Storage Nodes throughout the system. You should determine the cause of the loss and if recovery is possible. See Monitor and troubleshoot.

#### Erasure coded (EC) data

If your grid contains erasure-coded data, use the `repair-data start-ec-node-repair` command with the `--nodes` option to repair the entire Storage Node.

This command repairs the erasure-coded data on a Storage Node named SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

The operation returns a unique `repair ID` that identifies this `repair_data` operation. Use this `repair ID` to track the progress and result of the `repair_data` operation. No other feedback is returned as the recovery process completes.

> Repairs of erasure-coded data can begin while some Storage Nodes are offline. Repair will complete after all nodes are available.

### Repair data if only some volumes have failed

If only some of the volumes have failed, repair the affected volumes. Follow the instructions for **replicated data**, **erasure-coded (EC) data**, or both, based on whether you use replicated data, erasure-coded (EC) data, or both.

If all volumes have failed, go to Repair data if all volumes have failed.

Enter the volume IDs in hexadecimal. For example, `0000` is the first volume and `000F` is the sixteenth volume.

You can specify one volume, a range of volumes, or multiple volumes that are not in a sequence.

All the volumes must be on the same Storage Node. If you need to restore volumes for more than one Storage Node, contact technical support.

#### Replicated data

If your grid contains replicated data, use the `start-replicated-volume-repair` command with the `--nodes` option to identify the node. Then add either the `--volumes` or `--volume-range` option, as shown in the following examples.

**Single volume**: This command restores replicated data to volume `0002` on a Storage Node named SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

**Range of volumes**: This command restores replicated data to all volumes in the range `0003` to `0009` on a Storage Node named SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

**Multiple volumes not in a sequence**: This command restores replicated data to volumes `0001`, `0005`, and `0008` on a Storage Node named SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> As object data is restored, the **Objects Lost** alert is triggered if the StorageGRID system cannot locate replicated object data. Alerts might be triggered on Storage Nodes throughout the system. You should determine the cause of the loss and if recovery is possible. See the instructions for monitoring and troubleshooting StorageGRID.

#### Erasure coded (EC) data

If your grid contains erasure-coded data, use the `start-ec-volume-repair` command with the `--nodes` option to identify the node. Then add either the `--volumes` or `--volume-range` option, as shown in the following examples.

**Single volume**: This command restores erasure-coded data to volume `0007` on a Storage Node named SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

**Range of volumes**: This command restores erasure-coded data to all volumes in the range `0004` to `0006` on a Storage Node named SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

**Multiple volumes not in a sequence**: This command restores erasure-coded data to volumes `000A`, `000C`, and `000E` on a Storage Node named SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

The `repair-data` operation returns a unique `repair ID` that identifies this `repair_data` operation. Use this `repair ID` to track the progress and result of the `repair_data` operation. No other feedback is returned as the recovery process completes.

> Repairs of erasure-coded data can begin while some Storage Nodes are offline. Repair will complete after all nodes are available.

### Monitor repairs

Monitor the status of the repair jobs, based on whether you use **replicated data**, **erasure-coded (EC) data**, or both.

**Replicated data**

- To determine if repairs are complete:
  1. Select **NODES** > ***Storage Node being repaired*** > **ILM**.
  2. Review the attributes in the Evaluation section. When repairs are complete, the **Awaiting - All** attribute indicates 0 objects.
- To monitor the repair in more detail:
  1. Select **SUPPORT** > **Tools** > **Grid topology**.
  2. Select ***grid*** > ***Storage Node being repaired*** > **LDR** > **Data Store**.
  3. Use a combination of the following attributes to determine, as well as possible, if replicated repairs are complete.

     Cassandra inconsistencies might be present, and failed repairs are not tracked.

     - **Repairs Attempted (XRPA)**: Use this attribute to track the progress of replicated repairs. This attribute increases each time a Storage Node tries to repair a high-risk object. When this attribute does not increase for a period longer than the current scan period (provided by the **Scan Period — Estimated** attribute), it means that ILM scanning found no high-risk objects that need to be repaired on any nodes.

       High-risk objects are objects that are at risk of being completely lost. This does not include objects that do not satisfy their ILM configuration.

     - **Scan Period — Estimated (XSCM)**: Use this attribute to estimate when a policy change will be applied to previously ingested objects. If the **Repairs Attempted** attribute does not increase for a period longer than the current scan period, it is probable that replicated repairs are done. Note that the scan period can change. The **Scan Period — Estimated (XSCM)** attribute applies to the entire grid and is the maximum of all node scan periods. You can query the **Scan Period — Estimated** attribute history for the grid to determine an appropriate time frame.
- Optionally, to get an estimated percent completion for the replicated repair, add the `show-replicated-repair-status` option to the repair-data command.

  ```
  repair-data show-replicated-repair-status
  ```

  The `show-replicated-repair-status` option is available for technical preview in StorageGRID 11.6. This feature is under development, and the value returned might be incorrect or delayed. To determine if a repair is complete, use **Awaiting – All**, **Repairs Attempted (XRPA)**, and **Scan Period — Estimated (XSCM)** as described in Monitor repairs.

**Erasure coded (EC) data**

To monitor the repair of erasure-coded data and retry any requests that might have failed:

1. Determine the status of erasure-coded data repairs:
   - Select **SUPPORT** > **Tools** > **Metrics** to view the estimated time to completion and the completion percentage for the current job. Then, select **EC Overview** in the Grafana section. Look at the **Grid EC Job Estimated Time to Completion** and **Grid EC Job Percentage Completed** dashboards.

- Use this command to see the status of a specific `repair-data` operation:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Use this command to list all repairs:

  ```
  repair-data show-ec-repair-status
  ```

  The output lists information, including `repair ID`, for all previously and currently running repairs.

2. If the output shows that the repair operation failed, use the `--repair-id` option to retry the repair.

   This command retries a failed node repair, using the repair ID 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   This command retries a failed volume repair, using the repair ID 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

#### Check storage state after recovering appliance Storage Node

After recovering an appliance Storage Node, you must verify that the desired state of the appliance Storage Node is set to online and ensure that the state will be online by default whenever the Storage Node server is restarted.

**What you'll need**

- You must be signed in to the Grid Manager using a supported web browser.
- The Storage Node has been recovered, and data recovery is complete.

**Steps**

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Check the values of **Recovered Storage Node** > **LDR** > **Storage** > **Storage State — Desired** and **Storage State — Current**.

   The value of both attributes should be Online.

3. If the Storage State — Desired is set to Read-only, complete the following steps:
   a. Click the **Configuration** tab.
   b. From the **Storage State — Desired** drop-down list, select **Online**.
   c. Click **Apply Changes**.
   d. Click the **Overview** tab and confirm that the values of **Storage State — Desired** and **Storage State — Current** are updated to Online.

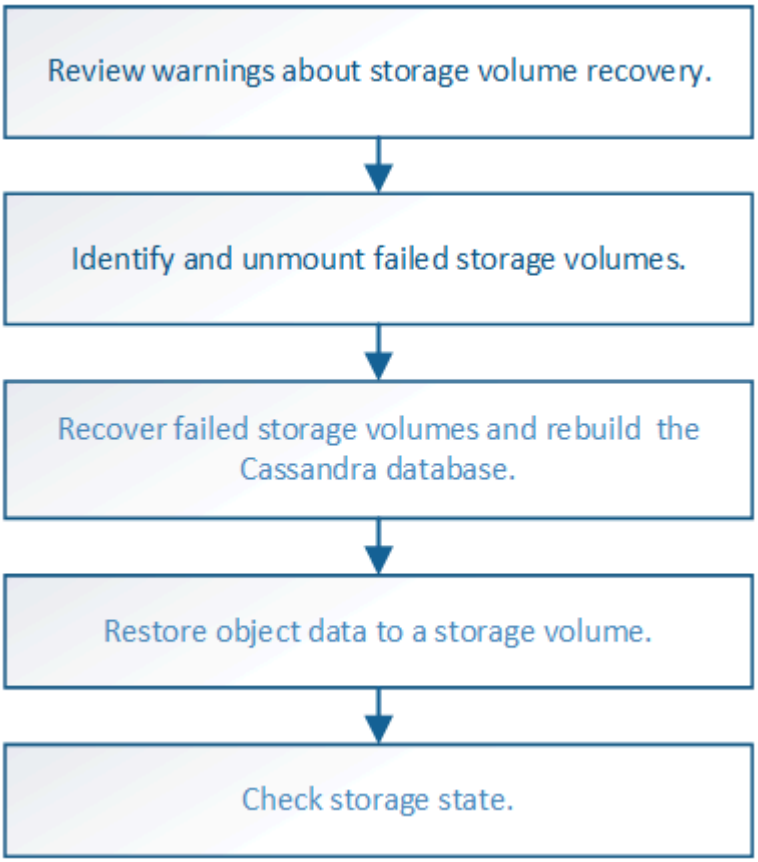
#### Recover from storage volume failure where system drive is intact

You must complete a series of tasks to recover a software-based Storage Node where one or more storage volumes on the Storage Node have failed, but the system drive is

intact. If only storage volumes have failed, the Storage Node is still available to the StorageGRID system.

**About this task**

This recovery procedure applies to software-based Storage Nodes only. If storage volumes have failed on an appliance Storage Node, use the procedure for “Recover appliance Storage Node.”




**Related information**

Recover appliance Storage Node

**Review warnings about storage volume recovery**

Before recovering failed storage volumes for a Storage Node, you must review the following warnings.

The storage volumes (or rangedbs) in a Storage Node are identified by a hexadecimal number, which is known as the volume ID. For example, 0000 is the first volume and 000F is the sixteenth volume. The first object store (volume 0) on each Storage Node uses up to 4 TB of space for object metadata and Cassandra database operations; any remaining space on that volume is used for object data. All other storage volumes are used exclusively for object data.

If volume 0 fails and needs to be recovered, the Cassandra database might be rebuilt as part of the volume recovery procedure. Cassandra might also be rebuilt in the following circumstances:

- A Storage Node is brought back online after having been offline for more than 15 days.
- The system drive and one or more storage volumes fails and is recovered.

When Cassandra is rebuilt, the system uses information from other Storage Nodes. If too many Storage Nodes are offline, some Cassandra data might not be available. If Cassandra has been rebuilt recently, Cassandra data might not yet be consistent across the grid. Data loss can occur if Cassandra is rebuilt when too many Storage Nodes are offline or if two or more Storage Nodes are rebuilt within 15 days of each other.

> If more than one Storage Node has failed (or is offline), contact technical support. Do not perform the following recovery procedure. Data loss could occur.

> If this is the second Storage Node failure in less than 15 days after a Storage Node failure or recovery, contact technical support. Rebuilding Cassandra on two or more Storage Nodes within 15 days can result in data loss.

> If more than one Storage Node at a site has failed, a site recovery procedure might be required. Contact technical support.

How site recovery is performed by technical support

> If ILM rules are configured to store only one replicated copy and the copy exists on a storage volume that has failed, you will not be able to recover the object.

> If you encounter a Services: Status - Cassandra (SVST) alarm during recovery, see the monitoring and troubleshooting instructions to recover from the alarm by rebuilding Cassandra. After Cassandra is rebuilt, alarms should clear. If alarms do not clear, contact technical support.

**Related information**

Monitor and troubleshoot

Warnings and considerations for grid node recovery

### Identify and unmount failed storage volumes

When recovering a Storage Node with failed storage volumes, you must identify and unmount the failed volumes. You must verify that only the failed storage volumes are reformatted as part of the recovery procedure.

**What you'll need**

You must be signed in to the Grid Manager using a supported web browser.

**About this task**

You should recover failed storage volumes as soon as possible.

The first step of the recovery process is to detect volumes that have become detached, need to be unmounted, or have I/O errors. If failed volumes are still attached but have a randomly corrupted file system, the system might not detect any corruption in unused or unallocated parts of the disk.

> You must finish this procedure before performing manual steps to recover the volumes, such as adding or re-attaching the disks, stopping the node, starting the node, or rebooting. Otherwise, when you run the `reformat_storage_block_devices.rb` script, you might encounter a file system error that causes the script to hang or fail.

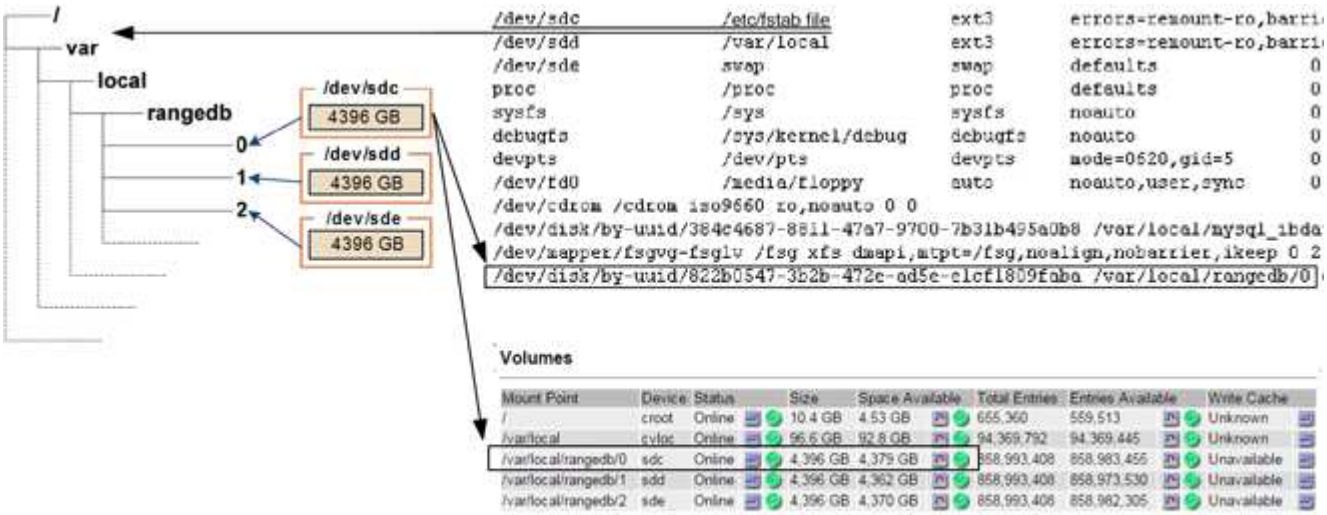
Repair the hardware and properly attach the disks before running the `reboot` command.

Identify failed storage volumes carefully. You will use this information to verify which volumes must be reformatted. Once a volume has been reformatted, data on the volume cannot be recovered.

To correctly recover failed storage volumes, you need to know both the device names of the failed storage volumes and their volume IDs.

At installation, each storage device is assigned a file system universal unique identifier (UUID) and is mounted to a rangedb directory on the Storage Node using that assigned file system UUID. The file system UUID and the rangedb directory are listed in the `/etc/fstab` file. The device name, rangedb directory, and the size of the mounted volume are displayed in the Grid Manager.

In the following example, device `/dev/sdc` has a volume size of 4 TB, is mounted to `/var/local/rangedb/0`, using the device name `/dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba` in the `/etc/fstab` file:




**Steps**

1. Complete the following steps to record the failed storage volumes and their device names:
   a. Select **SUPPORT** > **Tools** > **Grid topology**.
   b. Select **site** > **failed Storage Node** > **LDR** > **Storage** > **Overview** > **Main**, and look for object stores with alarms.

   **Object Stores**

   | ID | Total | Available | Stored Data | Stored (%) | Health |
   |---|---|---|---|---|---|
   | 0000 | 96.6 GB | 96.6 GB | 823 KB | 0.001 % | Error |
   | 0001 | 107 GB | 107 GB | 0 B | 0 % | No Errors |
   | 0002 | 107 GB | 107 GB | 0 B | 0 % | No Errors |

   c. Select **site** > **failed Storage Node** > **SSM** > **Resources** > **Overview** > **Main**. Determine the mount point and volume size of each failed storage volume identified in the previous step.

Object stores are numbered in hex notation. For example, 0000 is the first volume and 000F is the sixteenth volume. In the example, the object store with an ID of 0000 corresponds to `/var/local/rangedb/0` with device name sdc and a size of 107 GB.

**Volumes**

| Mount Point | Device | Status | Size | Space Available | Total Entries | Entries Available | Write Cache |
|---|---|---|---|---|---|---|---|
| / | croot | Online | 10.4 GB | 4.17 GB | 655,360 | 554,806 | Unknown |
| /var/local | cvloc | Online | 96.6 GB | 96.1 GB | 94,369,792 | 94,369,423 | Unknown |
| /var/local/rangedb/0 | sdc | Online | 107 GB | 107 GB | 104,857,600 | 104,856,202 | Enabled |
| /var/local/rangedb/1 | sdd | Online | 107 GB | 107 GB | 104,857,600 | 104,856,536 | Enabled |
| /var/local/rangedb/2 | sde | Online | 107 GB | 107 GB | 104,857,600 | 104,856,536 | Enabled |

2. Log in to the failed Storage Node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

3. Run the following script to stop the storage services and unmount a failed storage volume:

   ```
   sn-unmount-volume object_store_ID
   ```

   The `object_store_ID` is the ID of the failed storage volume. For example, specify `0` in the command for an object store with ID 0000.

4. If prompted, press **y** to stop the storage services on the Storage Node.

   > If the storage services are already stopped, you are not prompted. The Cassandra service is stopped only for volume 0.

   ```
   root@Storage-180:~ # sn-unmount-volume 0
   Storage services (ldr, chunk, dds, cassandra) are not down.
   Storage services must be stopped before running this script.
   Stop storage services [y/N]? y
   Shutting down storage services.
   Storage services stopped.
   Unmounting /var/local/rangedb/0
   /var/local/rangedb/0 is unmounted.
   ```

   In a few seconds, the storage services are stopped and the volume is unmounted. Messages appear indicating each step of the process. The final message indicates that the volume is unmounted.

#### Recover failed storage volumes and rebuild Cassandra database

You must run a script that reformats and remounts storage on failed storage volumes, and rebuilds the Cassandra database on the Storage Node if the system determines that it is necessary.

- You must have the `Passwords.txt` file.
- The system drives on the server must be intact.
- The cause of the failure must have been identified and, if necessary, replacement storage hardware must already have been acquired.
- The total size of the replacement storage must be the same as the original.
- You have checked that a Storage Node decommissioning is not in progress, or you have paused the node decommission procedure. (In the Grid Manager, select **MAINTENANCE** > **Tasks** > **Decommission**.)
- You have checked that an expansion is not in progress. (In the Grid Manager, select **MAINTENANCE** > **Tasks** > **Expansion**.)
- You have reviewed the warnings about storage volume recovery.

1. As needed, replace failed physical or virtual storage associated with the failed storage volumes that you identified and unmounted earlier.

   After you replace the storage, make sure you rescan or reboot to make sure that it is recognized by the operating system, but do not remount the volumes. The storage is remounted and added to `/etc/fstab` in a later step.

2. Log in to the failed Storage Node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

1. Use a text editor (vi or vim) to delete failed volumes from the `/etc/fstab` file and then save the file.

   > Commenting out a failed volume in the `/etc/fstab` file is insufficient. The volume must be deleted from `fstab` as the recovery process verifies that all lines in the `fstab` file match the mounted file systems.

2. Reformat any failed storage volumes and rebuild the Cassandra database if it is necessary. Enter: `reformat_storage_block_devices.rb`
   - If storage services are running, you will be prompted to stop them. Enter: **y**
   - You will be prompted to rebuild the Cassandra database if it is necessary.
     - Review the warnings. If none of them apply, rebuild the Cassandra database. Enter: **y**
     - If more than one Storage Node is offline or if another Storage Node has been rebuilt in the last 15 days. Enter: **n**

The script will exit without rebuilding Cassandra. Contact technical support.

- For each rangedb drive on the Storage Node, when you are asked: `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`, enter one of the following responses:
  - **y** to reformat a drive that had errors. This reformats the storage volume and adds the reformatted storage volume to the `/etc/fstab` file.
  - **n** if the drive contains no errors, and you do not want to reformat it.

> Selecting **n** exits the script. Either mount the drive (if you think the data on the drive should be retained and the drive was unmounted in error) or remove the drive. Then, run the `reformat_storage_block_devices.rb` command again.

> Some StorageGRID recovery procedures use Reaper to handle Cassandra repairs. Repairs occur automatically as soon as the related or required services have started. You might notice script output that mentions “reaper” or “Cassandra repair.” If you see an error message indicating the repair has failed, run the command indicated in the error message.

In the following example output, the drive `/dev/sdf` must be reformatted, and Cassandra did not need to be rebuilt:

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Storage services must be stopped before running this script.
Stop storage services [y/N]? **y**
Shutting down storage services.
Storage services stopped.
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? **y**
Successfully formatted /dev/sdf with UUID c817f87f-f989-4a21-
8f03-b6f42180063f
Skipping in use device /dev/sdg
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12075630
Cassandra does not need rebuilding.
Starting services.

Reformatting done.  Now do manual steps to
restore copies of data.
```

### Restore object data to storage volume where system drive is intact

After recovering a storage volume on a Storage Node where the system drive is intact, you can restore the object data that was lost when the storage volume failed.

#### What you'll need

- You must have confirmed that the recovered Storage Node has a Connection State of **Connected** on the **NODES** > **Overview** tab in the Grid Manager.

#### About this task

Object data can be restored from other Storage Nodes, an Archive Node, or a Cloud Storage Pool, assuming that the grid's ILM rules were configured such that object copies are available.

Note the following:

- If an ILM rule was configured to store only one replicated copy and that copy existed on a storage volume that failed, you will not be able to recover the object.
- If the only remaining copy of an object is in a Cloud Storage Pool, StorageGRID must issue multiple requests to the Cloud Storage Pool endpoint to restore object data. Before performing this procedure, contact technical support for help in estimating the recovery time frame and the associated costs.
- If the only remaining copy of an object is on an Archive Node, object data is retrieved from the Archive Node. Restoring object data to a Storage Node from an Archive Node takes longer than restoring copies from other Storage Nodes because of the latency associated with retrievals from external archival storage systems.

#### About the `repair-data` script

To restore object data, you run the `repair-data` script. This script begins the process of restoring object data and works with ILM scanning to ensure that ILM rules are met.

Select **Replicated data** or **Erasure-coded (EC) data** below to learn the different options for the `repair-data` script, based on whether you are restoring replicated data or erasure-coded data. If you need to restore both types of data, you must run both sets of commands.

> For more information about the `repair-data` script, enter `repair-data --help` from the command line of the primary Admin Node.

**Replicated data**

Two commands are available for restoring replicated data, based on whether you need to repair the entire node or only certain volumes on the node:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

You can track repairs of replicated data with this command:

```
repair-data show-replicated-repair-status
```

> The `show-replicated-repair-status` option is available for technical preview in StorageGRID 11.6. This feature is under development, and the value returned might be incorrect or delayed. To determine if a repair is complete, use **Awaiting – All**, **Repairs Attempted (XRPA)**, and **Scan Period — Estimated (XSCM)** as described in Monitor repairs.

**Erasure coded (EC) data**

Two commands are available for restoring erasure-coded data, based on whether you need to repair the entire node or only certain volumes on the node:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Repairs of erasure-coded data can begin while some Storage Nodes are offline. Repair will complete after all nodes are available.

You can track repairs of erasure-coded data with this command:

```
repair-data show-ec-repair-status
```

> The EC repair job temporarily reserves a large amount of storage. Storage alerts might be triggered, but will resolve when the repair is complete. If there is not enough storage for the reservation, the EC repair job will fail. Storage reservations are released when the EC repair job completes, whether the job failed or succeeded.

### Find hostname for Storage Node

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.

2. Use the `/etc/hosts` file to find the hostname of the Storage Node for the restored storage volumes. To see a list of all nodes in the grid, enter the following: `cat /etc/hosts`.

### Repair data if all volumes have failed

If all storage volumes have failed, repair the entire node. Follow the instructions for **replicated data**, **erasure-coded (EC) data**, or both, based on whether you use replicated data, erasure-coded (EC) data, or both.

If only some volumes have failed, go to Repair data if only some volumes have failed.

> You cannot run `repair-data` operations for more than one node at the same time. To recover multiple nodes, contact technical support.

#### Replicated data

If your grid includes replicated data, use the `repair-data start-replicated-node-repair` command with the `--nodes` option to repair the entire Storage Node.

This command repairs the replicated data on a Storage Node named SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> As object data is restored, the **Objects Lost** alert is triggered if the StorageGRID system cannot locate replicated object data. Alerts might be triggered on Storage Nodes throughout the system. You should determine the cause of the loss and if recovery is possible. See Monitor and troubleshoot.

#### Erasure coded (EC) data

If your grid contains erasure-coded data, use the `repair-data start-ec-node-repair` command with the `--nodes` option to repair the entire Storage Node.

This command repairs the erasure-coded data on a Storage Node named SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

The operation returns a unique `repair ID` that identifies this `repair_data` operation. Use this `repair ID` to track the progress and result of the `repair_data` operation. No other feedback is returned as the recovery process completes.

> Repairs of erasure-coded data can begin while some Storage Nodes are offline. Repair will complete after all nodes are available.

### Repair data if only some volumes have failed

If only some of the volumes have failed, repair the affected volumes. Follow the instructions for **replicated data**, **erasure-coded (EC) data**, or both, based on whether you use replicated data, erasure-coded (EC) data, or both.

If all volumes have failed, go to Repair data if all volumes have failed.

Enter the volume IDs in hexadecimal. For example, `0000` is the first volume and `000F` is the sixteenth volume.

You can specify one volume, a range of volumes, or multiple volumes that are not in a sequence.

All the volumes must be on the same Storage Node. If you need to restore volumes for more than one Storage Node, contact technical support.

#### Replicated data

If your grid contains replicated data, use the `start-replicated-volume-repair` command with the `--nodes` option to identify the node. Then add either the `--volumes` or `--volume-range` option, as shown in the following examples.

**Single volume**: This command restores replicated data to volume `0002` on a Storage Node named SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

**Range of volumes**: This command restores replicated data to all volumes in the range `0003` to `0009` on a Storage Node named SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

**Multiple volumes not in a sequence**: This command restores replicated data to volumes `0001`, `0005`, and `0008` on a Storage Node named SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> As object data is restored, the **Objects Lost** alert is triggered if the StorageGRID system cannot locate replicated object data. Alerts might be triggered on Storage Nodes throughout the system. You should determine the cause of the loss and if recovery is possible. See the instructions for monitoring and troubleshooting StorageGRID.

#### Erasure coded (EC) data

If your grid contains erasure-coded data, use the `start-ec-volume-repair` command with the `--nodes` option to identify the node. Then add either the `--volumes` or `--volume-range` option, as shown in the following examples.

**Single volume**: This command restores erasure-coded data to volume `0007` on a Storage Node named SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

**Range of volumes**: This command restores erasure-coded data to all volumes in the range `0004` to `0006` on a Storage Node named SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

**Multiple volumes not in a sequence**: This command restores erasure-coded data to volumes `000A`, `000C`, and `000E` on a Storage Node named SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

The `repair-data` operation returns a unique `repair ID` that identifies this `repair_data` operation. Use this `repair ID` to track the progress and result of the `repair_data` operation. No other feedback is returned as the recovery process completes.

> Repairs of erasure-coded data can begin while some Storage Nodes are offline. Repair will complete after all nodes are available.

### Monitor repairs

Monitor the status of the repair jobs, based on whether you use **replicated data**, **erasure-coded (EC) data**, or both.

**Replicated data**

- To determine if repairs are complete:
  1. Select **NODES** > ***Storage Node being repaired*** > **ILM**.
  2. Review the attributes in the Evaluation section. When repairs are complete, the **Awaiting - All** attribute indicates 0 objects.
- To monitor the repair in more detail:
  1. Select **SUPPORT** > **Tools** > **Grid topology**.
  2. Select ***grid*** > ***Storage Node being repaired*** > **LDR** > **Data Store**.
  3. Use a combination of the following attributes to determine, as well as possible, if replicated repairs are complete.

     > Cassandra inconsistencies might be present, and failed repairs are not tracked.

     - **Repairs Attempted (XRPA)**: Use this attribute to track the progress of replicated repairs. This attribute increases each time a Storage Node tries to repair a high-risk object. When this attribute does not increase for a period longer than the current scan period (provided by the **Scan Period — Estimated** attribute), it means that ILM scanning found no high-risk objects that need to be repaired on any nodes.

       > High-risk objects are objects that are at risk of being completely lost. This does not include objects that do not satisfy their ILM configuration.

     - **Scan Period — Estimated (XSCM)**: Use this attribute to estimate when a policy change will be applied to previously ingested objects. If the **Repairs Attempted** attribute does not increase for a period longer than the current scan period, it is probable that replicated repairs are done. Note that the scan period can change. The **Scan Period — Estimated (XSCM)** attribute applies to the entire grid and is the maximum of all node scan periods. You can query the **Scan Period — Estimated** attribute history for the grid to determine an appropriate time frame.
- Optionally, to get an estimated percent completion for the replicated repair, add the `show-replicated-repair-status` option to the repair-data command.

  ```
  repair-data show-replicated-repair-status
  ```

  > The `show-replicated-repair-status` option is available for technical preview in StorageGRID 11.6. This feature is under development, and the value returned might be incorrect or delayed. To determine if a repair is complete, use **Awaiting – All**, **Repairs Attempted (XRPA)**, and **Scan Period — Estimated (XSCM)** as described in Monitor repairs.

**Erasure coded (EC) data**

To monitor the repair of erasure-coded data and retry any requests that might have failed:

1. Determine the status of erasure-coded data repairs:
   - Select **SUPPORT** > **Tools** > **Metrics** to view the estimated time to completion and the completion percentage for the current job. Then, select **EC Overview** in the Grafana section. Look at the **Grid EC Job Estimated Time to Completion** and **Grid EC Job Percentage Completed** dashboards.

- Use this command to see the status of a specific `repair-data` operation:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Use this command to list all repairs:

  ```
  repair-data show-ec-repair-status
  ```

  The output lists information, including `repair ID`, for all previously and currently running repairs.

2. If the output shows that the repair operation failed, use the `--repair-id` option to retry the repair.

   This command retries a failed node repair, using the repair ID 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   This command retries a failed volume repair, using the repair ID 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

#### Check storage state after recovering storage volumes

After recovering storage volumes, you must verify that the desired state of the Storage Node is set to online and ensure that the state will be online by default whenever the Storage Node server is restarted.

**What you'll need**

- You must be signed in to the Grid Manager using a supported web browser.
- The Storage Node has been recovered, and data recovery is complete.

**Steps**

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Check the values of **Recovered Storage Node** > **LDR** > **Storage** > **Storage State — Desired** and **Storage State — Current**.

   The value of both attributes should be Online.

3. If the Storage State — Desired is set to Read-only, complete the following steps:
   a. Click the **Configuration** tab.
   b. From the **Storage State — Desired** drop-down list, select **Online**.
   c. Click **Apply Changes**.
   d. Click the **Overview** tab and confirm that the values of **Storage State — Desired** and **Storage State — Current** are updated to Online.

#### Recover from system drive failure

If the system drive on a software-based Storage Node has failed, the Storage Node is not available to the StorageGRID system. You must complete a specific set of tasks to

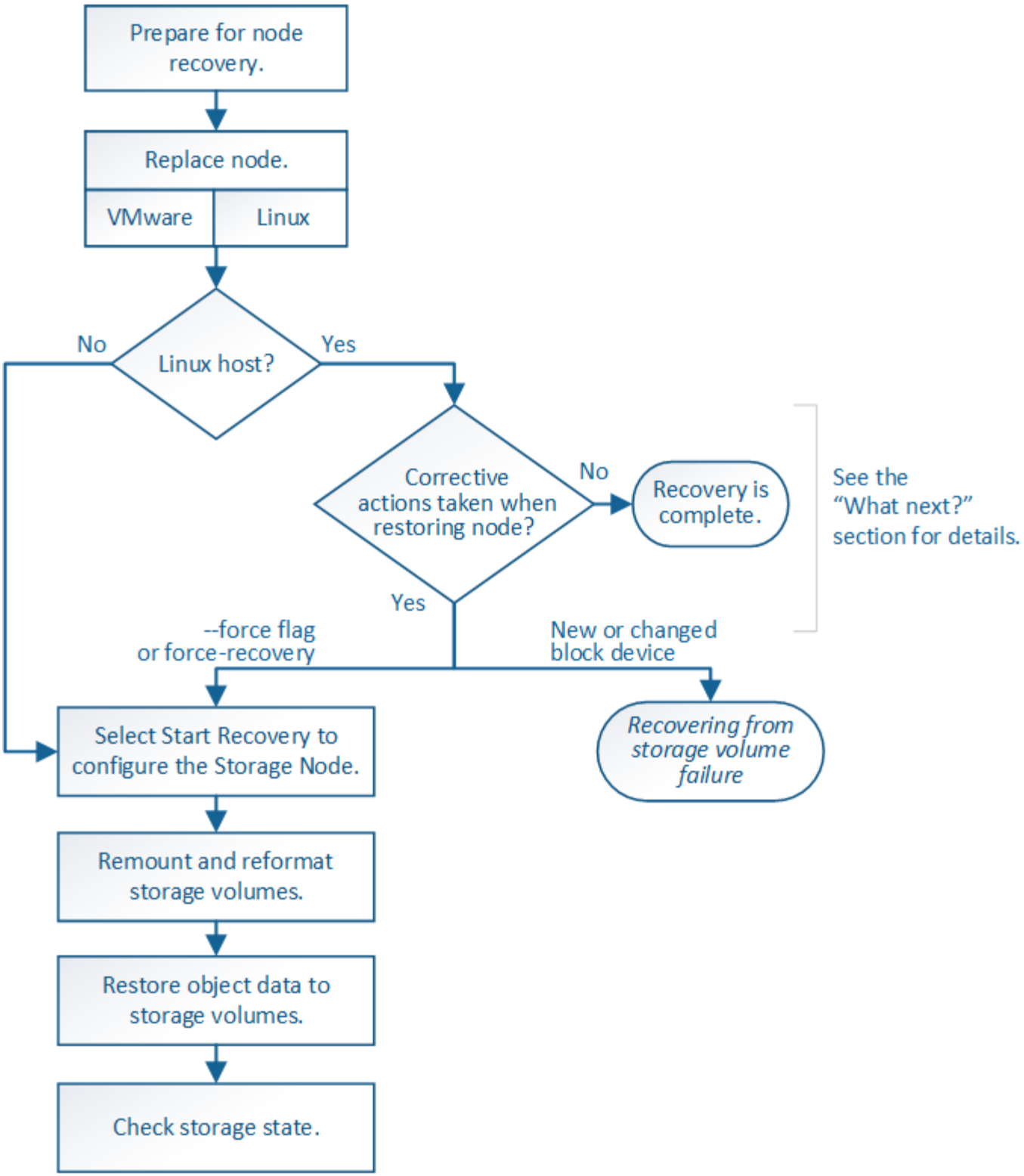
recover from a system drive failure.

**About this task**

Use this procedure to recover from a system drive failure on a software-based Storage Node. This procedure includes the steps to follow if any storage volumes also failed or cannot be remounted.

> This procedure applies to software-based Storage Nodes only. You must follow a different procedure to recover an appliance Storage Node.

Recover appliance Storage Node




**Review warnings for Storage Node system drive recovery**

Before recovering a failed system drive of a Storage Node, you must review the following warnings.

Storage Nodes have a Cassandra database that includes object metadata. The Cassandra database might be rebuilt in the following circumstances:

- A Storage Node is brought back online after having been offline for more than 15 days.
- A storage volume has failed and been recovered.
- The system drive and one or more storage volumes fails and is recovered.

When Cassandra is rebuilt, the system uses information from other Storage Nodes. If too many Storage Nodes are offline, some Cassandra data might not be available. If Cassandra has been rebuilt recently, Cassandra data might not yet be consistent across the grid. Data loss can occur if Cassandra is rebuilt when too many Storage Nodes are offline or if two or more Storage Nodes are rebuilt within 15 days of each other.

If more than one Storage Node has failed (or is offline), contact technical support. Do not perform the following recovery procedure. Data loss could occur.

If this is the second Storage Node failure in less than 15 days after a Storage Node failure or recovery, contact technical support. Rebuilding Cassandra on two or more Storage Nodes within 15 days can result in data loss.

If more than one Storage Node at a site has failed, a site recovery procedure might be required. Contact technical support.

How site recovery is performed by technical support

If this Storage Node is in read-only maintenance mode to allow for the retrieval of objects by another Storage Node with failed storage volumes, recover volumes on the Storage Node with failed storage volumes before recovering this failed Storage Node. See the instructions for recovering from loss of storage volumes where the system drive is intact.

If ILM rules are configured to store only one replicated copy and the copy exists on a storage volume that has failed, you will not be able to recover the object.

If you encounter a Services: Status - Cassandra (SVST) alarm during recovery, see the monitoring and troubleshooting instructions to recover from the alarm by rebuilding Cassandra. After Cassandra is rebuilt, alarms should clear. If alarms do not clear, contact technical support.

**Related information**

Monitor and troubleshoot

Warnings and considerations for grid node recovery

Recover from storage volume failure where system drive is intact

**Replace the Storage Node**

## If the system drive has failed, you must first replace the Storage Node.

You must select the node replacement procedure for your platform. The steps to replace a node are the same for all types of grid nodes.

This procedure applies to software-based Storage Nodes only. You must follow a different procedure to recover an appliance Storage Node.

Recover appliance Storage Node

**Linux:** If you are not sure if your system drive has failed, follow the instructions to replace the node to determine which recovery steps are required.

| Platform | Procedure |
| --- | --- |
| VMware | Replace a VMware node |
| Linux | Replace a Linux node |
| OpenStack | NetApp-provided virtual machine disk files and scripts for OpenStack are no longer supported for recovery operations. If you need to recover a node running in an OpenStack deployment, download the files for your Linux operating system. Then, follow the procedure for replacing a Linux node. |

### Select Start Recovery to configure Storage Node

After replacing a Storage Node, you must select Start Recovery in the Grid Manager to configure the new node as a replacement for the failed node.

#### What you'll need

- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Maintenance or Root Access permission.
- You must have the provisioning passphrase.
- You must have deployed and configured the replacement node.
- You must know the start date of any repair jobs for erasure-coded data.
- You must have verified that the Storage Node has not been rebuilt within the last 15 days.

#### About this task

If the Storage Node is installed as a container on a Linux host, you must perform this step only if one of these is true:

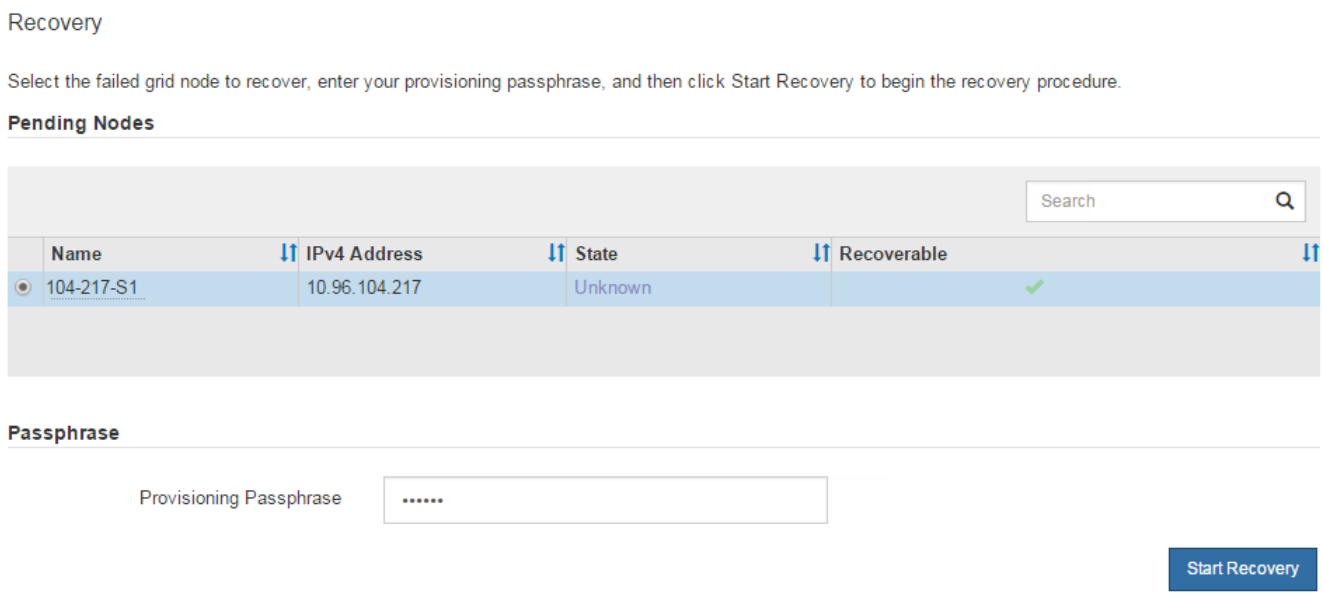
- You had to use the `--force` flag to import the node, or you issued `storagegrid node force-recovery` *`node-name`*
- You had to do a full node reinstall, or you needed to restore /var/local.

#### Steps

1. From the Grid Manager, select **MAINTENANCE** > **Tasks** > **Recovery**.
2. Select the grid node you want to recover in the Pending Nodes list.

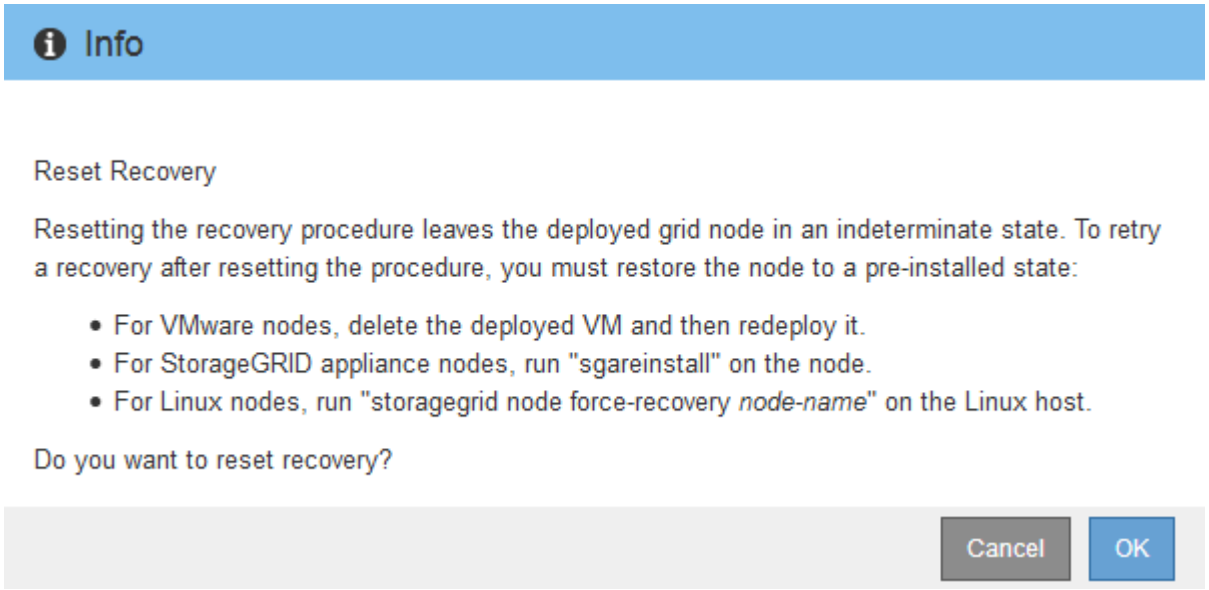
   Nodes appear in the list after they fail, but you cannot select a node until it has been reinstalled and is ready for recovery.

3. Enter the **Provisioning Passphrase**.
4. Click **Start Recovery**.




5. Monitor the progress of the recovery in the Recovering Grid Node table.

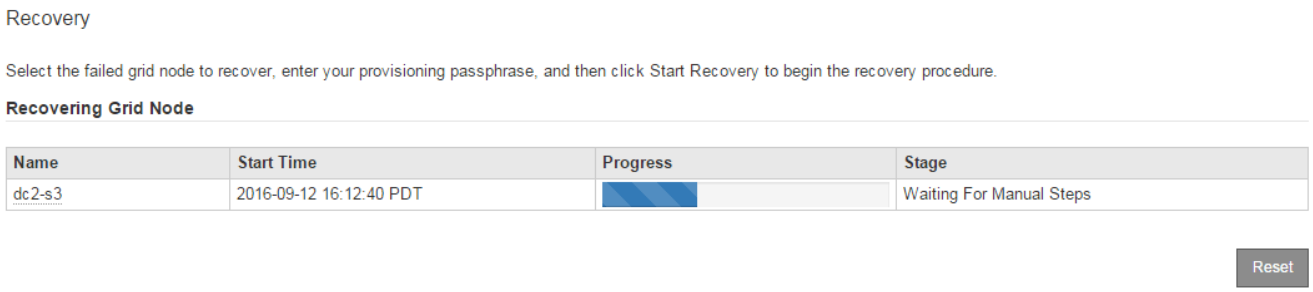
> While the recovery procedure is running, you can click **Reset** to start a new recovery. An Info dialog box appears, indicating that the node will be left in an indeterminate state if you reset the procedure.




If you want to retry the recovery after resetting the procedure, you must restore the node to a pre-installed state, as follows:

- **VMware**: Delete the deployed virtual grid node. Then, when you are ready to restart the recovery, redeploy the node.
- **Linux**: Restart the node by running this command on the Linux host: `storagegrid node force-recovery node-name`

6. When the Storage Node reaches the stage “Waiting for Manual Steps” stage, go to the next task in the recovery procedure to remount and reformat storage volumes.




### Related information

Prepare appliance for reinstallation (platform replacement only)

## Remount and reformat storage volumes (“Manual Steps”)

You must manually run two scripts to remount preserved storage volumes and to reformat any failed storage volumes. The first script remounts volumes that are properly formatted as StorageGRID storage volumes. The second script reformats any unmounted volumes, rebuilds Cassandra, if needed, and starts services.

### What you’ll need

- You have already replaced the hardware for any failed storage volumes that you know require replacement.

  Running the `sn-remount-volumes` script might help you identify additional failed storage volumes.

- You have checked that a Storage Node decommissioning is not in progress, or you have paused the node decommission procedure. (In the Grid Manager, select **MAINTENANCE** > **Tasks** > **Decommission**.)
- You have checked that an expansion is not in progress. (In the Grid Manager, select **MAINTENANCE** > **Tasks** > **Expansion**.)
- You have reviewed the warnings for Storage Node system drive recovery.

> Contact technical support if more than one Storage Node is offline or if a Storage Node in this grid has been rebuilt in the last 15 days. Do not run the `sn-recovery-postinstall.sh` script. Rebuilding Cassandra on two or more Storage Nodes within 15 days of each other might result in data loss.

### About this task

To complete this procedure, you perform these high-level tasks:

- Log in to the recovered Storage Node.
- Run the `sn-remount-volumes` script to remount properly formatted storage volumes. When this script runs, it does the following:
  - Mounts and unmounts each storage volume to replay the XFS journal.
  - Performs an XFS file consistency check.
  - If the file system is consistent, determines if the storage volume is a properly formatted StorageGRID storage volume.
  - If the storage volume is properly formatted, remounts the storage volume. Any existing data on the

volume remains intact.

- Review the script output and resolve any issues.
- Run the `sn-recovery-postinstall.sh` script. When this script runs, it does the following.

> Do not reboot a Storage Node during recovery before running `sn-recovery-postinstall.sh` to reformat the failed storage volumes and restore object metadata. Rebooting the Storage Node before `sn-recovery-postinstall.sh` completes causes errors for services that attempt to start and causes StorageGRID appliance nodes to exit maintenance mode. See the step for post-install script.

  - Reformats any storage volumes that the `sn-remount-volumes` script could not mount or that were found to be improperly formatted.

    > If a storage volume is reformatted, any data on that volume is lost. You must perform an additional procedure to restore object data from other locations in the grid, assuming that ILM rules were configured to store more than one object copy.

  - Rebuilds the Cassandra database on the node, if needed.
  - Starts the services on the Storage Node.

**Steps**

1. Log in to the recovered Storage Node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Run the first script to remount any properly formatted storage volumes.

   > If all storage volumes are new and need to be formatted, or if all storage volumes have failed, you can skip this step and run the second script to reformat all unmounted storage volumes.

   a. Run the script: `sn-remount-volumes`

      This script might take hours to run on storage volumes that contain data.

   b. As the script runs, review the output and answer any prompts.

      > As required, you can use the `tail -f` command to monitor the contents of the script's log file (`/var/local/log/sn-remount-volumes.log`) . The log file contains more detailed information than the command line output.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740
```

```
====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
```

```
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

In the example output, one storage volume was remounted successfully and three storage volumes had errors.

- `/dev/sdb` passed the XFS file system consistency check and had a valid volume structure, so it was remounted successfully. Data on devices that are remounted by the script is preserved.
- `/dev/sdc` failed the XFS file system consistency check because the storage volume was new or corrupt.

- `/dev/sdd` could not be mounted because the disk was uninitialized or the disk's superblock was corrupted. When the script cannot mount a storage volume, it asks if you want to run the file system consistency check.
  - If the storage volume is attached to a new disk, answer **N** to the prompt. You do not need check the file system on a new disk.
  - If the storage volume is attached to an existing disk, answer **Y** to the prompt. You can use the results of the file system check to determine the source of the corruption. The results are saved in the `/var/local/log/sn-remount-volumes.log` log file.
- `/dev/sde` passed the XFS file system consistency check and had a valid volume structure; however, the LDR node ID in the volID file did not match the ID for this Storage Node (the `configured LDR noid` displayed at the top). This message indicates that this volume belongs to another Storage Node.

3. Review the script output and resolve any issues.

> If a storage volume failed the XFS file system consistency check or could not be mounted, carefully review the error messages in the output. You must understand the implications of running the `sn-recovery-postinstall.sh` script on these volumes.

a. Check to make sure that the results include an entry for all of the volumes you expected. If any volumes are not listed, rerun the script.

b. Review the messages for all mounted devices. Make sure there are no errors indicating that a storage volume does not belong to this Storage Node.

   In the example, the output for `/dev/sde` includes the following error message:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> If a storage volume is reported as belonging to another Storage Node, contact technical support. If you run the `sn-recovery-postinstall.sh` script, the storage volume will be reformatted, which might cause data loss.

c. If any storage devices could not be mounted, make a note of the device name, and repair or replace the device.

> You must repair or replace any storage devices that could not be mounted.

   You will use the device name to look up the volume ID, which is required input when you run the `repair-data` script to restore object data to the volume (the next procedure).

d. After repairing or replacing all unmountable devices, run the `sn-remount-volumes` script again to confirm that all storage volumes that can be remounted have been remounted.

> If a storage volume cannot be mounted or is improperly formatted, and you continue to the next step, the volume and any data on the volume will be deleted. If you had two copies of object data, you will have only a single copy until you complete the next procedure (restoring object data).

> Do not run the `sn-recovery-postinstall.sh` script if you believe that the data remaining on a failed storage volume cannot be rebuilt from elsewhere in the grid (for example, if your ILM policy uses a rule that makes only one copy or if volumes have failed on multiple nodes). Instead, contact technical support to determine how to recover your data.

4. Run the `sn-recovery-postinstall.sh` script: `sn-recovery-postinstall.sh`

   This script reformats any storage volumes that could not be mounted or that were found to be improperly formatted; rebuilds the Cassandra database on the node, if needed; and starts the services on the Storage Node.

   Be aware of the following:

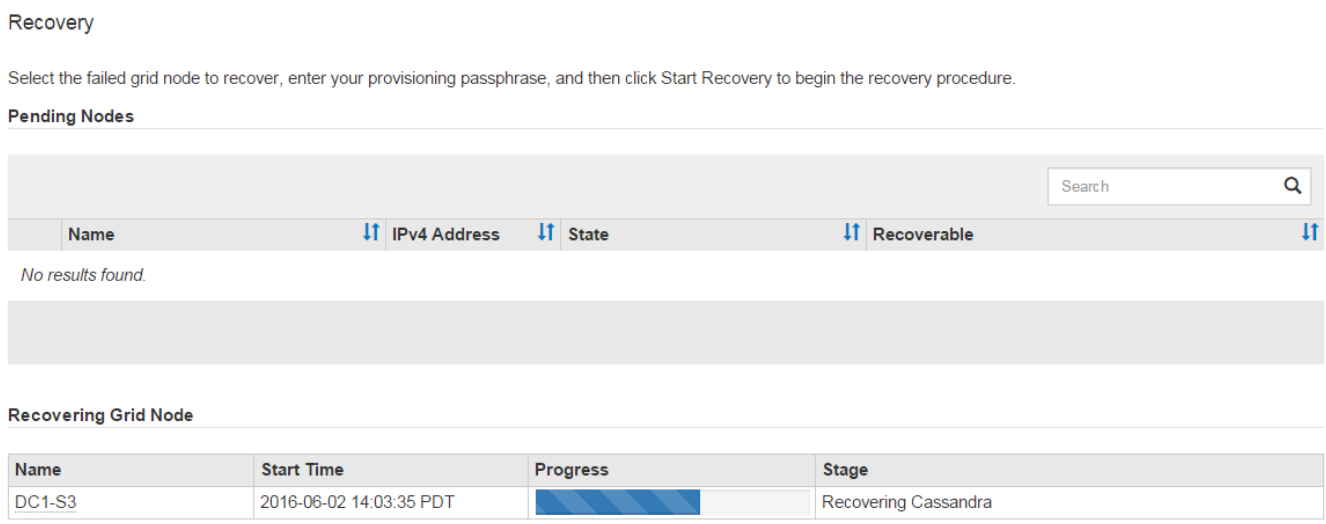
   - The script might take hours to run.
   - In general, you should leave the SSH session alone while the script is running.
   - Do not press **Ctrl+C** while the SSH session is active.
   - The script will run in the background if a network disruption occurs and terminates the SSH session, but you can view the progress from the Recovery page.
   - If the Storage Node uses the RSM service, the script might appear to stall for 5 minutes as node services are restarted. This 5-minute delay is expected whenever the RSM service boots for the first time.

     > The RSM service is present on Storage Nodes that include the ADC service.

   > Some StorageGRID recovery procedures use Reaper to handle Cassandra repairs. Repairs occur automatically as soon as the related or required services have started. You might notice script output that mentions “reaper” or “Cassandra repair.” If you see an error message indicating the repair has failed, run the command indicated in the error message.

5. As the `sn-recovery-postinstall.sh` script runs, monitor the Recovery page in the Grid Manager.

   The Progress bar and the Stage column on the Recovery page provide a high-level status of the `sn-recovery-postinstall.sh` script.



After the `sn-recovery-postinstall.sh` script has started services on the node, you can restore object data to any storage volumes that were formatted by the script, as described in that procedure.

**Related information**

Review warnings for Storage Node system drive recovery

Restore object data to storage volume, if required

### Restore object data to storage volume, if required

If the `sn-recovery-postinstall.sh` script is needed to reformat one or more failed storage volumes, you must restore object data to the reformatted storage volume from other Storage Nodes and Archive Nodes. These steps are not required unless one or more storage volumes were reformatted.

**What you'll need**

- You must have confirmed that the recovered Storage Node has a Connection State of **Connected** on the **NODES** > **Overview** tab in the Grid Manager.

**About this task**

Object data can be restored from other Storage Nodes, an Archive Node, or a Cloud Storage Pool, assuming that the grid's ILM rules were configured such that object copies are available.

Note the following:

- If an ILM rule was configured to store only one replicated copy and that copy existed on a storage volume that failed, you will not be able to recover the object.
- If the only remaining copy of an object is in a Cloud Storage Pool, StorageGRID must issue multiple requests to the Cloud Storage Pool endpoint to restore object data. Before performing this procedure, contact technical support for help in estimating the recovery time frame and the associated costs.
- If the only remaining copy of an object is on an Archive Node, object data is retrieved from the Archive Node. Restoring object data to a Storage Node from an Archive Node takes longer than restoring copies from other Storage Nodes because of the latency associated with retrievals from external archival storage systems.

**About the `repair-data` script**

To restore object data, you run the `repair-data` script. This script begins the process of restoring object data and works with ILM scanning to ensure that ILM rules are met.

Select **Replicated data** or **Erasure-coded (EC) data** below to learn the different options for the `repair-data` script, based on whether you are restoring replicated data or erasure-coded data. If you need to restore both types of data, you must run both sets of commands.

> For more information about the `repair-data` script, enter `repair-data --help` from the command line of the primary Admin Node.

**Replicated data**

Two commands are available for restoring replicated data, based on whether you need to repair the entire node or only certain volumes on the node:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

You can track repairs of replicated data with this command:

```
repair-data show-replicated-repair-status
```

> The `show-replicated-repair-status` option is available for technical preview in StorageGRID 11.6. This feature is under development, and the value returned might be incorrect or delayed. To determine if a repair is complete, use **Awaiting – All**, **Repairs Attempted (XRPA)**, and **Scan Period — Estimated (XSCM)** as described in Monitor repairs.

**Erasure coded (EC) data**

Two commands are available for restoring erasure-coded data, based on whether you need to repair the entire node or only certain volumes on the node:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Repairs of erasure-coded data can begin while some Storage Nodes are offline. Repair will complete after all nodes are available.

You can track repairs of erasure-coded data with this command:

```
repair-data show-ec-repair-status
```

> The EC repair job temporarily reserves a large amount of storage. Storage alerts might be triggered, but will resolve when the repair is complete. If there is not enough storage for the reservation, the EC repair job will fail. Storage reservations are released when the EC repair job completes, whether the job failed or succeeded.

### Find hostname for Storage Node

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.

2. Use the `/etc/hosts` file to find the hostname of the Storage Node for the restored storage volumes. To see a list of all nodes in the grid, enter the following: `cat /etc/hosts`.

### Repair data if all volumes have failed

If all storage volumes have failed, repair the entire node. Follow the instructions for **replicated data**, **erasure-coded (EC) data**, or both, based on whether you use replicated data, erasure-coded (EC) data, or both.

If only some volumes have failed, go to Repair data if only some volumes have failed.

> You cannot run `repair-data` operations for more than one node at the same time. To recover multiple nodes, contact technical support.

#### Replicated data

If your grid includes replicated data, use the `repair-data start-replicated-node-repair` command with the `--nodes` option to repair the entire Storage Node.

This command repairs the replicated data on a Storage Node named SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> As object data is restored, the **Objects Lost** alert is triggered if the StorageGRID system cannot locate replicated object data. Alerts might be triggered on Storage Nodes throughout the system. You should determine the cause of the loss and if recovery is possible. See Monitor and troubleshoot.

#### Erasure coded (EC) data

If your grid contains erasure-coded data, use the `repair-data start-ec-node-repair` command with the `--nodes` option to repair the entire Storage Node.

This command repairs the erasure-coded data on a Storage Node named SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

The operation returns a unique `repair ID` that identifies this `repair_data` operation. Use this `repair ID` to track the progress and result of the `repair_data` operation. No other feedback is returned as the recovery process completes.

> Repairs of erasure-coded data can begin while some Storage Nodes are offline. Repair will complete after all nodes are available.

### Repair data if only some volumes have failed

If only some of the volumes have failed, repair the affected volumes. Follow the instructions for **replicated data**, **erasure-coded (EC) data**, or both, based on whether you use replicated data, erasure-coded (EC) data, or both.

If all volumes have failed, go to Repair data if all volumes have failed.

Enter the volume IDs in hexadecimal. For example, `0000` is the first volume and `000F` is the sixteenth volume.

You can specify one volume, a range of volumes, or multiple volumes that are not in a sequence.

All the volumes must be on the same Storage Node. If you need to restore volumes for more than one Storage Node, contact technical support.

#### Replicated data

If your grid contains replicated data, use the `start-replicated-volume-repair` command with the `--nodes` option to identify the node. Then add either the `--volumes` or `--volume-range` option, as shown in the following examples.

**Single volume**: This command restores replicated data to volume `0002` on a Storage Node named SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

**Range of volumes**: This command restores replicated data to all volumes in the range `0003` to `0009` on a Storage Node named SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

**Multiple volumes not in a sequence**: This command restores replicated data to volumes `0001`, `0005`, and `0008` on a Storage Node named SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> As object data is restored, the **Objects Lost** alert is triggered if the StorageGRID system cannot locate replicated object data. Alerts might be triggered on Storage Nodes throughout the system. You should determine the cause of the loss and if recovery is possible. See the instructions for monitoring and troubleshooting StorageGRID.

#### Erasure coded (EC) data

If your grid contains erasure-coded data, use the `start-ec-volume-repair` command with the `--nodes` option to identify the node. Then add either the `--volumes` or `--volume-range` option, as shown in the following examples.

**Single volume**: This command restores erasure-coded data to volume `0007` on a Storage Node named SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

**Range of volumes**: This command restores erasure-coded data to all volumes in the range `0004` to `0006` on a Storage Node named SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

**Multiple volumes not in a sequence**: This command restores erasure-coded data to volumes `000A`, `000C`, and `000E` on a Storage Node named SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

The `repair-data` operation returns a unique `repair ID` that identifies this `repair_data` operation. Use this `repair ID` to track the progress and result of the `repair_data` operation. No other feedback is returned as the recovery process completes.

> Repairs of erasure-coded data can begin while some Storage Nodes are offline. Repair will complete after all nodes are available.

### Monitor repairs

Monitor the status of the repair jobs, based on whether you use **replicated data**, **erasure-coded (EC) data**, or both.

**Replicated data**

- To determine if repairs are complete:
  1. Select **NODES** > ***Storage Node being repaired*** > **ILM**.
  2. Review the attributes in the Evaluation section. When repairs are complete, the **Awaiting - All** attribute indicates 0 objects.
- To monitor the repair in more detail:
  1. Select **SUPPORT** > **Tools** > **Grid topology**.
  2. Select ***grid*** > ***Storage Node being repaired*** > **LDR** > **Data Store**.
  3. Use a combination of the following attributes to determine, as well as possible, if replicated repairs are complete.

     Cassandra inconsistencies might be present, and failed repairs are not tracked.

     - **Repairs Attempted (XRPA)**: Use this attribute to track the progress of replicated repairs. This attribute increases each time a Storage Node tries to repair a high-risk object. When this attribute does not increase for a period longer than the current scan period (provided by the **Scan Period — Estimated** attribute), it means that ILM scanning found no high-risk objects that need to be repaired on any nodes.

       High-risk objects are objects that are at risk of being completely lost. This does not include objects that do not satisfy their ILM configuration.

     - **Scan Period — Estimated (XSCM)**: Use this attribute to estimate when a policy change will be applied to previously ingested objects. If the **Repairs Attempted** attribute does not increase for a period longer than the current scan period, it is probable that replicated repairs are done. Note that the scan period can change. The **Scan Period — Estimated (XSCM)** attribute applies to the entire grid and is the maximum of all node scan periods. You can query the **Scan Period — Estimated** attribute history for the grid to determine an appropriate time frame.
- Optionally, to get an estimated percent completion for the replicated repair, add the `show-replicated-repair-status` option to the repair-data command.

  ```
  repair-data show-replicated-repair-status
  ```

  The `show-replicated-repair-status` option is available for technical preview in StorageGRID 11.6. This feature is under development, and the value returned might be incorrect or delayed. To determine if a repair is complete, use **Awaiting – All**, **Repairs Attempted (XRPA)**, and **Scan Period — Estimated (XSCM)** as described in Monitor repairs.

**Erasure coded (EC) data**

To monitor the repair of erasure-coded data and retry any requests that might have failed:

1. Determine the status of erasure-coded data repairs:
   - Select **SUPPORT** > **Tools** > **Metrics** to view the estimated time to completion and the completion percentage for the current job. Then, select **EC Overview** in the Grafana section. Look at the **Grid EC Job Estimated Time to Completion** and **Grid EC Job Percentage Completed** dashboards.

- Use this command to see the status of a specific `repair-data` operation:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Use this command to list all repairs:

  ```
  repair-data show-ec-repair-status
  ```

  The output lists information, including `repair ID`, for all previously and currently running repairs.

2. If the output shows that the repair operation failed, use the `--repair-id` option to retry the repair.

   This command retries a failed node repair, using the repair ID 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   This command retries a failed volume repair, using the repair ID 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

#### Check storage state after recovering Storage Node system drive

After recovering the system drive for a Storage Node, you must verify that the desired state of the Storage Node is set to online and ensure that the state will be online by default whenever the Storage Node server is restarted.

**What you'll need**

- You must be signed in to the Grid Manager using a supported web browser.
- The Storage Node has been recovered, and data recovery is complete.

**Steps**

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Check the values of **Recovered Storage Node** > **LDR** > **Storage** > **Storage State — Desired** and **Storage State — Current**.

   The value of both attributes should be Online.

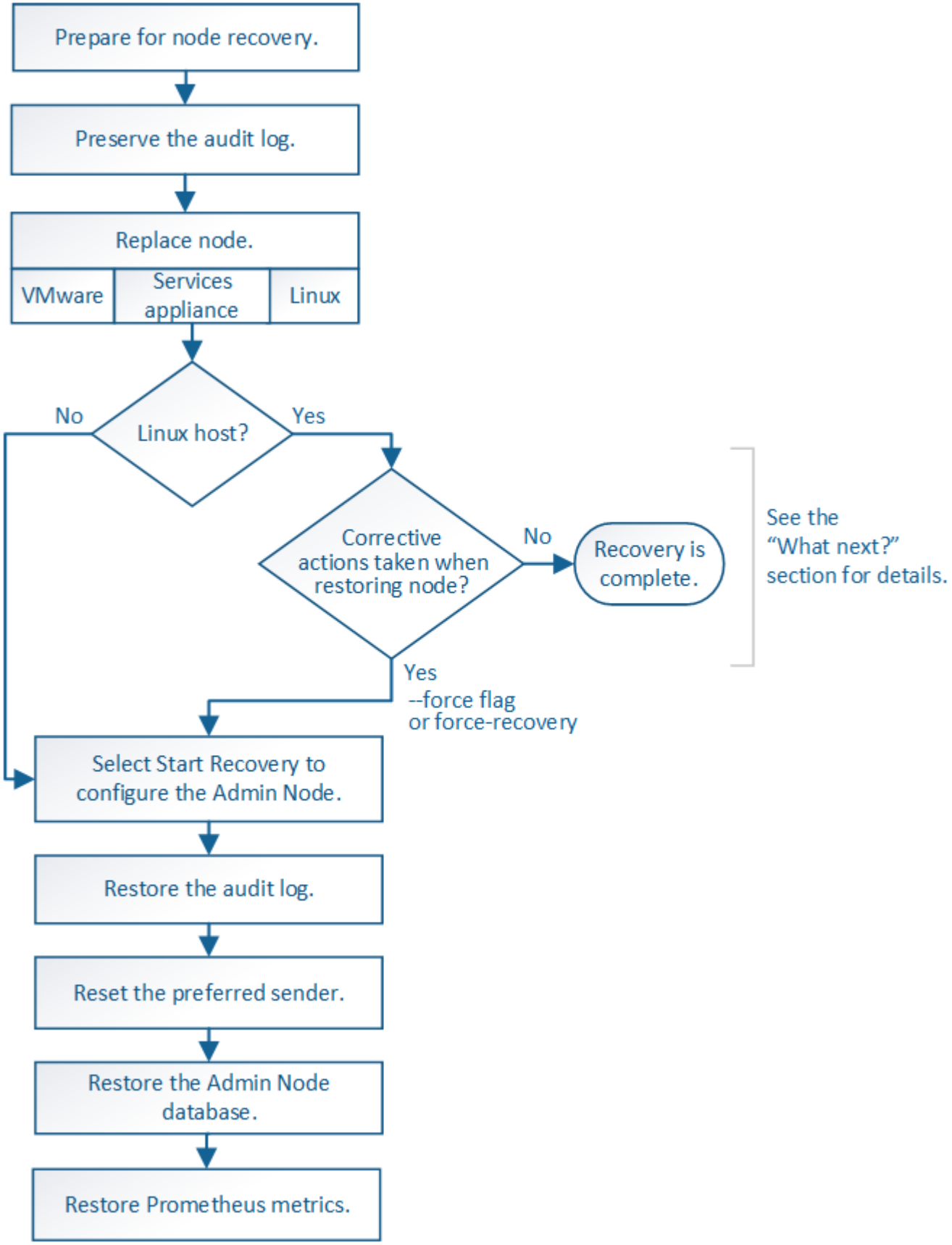
3. If the Storage State — Desired is set to Read-only, complete the following steps:
   a. Click the **Configuration** tab.
   b. From the **Storage State — Desired** drop-down list, select **Online**.
   c. Click **Apply Changes**.
   d. Click the **Overview** tab and confirm that the values of **Storage State — Desired** and **Storage State — Current** are updated to Online.

#### Recover from Admin Node failures

The recovery process for an Admin Node depends on whether it is the primary Admin Node or a non-primary Admin Node.

**About this task**

The high-level steps for recovering a primary or non-primary Admin Node are the same, although the details of the steps differ.



Always follow the correct recovery procedure for the Admin Node you are recovering. The procedures look the same at a high level, but differ in the details.

**Related information**

SG100 and SG1000 services appliances

**Choices**

- Recover from primary Admin Node failures
- Recover from non-primary Admin Node failures

#### Recover from primary Admin Node failures

You must complete a specific set of tasks to recover from a primary Admin Node failure. The primary Admin Node hosts the Configuration Management Node (CMN) service for the grid.

**About this task**

A failed primary Admin Node should be replaced promptly. The Configuration Management Node (CMN) service on the primary Admin Node is responsible for issuing blocks of object identifiers for the grid. These identifiers are assigned to objects as they are ingested. New objects cannot be ingested unless there are identifiers available. Object ingest can continue while the CMN is unavailable because approximately one month's supply of identifiers is cached in the grid. However, after cached identifiers are exhausted, no new objects can be added.

> You must repair or replace a failed primary Admin Node within approximately a month or the grid might lose its ability to ingest new objects. The exact time period depends on your rate of object ingest: if you need a more accurate assessment of the time frame for your grid, contact technical support.

**Copy audit logs from failed primary Admin Node**

If you are able to copy audit logs from the failed primary Admin Node, you should preserve them to maintain the grid's record of system activity and usage. You can restore the preserved audit logs to the recovered primary Admin Node after it is up and running.

This procedure copies the audit log files from the failed Admin Node to a temporary location on a separate grid node. These preserved audit logs can then be copied to the replacement Admin Node. Audit logs are not automatically copied to the new Admin Node.

Depending on the type of failure, you might not be able to copy audit logs from a failed Admin Node. If the deployment has only one Admin Node, the recovered Admin Node starts recording events to the audit log in a new empty file and previously recorded data is lost. If the deployment includes more than one Admin Node, you can recover the audit logs from another Admin Node.

> If the audit logs are not accessible on the failed Admin Node now, you might be able to access them later, for example, after host recovery.

1. Log in to the failed Admin Node if possible. Otherwise, log in to the primary Admin Node or another Admin Node, if available.
   a. Enter the following command: `ssh admin@grid_node_IP`

b. Enter the password listed in the `Passwords.txt` file.

c. Enter the following command to switch to root: `su -`

d. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

2. Stop the AMS service to prevent it from creating a new log file:`service ams stop`

3. Rename the audit.log file so that it does not overwrite the existing file when you copy it to the recovered Admin Node.

   Rename audit.log to a unique numbered file name such as yyyy-mm-dd.txt.1. For example, you can rename the audit.log file to 2015-10-25.txt.1`cd /var/local/audit/exportls -l``mv audit.log 2015-10-25.txt.1`

4. Restart the AMS service: `service ams start`

5. Create the directory to copy all audit log files to a temporary location on a separate grid node: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   When prompted, enter the password for admin.

6. Copy all audit log files: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   When prompted, enter the password for admin.

7. Log out as root: `exit`

#### Replace primary Admin Node

To recover a primary Admin Node, you must first replace the physical or virtual hardware.

You can replace a failed primary Admin Node with a primary Admin Node running on the same platform, or you can replace a primary Admin Node running on VMware or a Linux host with a primary Admin Node hosted on a services appliance.

Use the procedure that matches the replacement platform you select for the node. After you complete the node replacement procedure (which is suitable for all node types), that procedure will direct you to the next step for primary Admin Node recovery.

| Replacement platform | Procedure |
|---|---|
| VMware | Replace a VMware node |
| Linux | Replace a Linux node |
| SG100 and SG1000 services appliances | Replace a services appliance |

| Replacement platform | Procedure |
| --- | --- |
| OpenStack | NetApp-provided virtual machine disk files and scripts for OpenStack are no longer supported for recovery operations. If you need to recover a node running in an OpenStack deployment, download the files for your Linux operating system. Then, follow the procedure for replacing a Linux node. |

### Configure replacement primary Admin Node

The replacement node must be configured as the primary Admin Node for your StorageGRID system.

#### What you'll need

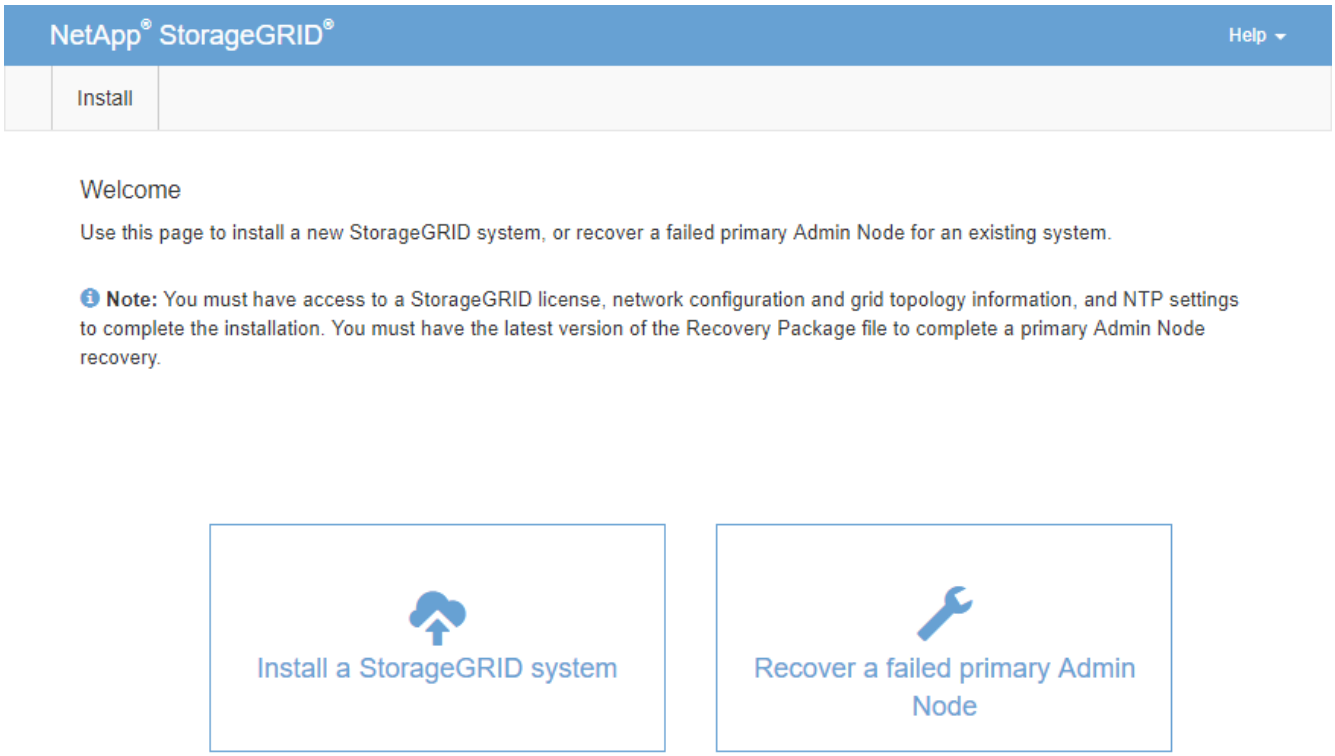
- For primary Admin Nodes hosted on virtual machines, the virtual machine must be deployed, powered on, and initialized.
- For primary Admin Nodes hosted on a services appliance, you have replaced the appliance and have installed software. See the installation guide for your appliance.

  SG100 and SG1000 services appliances

- You must have the latest backup of the Recovery Package file (`sgws-recovery-package-`*`id-revision`*`.zip`).
- You must have the provisioning passphrase.

#### Steps

1. Open your web browser and navigate to `https://primary_admin_node_ip`.



2. Click **Recover a failed primary Admin Node**.
3. Upload the most recent backup of the Recovery Package:
   a. Click **Browse**.
   b. Locate the most recent Recovery Package file for your StorageGRID system, and click **Open**.
4. Enter the provisioning passphrase.
5. Click **Start Recovery**.

   The recovery process begins. The Grid Manager might become unavailable for a few minutes as the required services start. When the recovery is complete, the sign in page is displayed.

6. If single sign-on (SSO) is enabled for your StorageGRID system and the relying party trust for the Admin Node you recovered was configured to use the default management interface certificate, update (or delete and recreate) the node's relying party trust in Active Directory Federation Services (AD FS). Use the new default server certificate that was generated during the Admin Node recovery process.

   > To configure a relying party trust, see the instructions for administering StorageGRID. To access the default server certificate, log in to the command shell of the Admin Node. Go to the `/var/local/mgmt-api` directory, and select the `server.crt` file.

7. Determine if you need to apply a hotfix.
   a. Sign in to the Grid Manager using a supported web browser.
   b. Select **NODES**.
   c. From the list on the left, select the primary Admin Node.
   d. On the Overview tab, note the version displayed in the **Software Version** field.
   e. Select any other grid node.
   f. On the Overview tab, note the version displayed in the **Software Version** field.
      - If the versions displayed in the **Software Version** fields are the same, you do not need to apply a hotfix.
      - If the versions displayed in the **Software Version** fields are different, you must apply a hotfix to update the recovered primary Admin Node to the same version.

**Related information**

Administer StorageGRID

StorageGRID hotfix procedure

### Restore audit log on recovered primary Admin Node

If you were able to preserve the audit log from the failed primary Admin Node, you can copy it to the primary Admin Node you are recovering.

- The recovered Admin Node must be installed and running.
- You must have copied the audit logs to another location after the original Admin Node failed.

If an Admin Node fails, audit logs saved to that Admin Node are potentially lost. It might be possible to preserve data from loss by copying audit logs from the failed Admin Node and then restoring these audit logs to the recovered Admin Node. Depending on the failure, it might not be possible to copy audit logs from the

failed Admin Node. In that case, if the deployment has more than one Admin Node, you can recover audit logs from another Admin Node as audit logs are replicated to all Admin Nodes.

If there is only one Admin Node and the audit log cannot be copied from the failed node, the recovered Admin Node starts recording events to the audit log as if the installation is new.

You must recover an Admin Node as soon as possible to restore logging functionality.

> By default, audit information is sent to the audit log on Admin Nodes. You can skip these steps if either of the following applies:
>
> - You configured an external syslog server and audit logs are now being sent to the syslog server instead of to Admin Nodes.
> - You explicitly specified that audit messages should be saved only on the local nodes that generated them.
>
> See Configure audit messages and log destinations for details.

**Steps**

1. Log in to the recovered Admin Node:

   a. Enter the following command: `ssh admin@recovery_Admin_Node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   After you are logged in as root, the prompt changes from `$` to `#`.

2. Check which audit files have been preserved: `cd /var/local/audit/export`

3. Copy the preserved audit log files to the recovered Admin Node: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   When prompted, enter the password for admin.

4. For security, delete the audit logs from the failed grid node after verifying that they have been copied successfully to the recovered Admin Node.

5. Update the user and group settings of the audit log files on the recovered Admin Node: `chown ams-user:bycast *`

6. Log out as root: `exit`

You must also restore any pre-existing client access to the audit share. For more information, see the instructions for administering StorageGRID.

**Related information**

Administer StorageGRID

**Reset preferred sender on recovered primary Admin Node**

If the primary Admin Node you are recovering is currently set as the preferred sender of alert notifications, alarm notifications, and AutoSupport messages, you must reconfigure

this setting.

**What you'll need**

- You must be signed in to the Grid Manager using a supported web browser.
- You must have specific access permissions.
- The recovered Admin Node must be installed and running.

**Steps**

1. Select **CONFIGURATION** > **System** > **Display options**.
2. Select the recovered Admin Node from the **Preferred Sender** drop-down list.
3. Click **Apply Changes**.

**Related information**

Administer StorageGRID

### Restore Admin Node database when recovering primary Admin Node

If you want to retain the historical information about attributes, alarms, and alerts on a primary Admin Node that has failed, you can restore the Admin Node database. You can only restore this database if your StorageGRID system includes another Admin Node.

- The recovered Admin Node must be installed and running.
- The StorageGRID system must include at least two Admin Nodes.
- You must have the `Passwords.txt` file.
- You must have the provisioning passphrase.

If an Admin Node fails, the historical information stored in its Admin Node database is lost. This database includes the following information:

- Alert history
- Alarm history
- Historical attribute data, which is used in the charts and text reports available from the **SUPPORT** > **Tools** > **Grid topology** page.

When you recover an Admin Node, the software installation process creates an empty Admin Node database on the recovered node. However, the new database only includes information for servers and services that are currently part of the system or added later.

If you restored a primary Admin Node and your StorageGRID system has another Admin Node, you can restore the historical information by copying the Admin Node database from a non-primary Admin Node (the *source Admin Node*) to the recovered primary Admin Node. If your system has only a primary Admin Node, you cannot restore the Admin Node database.

> Copying the Admin Node database might take several hours. Some Grid Manager features will be unavailable while services are stopped on the source Admin Node.

1. Log in to the source Admin Node:
   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.
2. From the source Admin Node, stop the MI service: `service mi stop`
3. From the source Admin Node, stop the Management Application Program Interface (mgmt-api) service: `service mgmt-api stop`
4. Complete the following steps on the recovered Admin Node:
   a. Log in to the recovered Admin Node:
      i. Enter the following command: `ssh admin@grid_node_IP`
      ii. Enter the password listed in the `Passwords.txt` file.
      iii. Enter the following command to switch to root: `su -`
      iv. Enter the password listed in the `Passwords.txt` file.
   b. Stop the MI service: `service mi stop`
   c. Stop the mgmt-api service: `service mgmt-api stop`
   d. Add the SSH private key to the SSH agent. Enter:`ssh-add`
   e. Enter the SSH Access Password listed in the `Passwords.txt` file.
   f. Copy the database from the source Admin Node to the recovered Admin Node: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. When prompted, confirm that you want to overwrite the MI database on the recovered Admin Node.

      The database and its historical data are copied to the recovered Admin Node. When the copy operation is done, the script starts the recovered Admin Node.

   h. When you no longer require passwordless access to other servers, remove the private key from the SSH agent. Enter:`ssh-add -D`
5. Restart the services on the source Admin Node: `service servermanager start`

#### Restore Prometheus metrics when recovering primary Admin Node

Optionally, you can retain the historical metrics maintained by Prometheus on a primary Admin Node that has failed. The Prometheus metrics can only be restored if your StorageGRID system includes another Admin Node.

- The recovered Admin Node must be installed and running.
- The StorageGRID system must include at least two Admin Nodes.
- You must have the `Passwords.txt` file.
- You must have the provisioning passphrase.

If an Admin Node fails, the metrics maintained in the Prometheus database on the Admin Node are lost. When you recover the Admin Node, the software installation process creates a new Prometheus database. After the recovered Admin Node is started, it records metrics as if you had performed a new installation of the StorageGRID system.

If you restored a primary Admin Node and your StorageGRID system has another Admin Node, you can restore the historical metrics by copying the Prometheus database from a non-primary Admin Node (the *source Admin Node*) to the recovered primary Admin Node. If your system has only a primary Admin Node, you cannot restore the Prometheus database.

> Copying the Prometheus database might take an hour or more. Some Grid Manager features will be unavailable while services are stopped on the source Admin Node.

1. Log in to the source Admin Node:
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.
2. From the source Admin Node, stop the Prometheus service: `service prometheus stop`
3. Complete the following steps on the recovered Admin Node:
   a. Log in to the recovered Admin Node:
      i. Enter the following command: `ssh admin@grid_node_IP`
      ii. Enter the password listed in the `Passwords.txt` file.
      iii. Enter the following command to switch to root: `su -`
      iv. Enter the password listed in the `Passwords.txt` file.
   b. Stop the Prometheus service: `service prometheus stop`
   c. Add the SSH private key to the SSH agent. Enter:`ssh-add`
   d. Enter the SSH Access Password listed in the `Passwords.txt` file.
   e. Copy the Prometheus database from the source Admin Node to the recovered Admin Node: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. When prompted, press **Enter** to confirm that you want to destroy the new Prometheus database on the recovered Admin Node.

      The original Prometheus database and its historical data are copied to the recovered Admin Node. When the copy operation is done, the script starts the recovered Admin Node. The following status appears:

      Database cloned, starting services

   g. When you no longer require passwordless access to other servers, remove the private key from the SSH agent. Enter:`ssh-add -D`
4. Restart the Prometheus service on the source Admin Node.`service prometheus start`

#### Recover from non-primary Admin Node failures

You must complete the following tasks to recover from a non-primary Admin Node failure. One Admin Node hosts the Configuration Management Node (CMN) service and is known as the primary Admin Node. Although you can have multiple Admin Nodes, each

StorageGRID system includes only one primary Admin Node. All other Admin Nodes are non-primary Admin Nodes.

**Related information**

SG100 and SG1000 services appliances

### Copy audit logs from failed non-primary Admin Node

If you are able to copy audit logs from the failed Admin Node, you should preserve them to maintain the grid's record of system activity and usage. You can restore the preserved audit logs to the recovered non-primary Admin Node after it is up and running.

This procedure copies the audit log files from the failed Admin Node to a temporary location on a separate grid node. These preserved audit logs can then be copied to the replacement Admin Node. Audit logs are not automatically copied to the new Admin Node.

Depending on the type of failure, you might not be able to copy audit logs from a failed Admin Node. If the deployment has only one Admin Node, the recovered Admin Node starts recording events to the audit log in a new empty file and previously recorded data is lost. If the deployment includes more than one Admin Node, you can recover the audit logs from another Admin Node.

> If the audit logs are not accessible on the failed Admin Node now, you might be able to access them later, for example, after host recovery.

1. Log in to the failed Admin Node if possible. Otherwise, log in to the primary Admin Node or another Admin Node, if available.
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.
2. Stop the AMS service to prevent it from creating a new log file:`service ams stop`
3. Rename the audit.log file so that it does not overwrite the existing file when you copy it to the recovered Admin Node.

   Rename audit.log to a unique numbered file name such as yyyy-mm-dd.txt.1. For example, you can rename the audit.log file to 2015-10-25.txt.1`cd /var/local/audit/exportls -l``mv audit.log 2015-10-25.txt.1`
4. Restart the AMS service: `service ams start`
5. Create the directory to copy all audit log files to a temporary location on a separate grid node: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   When prompted, enter the password for admin.
6. Copy all audit log files: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

When prompted, enter the password for admin.

7. Log out as root: `exit`

### Replace non-primary Admin Node

## To recover a non-primary Admin Node, you first must replace the physical or virtual hardware.

You can replace a failed non-primary Admin Node with a non-primary Admin Node running on the same platform, or you can replace a non-primary Admin Node running on VMware or a Linux host with a non-primary Admin Node hosted on a services appliance.

Use the procedure that matches the replacement platform you select for the node. After you complete the node replacement procedure (which is suitable for all node types), that procedure will direct you to the next step for non-primary Admin Node recovery.

| Replacement platform | Procedure |
|---|---|
| VMware | Replace a VMware node |
| Linux | Replace a Linux node |
| SG100 and SG1000 services appliances | Replace a services appliance |
| OpenStack | NetApp-provided virtual machine disk files and scripts for OpenStack are no longer supported for recovery operations. If you need to recover a node running in an OpenStack deployment, download the files for your Linux operating system. Then, follow the procedure for replacing a Linux node. |

### Select Start Recovery to configure non-primary Admin Node

## After replacing a non-primary Admin Node, you must select Start Recovery in the Grid Manager to configure the new node as a replacement for the failed node.

#### What you'll need

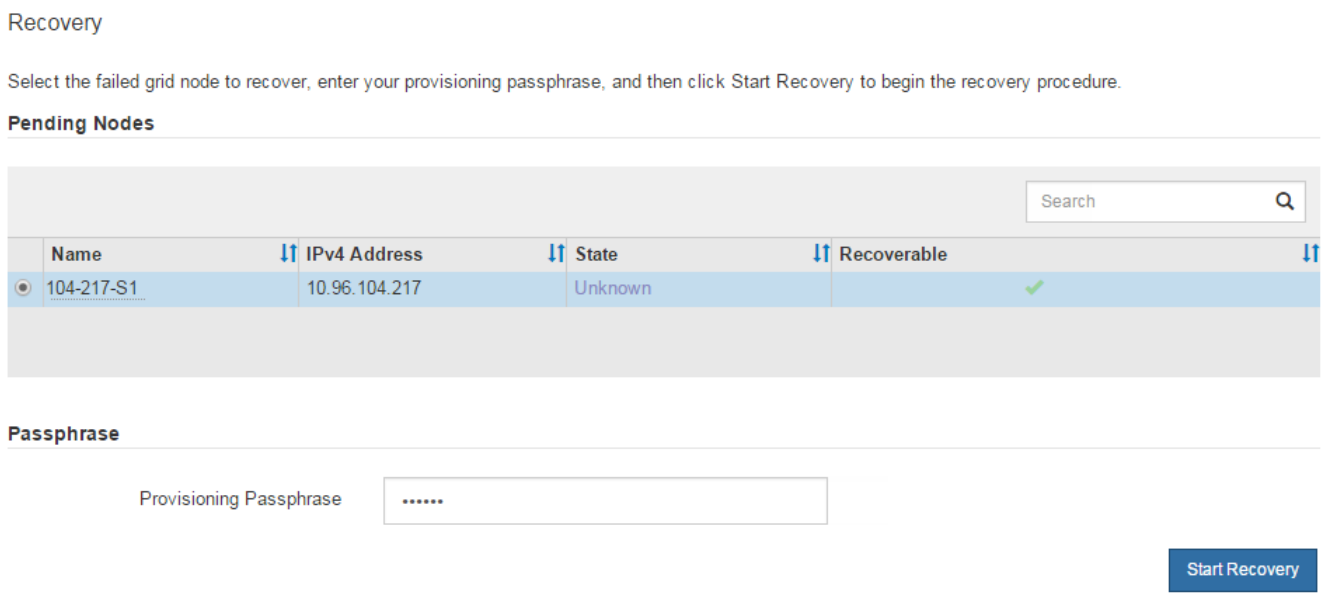
- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Maintenance or Root Access permission.
- You must have the provisioning passphrase.
- You must have deployed and configured the replacement node.

#### Steps

1. From the Grid Manager, select **MAINTENANCE** > **Tasks** > **Recovery**.
2. Select the grid node you want to recover in the Pending Nodes list.

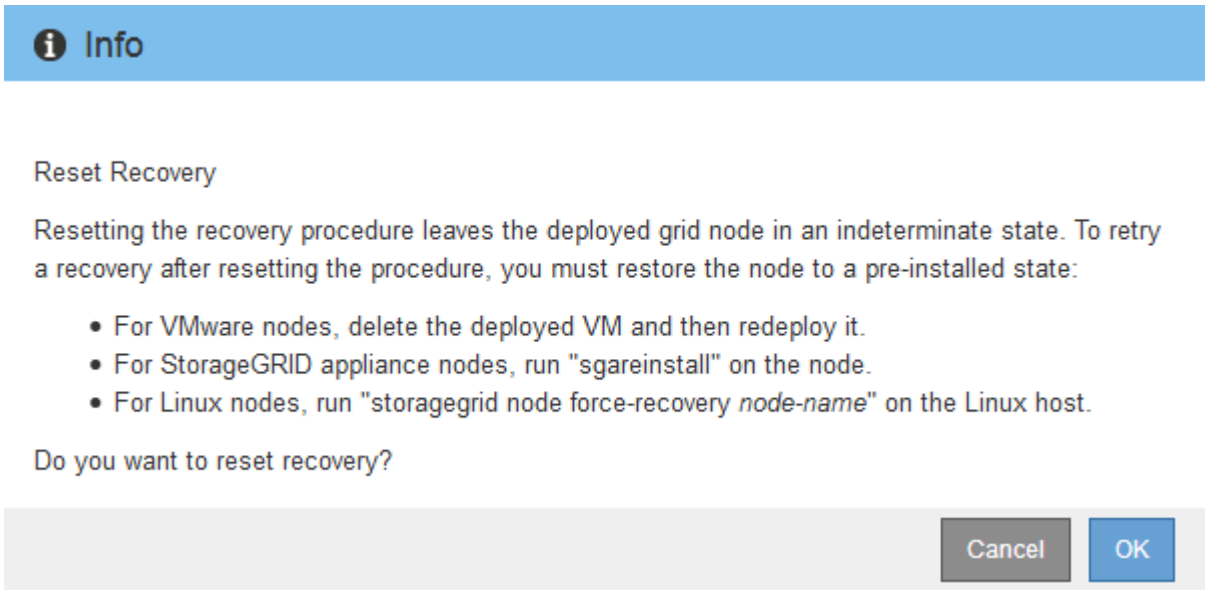
   Nodes appear in the list after they fail, but you cannot select a node until it has been reinstalled and is ready for recovery.

3. Enter the **Provisioning Passphrase**.
4. Click **Start Recovery**.




5. Monitor the progress of the recovery in the Recovering Grid Node table.

> While the recovery procedure is running, you can click **Reset** to start a new recovery. An Info dialog box appears, indicating that the node will be left in an indeterminate state if you reset the procedure.




If you want to retry the recovery after resetting the procedure, you must restore the node to a pre-installed state, as follows:

- **VMware**: Delete the deployed virtual grid node. Then, when you are ready to restart the recovery, redeploy the node.
- **Linux**: Restart the node by running this command on the Linux host: `storagegrid node force-recovery node-name`

- **Appliance**: If you want to retry the recovery after resetting the procedure, you must restore the appliance node to a pre-installed state by running `sgareinstall` on the node.

6. If single sign-on (SSO) is enabled for your StorageGRID system and the relying party trust for the Admin Node you recovered was configured to use the default management interface certificate, update (or delete and recreate) the node's relying party trust in Active Directory Federation Services (AD FS). Use the new default server certificate that was generated during the Admin Node recovery process.

> To configure a relying party trust, see the instructions for administering StorageGRID. To access the default server certificate, log in to the command shell of the Admin Node. Go to the `/var/local/mgmt-api` directory, and select the `server.crt` file.

**Related information**

Administer StorageGRID

Prepare appliance for reinstallation (platform replacement only)

### Restore audit log on recovered non-primary Admin Node

If you were able to preserve the audit log from the failed non-primary Admin Node, so that historical audit log information is retained, you can copy it to the non-primary Admin Node you are recovering.

- The recovered Admin Node must be installed and running.
- You must have copied the audit logs to another location after the original Admin Node failed.

If an Admin Node fails, audit logs saved to that Admin Node are potentially lost. It might be possible to preserve data from loss by copying audit logs from the failed Admin Node and then restoring these audit logs to the recovered Admin Node. Depending on the failure, it might not be possible to copy audit logs from the failed Admin Node. In that case, if the deployment has more than one Admin Node, you can recover audit logs from another Admin Node as audit logs are replicated to all Admin Nodes.

If there is only one Admin Node and the audit log cannot be copied from the failed node, the recovered Admin Node starts recording events to the audit log as if the installation is new.

You must recover an Admin Node as soon as possible to restore logging functionality.

> By default, audit information is sent to the audit log on Admin Nodes. You can skip these steps if either of the following applies:
>
> - You configured an external syslog server and audit logs are now being sent to the syslog server instead of to Admin Nodes.
> - You explicitly specified that audit messages should be saved only on the local nodes that generated them.
>
> See Configure audit messages and log destinations for details.

**Steps**

1. Log in to the recovered Admin Node:

   a. Enter the following command: + `ssh admin@recovery_Admin_Node_IP`

b. Enter the password listed in the `Passwords.txt` file.

c. Enter the following command to switch to root: `su -`

d. Enter the password listed in the `Passwords.txt` file.

After you are logged in as root, the prompt changes from `$` to `#`.

2. Check which audit files have been preserved:

```
cd /var/local/audit/export
```

3. Copy the preserved audit log files to the recovered Admin Node:

```
scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
```

When prompted, enter the password for admin.

4. For security, delete the audit logs from the failed grid node after verifying that they have been copied successfully to the recovered Admin Node.
5. Update the user and group settings of the audit log files on the recovered Admin Node:

```
chown ams-user:bycast *
```

6. Log out as root: `exit`

You must also restore any pre-existing client access to the audit share. For more information, see the instructions for administering StorageGRID.

**Related information**

Administer StorageGRID

### Reset preferred sender on recovered non-primary Admin Node

If the non-primary Admin Node you are recovering is currently set as the preferred sender of alert notifications, alarm notifications, and AutoSupport messages, you must reconfigure this setting in the StorageGRID system.

**What you'll need**

- You must be signed in to the Grid Manager using a supported web browser.
- You must have specific access permissions.
- The recovered Admin Node must be installed and running.

**Steps**

1. Select **CONFIGURATION** > **System** > **Display options**.
2. Select the recovered Admin Node from the **Preferred Sender** drop-down list.
3. Click **Apply Changes**.

**Related information**

Administer StorageGRID

#### Restore Admin Node database when recovering non-primary Admin Node

If you want to retain the historical information about attributes, alarms, and alerts on a non-primary Admin Node that has failed, you can restore the Admin Node database from the primary Admin Node.

- The recovered Admin Node must be installed and running.
- The StorageGRID system must include at least two Admin Nodes.
- You must have the `Passwords.txt` file.
- You must have the provisioning passphrase.

If an Admin Node fails, the historical information stored in its Admin Node database is lost. This database includes the following information:

- Alert history
- Alarm history
- Historical attribute data, which is used in the charts and text reports available from the **SUPPORT** > **Tools** > **Grid topology** page.

When you recover an Admin Node, the software installation process creates an empty Admin Node database on the recovered node. However, the new database only includes information for servers and services that are currently part of the system or added later.

If you restored a non-primary Admin Node, you can restore the historical information by copying the Admin Node database from the primary Admin Node (the *source Admin Node*) to the recovered node.

> Copying the Admin Node database might take several hours. Some Grid Manager features will be unavailable while services are stopped on the source node.

1. Log in to the source Admin Node:
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.
2. Run the following command from the source Admin Node. Then, enter the provisioning passphrase if prompted. `recover-access-points`
3. From the source Admin Node, stop the MI service: `service mi stop`
4. From the source Admin Node, stop the Management Application Program Interface (mgmt-api) service: `service mgmt-api stop`
5. Complete the following steps on the recovered Admin Node:
   a. Log in to the recovered Admin Node:
      i. Enter the following command: `ssh admin@grid_node_IP`
      ii. Enter the password listed in the `Passwords.txt` file.
      iii. Enter the following command to switch to root: `su -`

iv. Enter the password listed in the `Passwords.txt` file.

b. Stop the MI service: `service mi stop`

c. Stop the mgmt-api service: `service mgmt-api stop`

d. Add the SSH private key to the SSH agent. Enter:`ssh-add`

e. Enter the SSH Access Password listed in the `Passwords.txt` file.

f. Copy the database from the source Admin Node to the recovered Admin Node: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. When prompted, confirm that you want to overwrite the MI database on the recovered Admin Node.

   The database and its historical data are copied to the recovered Admin Node. When the copy operation is done, the script starts the recovered Admin Node.

h. When you no longer require passwordless access to other servers, remove the private key from the SSH agent. Enter:`ssh-add -D`

6. Restart the services on the source Admin Node: `service servermanager start`

#### Restore Prometheus metrics when recovering non-primary Admin Node

Optionally, you can retain the historical metrics maintained by Prometheus on a non-primary Admin Node that has failed.

- The recovered Admin Node must be installed and running.
- The StorageGRID system must include at least two Admin Nodes.
- You must have the `Passwords.txt` file.
- You must have the provisioning passphrase.

If an Admin Node fails, the metrics maintained in the Prometheus database on the Admin Node are lost. When you recover the Admin Node, the software installation process creates a new Prometheus database. After the recovered Admin Node is started, it records metrics as if you had performed a new installation of the StorageGRID system.

If you restored a non-primary Admin Node, you can restore the historical metrics by copying the Prometheus database from the primary Admin Node (the *source Admin Node*) to the recovered Admin Node.

> Copying the Prometheus database might take an hour or more. Some Grid Manager features will be unavailable while services are stopped on the source Admin Node.

1. Log in to the source Admin Node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

2. From the source Admin Node, stop the Prometheus service: `service prometheus stop`

3. Complete the following steps on the recovered Admin Node:

a. Log in to the recovered Admin Node:
   i. Enter the following command: `ssh admin@grid_node_IP`
   ii. Enter the password listed in the `Passwords.txt` file.
   iii. Enter the following command to switch to root: `su -`
   iv. Enter the password listed in the `Passwords.txt` file.
b. Stop the Prometheus service: `service prometheus stop`
c. Add the SSH private key to the SSH agent. Enter:`ssh-add`
d. Enter the SSH Access Password listed in the `Passwords.txt` file.
e. Copy the Prometheus database from the source Admin Node to the recovered Admin Node: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
f. When prompted, press **Enter** to confirm that you want to destroy the new Prometheus database on the recovered Admin Node.

   The original Prometheus database and its historical data are copied to the recovered Admin Node. When the copy operation is done, the script starts the recovered Admin Node. The following status appears:

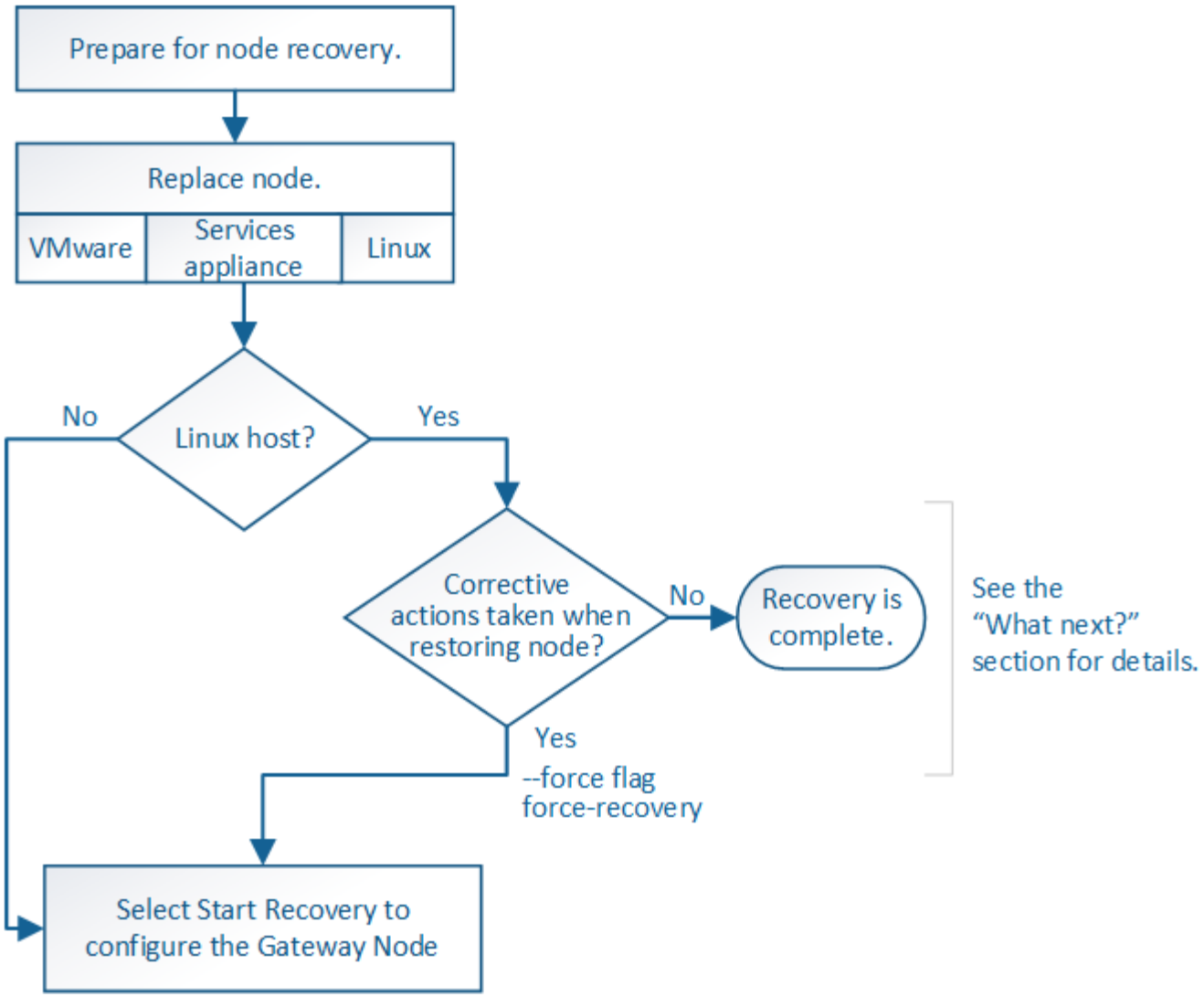
   Database cloned, starting services

g. When you no longer require passwordless access to other servers, remove the private key from the SSH agent. Enter:`ssh-add -D`

4. Restart the Prometheus service on the source Admin Node.`service prometheus start`

#### Recover from Gateway Node failures

You must complete a sequence of tasks in exact order to recover from a Gateway Node failure.




**Related information**

SG100 and SG1000 services appliances

#### Replace Gateway Node

You can replace a failed Gateway Node with a Gateway Node running on the same physical or virtual hardware, or you can replace a Gateway Node running on VMware or a Linux host with a Gateway Node hosted on a services appliance.

The node replacement procedure you must follow depends on which platform will be used by the replacement node. After you complete the node replacement procedure (which is suitable for all node types), that procedure will direct you to the next step for Gateway Node recovery.

| Replacement platform | Procedure |
|---|---|
| VMware | Replace a VMware node |
| Linux | Replace a Linux node |

| Replacement platform | Procedure |
| --- | --- |
| SG100 and SG1000 services appliances | Replace a services appliance |
| OpenStack | NetApp-provided virtual machine disk files and scripts for OpenStack are no longer supported for recovery operations. If you need to recover a node running in an OpenStack deployment, download the files for your Linux operating system. Then, follow the procedure for replacing a Linux node. |

#### Select Start Recovery to configure Gateway Node

After replacing a Gateway Node, you must select Start Recovery in the Grid Manager to configure the new node as a replacement for the failed node.

### What you'll need

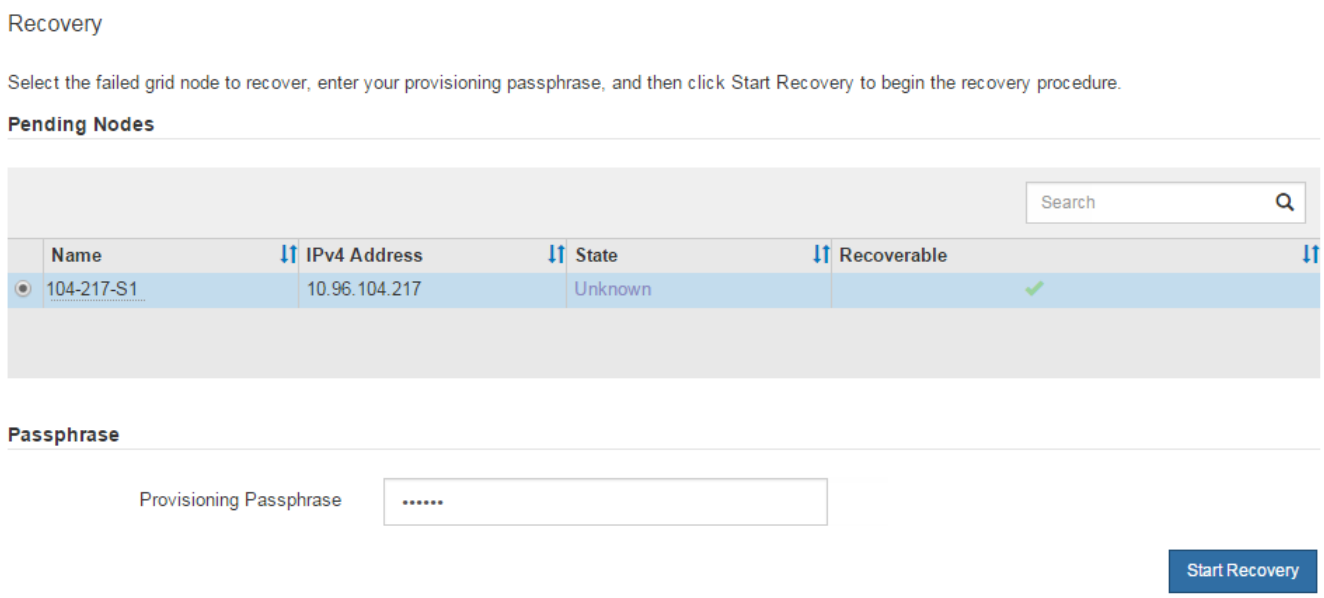
- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Maintenance or Root Access permission.
- You must have the provisioning passphrase.
- You must have deployed and configured the replacement node.

### Steps

1. From the Grid Manager, select **MAINTENANCE** > **Tasks** > **Recovery**.
2. Select the grid node you want to recover in the Pending Nodes list.

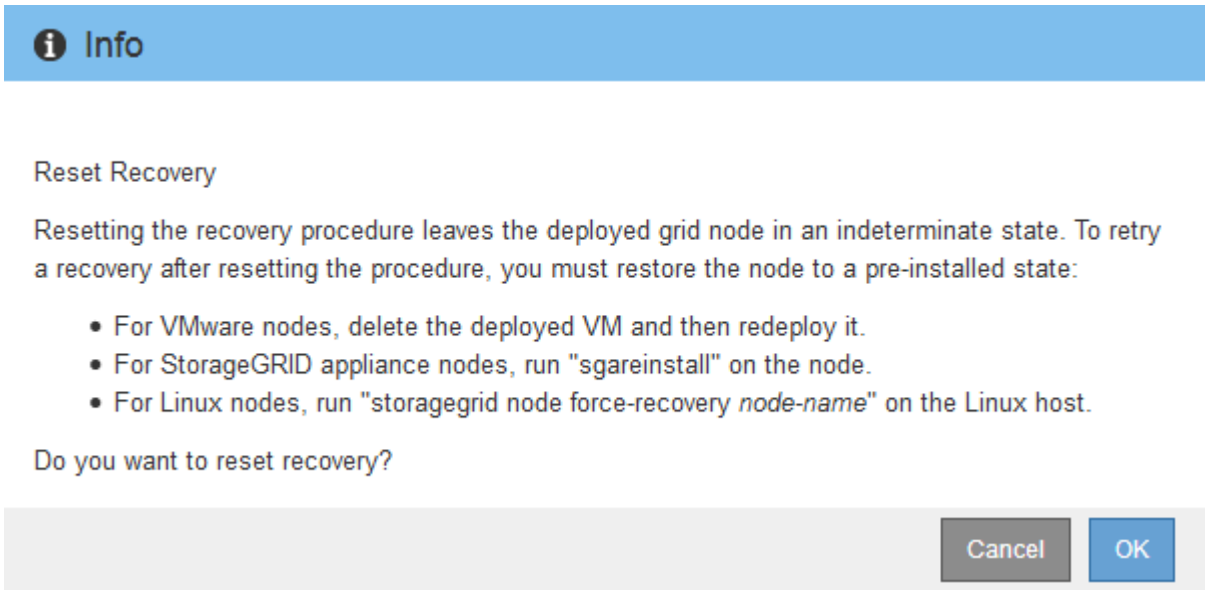
   Nodes appear in the list after they fail, but you cannot select a node until it has been reinstalled and is ready for recovery.

3. Enter the **Provisioning Passphrase**.
4. Click **Start Recovery**.



5. Monitor the progress of the recovery in the Recovering Grid Node table.

> While the recovery procedure is running, you can click **Reset** to start a new recovery. An Info dialog box appears, indicating that the node will be left in an indeterminate state if you reset the procedure.




If you want to retry the recovery after resetting the procedure, you must restore the node to a pre-installed state, as follows:

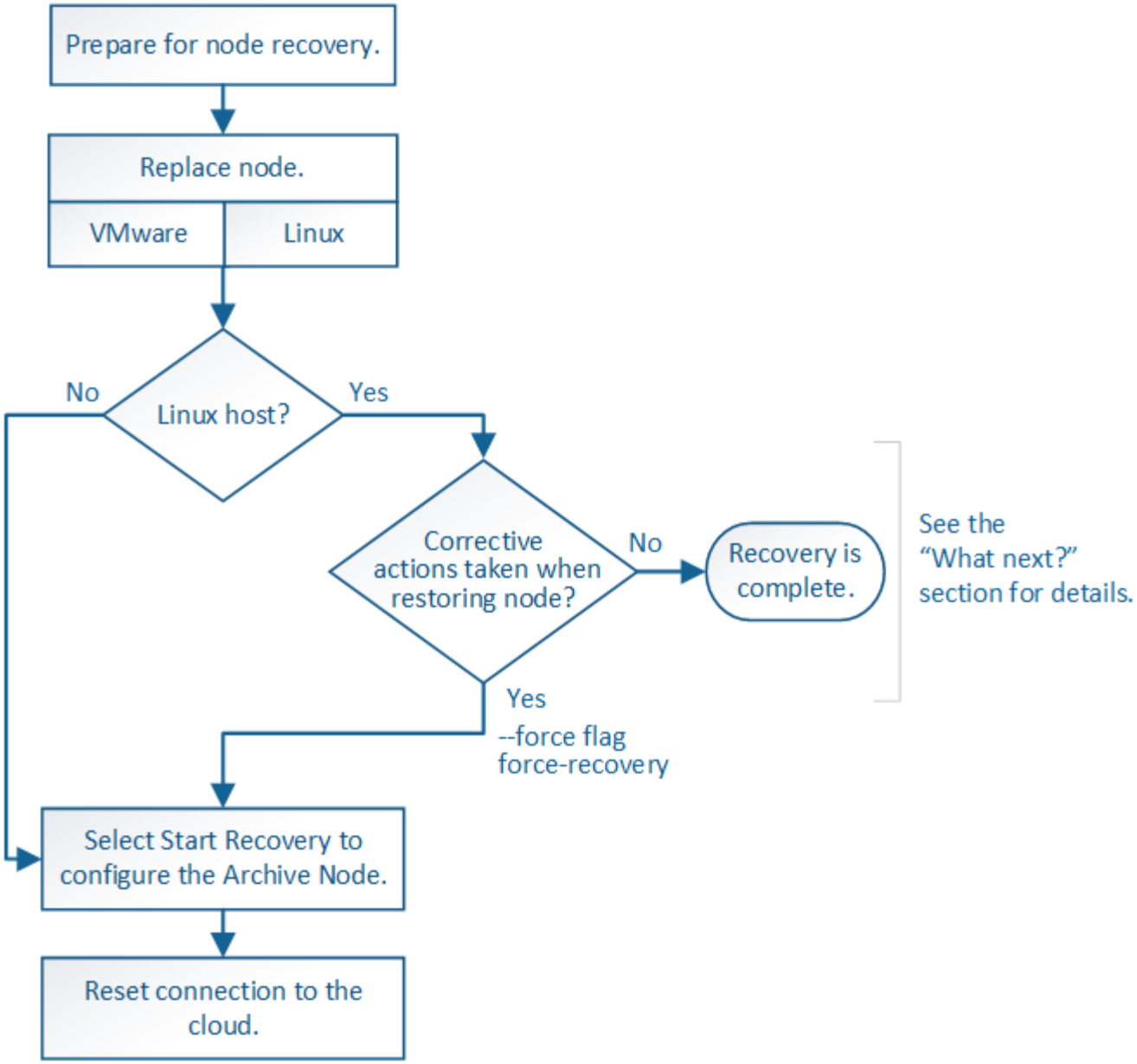
- **VMware**: Delete the deployed virtual grid node. Then, when you are ready to restart the recovery, redeploy the node.
- **Linux**: Restart the node by running this command on the Linux host: `storagegrid node force-recovery node-name`
- **Appliance**: If you want to retry the recovery after resetting the procedure, you must restore the appliance node to a pre-installed state by running `sgareinstall` on the node.

**Related information**

Prepare appliance for reinstallation (platform replacement only)

### Recover from Archive Node failures

You must complete a sequence of tasks in exact order to recover from an Archive Node failure.




**About this task**

Archive Node recovery is affected by the following issues:

- If the ILM policy is configured to replicate a single copy.

  In a StorageGRID system that is configured to make a single copy of objects, an Archive Node failure might result in an unrecoverable loss of data. If there is a failure, all such objects are lost; however, you must still perform recovery procedures to "clean up" your StorageGRID system and purge lost object information from the database.

- If an Archive Node failure occurs during Storage Node recovery.

  If the Archive Node fails while processing bulk retrievals as part of a Storage Node recovery, you must repeat the procedure to recover copies of object data to the Storage Node from the beginning to ensure that all object data retrieved from the Archive Node is restored to the Storage Node.

#### Replace Archive Node

## To recover an Archive Node, you must first replace the node.

You must select the node replacement procedure for your platform. The steps to replace a node are the same for all types of grid nodes.

| Platform | Procedure |
| --- | --- |
| VMware | Replace a VMware node |
| Linux | Replace a Linux node |
| OpenStack | NetApp-provided virtual machine disk files and scripts for OpenStack are no longer supported for recovery operations. If you need to recover a node running in an OpenStack deployment, download the files for your Linux operating system. Then, follow the procedure for replacing a Linux node. |

#### Select Start Recovery to configure Archive Node

## After replacing an Archive Node, you must select Start Recovery in the Grid Manager to configure the new node as a replacement for the failed node.

**What you'll need**

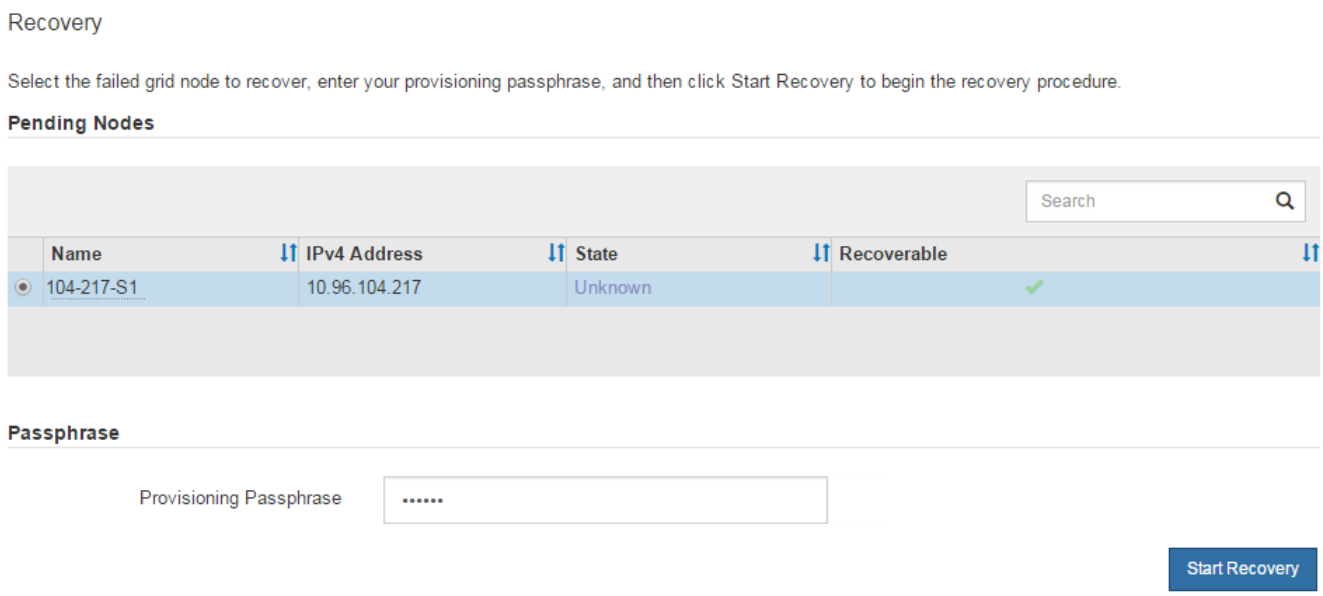
- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Maintenance or Root Access permission.
- You must have the provisioning passphrase.
- You must have deployed and configured the replacement node.

**Steps**

1. From the Grid Manager, select **MAINTENANCE** > **Tasks** > **Recovery**.
2. Select the grid node you want to recover in the Pending Nodes list.

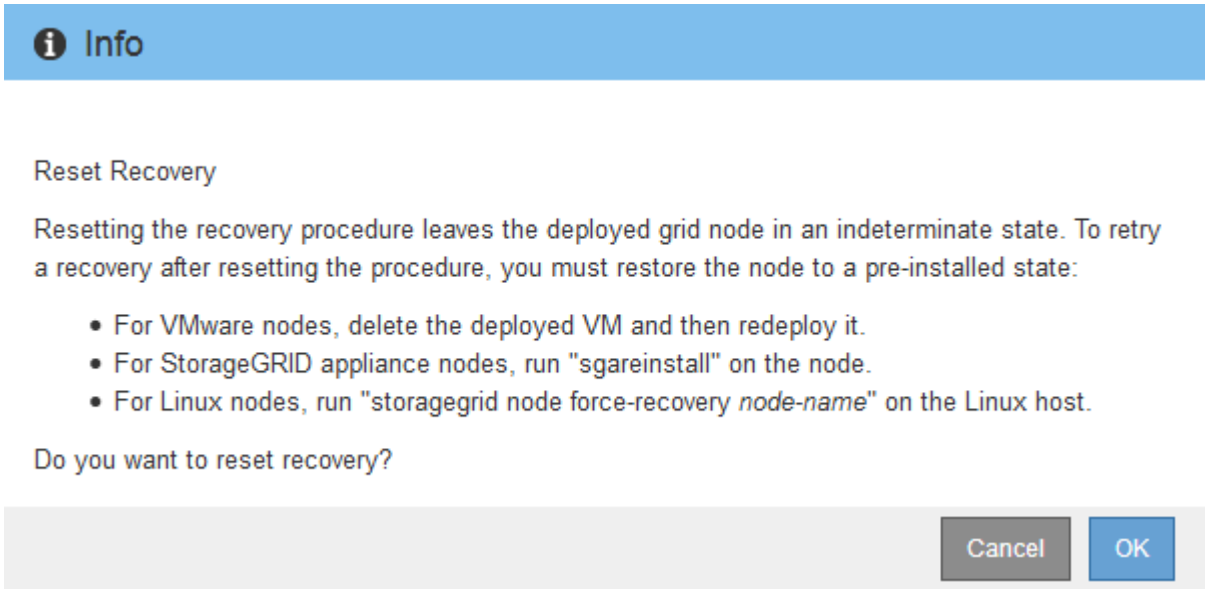
   Nodes appear in the list after they fail, but you cannot select a node until it has been reinstalled and is ready for recovery.

3. Enter the **Provisioning Passphrase**.
4. Click **Start Recovery**.




5. Monitor the progress of the recovery in the Recovering Grid Node table.

> While the recovery procedure is running, you can click **Reset** to start a new recovery. An Info dialog box appears, indicating that the node will be left in an indeterminate state if you reset the procedure.




If you want to retry the recovery after resetting the procedure, you must restore the node to a pre-installed state, as follows:

- **VMware**: Delete the deployed virtual grid node. Then, when you are ready to restart the recovery, redeploy the node.
- **Linux**: Restart the node by running this command on the Linux host: `storagegrid node force-recovery node-name`

#### Reset Archive Node connection to the cloud

After you recover an Archive Node that targets the cloud through the S3 API, you need to modify configuration settings to reset connections. An Outbound Replication Status (ORSU) alarm is triggered if the Archive Node is unable to retrieve object data.

> If your Archive Node connects to external storage through TSM middleware, then the node resets itself automatically and you do not need to reconfigure.

**What you'll need**

You must be signed in to the Grid Manager using a supported web browser.

**Steps**

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Select **Archive Node** > **ARC** > **Target**.
3. Edit the **Access Key** field by entering an incorrect value and click **Apply Changes**.
4. Edit the **Access Key** field by entering the correct value and click **Apply Changes**.

### All grid node types: Replace VMware node

When you recover a failed StorageGRID node that was hosted on VMware, you must remove the failed node and deploy a recovery node.

**What you'll need**

You must have determined that the virtual machine cannot be restored, and must be replaced.

**About this task**

You use the VMware vSphere Web Client to first remove the virtual machine associated with the failed grid node. Then, you can deploy a new virtual machine.

This procedure is only one step in the grid node recovery process. The node removal and deployment procedure is the same for all VMware nodes, including Admin Nodes, Storage Nodes, Gateway Nodes, and Archive Nodes.

**Steps**

1. Log in to VMware vSphere Web Client.
2. Navigate to the failed grid node virtual machine.
3. Make a note of all of the information required to deploy the recovery node.
   a. Right-click the virtual machine, select the **Edit Settings** tab, and note the settings in use.
   b. Select the **vApp Options** tab to view and record the grid node network settings.
4. If the failed grid node is a Storage Node, determine if any of the virtual hard disks used for data storage are undamaged and preserve them for reattachment to the recovered grid node.
5. Power off the virtual machine.
6. Select **Actions** > **All vCenter Actions** > **Delete from Disk** to delete the virtual machine.
7. Deploy a new virtual machine to be the replacement node, and connect it to one or more StorageGRID networks.

When you deploy the node, you can optionally remap node ports or increase CPU or memory settings.

> After deploying the new node, you can add new virtual disks according to your storage requirements, reattach any virtual hard disks preserved from the previously removed failed grid node, or both.

For instructions:

Install VMware > Deploying a StorageGRID node as a virtual machine

8. Complete the node recovery procedure, based on the type of node you are recovering.

| Type of node | Go to |
|---|---|
| Primary Admin Node | Configure replacement primary Admin Node |
| Non-primary Admin Node | Select Start Recovery to configure non-primary Admin Node |
| Gateway Node | Select Start Recovery to configure Gateway Node |
| Storage Node | Select Start Recovery to configure Storage Node |
| Archive Node | Select Start Recovery to configure Archive Node |

**All grid node types: Replace Linux node**

If a failure requires that you deploy one or more new physical or virtual hosts or reinstall Linux on an existing host, you must deploy and configure the replacement host before you can recover the grid node. This procedure is one step of the grid node recovery process for all types of grid nodes.

“Linux” refers to a Red Hat® Enterprise Linux®, Ubuntu®, CentOS, or Debian® deployment. Use the NetApp Interoperability Matrix Tool to get a list of supported versions.

This procedure is only performed as one step in the process of recovering software-based Storage Nodes, primary or non-primary Admin Nodes, Gateway Nodes, or Archive Nodes. The steps are identical regardless of the type of grid node you are recovering.

If more than one grid node is hosted on a physical or virtual Linux host, you can recover the grid nodes in any order. However, recovering a primary Admin Node first, if present, prevents the recovery of other grid nodes from stalling as they try to contact the primary Admin Node to register for recovery.

**Related information**

NetApp Interoperability Matrix Tool

**Deploy new Linux hosts**

With a few exceptions, you prepare the new hosts as you did during the initial installation process.

To deploy new or reinstalled physical or virtual Linux hosts, follow the procedure for preparing the hosts in the StorageGRID installation instructions for your Linux operating system.

This procedure includes steps to accomplish the following tasks:

1. Install Linux.
2. Configure the host network.
3. Configure host storage.
4. Install the container engine.
5. Install the StorageGRID host service.

> Stop after you complete the “Install StorageGRID host service” task in the installation instructions. Do not start the “Deploying grid nodes” task.

As you perform these steps, note the following important guidelines:

- Be sure to use the same host interface names you used on the original host.
- If you use shared storage to support your StorageGRID nodes, or you have moved some or all of the disk drives or SSDs from the failed to the replacement nodes, you must reestablish the same storage mappings that were present on the original host. For example, if you used WWIDs and aliases in `/etc/multipath.conf` as recommended in the installation instructions, be sure to use the same alias/WWID pairs in `/etc/multipath.conf` on the replacement host.
- If the StorageGRID node uses storage assigned from a NetApp ONTAP system, confirm that the volume does not have a FabricPool tiering policy enabled. Disabling FabricPool tiering for volumes used with StorageGRID nodes simplifies troubleshooting and storage operations.

> Never use FabricPool to tier any data related to StorageGRID back to StorageGRID itself. Tiering StorageGRID data back to StorageGRID increases troubleshooting and operational complexity.

**Related information**

Install Red Hat Enterprise Linux or CentOS

Install Ubuntu or Debian

#### Restore grid nodes to the host

To restore a failed grid node to a new Linux host, you restore the node configuration file using the appropriate commands.

When doing a fresh install, you create a node configuration file for each grid node to be installed on a host. When restoring a grid node to a replacement host, you restore or replace the node configuration file for any failed grid nodes.

If any block storage volumes were preserved from the previous host, you might have to perform additional recovery procedures. The commands in this section help you determine which additional procedures are required.

**Steps**

- Restore and validate grid nodes
- Start StorageGRID host service
- Recover nodes that fail to start normally

### Restore and validate grid nodes

You must restore the grid configuration files for any failed grid nodes, and then validate the grid configuration files and resolve any errors.

#### About this task

You can import any grid node that should be present on the host, as long as its `/var/local` volume was not lost as a result of the failure of the previous host. For example, the `/var/local` volume might still exist if you used shared storage for StorageGRID system data volumes, as described in the StorageGRID installation instructions for your Linux operating system. Importing the node restores its node configuration file to the host.

If it is not possible to import missing nodes, you must recreate their grid configuration files.

You must then validate the grid configuration file, and resolve any networking or storage issues that might occur before going on to restart StorageGRID. When you re-create the configuration file for a node, you must use the same name for the replacement node that was used for the node you are recovering.

See the installation instructions for more information on the location of the `/var/local` volume for a node.

#### Steps

1. At the command line of the recovered host, list all currently configured StorageGRID grid nodes:`sudo storagegrid node list`

   If no grid nodes are configured, there will be no output. If some grid nodes are configured, expect output in the following format:

   ```
   Name                Metadata-Volume
   ==================================================================
   dc1-adm1            /dev/mapper/sgws-adm1-var-local
   dc1-gw1             /dev/mapper/sgws-gw1-var-local
   dc1-sn1             /dev/mapper/sgws-sn1-var-local
   dc1-arc1            /dev/mapper/sgws-arc1-var-local
   ```

   If some or all of the grid nodes that should be configured on the host are not listed, you need to restore the missing grid nodes.

2. To import grid nodes that have a `/var/local` volume:

   a. Run the following command for each node you want to import:`sudo storagegrid node import node-var-local-volume-path`

      The `storagegrid node import` command succeeds only if the target node was shut down cleanly on the host on which it last ran. If that is not the case, you will observe an error similar to the following:

      `This node (node-name) appears to be owned by another host (UUID host-uuid).`

```
Use the --force flag if you are sure import is safe.
```

b. If you see the error about the node being owned by another host, run the command again with the `--force` flag to complete the import:`sudo storagegrid --force node import node-var-local-volume-path`

> Any nodes imported with the `--force` flag will require additional recovery steps before they can rejoin the grid, as described in What's next: Perform additional recovery steps, if required.

3. For grid nodes that do not have a `/var/local` volume, recreate the node's configuration file to restore it to the host.

   Follow the guidelines in "Create node configuration files" in the installation instructions.

> When you re-create the configuration file for a node, you must use the same name for the replacement node that was used for the node you are recovering. For Linux deployments, ensure that the configuration file name contains the node name. You should use the same network interfaces, block device mappings, and IP addresses when possible. This practice minimizes the amount of data that needs to be copied to the node during recovery, which could make the recovery significantly faster (in some cases, minutes rather than weeks).

> If you use any new block devices (devices that the StorageGRID node did not use previously) as values for any of the configuration variables that start with `BLOCK_DEVICE_` when you are recreating the configuration file for a node, be sure to follow all of the guidelines in Fix missing block device errors.

4. Run the following command on the recovered host to list all StorageGRID nodes.

```
sudo storagegrid node list
```

5. Validate the node configuration file for each grid node whose name was shown in the storagegrid node list output:

```
sudo storagegrid node validate node-name
```

   You must address any errors or warnings before starting the StorageGRID host service. The following sections give more detail on errors that might have special significance during recovery.

**Related information**

Install Red Hat Enterprise Linux or CentOS

Install Ubuntu or Debian

Fix missing network interface errors

### Fix missing network interface errors

If the host network is not configured correctly or a name is misspelled, an error occurs when StorageGRID checks the mapping specified in the `/etc/storagegrid/nodes/node-name.conf` file.

You might see an error or warning matching this pattern:

`Checking configuration file` `/etc/storagegrid/nodes/`*`node-name`*`.conf` for node *node-name*…` `ERROR: `*`node-name`*`: GRID_NETWORK_TARGET = `*`host-interface-name`*` ` *node-name*: Interface '*host-interface-name*' does not exist`

The error could be reported for the Grid Network, the Admin Network, or the Client Network. This error means that the `/etc/storagegrid/nodes/`*`node-name`*`.conf` file maps the indicated StorageGRID network to the host interface named *`host-interface-name`*, but there is no interface with that name on the current host.

If you receive this error, verify that you completed the steps in Deploy new Linux hosts. Use the same names for all host interfaces as were used on the original host.

If you are unable to name the host interfaces to match the node configuration file, you can edit the node configuration file and change the value of the GRID_NETWORK_TARGET, the ADMIN_NETWORK_TARGET, or the CLIENT_NETWORK_TARGET to match an existing host interface.

Make sure the host interface provides access to the appropriate physical network port or VLAN, and that the interface does not directly reference a bond or bridge device. You must either configure a VLAN (or other virtual interface) on top of the bond device on the host, or use a bridge and virtual Ethernet (veth) pair.

#### Fix missing block device errors

The system checks that each recovered node maps to a valid block device special file or a valid softlink to a block device special file. If StorageGRID finds invalid mapping in the `/etc/storagegrid/nodes/`*`node-name`*`.conf` file, a missing block device error displays.

If you observe an error matching this pattern:

`Checking configuration file /etc/storagegrid/nodes/`*`node-name`*`.conf for node` *`node-name`*… `ERROR: `*`node-name`*`: BLOCK_DEVICE_PURPOSE = `*`path-name`*` ` *node-name*: *path-name* does not exist`

It means that `/etc/storagegrid/nodes/`*`node-name`*`.conf` maps the block device used by *node-name* for PURPOSE to the given path-name in the Linux file system, but there is not a valid block device special file, or softlink to a block device special file, at that location.

Verify that you completed the steps in Deploy new Linux hosts. Use the same persistent device names for all block devices as were used on the original host.

If you are unable to restore or recreate the missing block device special file, you can allocate a new block device of the appropriate size and storage category and edit the node configuration file to change the value of BLOCK_DEVICE_PURPOSE to point to the new block device special file.

Determine the appropriate size and storage category from the tables in the “Storage requirements” section of the installation instructions for your Linux operating system. Review the recommendations in “Configuring host storage” before proceeding with the block device replacement.

> If you must provide a new block storage device for any of the configuration file variables starting with `BLOCK_DEVICE_` because the original block device was lost with the failed host, ensure the new block device is unformatted before attempting further recovery procedures. The new block device will be unformatted if you are using shared storage and have created a new volume. If you are unsure, run the following command against any new block storage device special files.

CAUTION:

Run the following command only for new block storage devices. Do not run this command if you believe the block storage still contains valid data for the node being recovered, as any data on the device will be lost.

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

**Related information**

Install Red Hat Enterprise Linux or CentOS

Install Ubuntu or Debian

#### Start StorageGRID host service

To start your StorageGRID nodes, and ensure they restart after a host reboot, you must enable and start the StorageGRID host service.

1. Run the following commands on each host:

   ```
   sudo systemctl enable storagegrid
   sudo systemctl start storagegrid
   ```

2. Run the following command to ensure the deployment is proceeding:

   `sudo storagegrid node status node-name`

   For any node that returns a status of Not-Running or Stopped, run the following command:

   `sudo storagegrid node start node-name`

3. If you have previously enabled and started the StorageGRID host service (or if you are unsure if the service has been enabled and started), also run the following command:

   ```
   sudo systemctl reload-or-restart storagegrid
   ```

#### Recover nodes that fail to start normally

If a StorageGRID node does not rejoin the grid normally and does not show up as recoverable, it may be corrupted. You can force the node into recovery mode.

To force the node into recovery mode:

```
sudo storagegrid node force-recovery node-name
```

Before issuing this command, confirm that the node's network configuration is correct; it may have failed to rejoin the grid due to incorrect network interface mappings or an incorrect Grid Network IP address or gateway.

After issuing the `storagegrid node force-recovery node-name` command, you must perform additional recovery steps for *node-name*.

**Related information**

What's next: Perform additional recovery steps, if required

#### What's next: Perform additional recovery steps, if required

Depending on the specific actions you took to get the StorageGRID nodes running on the replacement host, you might need to perform additional recovery steps for each node.

Node recovery is complete if you did not need to take any corrective actions while you replaced the Linux host or restored the failed grid node to the new host.

**Corrective actions and next steps**

During node replacement, you may have needed to take one of these corrective actions:

- You had to use the `--force` flag to import the node.
- For any `<PURPOSE>`, the value of the `BLOCK_DEVICE_<PURPOSE>` configuration file variable refers to a block device that does not contain the same data it did before the host failure.
- You issued `storagegrid node force-recovery node-name` for the node.
- You added a new block device.

If you took **any** of these corrective actions, you must perform additional recovery steps.

| Type of recovery | Next step |
|---|---|
| Primary Admin Node | Configure replacement primary Admin Node |
| Non-primary Admin Node | Select Start Recovery to configure non-primary Admin Node |
| Gateway Node | Select Start Recovery to configure Gateway Node |
| Archive Node | Select Start Recovery to configure Archive Node |

| Type of recovery | Next step |
| --- | --- |
| Storage Node (software-based):<br>• If you had to use the `--force` flag to import the node, or you issued `storagegrid node force-recovery node-name`<br>• If you had to do a full node reinstall, or you needed to restore /var/local | Select Start Recovery to configure Storage Node |
| Storage Node (software-based):<br>• If you added a new block device.<br>• If, for any `<PURPOSE>`, the value of the `BLOCK_DEVICE_<PURPOSE>` configuration file variable refers to a block device that does not contain the same data it did before the host failure. | Recover from storage volume failure where system drive is intact |

### Replace failed node with services appliance

You can use an SG100 or SG1000 services appliance to recover a failed Gateway Node, a failed non-primary Admin Node, or a failed primary Admin Node that was hosted on VMware, a Linux host, or a services appliance. This procedure is one step of the grid node recovery procedure.

#### What you'll need

- You must have determined that one of the following situations is true:
  - The virtual machine hosting the node cannot be restored.
  - The physical or virtual Linux host for the grid node has failed, and must be replaced.
  - The services appliance hosting the grid node must be replaced.
- You must make sure that the StorageGRID Appliance Installer version on the services appliance matches the software version of your StorageGRID system, as described in hardware installation and maintenance for verifying and upgrading the StorageGRID Appliance Installer version.

  SG100 and SG1000 services appliances

> Do not deploy both an SG100 and an SG1000 service appliance in the same site. Unpredictable performance might result.

#### About this task

You can use an SG100 or SG1000 services appliance to recover a failed grid node in the following cases:

- The failed node was hosted on VMware or Linux (platform change)
- The failed node was hosted on a services appliance (platform replacement)

#### Install services appliance (platform change only)

When you are recovering a failed grid node that was hosted on VMware or a Linux host and you are using an SG100 or SG1000 services appliance for the replacement node, you must first install the new appliance hardware using the same node name as the failed node.

You must have the following information about the failed node:

- **Node name**: You must install the services appliance using the same node name as the failed node.
- **IP addresses**: You can assign the services appliance the same IP addresses as the failed node, which is the preferred option, or you can select a new unused IP address on each network.

Perform this procedure only if you are recovering a failed node that was hosted on VMware or Linux and are replacing it with a node hosted on a services appliance.

1. Follow the instructions for installing a new SG100 or SG1000 services appliance.
2. When prompted for a node name, use the node name of the failed node.

**Related information**

SG100 and SG1000 services appliances

#### Prepare appliance for reinstallation for reinstallation (platform replacement only)

When recovering a grid node that was hosted on a services appliance, you must first prepare the appliance for reinstallation of StorageGRID software.

Perform this procedure only if you are replacing a failed node that was hosted on a services appliance. Do not follow these steps if the failed node was originally hosted on VMware or a Linux host.

1. Log in to the failed grid node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Prepare the appliance for the installation of StorageGRID software. Enter: `sgareinstall`
3. When prompted to continue, enter: `y`

   The appliance reboots, and your SSH session ends. It usually takes about 5 minutes for the StorageGRID Appliance Installer to become available, although in some cases you might need to wait up to 30 minutes.

   The services appliance is reset, and data on the grid node is no longer accessible. IP addresses configured during the original installation process should remain intact; however, it is recommended that you confirm this when the procedure completes.

   After executing the `sgareinstall` command, all StorageGRID-provisioned accounts, passwords, and SSH keys are removed, and new host keys are generated.

#### Start software installation on services appliance

## To install a Gateway Node or Admin Node on an SG100 or SG1000 services appliance, you use the StorageGRID Appliance Installer, which is included on the appliance.

### What you'll need

- The appliance must be installed in a rack, connected to your networks, and powered on.
- Network links and IP addresses must be configured for the appliance using the StorageGRID Appliance Installer.
- If you are installing a Gateway Node or non-primary Admin Node, you know the IP address of the primary Admin Node for the StorageGRID grid.
- All Grid Network subnets listed on the IP Configuration page of the StorageGRID Appliance Installer must be defined in the Grid Network Subnet List on the primary Admin Node.

For instructions for completing these prerequisite tasks, see the installation and maintenance instructions for an SG100 or SG1000 services appliance.

- You must be using a supported web browser.
- You must know one of the IP addresses assigned to the appliance. You can use the IP address for the Admin Network, the Grid Network, or the Client Network.
- If you are installing a primary Admin Node, you have the Ubuntu or Debian install files for this version of StorageGRID available.

> A recent version of StorageGRID software is preloaded onto the services appliance during manufacturing. If the preloaded version of software matches the version being used in your StorageGRID deployment, you do not need the installation files.

### About this task

To install StorageGRID software on an SG100 or SG1000 services appliance:

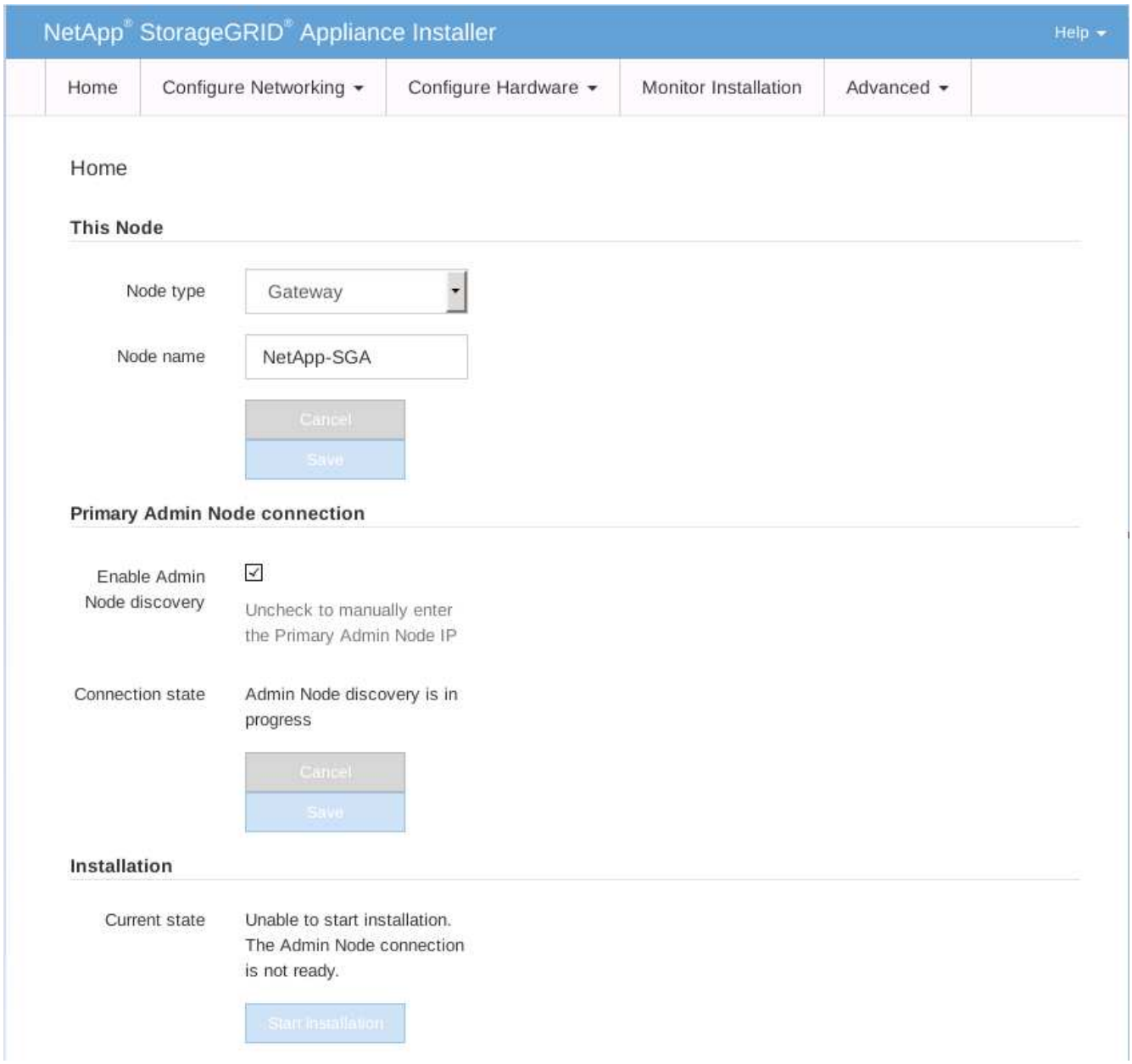
- For a primary Admin Node, you specify the name of the node and then upload the appropriate software packages (if required).
- For a non-primary Admin Node or a Gateway Node, you specify or confirm the IP address of the primary Admin Node and the name of the node.
- You start the installation and wait as volumes are configured and the software is installed.
- Partway through the process, the installation pauses. To resume the installation, you must sign into the Grid Manager and configure the pending node as a replacement for the failed node.
- After you have configured the node, the appliance installation process completes, and the appliance is rebooted.

### Steps

1. Open a browser and enter one of the IP addresses for the SG100 or SG1000 services appliance.

   ```
   https://Controller_IP:8443
   ```

   The StorageGRID Appliance Installer Home page appears.

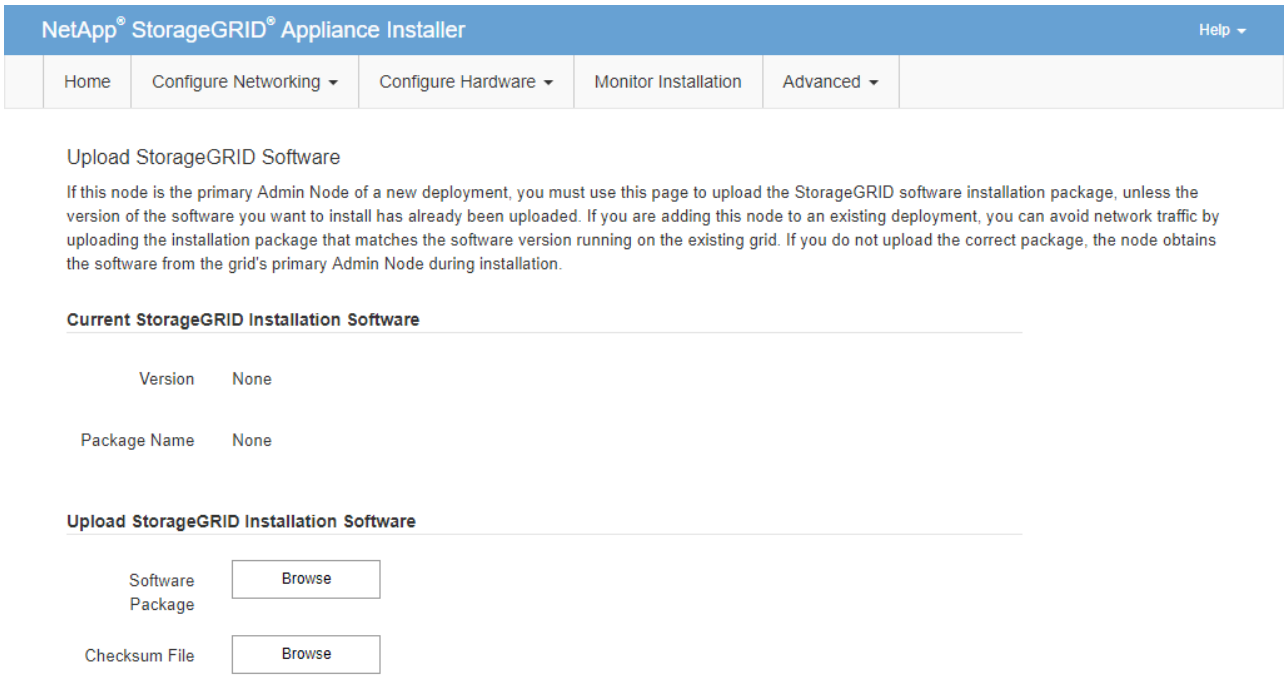



2. To install a Primary Admin Node:
   a. In the This Node section, for **Node Type**, select **Primary Admin**.
   b. In the **Node Name** field, enter the same name that was used for the node you are recovering, and click **Save**.
   c. In the Installation section, check the software version listed under Current state

      If the version of software that is ready to install is correct, skip ahead to the Installation step.

   d. If you need to upload a different version of software, under the **Advanced** menu, select **Upload StorageGRID Software**.

      TheUpload StorageGRID Software page appears.




e. Click **Browse** to upload the **Software Package** and **Checksum File** for StorageGRID software.

   The files are automatically uploaded after you select them.

f. Click **Home** to return to the StorageGRID Appliance Installer Home page.

3. To install a Gateway Node or non-Primary Admin Node:

   a. In the This Node section, for **Node Type**, select **Gateway** or **Non-Primary Admin**, depending on the type of node you are restoring.

   b. In the **Node Name** field, enter the same name that was used for the node you are recovering, and click **Save**.

   c. In the Primary Admin Node connection section, determine whether you need to specify the IP address for the primary Admin Node.

      The StorageGRID Appliance Installer can discover this IP address automatically, assuming the primary Admin Node, or at least one other grid node with ADMIN_IP configured, is present on the same subnet.

   d. If this IP address is not shown or you need to change it, specify the address:

| Option | Description |
|---|---|
| Manual IP entry | a. Unselect the **Enable Admin Node discovery** check box.<br>b. Enter the IP address manually.<br>c. Click **Save**.<br>d. Wait while the connection state for the new IP address becomes "ready." |

| Option | Description |
| --- | --- |
| Automatic discovery of all connected primary Admin Nodes | a. Select the **Enable Admin Node discovery** check box.<br>b. From the list of discovered IP addresses, select the primary Admin Node for the grid where this services appliance will be deployed.<br>c. Click **Save**.<br>d. Wait while the connection state for the new IP address becomes “ready.” |

4. In the Installation section, confirm that the current state is Ready to start installation of node name and that the **Start Installation** button is enabled.

   If the **Start Installation** button is not enabled, you might need to change the network configuration or port settings. For instructions, see the installation and maintenance instructions for your appliance.

5. From the StorageGRID Appliance Installer home page, click **Start Installation**.

   The Current state changes to “Installation is in progress,” and the Monitor Installation page is displayed.

   > If you need to access the Monitor Installation page manually, click **Monitor Installation** from the menu bar.

**Related information**

SG100 and SG1000 services appliances

#### Monitor services appliance installation

The StorageGRID Appliance Installer provides status until installation is complete. When the software installation is complete, the appliance is rebooted.

1. To monitor the installation progress, click **Monitor Installation** from the menu bar.

   The Monitor Installation page shows the installation progress.

Monitor Installation

| | |
|---|---|
| 1. Configure storage | Complete |
| 2. Install OS | Running |

| Step | Progress | Status |
|---|---|---|
| Obtain installer binaries | | Complete |
| Configure installer | | Complete |
| Install OS | | Installer VM running |

| | |
|---|---|
| 3. Install StorageGRID | Pending |
| 4. Finalize installation | Pending |

The blue status bar indicates which task is currently in progress. Green status bars indicate tasks that have completed successfully.

> The installer ensures that tasks completed in a previous install are not re-run. If you are re-running an installation, any tasks that do not need to be re-run are shown with a green status bar and a status of “Skipped.”

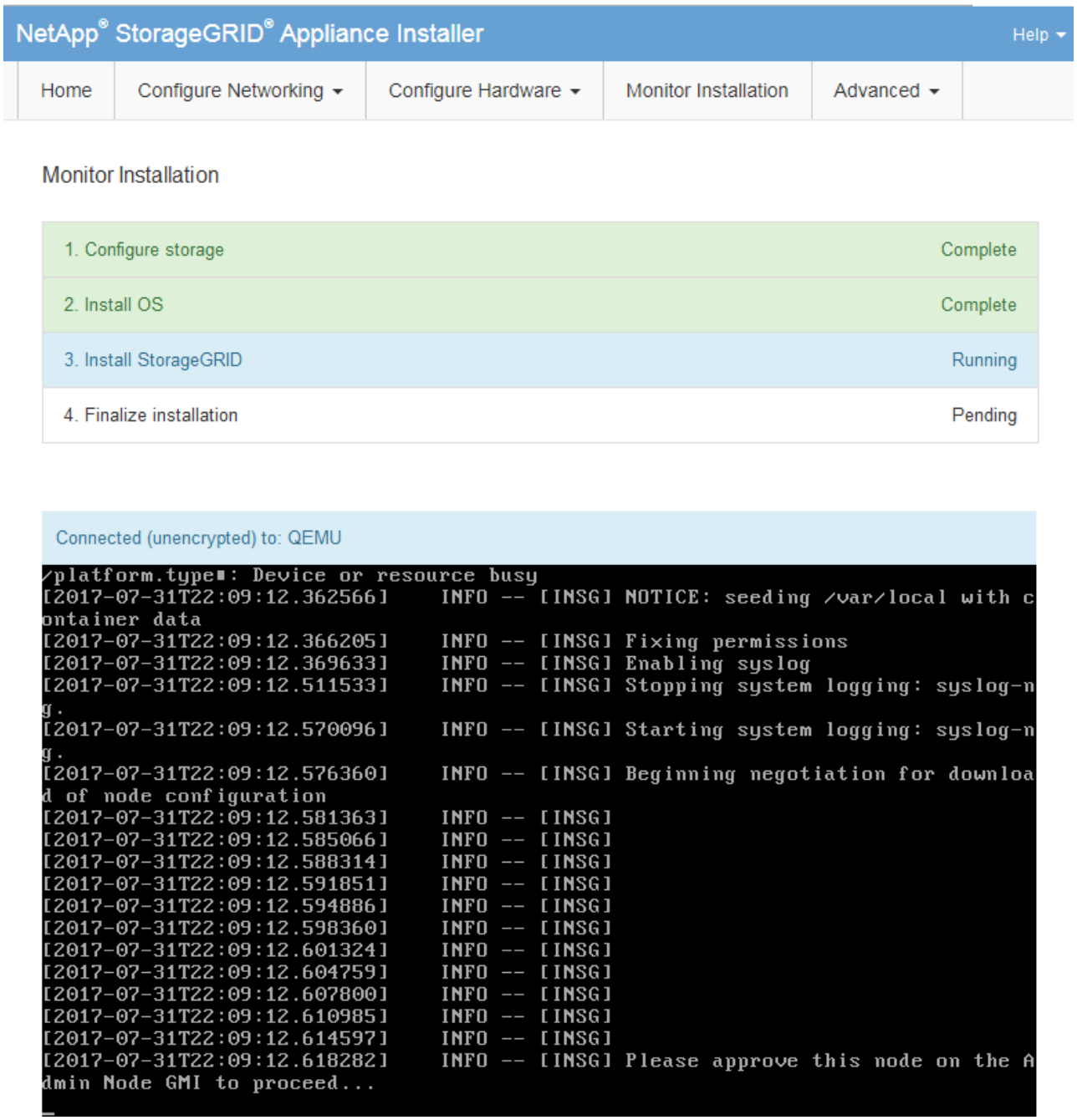
2. Review the progress of first two installation stages.
   - **1. Configure storage**

     During this stage, the installer clears any existing configuration from the drives, and configures host settings.

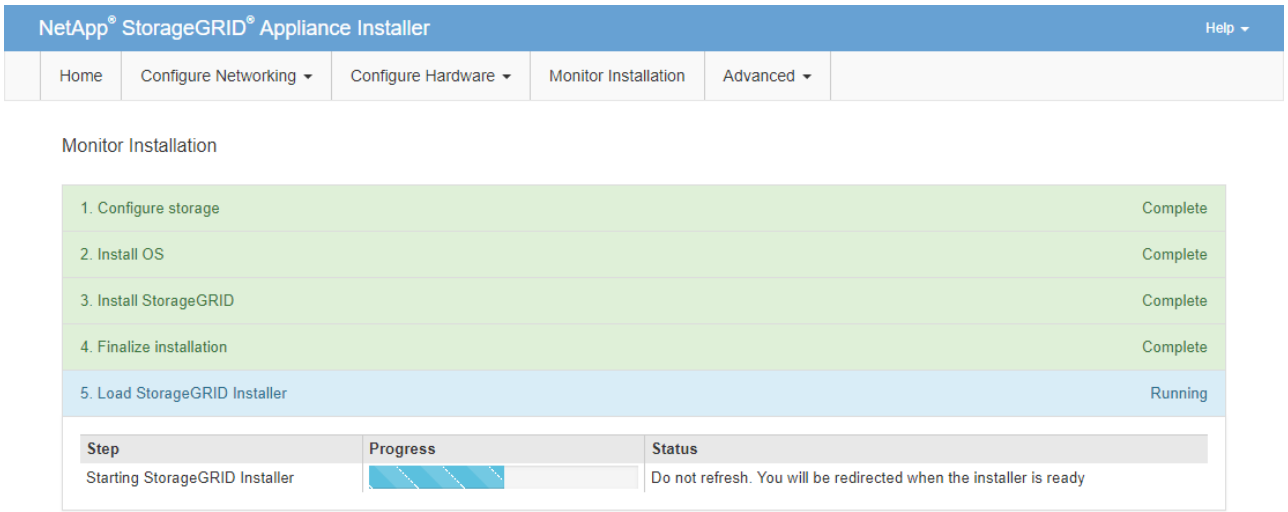
   - **2. Install OS**

     During this stage, the installer copies the base operating system image for StorageGRID from the primary Admin Node to the appliance or installs the base operating system from the installation package for the primary Admin Node.

3. Continue monitoring the installation progress until one of the following occurs:
   - For appliance Gateway Nodes or non-primary appliance Admin Nodes, the **Install StorageGRID** stage pauses and a message appears on the embedded console, prompting you to approve this node on the Admin Node using the Grid Manager.




- For appliance primary Admin Nodes, a fifth phase (Load StorageGRID Installer) appears. If the fifth phase is in progress for more than 10 minutes, refresh the page manually.




4. Go on to the next step of the recovery process for the type of appliance grid node that you are recovering.

| Type of recovery | Reference |
|---|---|
| Gateway Node | Select Start Recovery to configure Gateway Node |
| Non-primary Admin Node | Select Start Recovery to configure non-primary Admin Node |
| Primary Admin Node | Configure replacement primary Admin Node |

## How site recovery is performed by technical support

If an entire StorageGRID site fails or if multiple Storage Nodes fail, you must contact technical support. Technical support will assess your situation, develop a recovery plan, and then recover the failed nodes or site in a way that meets your business objectives, optimizes recovery time, and prevents unnecessary data loss.

Site recovery can only be performed by technical support.

StorageGRID systems are resilient to a wide variety of failures, and you can successfully perform many recovery and maintenance procedures yourself. However, it is difficult to create a simple, generalized site recovery procedure because the detailed steps depend on factors that are specific to your situation. For example:

- **Your business objectives**: After the complete loss of a StorageGRID site, you should evaluate how best to meet your business objectives. For example, do you want to rebuild the lost site in-place? Do you want to replace the lost StorageGRID site in a new location? Every customer's situation is different, and your recovery plan must be designed to address your priorities.
- **Exact nature of the failure**: Before beginning a site recovery, it is important to establish if any nodes at the failed site are intact or if any Storage Nodes contain recoverable objects. If you rebuild nodes or storage volumes that contain valid data, unnecessary data loss could occur.
- **Active ILM policy**: The number, type, and location of object copies in your grid is controlled by your active ILM policy. The specifics of your ILM policy can affect the amount of recoverable data, as well as the specific techniques required for recovery.

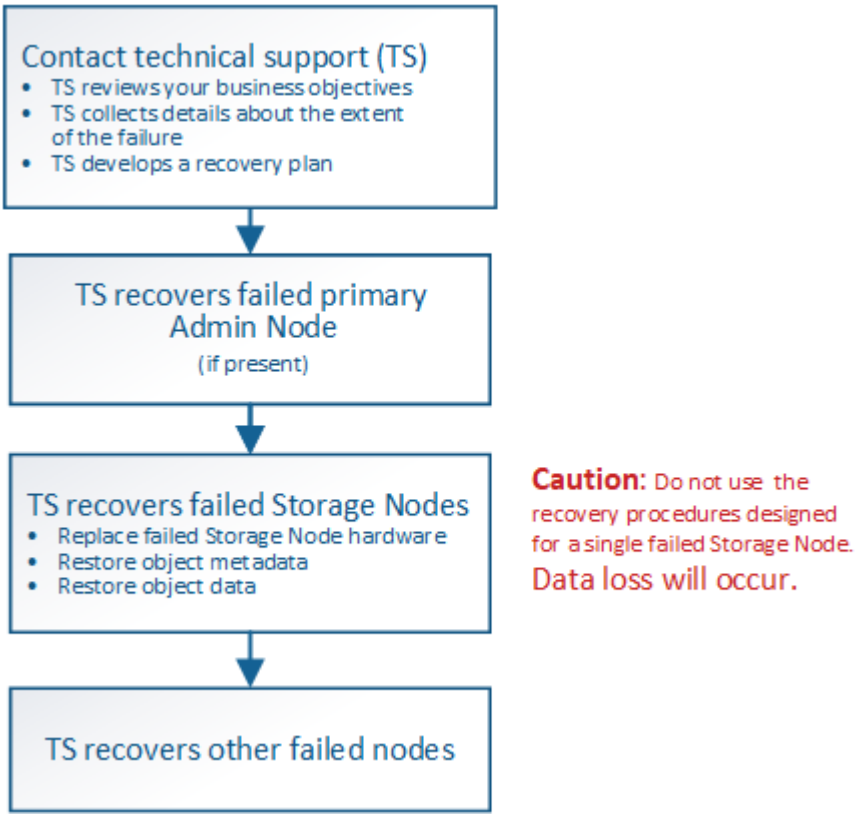
If a site contains the only copy of an object and the site is lost, the object is lost.

- **Bucket (or container) consistency**: The consistency level applied to a bucket (or container) affects whether StorageGRID fully replicates object metadata to all nodes and sites before telling a client that object ingest was successful. If your consistency level allows for eventual consistency, some object metadata might have been lost in the site failure. This can affect the amount of recoverable data and potentially the details of the recovery procedure.
- **History of recent changes**: The details of your recovery procedure can be affected by whether any maintenance procedures were in progress at the time of the failure or whether any recent changes were made to your ILM policy. Technical support must assess the recent history of your grid as well as its current situation before beginning a site recovery.

### Overview of site recovery

This is a general overview of the process that technical support uses to recover a failed site.

Site recovery can only be performed by technical support.




1. Contact technical support.

   Technical support does a detailed assessment of the failure and works with you to review your business objectives. Based on this information, technical support develops a recovery plan tailored for your situation.

2. Technical support recovers the primary Admin Node if it has failed.
3. Technical support recovers all Storage Nodes, following this outline:
   a. Replace Storage Node hardware or virtual machines as required.
   b. Restore object metadata to the failed site.

c. Restore object data to the recovered Storage Nodes.

> Data loss will occur if the recovery procedures for a single failed Storage Node are used.

> When an entire site has failed, specialized commands are required to successfully restore objects and object metadata.

4. Technical support recovers other failed nodes.

   After object metadata and data have been recovered, failed Gateway Nodes, non-primary Admin Nodes, or Archive Nodes can be recovered using standard procedures.

**Related information**

Site decommission

## Decommission procedure

You can perform a decommission procedure to permanently remove grid nodes or an entire site from the StorageGRID system.

To remove a grid node or a site, you perform one of the following decommission procedures:

- Perform a **node decommission** to remove one or more nodes, which can be at one or more sites. The nodes you remove can be online and connected to the StorageGRID system, or they can be offline and disconnected.
- Perform a **connected site decommission** to remove a site in which all nodes are connected to StorageGRID.
- Perform a **disconnected site decommission** to remove a site in which all nodes are disconnected from StorageGRID.

> Before performing a disconnected site decommission, you must contact your NetApp account representative. NetApp will review your requirements before enabling all steps in the Decommission Site wizard. You should not attempt a disconnected site decommission if you believe it might be possible to recover the site or to recover object data from the site.

If a site contains a mixture of connected ( ) and disconnected nodes ( or ), you must bring all offline nodes back online.

> If you need to perform a second maintenance procedure, you can pause the decommission procedure while the Storage Nodes are being removed. The **Pause** button is enabled only when the ILM evaluation or erasure-coded data decommissioning stages are reached; however, ILM evaluation (data migration) will continue to run in the background. After the second maintenance procedure is complete, you can resume decommissioning.

**Related information**

Grid node decommission

Site decommission

## Grid node decommission

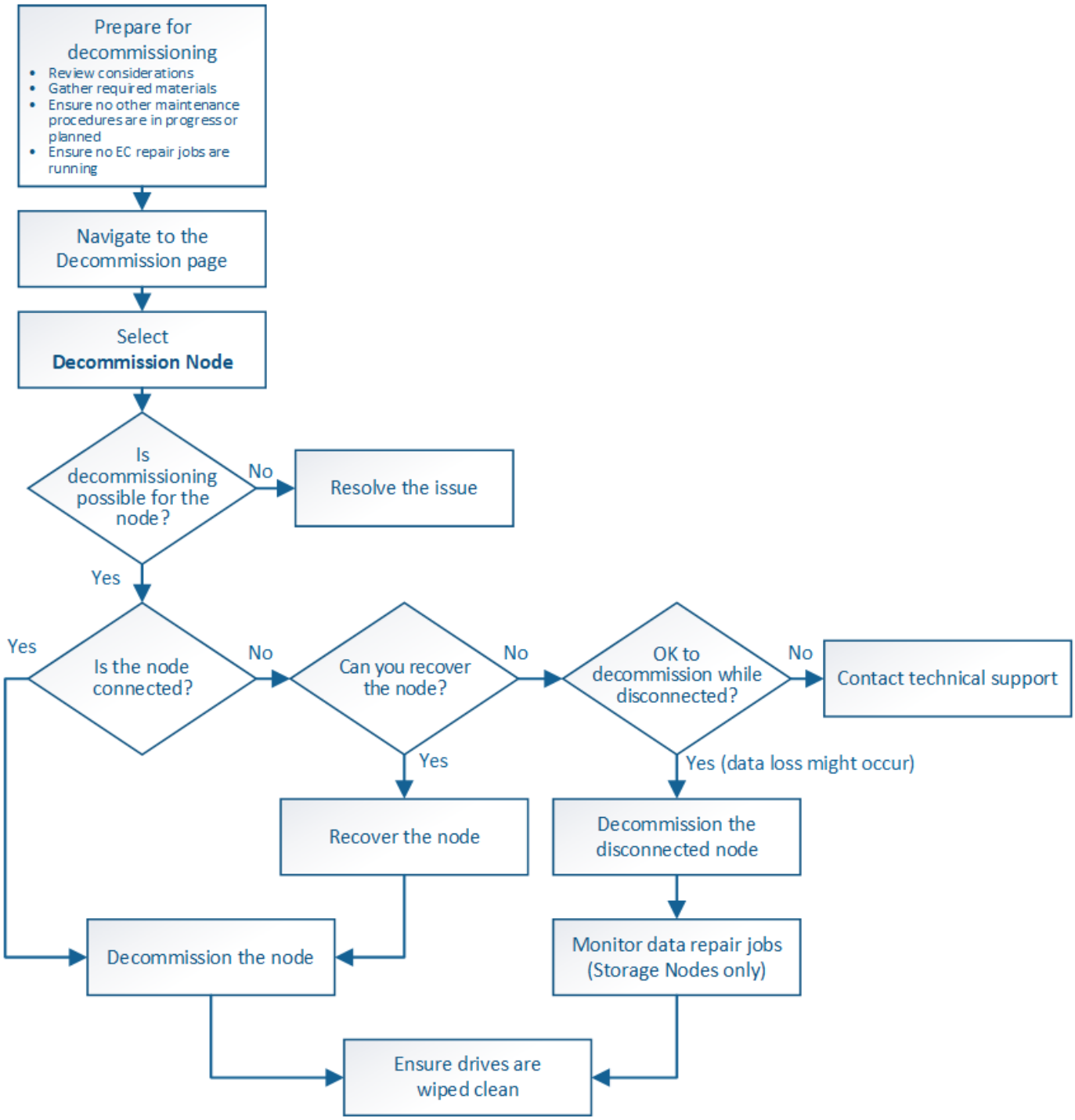
You can use the node decommission procedure to remove one or more Storage Nodes, Gateway Nodes, or non-primary Admin Nodes at one or more sites. You cannot decommission the primary Admin Node or an Archive Node.

In general, you should decommission grid nodes only while they are connected to the StorageGRID system and all nodes are in normal health (have green icons on the **NODES** pages and on the **Decommission Nodes** page). However, if required, you can decommission a grid node that is disconnected. Before removing a disconnected node, make sure you understand the implications and restrictions of that process.

Use the node decommission procedure when any of the following are true:

- You have added a larger Storage Node to the system and you want to remove one or more smaller Storage Nodes, while at the same time preserving objects.
- You require less total storage.
- You no longer require a Gateway Node.
- You no longer require a non-primary Admin Node.
- Your grid includes a disconnected node that you cannot recover or bring back online.

The flowchart shows the high-level steps for decommissioning grid nodes.




**Prepare to decommission grid nodes**

You must review the considerations for removing grid nodes and confirm no repair jobs are active for erasure-coded data.

**Considerations for grid node decommission**

Before you start this procedure to decommission one or more nodes, you must understand the implications of removing each type of node. Upon the successful decommissioning of a node, its services will be disabled and the node will be automatically shut down.

You cannot decommission a node if doing so will leave StorageGRID in an invalid state. The following rules are enforced:

- You cannot decommission the primary Admin Node.
- You cannot decommission Archive Nodes.
- You cannot decommission an Admin Node or a Gateway Node if one of its network interfaces is part of a high availability (HA) group.
- You cannot decommission a Storage Node if its removal would affect the ADC quorum.
- You cannot decommission a Storage Node if it is required for the active ILM policy.
- You should not decommission more than 10 Storage Nodes in a single Decommission Node procedure.
- You cannot decommission a connected node if your grid includes any disconnected nodes (nodes whose health is Unknown or Administratively Down). You must decommission or recover the disconnected nodes first.
- If your grid contains multiple disconnected nodes, the software requires you to decommission them all at the same time, which increases the potential for unexpected results.
- If a disconnected node cannot be removed (for example, a Storage Node that is required for the ADC quorum), no other disconnected node can be removed.
- If you want to replace an older appliance with a newer appliance, consider cloning the appliance node instead of decommissioning the old node and adding the new node in an expansion.

> Do not remove a grid node's virtual machine or other resources until instructed to do so in decommission procedures.

#### Considerations for Admin Node or Gateway Node decommission

Review the following considerations before decommissioning an Admin Node or a Gateway Node.

- The decommission procedure requires exclusive access to some system resources, so you must confirm that no other maintenance procedures are running.
- You cannot decommission the primary Admin Node.
- You cannot decommission an Admin Node or a Gateway Node if one of its network interfaces is part of a high availability (HA) group. You must first remove the network interfaces from the HA group. See the instructions for administering StorageGRID.
- As required, you can safely change the ILM policy while decommissioning a Gateway Node or an Admin Node.
- If you decommission an Admin Node and single sign-on (SSO) is enabled for your StorageGRID system, you must remember to remove the node's relying party trust from Active Directory Federation Services (AD FS).

#### Related information

Administer StorageGRID

#### Considerations for Storage Node decommission

If you plan to decommission a Storage Node, you must understand how StorageGRID manages the object data and metadata on that node.

The following considerations and restrictions apply when decommissioning Storage Nodes:

- The system must, at all times, include enough Storage Nodes to satisfy operational requirements, including the ADC quorum and the active ILM policy. To satisfy this restriction, you might need to add a new Storage Node in an expansion operation before you can decommission an existing Storage Node.
- If the Storage Node is disconnected when you decommission it, the system must reconstruct the data using data from the connected Storage Nodes, which can result in data loss.
- When you remove a Storage Node, large volumes of object data must be transferred over the network. Although these transfers should not affect normal system operations, they can have an impact on the total amount of network bandwidth consumed by the StorageGRID system.
- Tasks associated with Storage Node decommissioning are given a lower priority than tasks associated with normal system operations. This means that decommissioning does not interfere with normal StorageGRID system operations, and does not need to be scheduled for a period of system inactivity. Because decommissioning is performed in the background, it is difficult to estimate how long the process will take to complete. In general, decommissioning finishes more quickly when the system is quiet, or if only one Storage Node is being removed at a time.
- It might take days or weeks to decommission a Storage Node. Plan this procedure accordingly. While the decommission process is designed to not impact system operations, it can limit other procedures. In general, you should perform any planned system upgrades or expansions before you remove grid nodes.
- Decommission procedures that involve Storage Nodes can be paused during certain stages to allow other maintenance procedures to run if needed, and resumed once they are complete.
- You cannot run data repair operations on any grid nodes when a decommission task is running.
- You should not make any changes to the ILM policy while a Storage Node is being decommissioned.
- When you remove a Storage Node, data on the node is migrated to other grid nodes; however, this data is not completely removed from the decommissioned grid node. To permanently and securely remove data, you must wipe the decommissioned grid node's drives after the decommission procedure is complete.
- When you decommission a Storage Node, the following alerts and alarms might be raised and you might receive related email and SNMP notifications:
  - **Unable to communicate with node** alert. This alert is triggered when you decommission a Storage Node that includes the ADC service. The alert is resolved when the decommission operation completes.
  - VSTU (Object Verification Status) alarm. This notice-level alarm indicates that the Storage Node is going into maintenance mode during the decommission process.
  - CASA (Data Store Status) alarm. This major-level alarm indicates that the Cassandra database is going down because services have stopped.

**Related information**

Restore object data to storage volume, if required

### Understand the ADC quorum

You might not be able to decommission certain Storage Nodes at a data center site if too few Administrative Domain Controller (ADC) services would remain after the decommissioning. This service, which is found on some Storage Nodes, maintains grid topology information and provides configuration services to the grid. The StorageGRID system requires a quorum of ADC services to be available at each site and at all times.

You cannot decommission a Storage Node if removing the node would cause the ADC quorum to no longer be

met. To satisfy the ADC quorum during a decommissioning, a minimum of three Storage Nodes at each data center site must have the ADC service. If a data center site has more than three Storage Nodes with the ADC service, a simple majority of those nodes must remain available after the decommissioning ((0.5 * `Storage Nodes with ADC`) + 1).

For example, suppose a data center site currently includes six Storage Nodes with ADC services and you want to decommission three Storage Nodes. Because of the ADC quorum requirement, you must complete two decommission procedures, as follows:

- In the first decommission procedure, you must ensure that four Storage Nodes with ADC services remain available ((0.5 * 6) +1) . This means that you can only decommission two Storage Nodes initially.
- In the second decommission procedure, you can remove the third Storage Node because the ADC quorum now only requires three ADC services to remain available ((0.5 * 4) + 1).

If you need to decommission a Storage Node but are unable to because of the ADC quorum requirement, you must add a new Storage Node in an expansion and specify that it should have an ADC service. Then, you can decommission the existing Storage Node.

**Related information**

Expand your grid

### Review ILM policy and storage configuration

If you plan to decommission a Storage Node, you should review your StorageGRID system's ILM policy before starting the decommissioning process.

During decommissioning, all object data is migrated from the decommissioned Storage Node to other Storage Nodes.

> The ILM policy you have *during* the decommission will be the one used *after* the decommission. You must ensure this policy meets your data requirements both before you start the decommission and after the decommission is complete.

You should review the rules in the active ILM policy to ensure that the StorageGRID system will continue to have enough capacity of the correct type and in the correct locations to accommodate the decommissioning of a Storage Node.

Consider the following:

- Will it be possible for ILM evaluation services to copy object data such that ILM rules are satisfied?
- What happens if a site becomes temporarily unavailable while decommissioning is in progress? Can additional copies be made in an alternate location?
- How will the decommissioning process affect the final distribution of content? As described in Consolidate Storage Nodes, you should add new Storage Nodes before decommissioning old ones. If you add a larger replacement Storage Node after decommissioning a smaller Storage Node, the old Storage Nodes could be close to capacity and the new Storage Node could have almost no content. Most write operations for new object data would then be directed at the new Storage Node, reducing the overall efficiency of system operations.
- Will the system, at all times, include enough Storage Nodes to satisfy the active ILM policy?

> An ILM policy that cannot be satisfied will lead to backlogs and alarms, and can halt operation of the StorageGRID system.

Verify that the proposed topology that will result from the decommissioning process satisfies the ILM policy by assessing the factors listed in the table.

| Area to assess | Notes |
| --- | --- |
| Available capacity | Will there be enough storage capacity to accommodate all of the object data stored in the StorageGRID system, including the permanent copies of object data currently stored on the Storage Node to be decommissioned?Will there be enough capacity to handle the anticipated growth in stored object data for a reasonable interval of time after decommissioning is complete? |
| Location of storage | If enough capacity remains in the StorageGRID system as a whole, is the capacity in the right locations to satisfy the StorageGRID system's business rules? |
| Storage type | Will there be enough storage of the appropriate type after decommissioning is complete? For example, ILM rules might dictate that content be moved from one type of storage to another as content ages. If so, you must ensure that enough storage of the appropriate type is available in the final configuration of the StorageGRID system. |

**Related information**

Manage objects with ILM

Expand your grid

### Decommission disconnected Storage Nodes

## You must understand what can happen if you decommission a Storage Node while it is disconnected (health is Unknown or Administratively Down).

When you decommission a Storage Node that is disconnected from the grid, StorageGRID uses data from other Storage Nodes to reconstruct the object data and metadata that was on the disconnected node. It does this by automatically starting data repair jobs at the end of the decommissioning process.

Before decommissioning a disconnected Storage Node, be aware of the following:

- You should never decommission a disconnected node unless you are sure it cannot be brought online or recovered.

  > Do not perform this procedure if you believe it might be possible to recover object data from the node. Instead, contact technical support to determine if node recovery is possible.

- If a disconnected Storage Node contains the only copy of an object, that object will be lost when you decommission the node. The data repair jobs can only reconstruct and recover objects if at least one replicated copy or enough erasure-coded fragments exist on Storage Nodes that are currently connected.

- When you decommission a disconnected Storage Node, the decommission procedure completes relatively quickly. However, the data repair jobs can take days or weeks to run and are not monitored by the decommission procedure. You must manually monitor these jobs and restart them as needed. See Check data repair jobs.
- If you decommission more than one disconnected Storage Node at a time, data loss might occur. The system might not be able to reconstruct data if too few copies of object data, metadata, or erasure-coded fragments remain available.

> If you have more than one disconnected Storage Node that you cannot recover, contact technical support to determine the best course of action.

#### Consolidate Storage Nodes

You can consolidate Storage Nodes to reduce the Storage Node count for a site or deployment while increasing storage capacity.

When you consolidate Storage Nodes, you expand the StorageGRID system to add new, larger capacity Storage Nodes and then decommission the old, smaller capacity Storage Nodes. During the decommission procedure, objects are migrated from the old Storage Nodes to the new Storage Nodes.

> If you are consolidating older and smaller appliances with new models or larger capacity appliances, you many use the node clone feature or the node clone procedure and the decommission procedure if you are not doing a one-to-one replacement.

For example, you might add two new, larger capacity Storage Nodes to replace three older Storage Nodes. You would first use the expansion procedure to add the two new, larger Storage Nodes, and then use the decommission procedure to remove the three old, smaller capacity Storage Nodes.

By adding new capacity before removing existing Storage Nodes, you ensure a more balanced distribution of data across the StorageGRID system. You also reduce the possibility that an existing Storage Node might be pushed beyond the storage watermark level.

**Related information**

Expand your grid

#### Decommission multiple Storage Nodes

If you need to remove more than one Storage Node, you can decommission them either sequentially or in parallel.

- If you decommission Storage Nodes sequentially, you must wait for the first Storage Node to complete decommissioning before starting to decommission the next Storage Node.
- If you decommission Storage Nodes in parallel, the Storage Nodes simultaneously process decommission tasks for all Storage Nodes being decommissioned. This can result in a situation where all permanent copies of a file are marked as “read-only,” temporarily disabling deletion in grids where this functionality is enabled.

#### Check data repair jobs

Before decommissioning a grid node, you must confirm that no data repair jobs are

active. If any repairs have failed, you must restart them and allow them to complete before performing the decommission procedure.

If you need to decommission a disconnected Storage Node, you will also complete these steps after the decommission procedure completes in order to ensure the data repair job has completed successfully. You must ensure that any erasure-coded fragments that were on the removed node have been restored successfully.

These steps only apply to systems that have erasure-coded objects.

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@grid_node_IP`

      When you are logged in as root, the prompt changes from `$` to `#`.

   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.
2. Check for running repairs: `repair-data show-ec-repair-status`
   - If you have never run a data repair job, the output is `No job found`. You do not need to restart any repair jobs.
   - If the data repair job was run previously or is running currently, the output lists information for the repair. Each repair has a unique repair ID. Go to the next step.

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time End Time State Est/Affected Bytes Repaired
Retry Repair
=========================================================================
===========
949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359 0
Yes
949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359 0
Yes
949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359 0
Yes
```

3. If the State for all repairs is `Success`, you do not need to restart any repair jobs.
4. If the State for any repair is `Failure`, you must restart that repair.
   a. Obtain the repair ID for the failed repair from the output.
   b. Run the `repair-data start-ec-node-repair` command.

      Use the `--repair-id` option to specify the Repair ID. For example, if you want to retry a repair with

repair ID 949292, run this command: `repair-data start-ec-node-repair --repair-id 949292`

c. Continue to track the status of EC data repairs until the State for all repairs is `Success`.

#### Gather required materials

Before performing a grid node decommission, you must obtain the following information.

| Item | Notes |
|---|---|
| Recovery Package `.zip` file | You must download the most recent Recovery Package `.zip` file (`sgws-recovery-package-`*`id-revision`*`.zip`). You can use the Recovery Package file to restore the system if a failure occurs. |
| `Passwords.txt` file | This file contains the passwords required to access grid nodes on the command line and is included in the Recovery Package. |
| Provisioning passphrase | The passphrase is created and documented when the StorageGRID system is first installed. The provisioning passphrase is not in the `Passwords.txt` file. |
| Description of StorageGRID system's topology before decommissioning | If available, obtain any documentation that describes the system's current topology. |

#### Related information

Web browser requirements

#### Access Decommission Nodes page

When you access the Decommission Nodes page in the Grid Manager, you can see at a glance which nodes can be decommissioned.

#### What you'll need

- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Maintenance or Root Access permission.

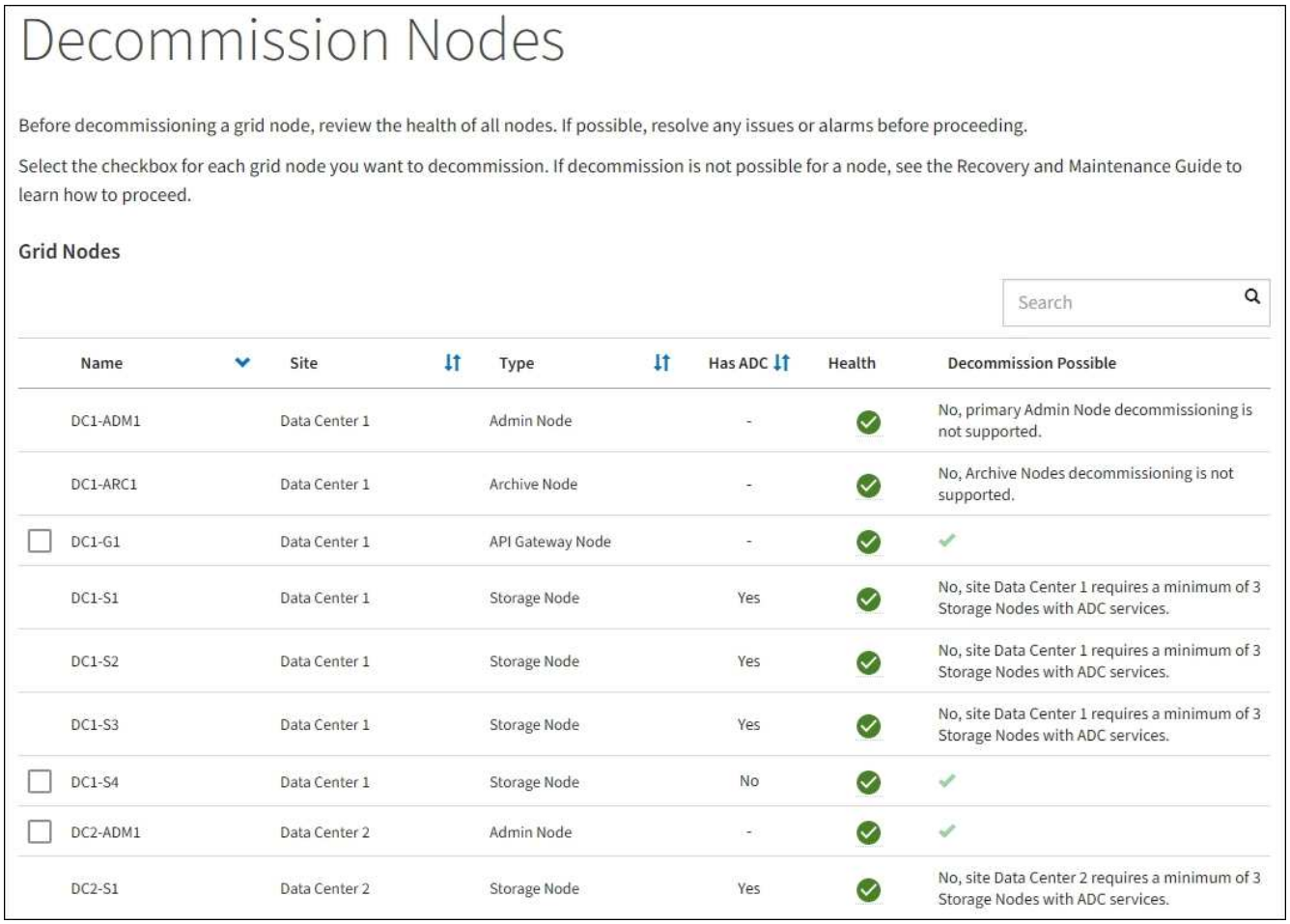
#### Steps

1. Select **MAINTENANCE** > **Tasks** > **Decommission**.
2. Select **Decommission Nodes**.

   The Decommission Nodes page appears. From this page, you can:

   - Determine which grid nodes can be decommissioned currently.
   - See the health of all grid nodes
   - Sort the list in ascending or descending order by **Name**, **Site**, **Type**, or **Has ADC**.
   - Enter search terms to quickly find particular nodes. For example, this page shows grid nodes in two data centers. The Decommission Possible column indicates that you can decommission the Gateway

Node, one of the five Storage Nodes, and the non-primary Admin Node.




3. Review the **Decommission Possible** column for each node you want to decommission.

   If a grid node can be decommissioned, this column includes a green check mark, and the left-most column includes a check box. If a node cannot be decommissioned, this column describes the issue. If there is more than one reason a node cannot be decommissioned, the most critical reason is shown.

| Decommission Possible reason | Description | Steps to resolve |
|---|---|---|
| No, node type decommissioning is not supported. | You cannot decommission the primary Admin Node or an Archive Node. | None. |

| Decommission Possible reason | Description | Steps to resolve |
|---|---|---|
| No, at least one grid node is disconnected.<br><br>**Note:** This message is shown for connected grid nodes only. | You cannot decommission a connected grid node if any grid node is disconnected.<br><br>The **Health** column includes one of these icons for grid nodes that are disconnected:<br><br>• (gray): Administratively Down<br>• (blue): Unknown | Go to the step that lists the decommission procedure choices. |
| No, one or more required nodes is currently disconnected and must be recovered.<br><br>**Note:** This message is shown for disconnected grid nodes only. | You cannot decommission a disconnected grid node if one or more required nodes is also disconnected (for example, a Storage Node that is required for the ADC quorum). | a. Review the Decommission Possible messages for all disconnected nodes.<br>b. Determine which nodes cannot be decommissioned because they are required.<br>◦ If the Health of a required node is Administratively Down, bring the node back online.<br>◦ If the health of a required node is Unknown, perform a node recovery procedure to recover the required node. |
| No, member of HA group(s): *x*. Before you can decommission this node, you must remove it from all HA groups. | You cannot decommission an Admin Node or a Gateway Node if a node interface belongs to a high availability (HA) group. | Edit the HA group to remove the node's interface or remove the entire HA group. See the instructions for administering StorageGRID. |
| No, site *x* requires a minimum of *n* Storage Nodes with ADC services. | **Storage Nodes only.** You cannot decommission a Storage Node if insufficient nodes would remain at the site to support ADC quorum requirements. | Perform an expansion. Add a new Storage Node to the site, and specify that it should have an ADC service. See information about the ADC quorum. |

| Decommission Possible reason | Description | Steps to resolve |
|---|---|---|
| No, one or more Erasure Coding profiles need at least *n* Storage Nodes. If the profile is not used in an ILM rule, you can deactivate it. | **Storage Nodes only.** You cannot decommission a Storage Node unless enough nodes would remain for the existing Erasure Coding profiles.<br><br>For example, if an Erasure Coding profile exists for 4+2 erasure coding, at least 6 Storage Nodes must remain. | For each affected Erasure Coding profile, perform one of the following steps, based on how the profile is being used:<br><br>• **Used in the active ILM policy**: Perform an expansion. Add enough new Storage Nodes to allow erasure coding to continue. See the instructions for expanding StorageGRID.<br>• **Used in an ILM rule but not in the active ILM policy**: Edit or delete the rule and then deactivate the Erasure Coding profile.<br>• **Not used in any ILM rule**: Deactivate the Erasure Coding profile.<br><br>**Note:** An error message appears if you attempt to deactivate an Erasure Coding profile and object data is still associated with the profile. You might need to wait several weeks before trying the deactivation process again.<br><br>Learn about deactivating an Erasure Coding profile in the instructions for managing objects with information lifecycle management. |

4. If decommissioning is possible for the node, determine which procedure you need to perform:

| If your grid includes… | Go to… |
|---|---|
| Any disconnected grid nodes | Decommission disconnected grid nodes |
| Only connected grid nodes | Decommission connected grid nodes |

**Related information**

Check data repair jobs

Understand the ADC quorum

Manage objects with ILM

Expand your grid

Administer StorageGRID

#### Decommission disconnected grid nodes

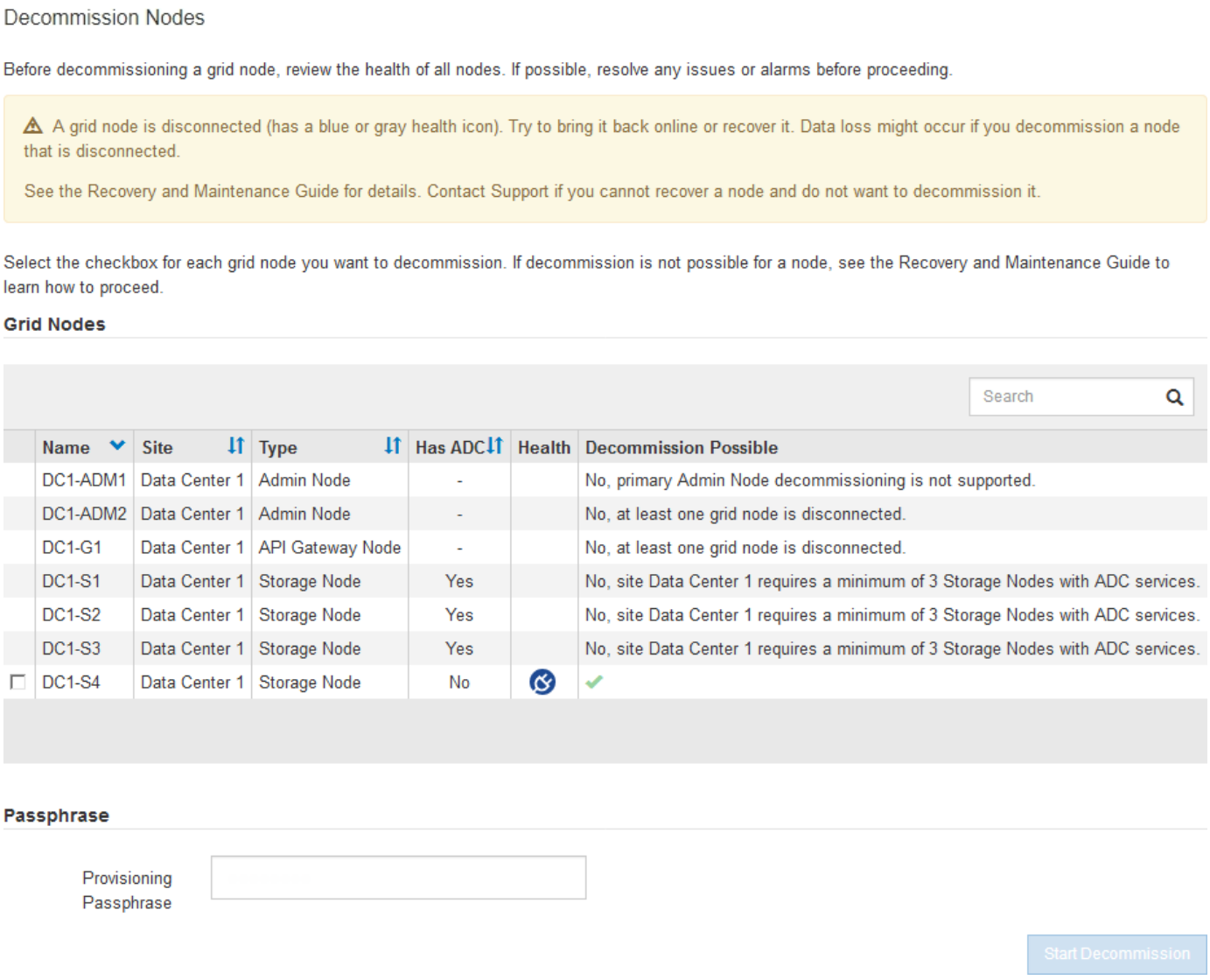
You might need to decommission a node that is not currently connected to the grid (one whose Health is Unknown or Administratively Down).

### What you'll need

- You understand the requirements and considerations for decommissioning grid nodes.
- You have obtained all prerequisite items.
- You have ensured that no data repair jobs are active. See Check data repair jobs.
- You have confirmed that Storage Node recovery is not in progress anywhere in the grid. If it is, you must wait until any Cassandra rebuild performed as part of the recovery is complete. You can then proceed with decommissioning.
- You have ensured that other maintenance procedures will not be run while the node decommission procedure is running, unless the node decommission procedure is paused.
- The **Decommission Possible** column for the disconnected node or nodes you want to decommission includes a green check mark.
- You must have the provisioning passphrase.

### About this task

You can identify disconnected nodes by looking for Unknown (blue) or Administratively Down (gray) icons in the **Health** column. In the example, the Storage Node named DC1-S4 is disconnected; all of the other nodes are connected.



Before decommissioning any disconnected node, note the following:

- This procedure is primarily intended for removing a single disconnected node. If your grid contains multiple disconnected nodes, the software requires you to decommission them all at the same time, which increases the potential for unexpected results.

> Be very careful when decommissioning more than one disconnected grid node at a time, especially if you are selecting multiple disconnected Storage Nodes.

- If a disconnected node cannot be removed (for example, a Storage Node that is required for the ADC quorum), no other disconnected node can be removed.

Before decommissioning a disconnected **Storage Node**, note the following

- You should never decommission a disconnected Storage Node unless you are sure it cannot be brought online or recovered.

> If you believe that object data can still be recovered from the node, do not perform this procedure. Instead, contact technical support to determine if node recovery is possible.

- If you decommission more than one disconnected Storage Node, data loss might occur. The system might not be able to reconstruct data if not enough object copies, erasure-coded fragments, or object metadata remain available.

> If you have more than one disconnected Storage Node that you cannot recover, contact technical support to determine the best course of action.

- When you decommission a disconnected Storage Node, StorageGRID starts data repair jobs at the end of the decommissioning process. These jobs attempt to reconstruct the object data and metadata that was stored on the disconnected node.
- When you decommission a disconnected Storage Node, the decommission procedure completes relatively quickly. However, the data repair jobs can take days or weeks to run and are not monitored by the decommission procedure. You must manually monitor these jobs and restart them as needed. See Check data repair jobs.
- If you decommission a disconnected Storage Node that contains the only copy of an object, the object will be lost. The data repair jobs can only reconstruct and recover objects if at least one replicated copy or enough erasure-coded fragments exist on Storage Nodes that are currently connected.

Before decommissioning a disconnected **Admin Node** or **Gateway Node**, note the following:

- When you decommission a disconnected Admin Node, you will lose the audit logs from that node; however, these logs should also exist on the primary Admin Node.
- You can safely decommission a Gateway Node while it is disconnected.

**Steps**

1. Attempt to bring any disconnected grid nodes back online or to recover them.

   See the recovery procedures for instructions.

2. If you are unable to recover a disconnected grid node and you want to decommission it while it is disconnected, select the check box for that node.

> If your grid contains multiple disconnected nodes, the software requires you to decommission them all at the same time, which increases the potential for unexpected results.

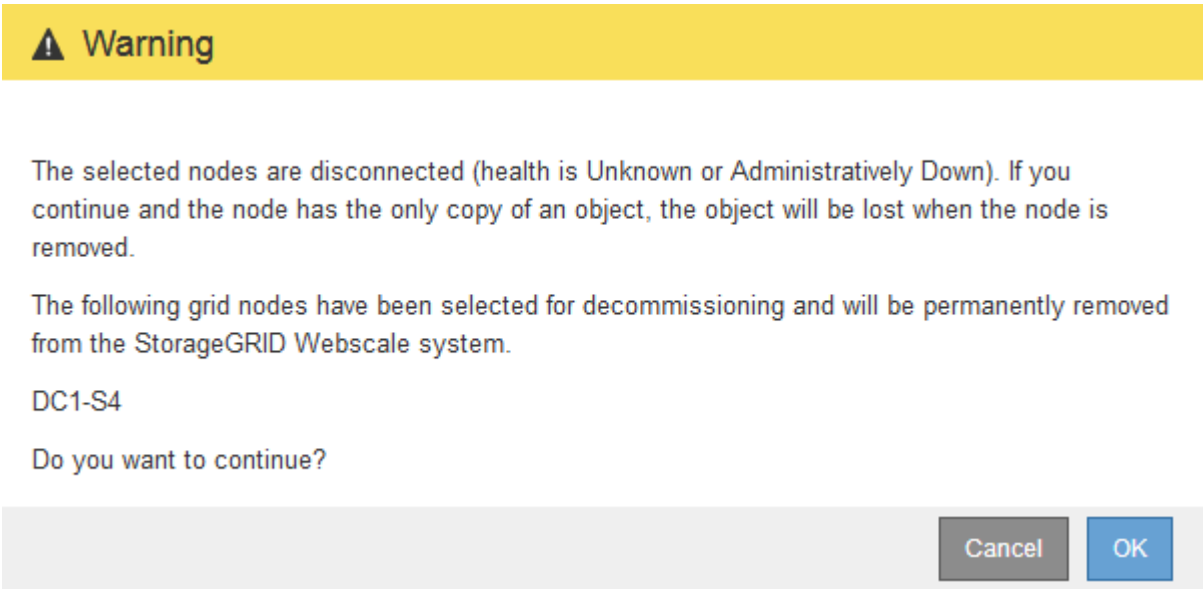
> Be very careful when choosing to decommission more than one disconnected grid node at a time, especially if you are selecting multiple disconnected Storage Nodes. If you have more than one disconnected Storage Node that you cannot recover, contact technical support to determine the best course of action.

3. Enter the provisioning passphrase.

   The **Start Decommission** button is enabled.

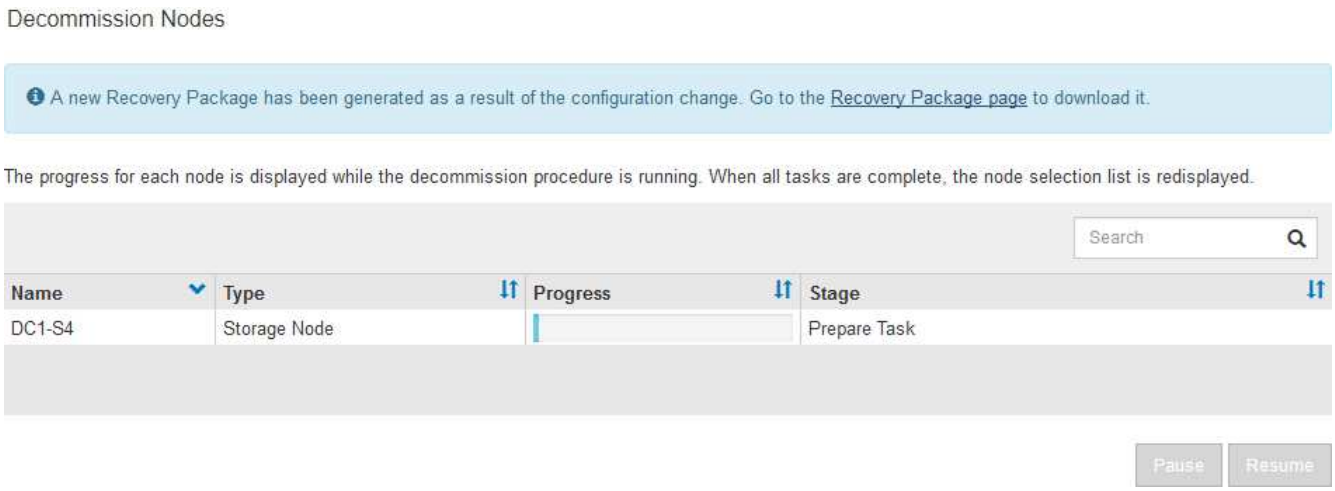
4. Click **Start Decommission**.

   A warning appears, indicating that you have selected a disconnected node and that object data will be lost if the node has the only copy of an object.




5. Review the list of nodes, and click **OK**.

   The decommission procedure starts, and the progress is displayed for each node. During the procedure, a new Recovery Package is generated containing the grid configuration change.




6. As soon as the new Recovery Package is available, click the link or select **MAINTENANCE** > **System** > **Recovery package** to access the Recovery Package page. Then, download the `.zip` file.

   See the instructions for downloading the Recovery Package.

   > Download the Recovery Package as soon as possible to ensure you can recover your grid if something goes wrong during the decommission procedure.

   > The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

7. Periodically monitor the Decommission page to ensure that all selected nodes are decommissioned successfully.

   Storage Nodes can take days or weeks to decommission. When all tasks are complete, the node selection list is redisplayed with a success message. If you decommissioned a disconnected Storage Node, an information message indicates that the repair jobs have been started.

# Decommission Nodes

The previous decommission procedure completed successfully.

Repair jobs for replicated and erasure-coded data have been started. These jobs restore object data that might have been on any disconnected Storage Nodes. To monitor the progress of these jobs and restart them as needed, see the Decommissioning section of the Recovery and Maintenance Guide.

Before decommissioning a grid node, review the health of all nodes. If possible, resolve any issues or alarms before proceeding.

Select the checkbox for each grid node you want to decommission. If decommission is not possible for a node, see the Recovery and Maintenance Guide to learn how to proceed.

**Grid Nodes**

Search

| | Name | Site | Type | Has ADC | Health | Decommission Possible |
|---|---|---|---|---|---|---|
| | DC1-ADM1 | Data Center 1 | Admin Node | - | ✓ | No, primary Admin Node decommissioning is not supported. |
| | DC1-ARC1 | Data Center 1 | Archive Node | - | ✓ | No, Archive Nodes decommissioning is not supported. |
| ☐ | DC1-G1 | Data Center 1 | API Gateway Node | - | ✓ | ✓ |
| | DC1-S1 | Data Center 1 | Storage Node | Yes | ✓ | No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services. |
| | DC1-S2 | Data Center 1 | Storage Node | Yes | ✓ | No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services. |
| | DC1-S3 | Data Center 1 | Storage Node | Yes | ✓ | No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services. |
| ☐ | DC1-S4 | Data Center 1 | Storage Node | No | ✓ | ✓ |
| ☐ | DC2-ADM1 | Data Center 2 | Admin Node | - | ✓ | ✓ |
| | DC2-S1 | Data Center 2 | Storage Node | Yes | ✓ | No, site Data Center 2 requires a minimum of 3 Storage Nodes with ADC services. |

8. After the nodes have shut down automatically as part of the decommission procedure, remove any remaining virtual machines or other resources that are associated with the decommissioned node.

   Do not perform this step until the nodes have shut down automatically.

9. If you are decommissioning a Storage Node, monitor the status of the **replicated data** and **erasure-coded (EC) data** repair jobs that are automatically started during the decommissioning process.

**Replicated data**

- To determine if repairs are complete:
  1. Select **NODES** > ***Storage Node being repaired*** > **ILM**.
  2. Review the attributes in the Evaluation section. When repairs are complete, the **Awaiting - All** attribute indicates 0 objects.
- To monitor the repair in more detail:
  1. Select **SUPPORT** > **Tools** > **Grid topology**.
  2. Select ***grid*** > ***Storage Node being repaired*** > **LDR** > **Data Store**.
  3. Use a combination of the following attributes to determine, as well as possible, if replicated repairs are complete.

     > Cassandra inconsistencies might be present, and failed repairs are not tracked.

     - **Repairs Attempted (XRPA)**: Use this attribute to track the progress of replicated repairs. This attribute increases each time a Storage Node tries to repair a high-risk object. When this attribute does not increase for a period longer than the current scan period (provided by the **Scan Period — Estimated** attribute), it means that ILM scanning found no high-risk objects that need to be repaired on any nodes.

       > High-risk objects are objects that are at risk of being completely lost. This does not include objects that do not satisfy their ILM configuration.

     - **Scan Period — Estimated (XSCM)**: Use this attribute to estimate when a policy change will be applied to previously ingested objects. If the **Repairs Attempted** attribute does not increase for a period longer than the current scan period, it is probable that replicated repairs are done. Note that the scan period can change. The **Scan Period — Estimated (XSCM)** attribute applies to the entire grid and is the maximum of all node scan periods. You can query the **Scan Period — Estimated** attribute history for the grid to determine an appropriate time frame.
- Optionally, to get an estimated percent completion for the replicated repair, add the `show-replicated-repair-status` option to the repair-data command.

  ```
  repair-data show-replicated-repair-status
  ```

  > The `show-replicated-repair-status` option is available for technical preview in StorageGRID 11.6. This feature is under development, and the value returned might be incorrect or delayed. To determine if a repair is complete, use **Awaiting – All**, **Repairs Attempted (XRPA)**, and **Scan Period — Estimated (XSCM)** as described in Monitor repairs.

**Erasure coded (EC) data**

To monitor the repair of erasure-coded data and retry any requests that might have failed:

1. Determine the status of erasure-coded data repairs:
   - Select **SUPPORT** > **Tools** > **Metrics** to view the estimated time to completion and the completion percentage for the current job. Then, select **EC Overview** in the Grafana section. Look at the **Grid EC Job Estimated Time to Completion** and **Grid EC Job Percentage Completed** dashboards.

- Use this command to see the status of a specific `repair-data` operation:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Use this command to list all repairs:

  ```
  repair-data show-ec-repair-status
  ```

  The output lists information, including `repair ID`, for all previously and currently running repairs.

2. If the output shows that the repair operation failed, use the `--repair-id` option to retry the repair.

   This command retries a failed node repair, using the repair ID 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   This command retries a failed volume repair, using the repair ID 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

**After you finish**

As soon as the disconnected nodes have been decommissioned and all data repair jobs have been completed, you can decommission any connected grid nodes as required.

Then, complete these steps after you complete the decommission procedure:

- Ensure that the drives of the decommissioned grid node are wiped clean. Use a commercially available data wiping tool or service to permanently and securely remove data from the drives.
- If you decommissioned an appliance node and the data on the appliance was protected using node encryption, use the StorageGRID Appliance Installer to clear the key management server configuration (Clear KMS). You must clear the KMS configuration if you want to add the appliance to another grid.
  - SG100 and SG1000 services appliances
  - SG5600 storage appliances
  - SG5700 storage appliances
  - SG6000 storage appliances

**Related information**

Grid node recovery procedures

#### Decommission connected grid nodes

You can decommission and permanently remove nodes that are connected to the grid.

- You must understand the requirements and considerations for decommissioning grid nodes.
- You must have gathered all required materials.
- You must have ensured that no data repair jobs are active.
- You must have confirmed that Storage Node recovery is not in progress anywhere in the grid. If it is, you must wait until any Cassandra rebuild performed as part of the recovery is complete. You can then proceed

with decommissioning.

- You must have ensured that other maintenance procedures will not be run while the node decommission procedure is running, unless the node decommission procedure is paused.
- You must have the provisioning passphrase.
- Grid nodes are connected.
- The **Decommission Possible** column for the node or nodes you want to decommission must include a green checkmark.
- All grid nodes must have Normal (green) health . If you see one of these icons in the **Health** column, you must try to resolve the issue:

| Icon | Color | Severity |
|---|---|---|
| | Yellow | Notice |
| | Light orange | Minor |
| | Dark orange | Major |
| | Red | Critical |

- If you previously decommissioned a disconnected Storage Node, the data repair jobs have all completed successfully. See Check data repair jobs.

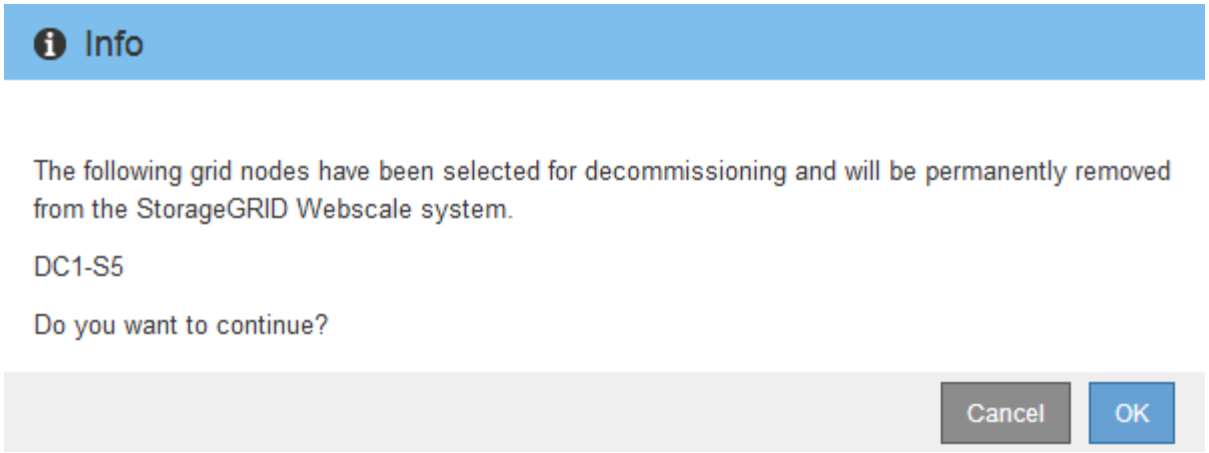
> Do not remove a grid node's virtual machine or other resources until instructed to do so in this procedure.

1. From the Decommission Nodes page, select the check box for each grid node you want to decommission.
2. Enter the provisioning passphrase.

   The **Start Decommission** button is enabled.

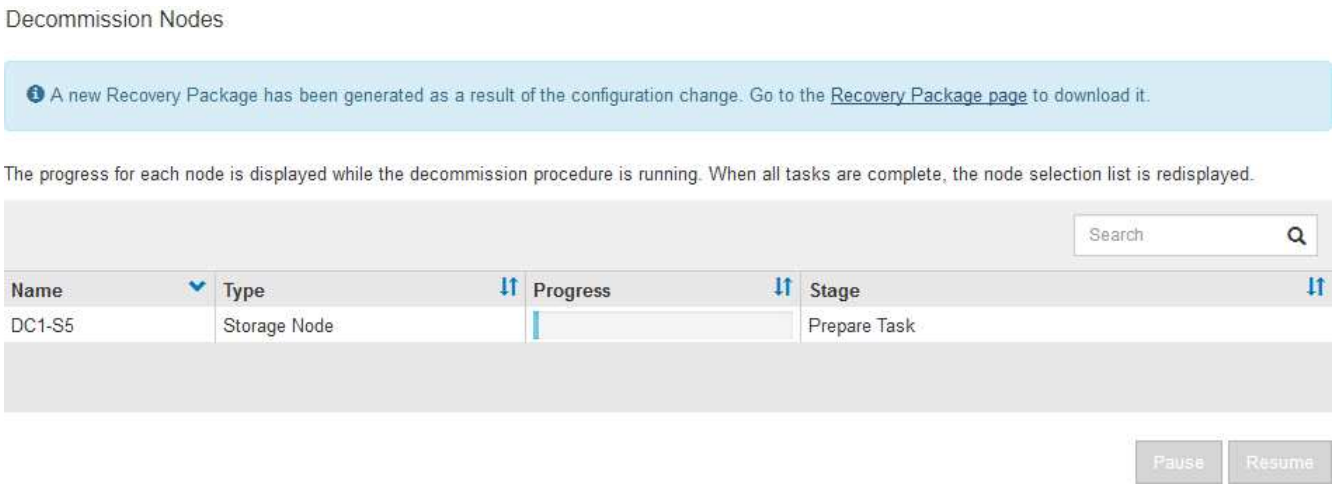
3. Click **Start Decommission**.

   A confirmation dialog box appears.




4. Review the list of selected nodes, and click **OK**.

   The node decommission procedure starts, and the progress is displayed for each node. During the procedure, a new Recovery Package is generated to show the grid configuration change.




   > Do not take a Storage Node offline after the decommission procedure has started. Changing the state might result in some content not being copied to other locations.

5. As soon as the new Recovery Package is available, click the link or select **MAINTENANCE** > **System** > **Recovery package** to access the Recovery Package page. Then, download the `.zip` file.

   See the instructions for downloading the Recovery Package.

   > Download the Recovery Package as soon as possible to ensure you can recover your grid if something goes wrong during the decommission procedure.

6. Periodically monitor the Decommission Nodes page to ensure that all selected nodes are decommissioned successfully.

   Storage Nodes can take days or weeks to decommission. When all tasks are complete, the node selection list is redisplayed with a success message.

# Decommission Nodes

The previous decommission procedure completed successfully.

Before decommissioning a grid node, review the health of all nodes. If possible, resolve any issues or alarms before proceeding.

Select the checkbox for each grid node you want to decommission. If decommission is not possible for a node, see the Recovery and Maintenance Guide to learn how to proceed.

**Grid Nodes**

Search

| Name | Site | Type | Has ADC | Health | Decommission Possible |
|---|---|---|---|---|---|
| DC1-ADM1 | Data Center 1 | Admin Node | - | ✓ | No, primary Admin Node decommissioning is not supported. |
| DC1-ARC1 | Data Center 1 | Archive Node | - | ✓ | No, Archive Nodes decommissioning is not supported. |
| ☐ DC1-G1 | Data Center 1 | API Gateway Node | - | ✓ | ✓ |
| DC1-S1 | Data Center 1 | Storage Node | Yes | ✓ | No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services. |
| DC1-S2 | Data Center 1 | Storage Node | Yes | ✓ | No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services. |
| DC1-S3 | Data Center 1 | Storage Node | Yes | ✓ | No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services. |
| ☐ DC1-S4 | Data Center 1 | Storage Node | No | ✓ | ✓ |
| ☐ DC2-ADM1 | Data Center 2 | Admin Node | - | ✓ | ✓ |
| DC2-S1 | Data Center 2 | Storage Node | Yes | ✓ | No, site Data Center 2 requires a minimum of 3 Storage Nodes with ADC services. |

7. Follow the appropriate step for your platform. For example:
   - **Linux**: You might want to detach the volumes and delete the node configuration files you created during installation.
   - **VMware**: You might want to use the vCenter “Delete from Disk” option to delete the virtual machine. You might also need to delete any data disks that are independent of the virtual machine.
   - **StorageGRID appliance**: The appliance node automatically reverts to an undeployed state where you can access the StorageGRID Appliance Installer. You can power off the appliance or add it to another StorageGRID system.

Complete these steps after you complete the node decommission procedure:

- Ensure that the drives of the decommissioned grid node are wiped clean. Use a commercially available data wiping tool or service to permanently and securely remove data from the drives.
- If you decommissioned an appliance node and the data on the appliance was protected using node encryption, use the StorageGRID Appliance Installer to clear the key management server configuration (Clear KMS). You must clear the KMS configuration if you want to use the appliance in another grid.

  SG100 and SG1000 services appliances

  SG5600 storage appliances

  SG5700 storage appliances

SG6000 storage appliances

**Related information**

Install Red Hat Enterprise Linux or CentOS

#### Pause and resume decommission process for Storage Nodes

If you need to perform a second maintenance procedure, you can pause the decommission procedure for a Storage Node during certain stages. After the other procedure is finished, you can resume decommissioning.

> The **Pause** button is enabled only when the ILM evaluation or erasure-coded data decommissioning stages are reached; however, ILM evaluation (data migration) will continue to run in the background.

**What you'll need**

- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Maintenance or Root Access permission.

**Steps**

1. Select **MAINTENANCE** > **Tasks** > **Decommission**.

   The Decommission page appears.

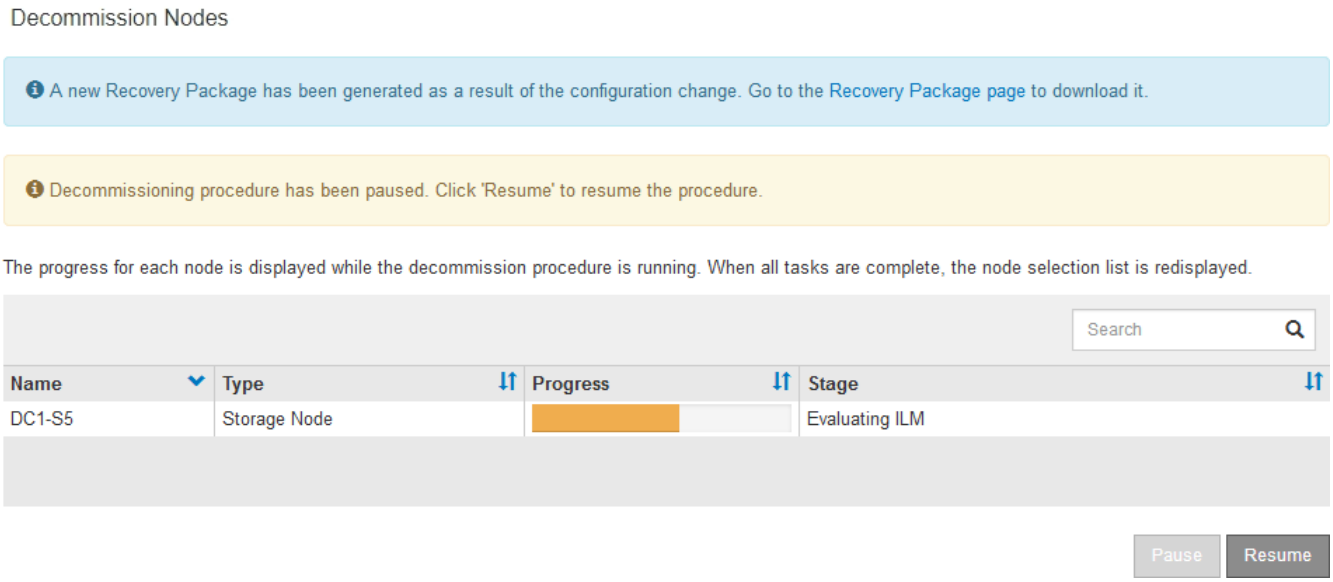
2. Select **Decommission Nodes**.

   The Decommission Nodes page appears. When the decommission procedure reaches either of the following stages, the **Pause** button is enabled.

   - Evaluating ILM
   - Decommissioning Erasure Coded data

3. Select **Pause** to suspend the procedure.

   The current stage is paused, and the **Resume** button is enabled.



4. After the other maintenance procedure is finished, select **Resume** to proceed with the decommission.

#### Troubleshoot node decommissioning

If the node decommission procedure stops because of an error, you can take specific steps to troubleshoot the problem.

**What you'll need**

You must be signed in to the Grid Manager using a supported web browser.

**About this task**

If you shut down the grid node being decommissioned, the task stops until the grid node is restarted. The grid node must be online.

**Steps**

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. In the Grid Topology tree, expand each Storage Node entry, and verify that the DDS and LDR services are both online.

   To perform Storage Node decommissioning, all nodes and all services need to be healthy at the start of an online node/site decommissioning.

3. To view the active grid tasks, select **primary Admin Node** > **CMN** > **Grid Tasks** > **Overview**.
4. Check the status of the decommissioning grid task.
   a. If the status of the decommissioning grid task indicates a problem with saving grid task bundles, select **primary Admin Node** > **CMN** > **Events** > **Overview**
   b. Check the number of Available Audit Relays.

      If the attribute Available Audit Relay is one or greater, the CMN service is connected to at least one ADC service. ADC services act as Audit Relays.

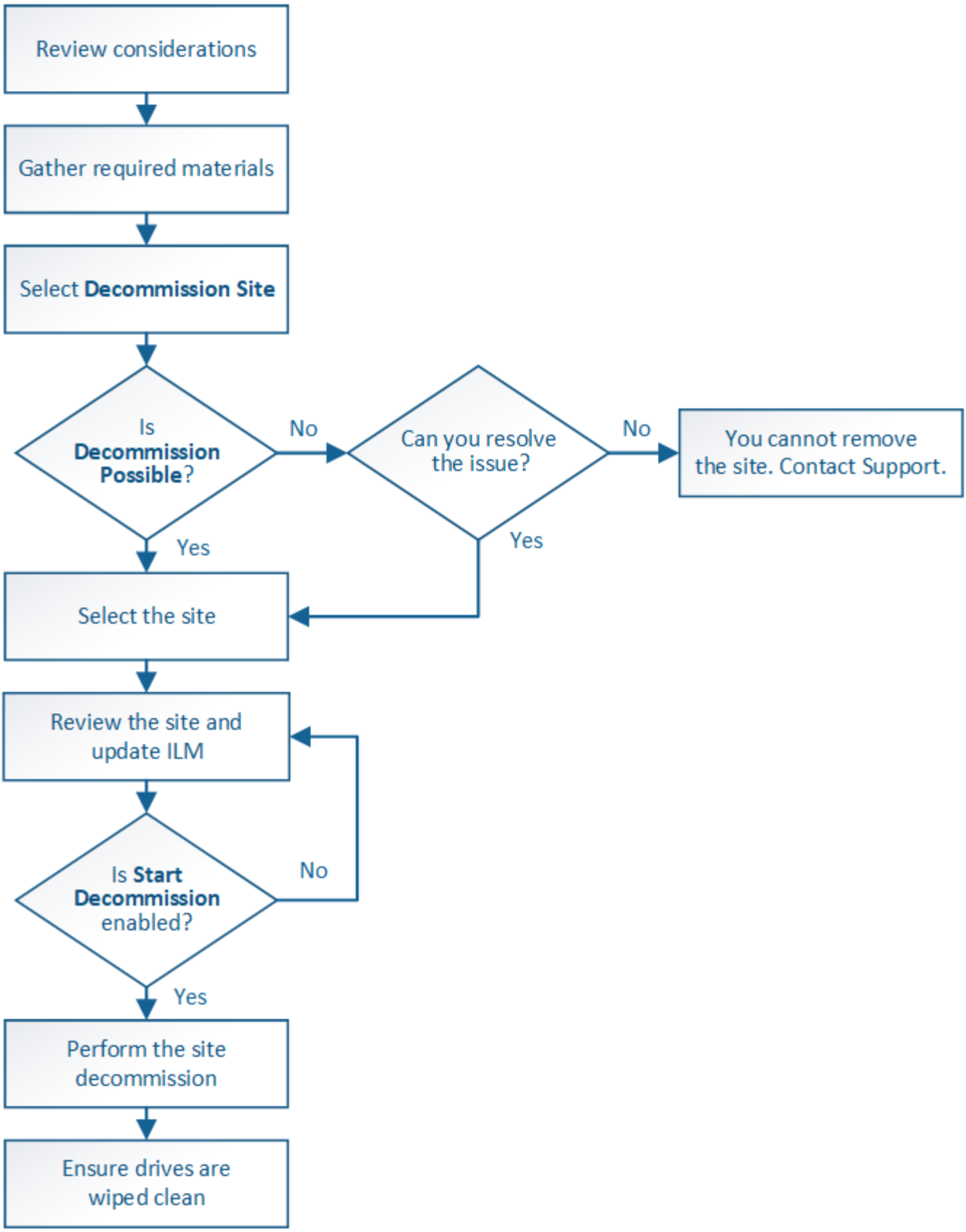
      The CMN service must be connected to at least one ADC service and a majority (50 percent plus one) of the StorageGRID system's ADC services must be available in order for a grid task to move from one stage of decommissioning to another and finish.

   c. If the CMN service is not connected to enough ADC services, ensure that Storage Nodes are online, and check network connectivity between the primary Admin Node and Storage Nodes.

### Site decommission

You might need to remove a data center site from the StorageGRID system. To remove a site, you must decommission it.

The flowchart shows the high-level steps for decommissioning a site.




**Considerations for removing a site**

Before using the site decommission procedure to remove a site, you must review the considerations.

### What happens when you decommission a site

When you decommission a site, StorageGRID permanently removes all nodes at the site and the site itself from the StorageGRID system.

When the site decommission procedure is complete:

- You can no longer use StorageGRID to view or access the site or any of the nodes at the site.
- You can no longer use any storage pools or Erasure Coding profiles that referred to the site. When StorageGRID decommissions a site, it automatically removes these storage pools and deactivates these Erasure Coding profiles.

### Differences between connected site and disconnected site decommission procedures

You can use the site decommission procedure to remove a site in which all nodes are connected to StorageGRID (referred to as a connected site decommission) or to remove a site in which all nodes are disconnected from StorageGRID (referred to as a disconnected site decommission). Before you begin, you must understand the differences between these procedures.

> If a site contains a mixture of connected ( ) and disconnected nodes ( or ), you must bring all offline nodes back online.

- A connected site decommission allows you to remove an operational site from the StorageGRID system. For example, you can perform a connected site decommission to remove a site that is functional but no longer needed.
- When StorageGRID removes a connected site, it uses ILM to manage the object data at the site. Before you can start a connected site decommission, you must remove the site from all ILM rules and activate a new ILM policy. The ILM processes to migrate object data and the internal processes to remove a site can occur at the same time, but the best practice is to allow the ILM steps to complete before you start the actual decommission procedure.
- A disconnected site decommission allows you to remove a failed site from the StorageGRID system. For example, you can perform a disconnected site decommission to remove a site that has been destroyed by a fire or flood.

  When StorageGRID removes a disconnected site, it considers all nodes to be unrecoverable and makes no attempt to preserve data. However, before you can start a disconnected site decommission, you must remove the site from all ILM rules and activate a new ILM policy.

  > Before performing a disconnected site decommission procedure, you must contact your NetApp account representative. NetApp will review your requirements before enabling all steps in the Decommission Site wizard. You should not attempt a disconnected site decommission if you believe it might be possible to recover the site or to recover object data from the site.

### General requirements for removing a connected or a disconnected site

Before removing a connected or disconnected site, you must be aware of the following requirements:

- You cannot decommission a site that includes the primary Admin Node.
- You cannot decommission a site that includes an Archive Node.

- You cannot decommission a site if any of the nodes have an interface that belongs to a high availability (HA) group. You must either edit the HA group to remove the node's interface or remove the entire HA group.
- You cannot decommission a site if it contains a mixture of connected ( ) and disconnected ( or ) nodes.
- You cannot decommission a site if any node at any other site is disconnected ( or ).
- You cannot start the site decommission procedure if an ec-node-repair operation is in progress. See Check data repair jobs to track repairs of erasure-coded data.
- While the site decommission procedure is running:
  - You cannot create ILM rules that refer to the site being decommissioned. You also cannot edit an existing ILM rule to refer to the site.
  - You cannot perform other maintenance procedures, such as expansion or upgrade.

    > If you need to perform another maintenance procedure during a connected site decommission, you can pause the procedure while the Storage Nodes are being removed. The **Pause** button is enabled only when the ILM evaluation or erasure-coded data decommissioning stages are reached; however, ILM evaluation (data migration) will continue to run in the background. After the second maintenance procedure is complete, you can resume decommissioning.

  - If you need to recover any node after starting the site decommission procedure, you must contact support.
- You cannot decommission more than one site at a time.
- If the site includes one or more Admin Nodes and single sign-on (SSO) is enabled for your StorageGRID system, you must remove all relying party trusts for the site from Active Directory Federation Services (AD FS).

**Requirements for information lifecycle management (ILM)**

As part of removing a site, you must update your ILM configuration. The Decommission Site wizard guides you through a number of prerequisite steps to ensure the following:

- The site is not referred to by the active ILM policy. If it is, you must create and activate a new ILM policy with new ILM rules.
- No proposed ILM policy exists. If you have a proposed policy, you must delete it.
- No ILM rules refer to the site, even if those rules are not used in the active or proposed policy. You must delete or edit all rules that refer to the site.

When StorageGRID decommissions the site, it will automatically deactivate any unused Erasure Coding profiles that refer to the site, and it will automatically delete any unused storage pools that refer to the site. The system-default All Storage Nodes storage pool is removed because it uses all sites.

> Before you can remove a site, you might be required to create new ILM rules and activate a new ILM policy. These instructions assume that you have a good understanding of how ILM works and that you are familiar with creating storage pools, Erasure Coding profiles, ILM rules, and simulating and activating an ILM policy. See the instructions for managing objects with information lifecycle management.

### Considerations for the object data at a connected site

If you are performing a connected site decommission, you must decide what to do with existing object data at the site when you create new ILM rules and a new ILM policy. You can do either or both of the following:

- Move object data from the selected site to one or more other sites in your grid.

  **Example for moving data**: Suppose you want to decommission a site in Raleigh because you added a new site in Sunnyvale. In this example, you want to move all object data from the old site to the new site. Before updating your ILM rules and ILM policy, you must review the capacity at both sites. You must ensure that the Sunnyvale site has enough capacity to accommodate the object data from the Raleigh site and that adequate capacity will remain in Sunnyvale for future growth.

  > To ensure that adequate capacity is available, you might need to add storage volumes or Storage Nodes to an existing site or add a new site before you perform this procedure. See the instructions for expanding a StorageGRID system.

- Delete object copies from the selected site.

  **Example for deleting data**: Suppose you currently use a 3-copy ILM rule to replicate object data across three sites. Before decommissioning a site, you can create an equivalent 2-copy ILM rule to store data at only two sites. When you activate a new ILM policy that uses the 2-copy rule, StorageGRID deletes the copies from the third site because they no longer satisfy ILM requirements. However, the object data will still be protected and the capacity of the two remaining sites will stay the same.

  > Never create a single-copy ILM rule to accommodate the removal of a site. An ILM rule that creates only one replicated copy for any time period puts data at risk of permanent loss. If only one replicated copy of an object exists, that object is lost if a Storage Node fails or has a significant error. You also temporarily lose access to the object during maintenance procedures such as upgrades.

### Additional requirements for a connected site decommission

Before StorageGRID can remove a connected site, you must ensure the following:

- All nodes in your StorageGRID system must have a Connection State of **Connected** ( ); however, the nodes can have active alerts.

  > You can complete Steps 1-4 of the Decommission Site wizard if one or more nodes are disconnected. However, you cannot complete Step 5 of the wizard, which starts the decommission process, unless all nodes are connected.

- If the site you plan to remove contains a Gateway Node or an Admin Node that is used for load balancing, you might need to perform an expansion procedure to add an equivalent new node at another site. Be sure clients can connect to the replacement node before starting the site decommission procedure.
- If the site you plan to remove contains any Gateway Node or Admin Nodes that are in an high availability (HA) group, you can complete Steps 1-4 of the Decommission Site wizard. However, you cannot complete Step 5 of the wizard, which starts the decommission process, until you remove these nodes from all HA groups. If existing clients connect to an HA group that includes nodes from the site, you must ensure they can continue to connect to StorageGRID after the site is removed.

- If clients connect directly to Storage Nodes at the site you are planning to remove, you must ensure that they can connect to Storage Nodes at other sites before starting the site decommission procedure.
- You must provide sufficient space on the remaining sites to accommodate any object data that will be moved because of changes to the active ILM policy. In some cases, you might need to expand your StorageGRID system by adding Storage Nodes, storage volumes, or new sites before you can complete a connected site decommission.
- You must allow adequate time for the decommission procedure to complete. StorageGRID ILM processes might take days, weeks, or even months to move or delete object data from the site before the site can be decommissioned.

  > Moving or deleting object data from a site might take days, weeks, or even months, depending on the amount of data at the site, the load on your system, network latencies, and the nature of the required ILM changes.

- Whenever possible, you should complete Steps 1-4 of the Decommission Site wizard as early as you can. The decommission procedure will complete more quickly and with fewer disruptions and performance impacts if you allow data to be moved from the site before starting the actual decommission procedure (by selecting **Start Decommission** in Step 5 of the wizard).

### Additional requirements for a disconnected site decommission

Before StorageGRID can remove a disconnected site, you must ensure the following:

- You have contacted your NetApp account representative. NetApp will review your requirements before enabling all steps in the Decommission Site wizard.

  > You should not attempt a disconnected site decommission if you believe it might be possible to recover the site or to recover any object data from the site.

- All nodes at the site must have a Connection State of one of the following:
  - **Unknown** ( ): The node is not connected to the grid for an unknown reason. For example, the network connection between nodes has been lost or the power is down.
  - **Administratively Down** ( ): The node is not connected to the grid for an expected reason. For example, the node or services on the node have been gracefully shut down.
- All nodes at all other sites must have a Connection State of **Connected** ( ); however, these other nodes can have active alerts.
- You must understand that you will no longer be able to use StorageGRID to view or retrieve any object data that was stored at the site. When StorageGRID performs this procedure, it makes no attempt to preserve any data from the disconnected site.

  > If your ILM rules and policy were designed to protect against the loss of a single site, copies of your objects still exist on the remaining sites.

- You must understand that if the site contained the only copy of an object, the object is lost and cannot be retrieved.

### Considerations for consistency controls when you remove a site

The consistency level for an S3 bucket or Swift container determines whether StorageGRID fully replicates object metadata to all nodes and sites before telling a client that object ingest was successful. Consistency controls provide a balance between the availability of the objects and the consistency of those objects across different Storage Nodes and sites.

When StorageGRID removes a site, it needs to ensure that no data is written to the site being removed. As a result, it temporarily overrides the consistency level for each bucket or container. After you start the site decommission process, StorageGRID temporarily uses strong-site consistency to prevent object metadata from being written to the site being removed.

As a result of this temporary override, be aware that any client write, update, and delete operations that occur during a site decommission can fail if multiple nodes become unavailable at the remaining sites.

#### Related information

How site recovery is performed by technical support

Manage objects with ILM

Expand your grid

### Gather required materials

Before you decommission a site, you must obtain the following materials.

| Item | Notes |
|---|---|
| Recovery Package `.zip` file | You must download the most recent Recovery Package `.zip` file (`sgws-recovery-package-id-revision.zip`). You can use the Recovery Package file to restore the system if a failure occurs. |
| `Passwords.txt` file | This file contains the passwords required to access grid nodes on the command line and is included in the Recovery Package. |
| Provisioning passphrase | The passphrase is created and documented when the StorageGRID system is first installed. The provisioning passphrase is not in the `Passwords.txt` file. |
| Description of StorageGRID system's topology before decommissioning | If available, obtain any documentation that describes the system's current topology. |

#### Related information

Web browser requirements

Download the Recovery Package

#### Step 1: Select Site

To determine if a site can be decommissioned, start by accessing the Decommission Site wizard.

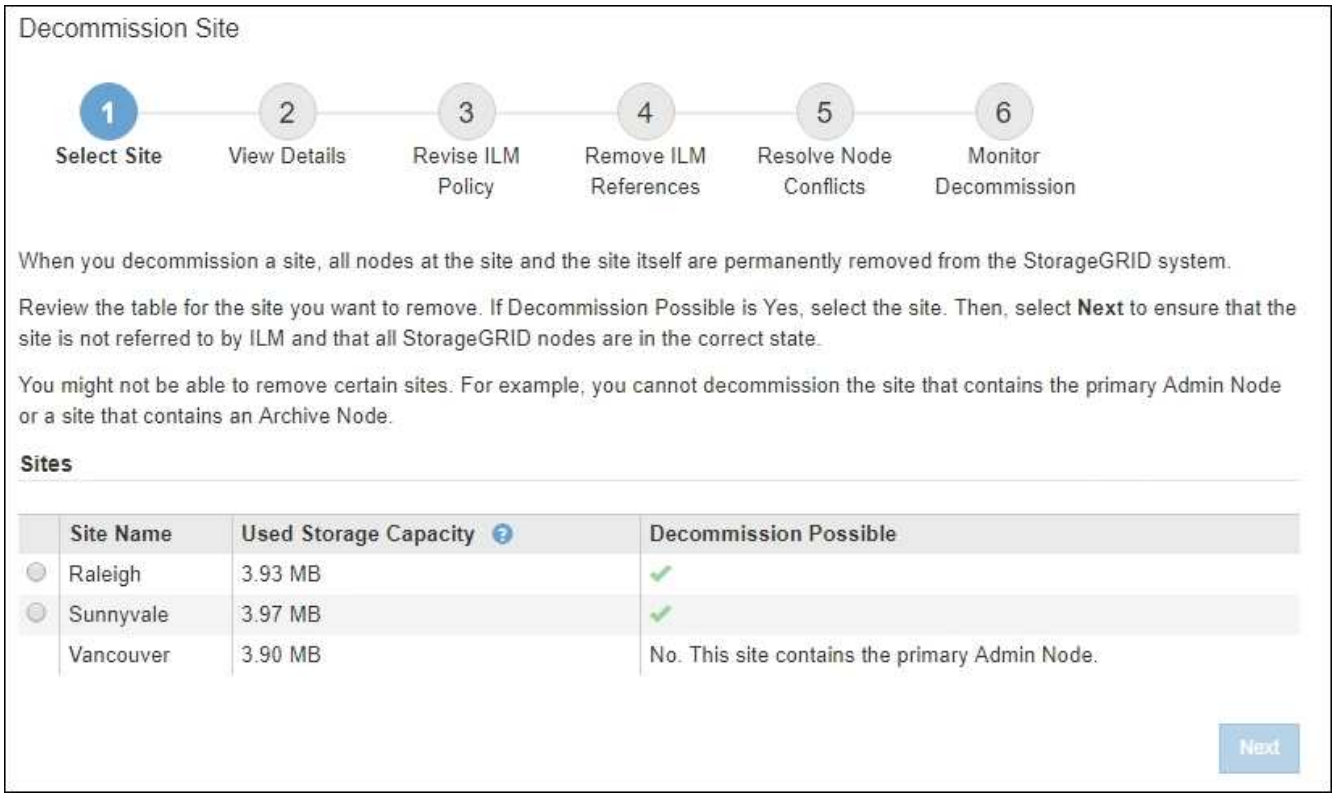
**What you'll need**

- You must have obtained all required materials.
- You must have reviewed the considerations for removing a site.
- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Root Access permission, or the Maintenance and ILM permissions.

**Steps**

1. Select **MAINTENANCE** > **Tasks** > **Decommission**.
2. Select **Decommission Site**.

   Step 1 (Select Site) of the Decommission Site wizard appears. This step includes an alphabetic list of the sites in your StorageGRID system.




3. View the values in the **Used Storage Capacity** column to determine how much storage is currently being used for object data at each site.

   The Used Storage Capacity is an estimate. If nodes are offline, the Used Storage Capacity is the last known value for the site.

   - For a connected site decommission, this value represents how much object data will need to be moved to other sites or deleted by ILM before you can safely decommission this site.
   - For a disconnected site decommission, this value represents how much of your system's data storage will become inaccessible when you decommission this site.

> If your ILM policy was designed to protect against the loss of a single site, copies of your object data should still exist on the remaining sites.

4. Review the reasons in the **Decommission Possible** column to determine which sites can be decommissioned currently.

> If there is more than one reason a site cannot be decommissioned, the most critical reason is shown.

| Decommission Possible reason | Description | Next step |
|---|---|---|
| Green checkmark ( ) | You can decommission this site. | Go to the next step. |
| No. This site contains the primary Admin Node. | You cannot decommission a site containing the primary Admin Node. | None. You cannot perform this procedure. |
| No. This site contains one or more Archive Nodes. | You cannot decommission a site containing an Archive Node. | None. You cannot perform this procedure. |
| No. All nodes at this site are disconnected. Contact your NetApp account representative. | You cannot perform a connected site decommission unless every node in the site is connected ( ). | If you want to perform a disconnected site decommission, you must contact your NetApp account representative, who will review your requirements and enable the rest of the Decommission Site wizard.<br><br>**IMPORTANT**: Never take online nodes offline so that you can remove a site. You will lose data. |

The example shows a StorageGRID system with three sites. The green checkmark ( ) for the Raleigh and Sunnyvale sites indicates that you can decommission those sites. However, you cannot decommission the Vancouver site because it contains the primary Admin Node.

5. If decommission is possible, select the radio button for the site.

   The **Next** button is enabled.

6. Select **Next**.

   Step 2 (View Details) appears.

#### Step 2: View Details

From Step 2 (View Details) of the Decommission Site wizard, you can review which nodes are included at the site, see how much space has been used on each Storage Node, and assess how much free space is available at the other sites in your grid.

### What you'll need

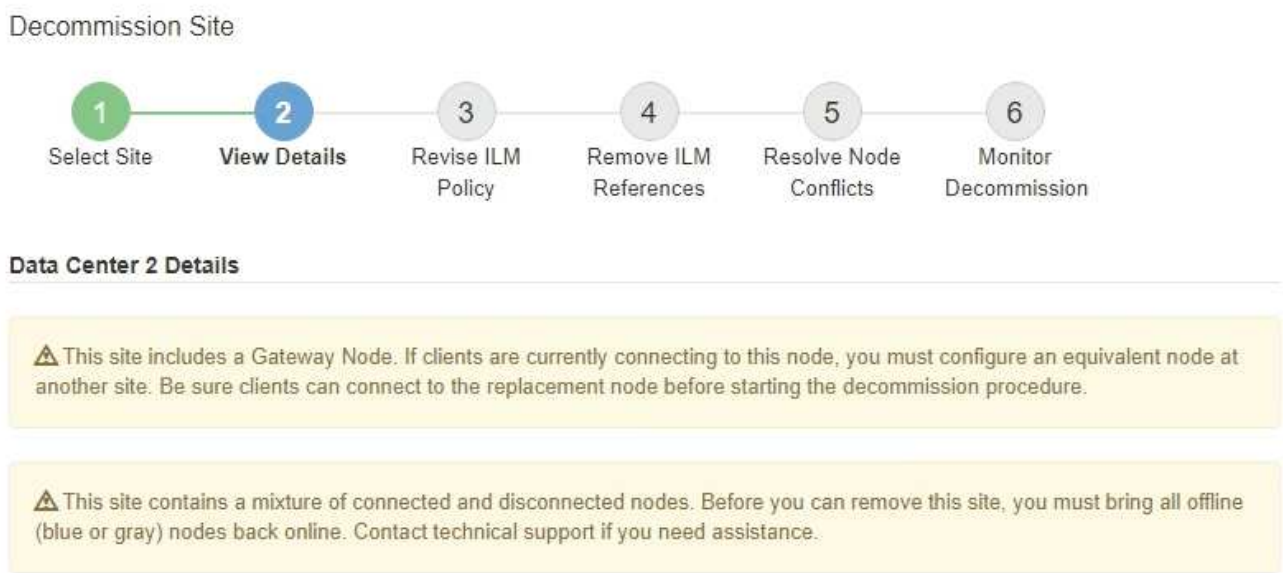
Before decommissioning a site, you must review how much object data exists at the site.

- If you are performing a connected site decommission, you must understand how much object data currently exists at the site before updating ILM. Based on site capacities and your data protection needs, you can create new ILM rules to move data to other sites or to delete object data from the site.
- Perform any required Storage Node expansions before starting the decommission procedure if possible.
- If you are performing a disconnected site decommission, you must understand how much object data will become permanently inaccessible when you remove the site.

> If you are performing a disconnected site decommission, ILM cannot move or delete object data. Any data that remains at the site will be lost. However, if your ILM policy was designed to protect against the loss of a single site, copies of your object data still exist on the remaining sites.

### Steps

1. From Step 2 (View Details), review any warnings related to the site you selected to remove.




   A warning appears in these cases:

   - The site includes a Gateway Node. If S3 and Swift clients are currently connecting to this node, you must configure an equivalent node at another site. Be sure clients can connect to the replacement node before continuing with the decommission procedure.
   - The site contains a mixture of connected ( ) and disconnected nodes ( or ). Before you can remove this site, you must bring all offline nodes back online.

2. Review details about the site you selected to remove.

Decommission Site

1 Select Site — 2 View Details — 3 Revise ILM Policy — 4 Remove ILM References — 5 Resolve Node Conflicts — 6 Monitor Decommission

**Raleigh Details**

**Number of Nodes:** 3
**Free Space:** 475.38 GB
**Used Space:** 3.93 MB
**Site Capacity:** 475.38 GB

| Node Name | Node Type | Connnection State | Details |
|---|---|---|---|
| RAL-S1-101-196 | Storage Node | ✔ | 1.30 MB used space |
| RAL-S2-101-197 | Storage Node | ✔ | 1.30 MB used space |
| RAL-S3-101-198 | Storage Node | ✔ | 1.34 MB used space |

**Details for Other Sites**

**Total Free Space for Other Sites:** 950.76 GB
**Total Capacity for Other Sites:** 950.77 GB

| Site Name | Free Space | Used Space | Site Capacity |
|---|---|---|---|
| Sunnyvale | 475.38 GB | 3.97 MB | 475.38 GB |
| Vancouver | 475.38 GB | 3.90 MB | 475.38 GB |
| **Total** | **950.76 GB** | **7.87 MB** | **950.77 GB** |

Previous Next

The following information is included for the selected site:

- Number of nodes
- The total used space, free space, and capacity of all Storage Nodes in the site.
  - For a connected site decommission, the **Used Space** value represents how much object data must be moved to other sites or deleted with ILM.
  - For a disconnected site decommission, the **Used Space** value indicates how much object data will become inaccessible when you remove the site.
- Node names, types, and connection states:
  - (Connected)
  - (Administratively Down)
  - (Unknown)
- Details about each node:
  - For each Storage Node, the amount of space that has been used for object data.

- For Admin Nodes and Gateway Nodes, whether the node is currently used in a high availability (HA) group. You cannot decommission an Admin Node or a Gateway Node that is used in an HA group. Before you start the decommission, you must edit HA groups to remove all nodes at the site. Or, you can remove the HA group if it only includes nodes from this site.

  Administer StorageGRID

3. In the Details for Other Sites section of the page, assess how much space is available at the other sites in your grid.

**Details for Other Sites**

| | |
|---|---|
| Total Free Space for Other Sites: | 950.76 GB |
| Total Capacity for Other Sites: | 950.77 GB |

| Site Name | Free Space | Used Space | Site Capacity |
|---|---|---|---|
| Sunnyvale | 475.38 GB | 3.97 MB | 475.38 GB |
| Vancouver | 475.38 GB | 3.90 MB | 475.38 GB |
| Total | 950.76 GB | 7.87 MB | 950.77 GB |

If you are performing a connected site decommission and you plan to use ILM to move object data from the selected site (instead of just deleting it), you must ensure that the other sites have enough capacity to accommodate the moved data and that adequate capacity remains for future growth.

> A warning appears if the **Used Space** for the site you want to remove is greater than the **Total Free Space for Other Sites**. To ensure that adequate storage capacity is available after the site is removed, you might need to perform an expansion before performing this procedure.

4. Select **Next**.

   Step 3 (Revise ILM Policy) appears.

**Related information**

Manage objects with ILM

#### Step 3: Revise ILM Policy

From Step 3 (Revise ILM Policy) of the Decommission Site wizard, you can determine if the site is referred to by the active ILM policy.

**What you'll need**

You have a good understanding of how ILM works and you are familiar with creating storage pools, Erasure Coding profiles, ILM rules, and simulating and activating an ILM policy.

Manage objects with ILM

**About this task**

StorageGRID cannot decommission a site if that site is referred to by any ILM rule in the active ILM policy.

If your current ILM policy refers to the site you want to remove, you must activate a new ILM policy that meets

certain requirements. Specifically, the new ILM policy:

- Cannot use a storage pool that refers to the site.
- Cannot use an Erasure Coding profile that refers to the site.
- Cannot use the default **All Storage Nodes** storage pool or the default **All Sites** site.
- Cannot use the stock **Make 2 Copies** rule.
- Must be designed to fully protect all object data.

> Never create a single-copy ILM rule to accommodate the removal of a site. An ILM rule that creates only one replicated copy for any time period puts data at risk of permanent loss. If only one replicated copy of an object exists, that object is lost if a Storage Node fails or has a significant error. You also temporarily lose access to the object during maintenance procedures such as upgrades.

If you are performing a *connected site decommission*, you must consider how StorageGRID should manage the object data currently at the site you want to remove. Depending on your data protection requirements, the new rules can move existing object data to different sites or they can delete any extra object copies that are no longer needed.

Contact technical support if you need assistance designing the new policy.

**Steps**

1. From Step 3 (Revise ILM Policy), determine if any ILM rules in the active ILM policy refer to the site you selected to remove.

Decommission Site

1 Select Site — 2 View Details — 3 **Revise ILM Policy** — 4 Remove ILM References — 5 Resolve Node Conflicts — 6 Monitor Decommission

If your current ILM policy refers to the site, you must activate a new policy before you can go to the next step.

The new ILM policy:

- Cannot use a storage pool that refers to the site.
- Cannot use an Erasure Coding profile that refers to the site.
- Cannot use the default **All Storage Nodes** storage pool or the default **All Sites** site.
- Cannot use the **Make 2 Copies** rule.
- Must be designed to fully protect all object data after one site is removed.

Contact technical support if you need assistance in designing the new policy.

If you are performing a connected site decommission, StorageGRID will begin to remove object data from the site as soon as you activate the new ILM policy. Moving or deleting all object copies might take weeks, but you can safely start a site decommission while object data still exists at the site.

**Rules Referring to Raleigh in the Active ILM Policy**

The table lists the ILM rules in the active ILM policy that refer to the site.

- If no ILM rules are listed, the active ILM policy does not refer to the site. Select **Next** to go to Step 4 (Remove ILM References).
- If one or more ILM rules are listed, you must create and activate a new policy that does not use these rules.

Active Policy Name: Data Protection for Three Sites

The active ILM policy refers to Raleigh. Before you can remove this site, you must propose and activate a new policy.

| Name | EC Profiles | Storage Pools |
|---|---|---|
| 3 copies for S3 tenant | — | Raleigh storage pool |
| 2 copy 2 sites for smaller objects | — | Raleigh storage pool |
| EC for larger objects | three site EC profile | All 3 Sites |

Previous Next

2. If no rules are listed, select **Next** to go to Step 4 (Remove ILM References)

   Step 4: Remove ILM References

3. If one or more ILM rules are listed in the table, select the link next to **Active Policy Name**.

   The ILM Policies page appears in a new browser tab. Use this tab to update ILM. The Decommission Site page will remain open on the other tab.

   a. If necessary, select **ILM** > **Storage pools** to create one or more storage pools that do not refer to the site.

   For details, see the instructions for managing objects with information lifecycle management.

b. If you plan to use erasure coding, select **ILM** > **Erasure coding** to create one or more Erasure Coding profiles.

   You must select storage pools that do not refer to the site.

   > Do not use the **All Storage Nodes** storage pool in the Erasure Coding profiles.

4. Select **ILM** > **Rules** and clone each of the rules listed in the table for Step 3 (Revise ILM Policy).

   > For details, see the instructions for managing objects with information lifecycle management.

   a. Use names that will make it easy to select these rules in a new policy.
   b. Update the placement instructions.

      Remove any storage pools or Erasure Coding profiles that refer to the site and replace them with new storage pools or Erasure Coding profiles.

      > Do not use the **All Storage Nodes** storage pool in the new rules.

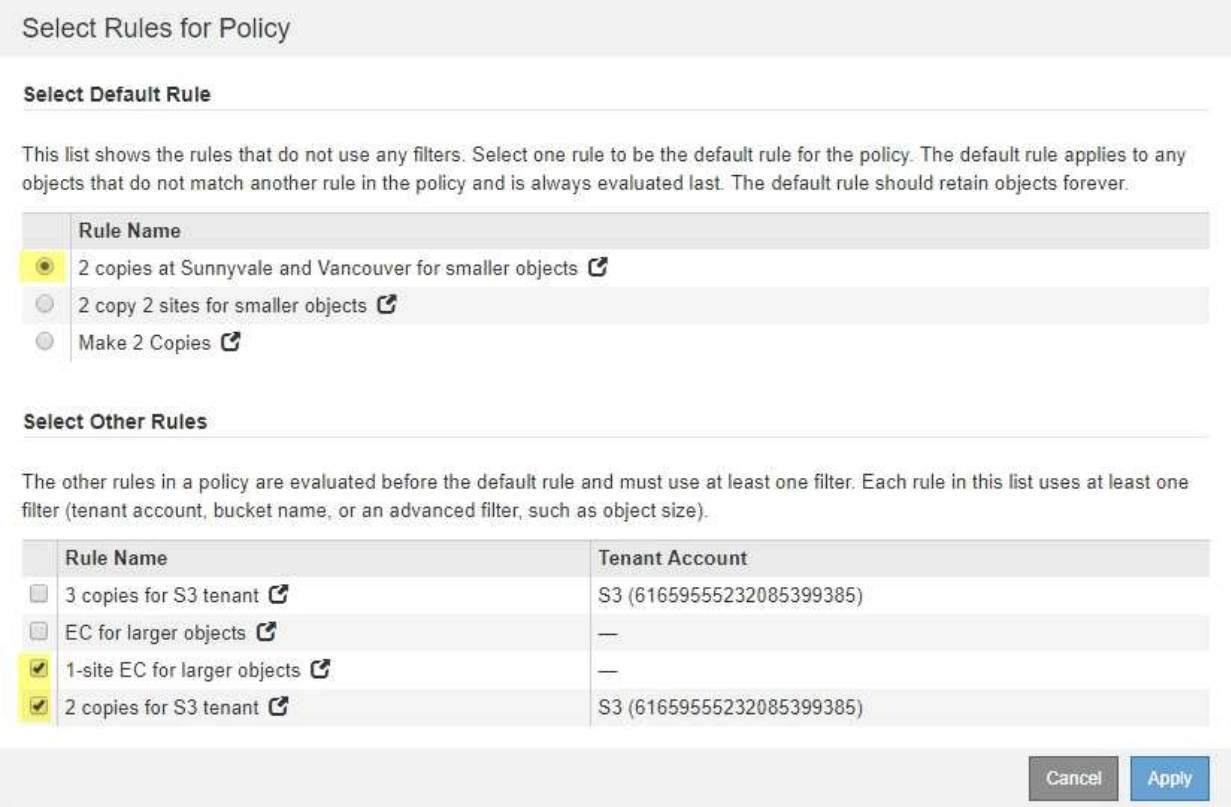
5. Select **ILM** > **Policies** and create a new policy that uses the new rules.

   > For details, see the instructions for managing objects with information lifecycle management.

   a. Select the active policy, and select **Clone**.
   b. Specify a policy name and a reason for change.
   c. Select rules for the cloned policy.
      - Unselect all rules listed for Step 3 (Revise ILM Policy) of the Decommission Site page.
      - Select a default rule that does not refer to the site.

        > Do not select the **Make 2 Copies** rule because that rule uses the **All Storage Nodes** storage pool, which is not allowed.

      - Select the other replacement rules you created. These rules should not refer to the site.




d. Select **Apply**.

e. Drag and drop the rows to reorder the rules in the policy.

   You cannot move the default rule.

   > You must confirm that the ILM rules are in the correct order. When the policy is activated, new and existing objects are evaluated by the rules in the order listed, starting at the top.

f. Save the proposed policy.

6. Ingest test objects, and simulate the proposed policy to ensure that the correct rules are applied.

   > Errors in an ILM policy can cause unrecoverable data loss. Carefully review and simulate the policy before activating it to confirm that it will work as intended.

   > When you activate a new ILM policy, StorageGRID uses it to manage all objects, including existing objects and newly ingested objects. Before activating a new ILM policy, review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

7. Activate the new policy.

   If you are performing a connected site decommission, StorageGRID begins to remove object data from the selected site as soon as you activate the new ILM policy. Moving or deleting all object copies might take weeks. Although you can safely start a site decommission while object data still exists at the site, the decommission procedure will complete more quickly and with fewer disruptions and performance impacts if you allow data to be moved from the site before starting the actual decommission procedure (by selecting

**Start Decommission** in Step 5 of the wizard).

8. Return to **Step 3 (Revise ILM Policy)** to ensure that no ILM rules in the new active policy refer to the site and the **Next** button is enabled.

> If any rules are listed, you must create and activate a new ILM policy before you can continue.

9. If no rules are listed, select **Next**.

   Step 4 (Remove ILM References) appears.

#### Step 4: Remove ILM References

From Step 4 (Remove ILM References) of the Decommission Site wizard, you can remove the proposed policy if one exists and delete or edit any unused ILM rules that still refer to the site.

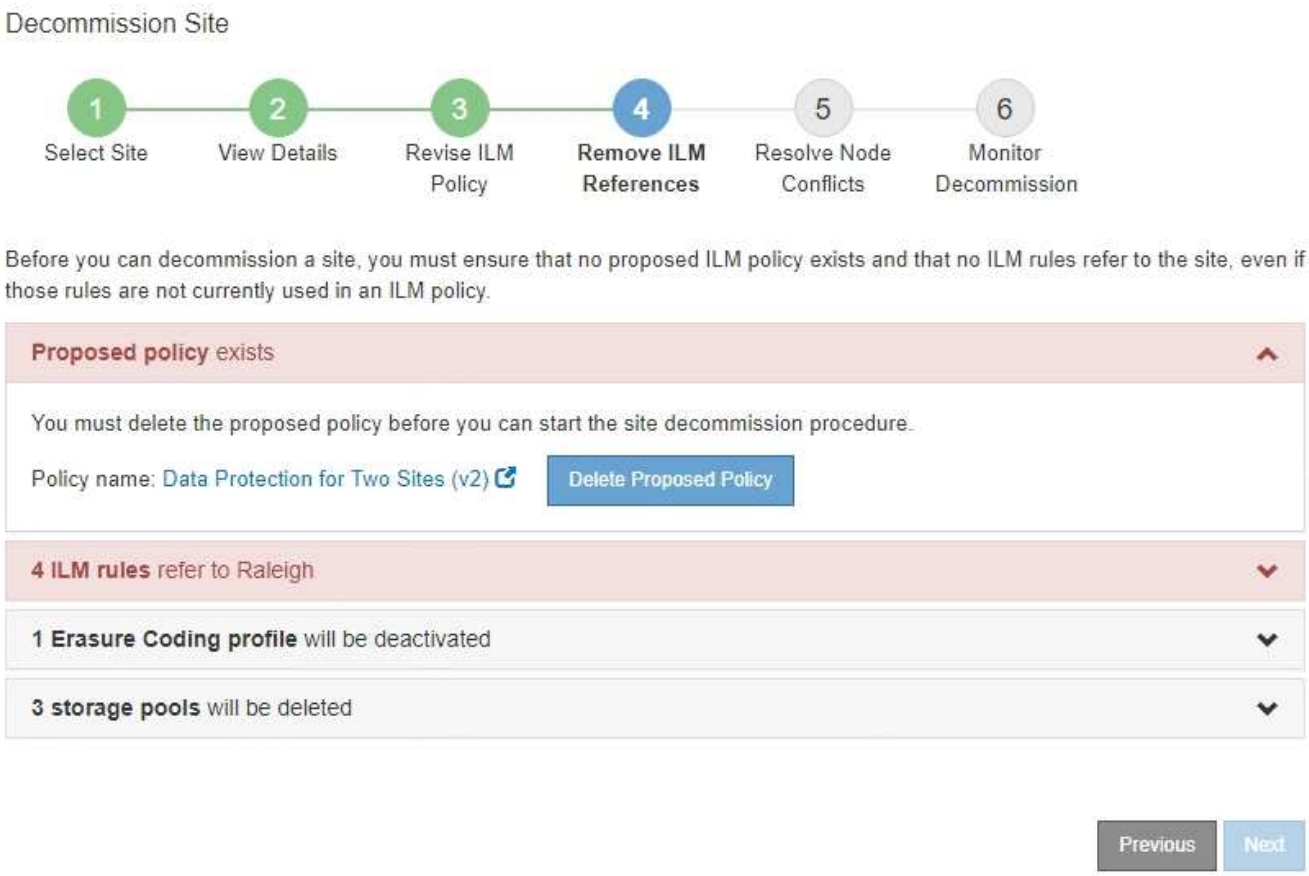
**About this task**

You are prevented from starting the site decommission procedure in these cases:

- A proposed ILM policy exists. If you have a proposed policy, you must delete it.
- Any ILM rule refers to the site, even if that rule is not used in any ILM policy. You must delete or edit all rules that refer to the site.

**Steps**

1. If a proposed policy is listed, remove it.




a. Select **Delete Proposed Policy**.

b. Select **OK** in the confirmation dialog box.

2. Determine whether any unused ILM rules refer to the site.

Decommission Site

1 Select Site — 2 View Details — 3 Revise ILM Policy — 4 **Remove ILM References** — 5 Resolve Node Conflicts — 6 Monitor Decommission

Before you can decommission a site, you must ensure that no proposed ILM policy exists and that no ILM rules refer to the site, even if those rules are not currently used in an ILM policy.

No proposed policy exists

**4 ILM rules** refer to Data Center 3

This table lists the unused ILM rules that still refer to the site. For each rule listed, you must do one of the following:

- Edit the rule to remove the Erasure Coding profile or storage pool from the placement instructions.
- Delete the rule.

Go to the ILM Rules page

| Name | EC Profiles | Storage Pools | Delete |
|---|---|---|---|
| Make 2 Copies | — | All Storage Nodes | |
| 3 copies for S3 tenant | — | Raleigh storage pool | |
| 2 copies 2 sites for smaller objects | — | Raleigh storage pool | |
| EC larger objects | three site EC profile | All 3 Sites | |

**1 Erasure Coding profile** will be deactivated

**3 storage pools** will be deleted

Any ILM rules that are listed still refer to the site but are not used in any policy. In the example:

- The stock **Make 2 Copies** rule uses the system-default **All Storage Nodes** storage pool, which uses the All Sites site.
- The unused **3 copies for S3 tenant** rule refers to the **Raleigh** storage pool.
- The unused **2 copy 2 sites for smaller objects** rule refers to the **Raleigh** storage pool.
- The unused **EC larger objects** rules uses the Raleigh site in the **All 3 Sites** Erasure Coding profile.
- If no ILM rules are listed, select **Next** to go to **Step 5 (Resolve Node Conflicts)**.

  Step 5: Resolve Node Conflicts (and start decommission)

  > When StorageGRID decommissions the site, it will automatically deactivate any unused Erasure Coding profiles that refer to the site, and it will automatically delete any unused storage pools that refer to the site. The system-default All Storage Nodes storage pool is removed because it uses the All Sites site.

- If one or more ILM rules are listed, go to the next step.

3. Edit or delete each unused rule:

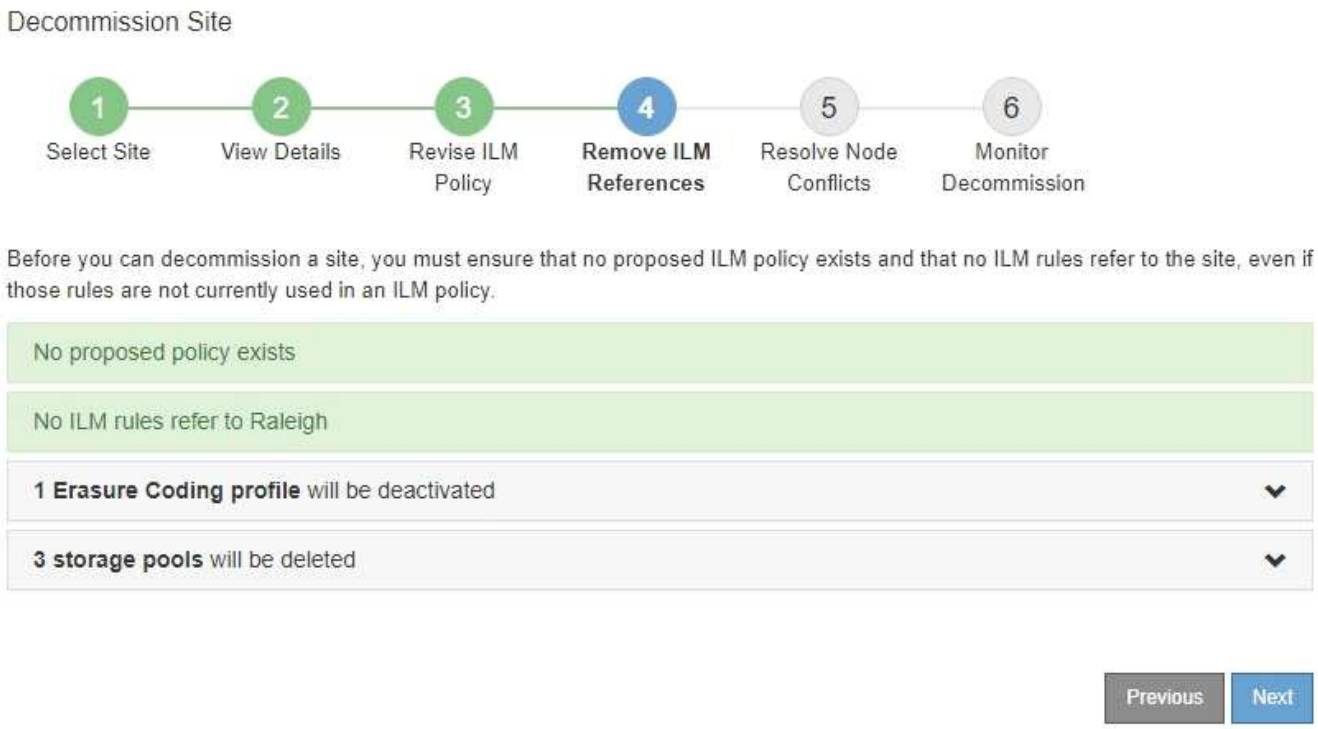
- To edit a rule, go the ILM Rules page and update all placements that use an Erasure Coding profile or storage pool that refers to the site. Then, return to **Step 4 (Remove ILM References)**.

  For details, see the instructions for managing objects with information lifecycle management.

- To delete a rule, select the trash can icon and select **OK**.

  You must delete the stock **Make 2 Copies** rule before you can decommission a site.

4. Confirm that no proposed ILM policy exists, no unused ILM rules refer to the site, and the **Next** button is enabled.




5. Select **Next**.

   Any remaining storage pools and Erasure Coding profiles that refer to the site will become invalid when the site is removed. When StorageGRID decommissions the site, it will automatically deactivate any unused Erasure Coding profiles that refer to the site, and it will automatically delete any unused storage pools that refer to the site. The system-default All Storage Nodes storage pool is removed because it uses the All Sites site.

   Step 5 (Resolve Node Conflicts) appears.

#### Step 5: Resolve Node Conflicts (and start decommission)

From Step 5 (Resolve Node Conflicts) of the Decommission Site wizard, you can determine if any nodes in your StorageGRID system are disconnected or if any nodes at the selected site belong to a high availability (HA) group. After any node conflicts are resolved, you start the decommission procedure from this page.

You must ensure that all nodes in your StorageGRID system are in the correct state, as follows:

- All nodes in your StorageGRID system must be connected ( ).

  > If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected, and all nodes at all other sites must be connected.

- No node at the site you are removing can have an interface that belongs to a high availability (HA) group.

If any node is listed for Step 5 (Resolve Node Conflicts), you must correct the issue before you can start the decommission.

Before starting the site decommission procedure from this page, review the following considerations:

- You must allow adequate time for the decommission procedure to complete.

  > Moving or deleting object data from a site might take days, weeks, or even months, depending on the amount of data at the site, the load on your system, network latencies, and the nature of the required ILM changes.

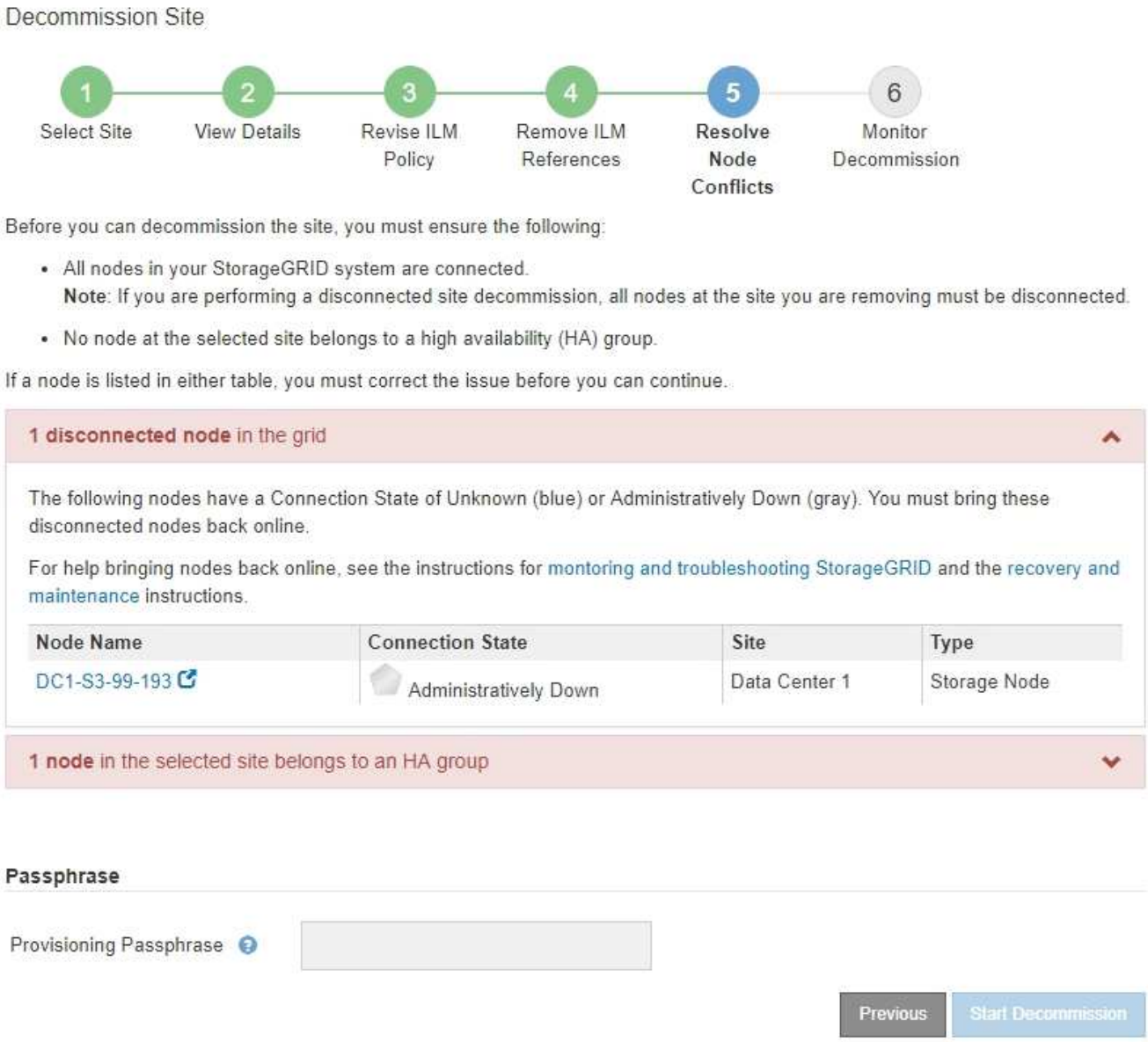
- While the site decommission procedure is running:
  - You cannot create ILM rules that refer to the site being decommissioned. You also cannot edit an existing ILM rule to refer to the site.
  - You cannot perform other maintenance procedures, such as expansion or upgrade.

    > If you need to perform another maintenance procedure during a connected site decommission, you can pause the procedure while the Storage Nodes are being removed. The **Pause** button is enabled during the “Decommissioning Replicated and Erasure Coded Data” stage.

  - If you need to recover any node after starting the site decommission procedure, you must contact support.

**Steps**

1. Review the disconnected nodes section of Step 5 (Resolve Node Conflicts) to determine if any nodes in your StorageGRID system have a Connection State of Unknown ( ) or Administratively Down ( ).

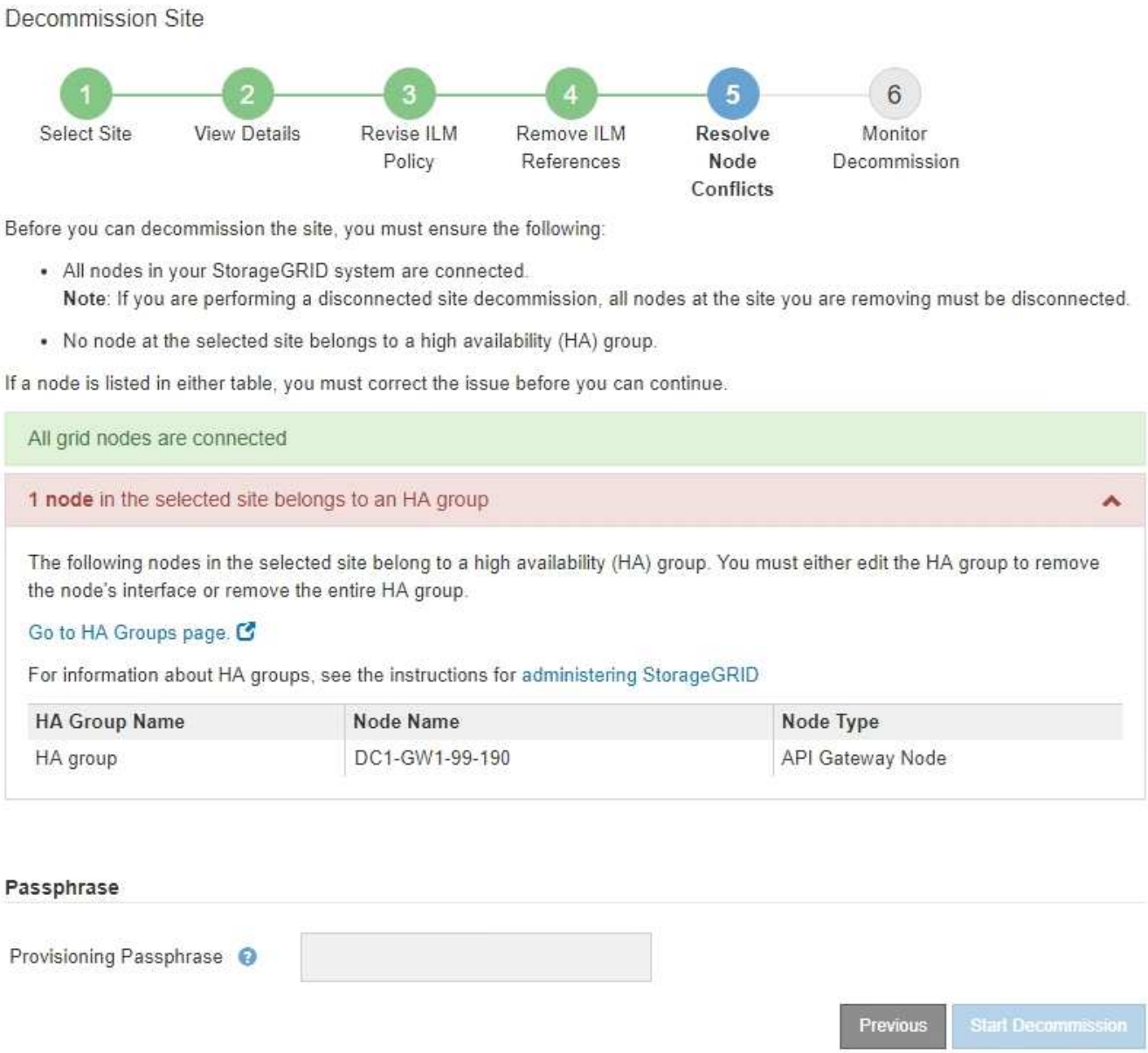



2. If any nodes are disconnected, bring them back online.

   See the instructions for monitoring and troubleshooting StorageGRID and the grid node procedures. Contact technical support if you need assistance.

3. When all disconnected nodes have been brought back online, review the HA groups section of Step 5 (Resolve Node Conflicts).

   This table lists any nodes at the selected site that belong to a high availability (HA) group.

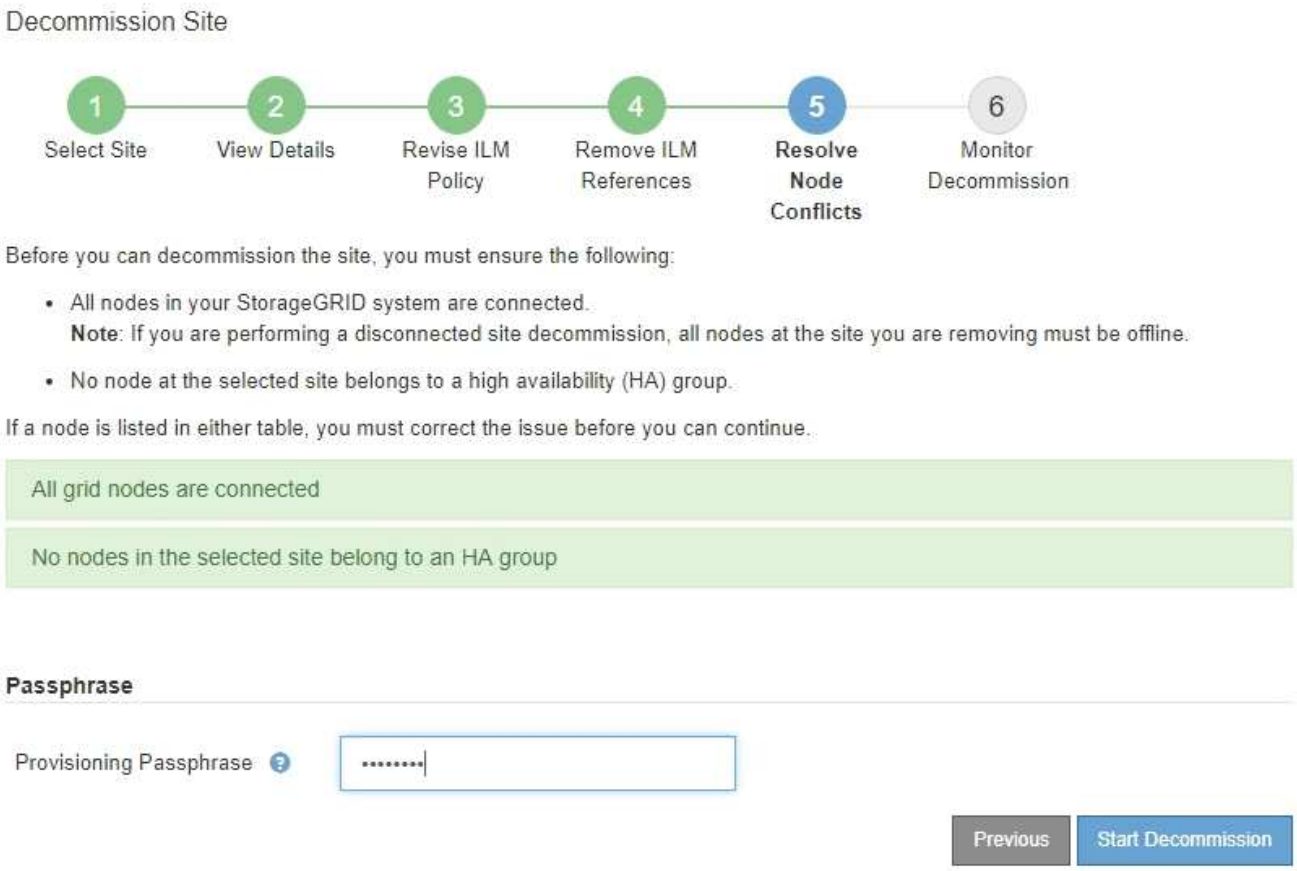



4. If any nodes are listed, do either of the following:
   - Edit each affected HA group to remove the node interface.
   - Remove an HA group that only includes nodes from this site. See the instructions for administering StorageGRID.

   If all nodes are connected and no nodes in the selected site are used in an HA group, the **Provisioning Passphrase** field is enabled.

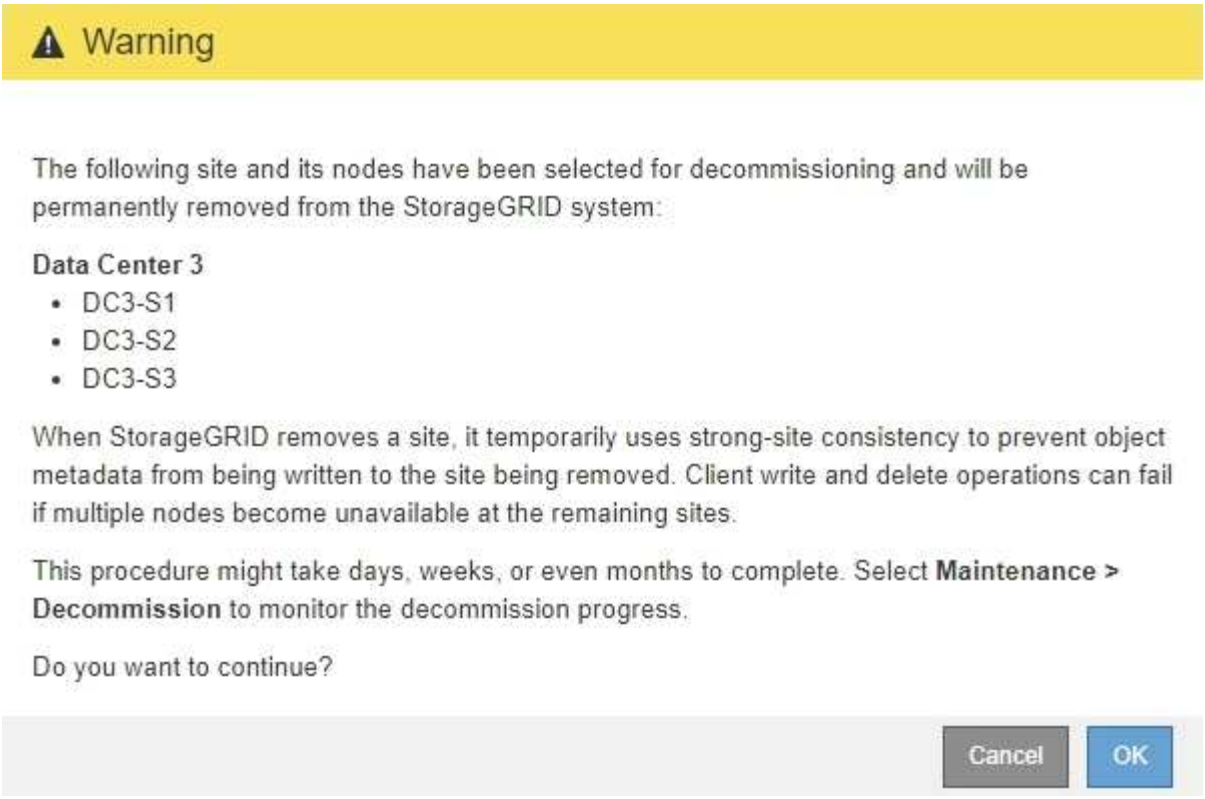
5. Enter the provisioning passphrase.

   The **Start Decommission** button becomes enabled.



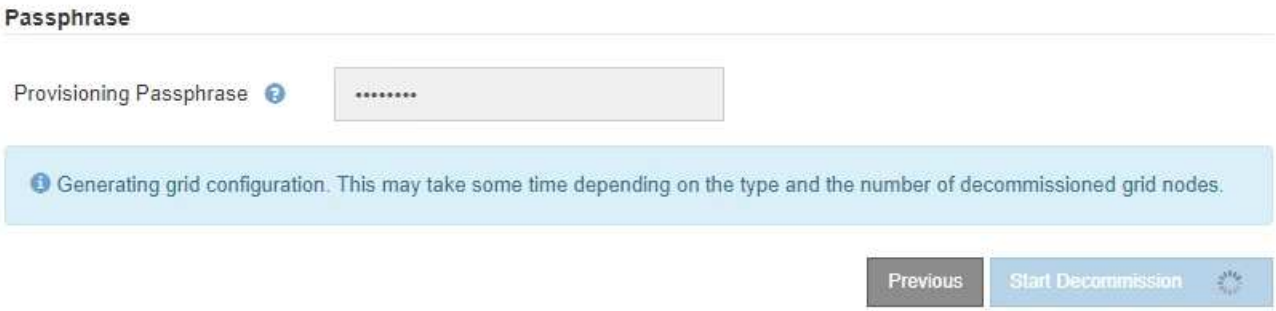

6. If you are ready to start the site decommission procedure, select **Start Decommission**.

   A warning lists the site and nodes that will be removed. You are reminded that it might take days, weeks, or even months to completely remove the site.




7. Review the warning. If you are ready to begin, select **OK**.

   A message appears as the new grid configuration is generated. This process might take some time, depending on the type and number of decommissioned grid nodes.




   When the new grid configuration has been generated, Step 6 (Monitor Decommission) appears.

   The **Previous** button remains disabled until the decommission is complete.

**Related information**

Monitor and troubleshoot

Grid node procedures

Administer StorageGRID

#### Step 6: Monitor Decommission

From Step 6 (Monitor Decommission) of the Decommission Site page wizard, you can monitor the progress as the site is removed.

**About this task**

When StorageGRID removes a connected site, it removes nodes in this order:

1. Gateway Nodes
2. Admin Nodes
3. Storage Nodes

When StorageGRID removes a disconnected site, it removes nodes in this order:

1. Gateway Nodes
2. Storage Nodes
3. Admin Nodes

Each Gateway Node or Admin Node might only require a few minutes or an hour to remove; however, Storage Nodes might take days or weeks.

**Steps**

1. As soon as a new Recovery Package has been generated, download the file.

> Download the Recovery Package as soon as possible to ensure you can recover your grid if something goes wrong during the decommission procedure.

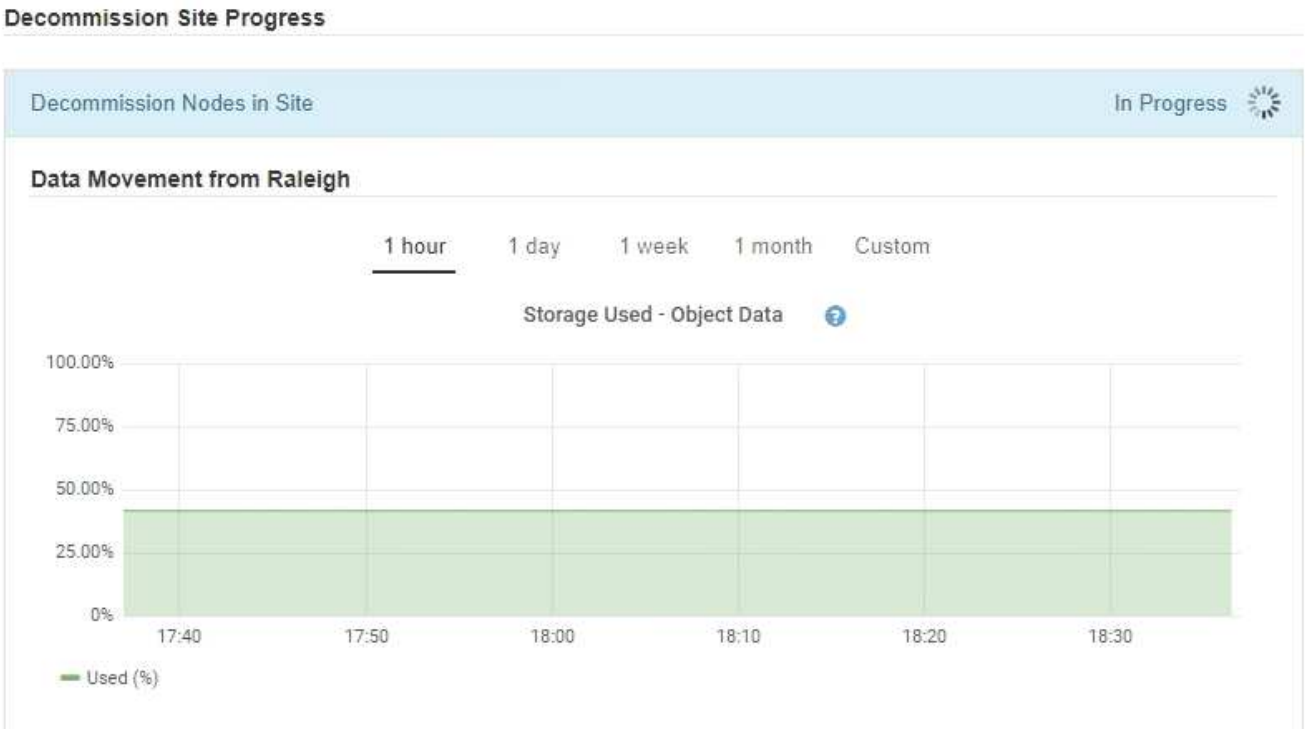
   a. Select the link in the message, or select **MAINTENANCE** > **System** > **Recovery package**.
   b. Download the `.zip` file.

      See the instructions for downloading the Recovery Package.

> The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

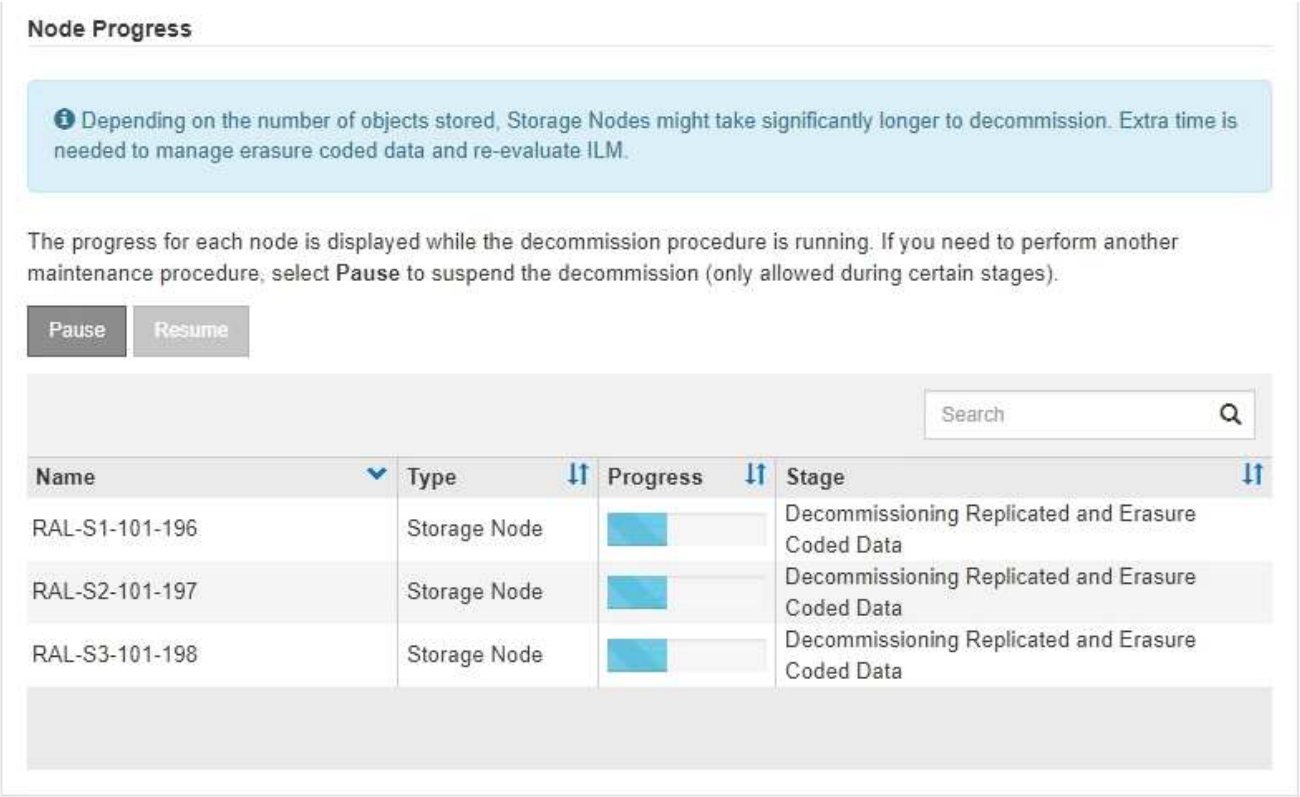
2. Using the Data Movement chart, monitor the movement of object data from this site to other sites.

   Data movement started when you activated the new ILM policy in Step 3 (Revise ILM Policy). Data movement will occur throughout the decommission procedure.




3. In the Node Progress section of the page, monitor the progress of the decommission procedure as nodes are removed.

   When a Storage Node is removed, each node goes through a series of stages. Although most of these stages occur quickly or even imperceptibly, you might need to wait days or even weeks for other stages to complete, based on how much data needs to moved. Additional time is required to manage erasure-coded data and re-evaluate ILM.



If you are monitoring the progress of a connected site decommission, refer to this table to understand the decommission stages for a Storage Node:

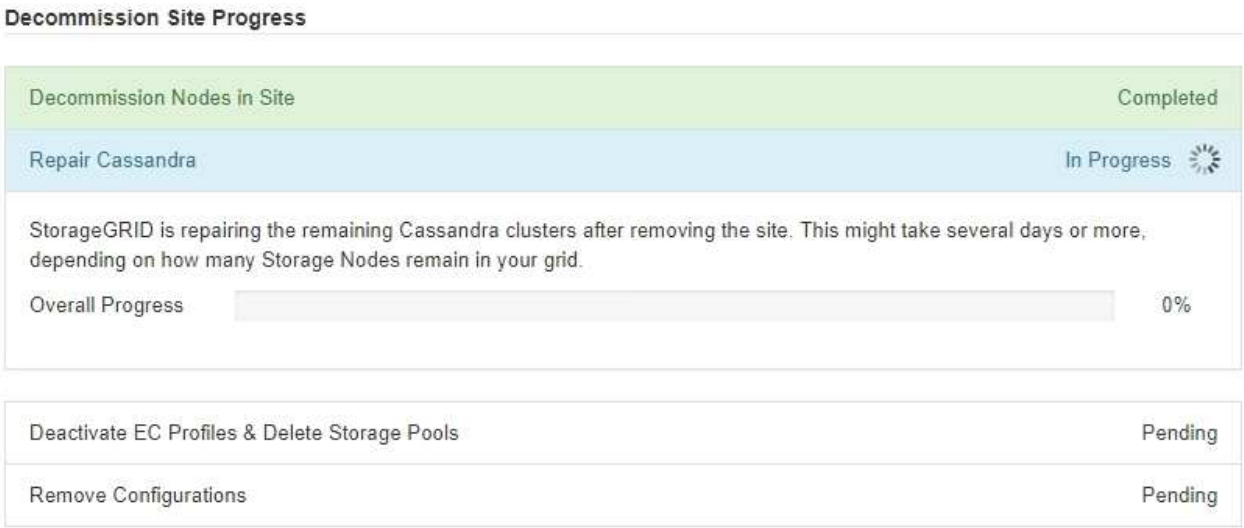
| Stage | Estimated duration |
|---|---|
| Pending | Minute or less |
| Wait for Locks | Minutes |
| Prepare Task | Minute or less |
| Marking LDR Decommissioned | Minutes |
| Decommissioning Replicated and Erasure Coded Data | Hours, days, or weeks based on the amount of data<br><br>**Note**: If you need to perform other maintenance activities, you can pause the site decommission during this stage. |
| LDR Set State | Minutes |
| Flush Audit Queues | Minutes to hours, based on the number of messages and network latency. |
| Complete | Minutes |

If you are monitoring the progress of a disconnected site decommission, refer to this table to understand the decommission stages for a Storage Node:

| Stage | Estimated duration |
|---|---|
| Pending | Minute or less |
| Wait for Locks | Minutes |
| Prepare Task | Minute or less |
| Disable External Services | Minutes |
| Certificate Revocation | Minutes |
| Node Unregister | Minutes |
| Storage Grade Unregister | Minutes |
| Storage Group Removal | Minutes |
| Entity Removal | Minutes |

| Stage | Estimated duration |
| --- | --- |
| Complete | Minutes |

4. After all nodes have reached the Complete stage, wait for the remaining site decommission operations to complete.
   - During the **Repair Cassandra** step, StorageGRID makes any necessary repairs to the Cassandra clusters that remain in your grid. These repairs might take several days or more, depending on how many Storage Nodes remain in your grid.

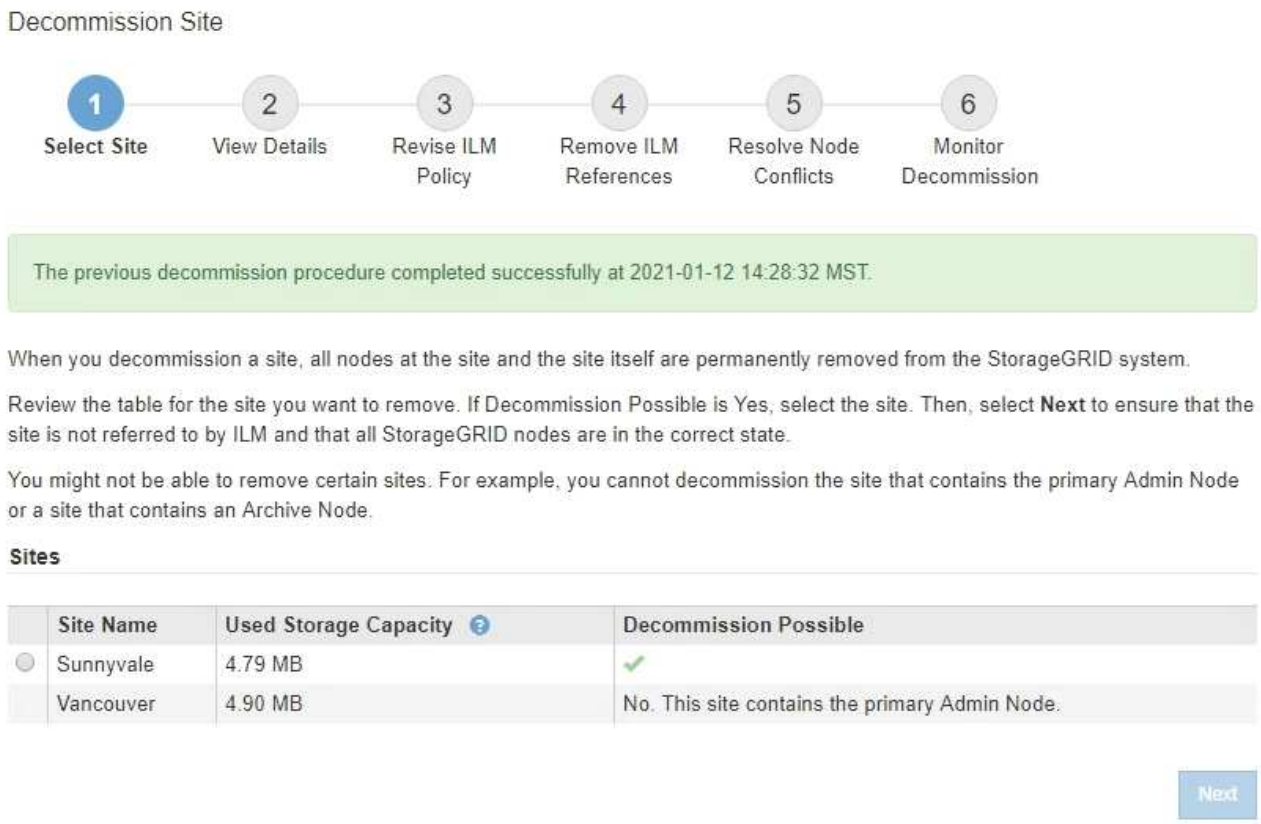



   - During the **Deactivate EC Profiles & Delete Storage Pools** step, the following ILM changes are made:
     - Any Erasure Coding profiles that referred to the site are deactivated.
     - Any Storage Pools that referred to the site are deleted.

> The system-default All Storage Nodes storage pool is also removed because it uses the All Sites site.

   - Finally, during the **Remove Configuration** step, any remaining references to the site and its nodes are removed from the rest of the grid.

5. When the decommission procedure has completed, the Decommission Site page shows a success message, and the removed site is no longer shown.




**After you finish**

Complete these tasks after you complete the site decommission procedure:

- Ensure that the drives of all Storage Nodes in the decommissioned site are wiped clean. Use a commercially available data wiping tool or service to permanently and securely remove data from the drives.
- If the site included one or more Admin Nodes and single sign-on (SSO) is enabled for your StorageGRID system, remove all relying party trusts for the site from Active Directory Federation Services (AD FS).
- After the nodes have been gracefully powered off automatically as part of the connected site decommission procedure, remove the associated virtual machines.

## Network maintenance procedures

### Update subnets for Grid Network

StorageGRID maintains a list of the network subnets used to communicate between grid nodes on the Grid Network (eth0). These entries include the subnets used for the Grid Network by each site in your StorageGRID system as well as any subnets used for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway. When you add grid nodes or a new site in an expansion, you might need to update or add subnets to the Grid Network.

**What you'll need**

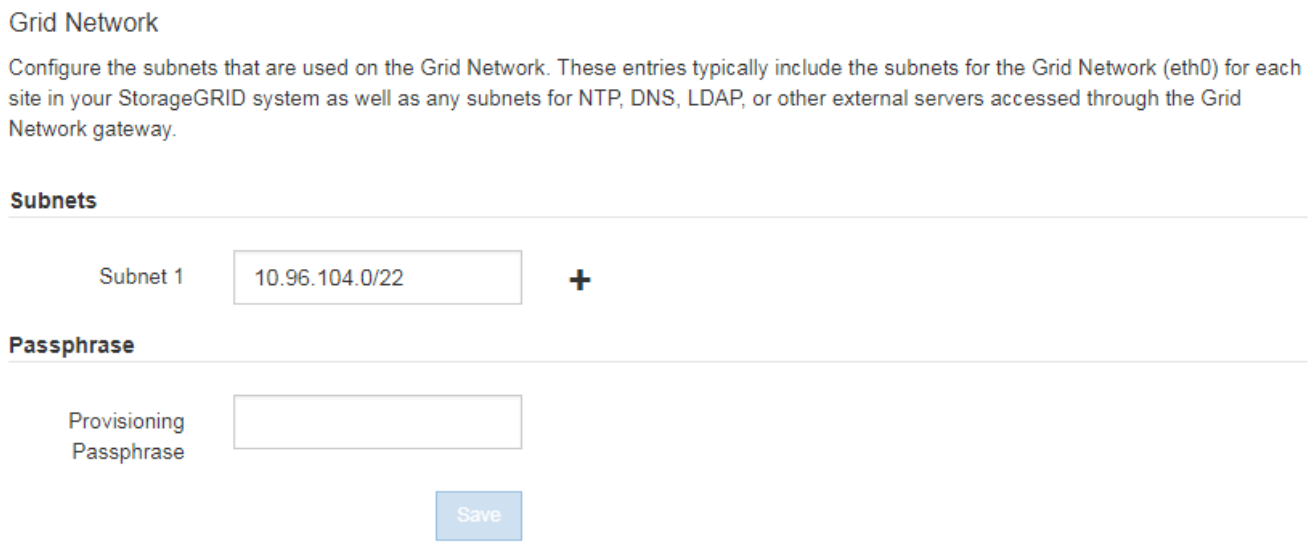
- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Maintenance or Root Access permission.
- You must have the provisioning passphrase.
- You must have the network addresses, in CIDR notation, of the subnets you want to configure.

**About this task**

If you are performing an expansion activity that includes adding a new subnet, you must add the new Grid subnet before you start the expansion procedure.

**Steps**

1. Select **MAINTENANCE** > **Network** > **Grid Network**.




2. In the Subnets list, click the plus sign to add a new subnet in CIDR notation.

   For example, enter `10.96.104.0/22`.

3. Enter the provisioning passphrase, and click **Save**.

   The subnets you have specified are configured automatically for your StorageGRID system.

4. Download a new Recovery Package from the Grid Manager.
   a. Select **MAINTENANCE** > **System** > **Recovery package**.
   b. Enter the provisioning passphrase.

**Configure IP addresses**

## You can perform network configuration by configuring IP addresses for grid nodes using the Change IP tool.

You must use the Change IP tool to make most changes to the networking configuration that was initially set during grid deployment. Manual changes using standard Linux networking commands and files might not propagate to all StorageGRID services, and might not persist across upgrades, reboots, or node recovery procedures.

If you want to change the Grid Network IP address for all nodes in the grid, use the special procedure for grid-wide changes.

If you are making changes to the Grid Network Subnet List only, use the Grid Manager to add or change the network configuration. Otherwise, use the Change IP tool if the Grid Manager is inaccessible due to a network configuration issue, or you are performing both a Grid Network routing change and other network changes at the same time.

The IP change procedure can be a disruptive procedure. Parts of the grid might be unavailable until the new configuration is applied.

**Ethernet interfaces**

The IP address assigned to eth0 is always the grid node's Grid Network IP address. The IP address assigned to eth1 is always the grid node's Admin Network IP address. The IP address assigned to eth2 is always the grid node's Client Network IP address.

Note that on some platforms, such as StorageGRID appliances, eth0, eth1, and eth2 might be aggregate interfaces composed of subordinate bridges or bonds of physical or VLAN interfaces. On these platforms, the **SSM** > **Resources** tab might show the Grid, Admin, and Client Network IP address assigned to other interfaces in addition to eth0, eth1, or eth2.

**DHCP**

You can only set up DHCP during the deployment phase. You cannot set up DHCP during configuration. You must use the IP address change procedures if you want to change IP addresses, subnet masks, and default gateways for a grid node. Using the Change IP tool will cause DHCP addresses to become static.

**High availability (HA) groups**

- If a Client network interface is contained in an HA group, you cannot change the Client network IP address for that interface to an address that is outside of the subnet configured for the HA group.
- You cannot change the Client Network IP address to the value of an existing virtual IP address assigned to an HA group configured on the Client Network interface.
- If a Grid network interface is contained in an HA group, you cannot change the Grid network IP address for that interface to an address that is outside of the subnet configured for the HA group.
- You cannot change the Grid Network IP address to the value of an existing virtual IP address assigned to an HA group configured on the Grid Network interface.

#### Change node network configuration

You can change the network configuration of one or more nodes using the Change IP tool. You can change the configuration of the Grid Network, or add, change, or remove the Admin or Client Networks.

**What you'll need**

You must have the `Passwords.txt` file.

**About this task**

**Linux:** If you are adding a grid node to the Admin Network or Client Network for the first time, and you did not previously configure ADMIN_NETWORK_TARGET or CLIENT_NETWORK_TARGET in the node configuration

file, you must do so now.

See the StorageGRID installation instructions for your Linux operating system.

**Appliances:** On StorageGRID appliances, if the Client or Admin Network was not configured in the StorageGRID Appliance Installer during the initial installation, the network cannot be added by using only the Change IP tool. First, you must place the appliance in maintenance mode, configure the links, return the appliance to normal operating mode, and then use the Change IP tool to modify the network configuration. See the procedure for configuring network links in the installation and maintenance instructions for your appliance.

You can change the IP address, subnet mask, gateway, or MTU value for one or more nodes on any network.

You can also add or remove a node from a Client Network or from an Admin Network:

- You can add a node to a Client Network or to an Admin Network by adding an IP address/subnet mask on that network to the node.
- You can remove a node from a Client Network or from an Admin Network by deleting the IP address/subnet mask for the node on that network.

  Nodes cannot be removed from the Grid Network.

> IP address swaps are not allowed. If you must exchange IP addresses between grid nodes, you must use a temporary intermediate IP address.

> If single sign-on (SSO) is enabled for your StorageGRID system and you are changing the IP address of an Admin Node, be aware that any relying party trust that was configured using the Admin Node's IP address (instead of its fully qualified domain name, as recommended) will become invalid. You will no longer be able to sign in to the node. Immediately after changing the IP address, you must update or reconfigure the node's relying party trust in Active Directory Federation Services (AD FS) with the new IP address. See the instructions for administering StorageGRID.

> Any changes you make to the network using the Change IP tool are propagated to the installer firmware for the StorageGRID appliances. That way, if StorageGRID software is reinstalled on an appliance, or if an appliance is placed into maintenance mode, the networking configuration will be correct.

**Steps**

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.
2. Start the Change IP tool by entering the following command: `change-ip`
3. Enter the provisioning passphrase at the prompt.

The main menu appears.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

4. Optionally select **1** to choose which nodes to update. Then select one of the following options:
   - **1**: Single node — select by name
   - **2**: Single node — select by site, then by name
   - **3**: Single node — select by current IP
   - **4**: All nodes at a site
   - **5**: All nodes in the grid

     **Note:** If you want to update all nodes, allow "all" to remain selected.

   After you make your selection, the main menu appears, with the **Selected nodes** field updated to reflect your choice. All subsequent actions are performed only on the nodes displayed.

5. On the main menu, select option **2** to edit IP/mask, gateway, and MTU information for the selected nodes.

   a. Select the network where you want to make changes:

      - **1**: Grid network
      - **2**: Admin network
      - **3**: Client network
      - **4**: All networks After you make your selection, the prompt shows the node name, network name (Grid, Admin, or Client), data type (IP/mask, Gateway, or MTU), and current value.

      Editing the IP address, prefix length, gateway, or MTU of a DHCP-configured interface will change the interface to static. When you select to change an interface configured by DHCP, a warning is displayed to inform you that the interface will change to static.

   Interfaces configured as `fixed` cannot be edited.

   a. To set a new value, enter it in the format shown for the current value.
   b. To leave the current value unchanged, press **Enter**.
   c. If the data type is `IP/mask`, you can delete the Admin or Client Network from the node by entering **d** or **0.0.0.0/0**.
   d. After editing all nodes you want to change, enter **q** to return to the main menu.

Your changes are held until cleared or applied.

6. Review your changes by selecting one of the following options:
   - **5**: Shows edits in output that is isolated to show only the changed item. Changes are highlighted in green (additions) or red (deletions), as shown in the example output:

```
==============================================================================
Site: RTP
==============================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
Press Enter to continue
```

   - **6**: Shows edits in output that displays the full configuration. Changes are highlighted in green (additions) or red (deletions).

> Certain command line interfaces might show additions and deletions using strikethrough formatting. Proper display depends on your terminal client supporting the necessary VT100 escape sequences.

7. Select option **7** to validate all changes.

   This validation ensures that the rules for the Grid, Admin, and Client Networks, such as not using overlapping subnets, are not violated.

   In this example, validation returned errors.

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

   In this example, validation passed.

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

8. Once validation passes, choose one of the following options:
   - **8**: Save unapplied changes.

     This option allows you to quit the Change IP tool and start it again later, without losing any unapplied changes.

   - **10**: Apply the new network configuration.
9. If you selected option **10**, choose one of the following options:
   - **apply**: Apply the changes immediately and automatically restart each node if necessary.

     If the new network configuration does not require any physical networking changes, you can select **apply** to apply the changes immediately. Nodes will be restarted automatically, if necessary. Nodes that need to be restarted will be displayed.

   - **stage**: Apply the changes the next time the nodes are restarted manually.

     If you need to make physical or virtual networking configuration changes for the new network configuration to function, you must use the **stage** option, shut down the affected nodes, make the necessary physical networking changes, and restart the affected nodes. If you select **apply** without first making these networking changes, the changes will usually fail.

     > If you use the **stage** option, you must restart the node as soon as possible after staging to minimize disruptions.

   - **cancel**: Do not make any network changes at this time.

     If you were unaware that the proposed changes require nodes to be restarted, you can defer the changes to minimize user impact. Selecting **cancel** returns you to the main menu and preserves your changes so you can apply them later.

     When you select **apply** or **stage**, a new network configuration file is generated, provisioning is performed, and nodes are updated with new working information.

     During provisioning, the output displays the status as updates are applied.

     ```
     Generating new grid networking description file...

     Running provisioning...

     Updating grid network configuration on Name
     ```

After applying or staging changes, a new Recovery Package is generated as a result of the grid configuration change.

10. If you selected **stage**, follow these steps after provisioning is complete:
    a. Make the physical or virtual networking changes that are required.

       **Physical networking changes**: Make the necessary physical networking changes, safely shutting down the node if necessary.

       **Linux**: If you are adding the node to an Admin Network or Client Network for the first time, ensure that you have added the interface as described in “Adding interfaces to an existing node.”

    b. Restart the affected nodes.
11. Select **0** to exit the Change IP tool after your changes are complete.
12. Download a new Recovery Package from the Grid Manager.
    a. Select **MAINTENANCE** > **System** > **Recovery package**.
    b. Enter the provisioning passphrase.

**Related information**

Linux: Add interfaces to existing node

Install Red Hat Enterprise Linux or CentOS

Install Ubuntu or Debian

SG100 and SG1000 services appliances

SG6000 storage appliances

SG5700 storage appliances

Administer StorageGRID

Configure IP addresses

#### Add to or change subnet lists on Admin Network

## You can add, delete, or change the subnets in the Admin Network Subnet List of one or more nodes.

**What you’ll need**

- You must have the `Passwords.txt` file.

You can add, delete, or change subnets to all nodes on the Admin Network Subnet List.

**Steps**

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

2. Start the Change IP tool by entering the following command: `change-ip`
3. Enter the provisioning passphrase at the prompt.

   The main menu appears.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

4. Optionally, limit the networks/nodes on which operations are performed. Choose one of the following:
   - Select the nodes to edit by choosing **1**, if you want to filter on specific nodes on which to perform the operation. Select one of the following options:
     - **1**: Single node (select by name)
     - **2**: Single node (select by site, then by name)
     - **3**: Single node (select by current IP)
     - **4**: All nodes at a site
     - **5**: All nodes in the grid
     - **0**: Go back
   - Allow “all” to remain selected. After the selection is made, the main menu screen appears. The Selected nodes field reflects your new selection, and now all operations selected will only be performed on this item.
5. On the main menu, select the option to edit subnets for the Admin Network (option **3**).
6. Choose one of the following:
   - Add a subnet by entering this command: `add CIDR`
   - Delete a subnet by entering this command: `del CIDR`
   - Set the list of subnets by entering this command: `set CIDR`

   For all commands, you can enter multiple addresses using this format: `add CIDR, CIDR`

   Example: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

   You can reduce the amount of typing required by using “up arrow” to recall previously typed values to the current input prompt, and then edit them if necessary.

The example input below shows adding subnets to the Admin Network Subnet List:

```
Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
  10.0.0.0/8
  172.19.0.0/16
  172.21.0.0/16
  172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16
```

7. When ready, enter **q** to go back to the main menu screen. Your changes are held until cleared or applied.

> If you selected any of the "all" node selection modes in step 2, you must press **Enter** (without **q**) to get to the next node in the list.

8. Choose one of the following:

   - Select option **5** to show edits in output that is isolated to show only the changed item. Changes are highlighted in green (additions) or red (deletions), as shown in the example output below:

```
==============================================================================
Site: Data Center 1
==============================================================================
DC1-ADM1-105-154 Admin  Subnets                          add 172.17.0.0/16
                                                         del 172.16.0.0/16
                                [      172.14.0.0/16 ]
                                [      172.15.0.0/16 ]
                                [      172.17.0.0/16 ]
                                [      172.19.0.0/16 ]
                                [      172.20.0.0/16 ]
                                [      172.21.0.0/16 ]
Press Enter to continue
```

   - Select option **6** to show edits in output that displays the full configuration. Changes are highlighted in green (additions) or red (deletions). **Note:** Certain terminal emulators might show additions and deletions using strikethrough formatting.

     When you attempt to change the subnet list, the following message is displayed:

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that are not
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
are not reachable using default StorageGRID routing, but are
reachable using a different interface and gateway. Making and
applying changes to the subnet list will make all automatically
applied subnets persistent. If you do not want that to happen, delete
the unwanted subnets before applying changes. If you know that all
/32 subnets in the list were added intentionally, you can ignore this
caution.
```

If you did not specifically assign the NTP and DNS server subnets to a network, StorageGRID creates a host route (/32) for the connection automatically. If, for example, you would rather have a /16 or /24 route for outbound connection to a DNS or NTP server, you should delete the automatically created /32 route and add the routes you want. If you do not delete the automatically created host route, it will be persisted after you apply any changes to the subnet list.

> Although you can use these automatically discovered host routes, in general you should manually configure the DNS and NTP routes to ensure connectivity.

9. Select option **7** to validate all staged changes.

   This validation ensures that the rules for the Grid, Admin, and Client Networks are followed, such as using overlapping subnets.

10. Optionally, select option **8** to save all staged changes and return later to continue making changes.

    This option allows you to quit the Change IP tool and start it again later, without losing any unapplied changes.

11. Do one of the following:
    - Select option **9** if you want to clear all changes without saving or applying the new network configuration.
    - Select option **10** if you are ready to apply changes and provision the new network configuration. During provisioning, the output displays the status as updates are applied as shown in the following sample output:

    ```
    Generating new grid networking description file...

    Running provisioning...

    Updating grid network configuration on Name
    ```

12. Download a new Recovery Package from the Grid Manager.
    a. Select **MAINTENANCE** > **System** > **Recovery package**.

b. Enter the provisioning passphrase.

**Related information**

Configure IP addresses

#### Add to or change subnet lists on Grid Network

## You can use the Change IP tool to add or change subnets on the Grid Network.

**What you'll need**

- You must have the `Passwords.txt` file.

You can add, delete, or change subnets in the Grid Network Subnet List. Changes will affect routing on all nodes in the grid.

> If you are making changes to the Grid Network Subnet List only, use the Grid Manager to add or change the network configuration. Otherwise, use the Change IP tool if the Grid Manager is inaccessible due to a network configuration issue, or you are performing both a Grid Network routing change and other network changes at the same time.

**Steps**

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.
2. Start the Change IP tool by entering the following command: `change-ip`
3. Enter the provisioning passphrase at the prompt.

   The main menu appears.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

4. On the main menu, select the option to edit subnets for the Grid Network (option **4**).

Changes to the Grid Network Subnet List are grid-wide.

5. Choose one of the following:
   - Add a subnet by entering this command: `add CIDR`
   - Delete a subnet by entering this command: `del CIDR`
   - Set the list of subnets by entering this command: `set CIDR`

     For all commands, you can enter multiple addresses using this format: `add CIDR, CIDR`

     Example: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

     You can reduce the amount of typing required by using “up arrow” to recall previously typed values to the current input prompt, and then edit them if necessary.

     The example input below shows setting subnets for the Grid Network Subnet List:

```
Editing: Grid Network Subnet List

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

Grid Network Subnet List
  172.16.0.0/21
  172.17.0.0/21
  172.18.0.0/21
  192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21
```

6. When ready, enter **q** to go back to the main menu screen. Your changes are held until cleared or applied.
7. Choose one of the following:
   - Select option **5** to show edits in output that is isolated to show only the changed item. Changes are highlighted in green (additions) or red (deletions), as shown in the example output below:

```
================================================================================
Grid Network Subnet List (GNSL)
================================================================================
                                                        add 172.30.0.0/21
                                                        add 172.31.0.0/21
                                                        del 172.16.0.0/21
                                                        del 172.17.0.0/21
                                                        del 172.18.0.0/21
                                  [      172.30.0.0/21 ]
                                  [      172.31.0.0/21 ]
                                  [     192.168.0.0/21 ]
Press Enter to continue
```

- Select option **6** to show edits in output that displays the full configuration. Changes are highlighted in green (additions) or red (deletions).

  > Certain command line interfaces might show additions and deletions using strikethrough formatting.

8. Select option **7** to validate all staged changes.

   This validation ensures that the rules for the Grid, Admin, and Client Networks are followed, such as using overlapping subnets.

9. Optionally, select option **8** to save all staged changes and return later to continue making changes.

   This option allows you to quit the Change IP tool and start it again later, without losing any unapplied changes.

10. Do one of the following:
    - Select option **9** if you want to clear all changes without saving or applying the new network configuration.
    - Select option **10** if you are ready to apply changes and provision the new network configuration. During provisioning, the output displays the status as updates are applied as shown in the following sample output:

      ```
      Generating new grid networking description file...

      Running provisioning...

      Updating grid network configuration on Name
      ```

11. If you selected option **10** when making Grid Network changes, select one of the following options:
    - **apply**: Apply the changes immediately and automatically restart each node if necessary.

      If the new network configuration will function simultaneously with the old network configuration without any external changes, you can use the **apply** option for a fully automated configuration change.

    - **stage**: Apply the changes the next time the nodes are restarted.

      If you need to make physical or virtual networking configuration changes for the new network configuration to function, you must use the **stage** option, shut down the affected nodes, make the necessary physical networking changes, and restart the affected nodes.

      > If you use the **stage** option, you must restart the node as soon as possible after staging to minimize disruptions.

    - **cancel**: Do not make any network changes at this time.

      If you were unaware that the proposed changes require nodes to be restarted, you can defer the changes to minimize user impact. Selecting **cancel** returns you to the main menu and preserves your changes so you can apply them later.

After applying or staging changes, a new Recovery Package is generated as a result of the grid configuration change.

12. If configuration is stopped due to errors, the following options are available:
    - To abort the IP change procedure and return to the main menu, enter **a**.
    - To retry the operation that failed, enter **r**.
    - To continue to the next operation, enter **c**.

      The failed operation can be retried later by selecting option **10** (Apply Changes) from the main menu. The IP change procedure will not be complete until all operations have completed successfully.

    - If you had to manually intervene (to reboot a node, for example) and are confident that the action the tool thinks has failed was actually completed successfully, enter **f** to mark it as successful and move to the next operation.
13. Download a new Recovery Package from the Grid Manager.
    a. Select **MAINTENANCE** > **System** > **Recovery package**.
    b. Enter the provisioning passphrase.

    > The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

**Related information**

Configure IP addresses

#### Change IP addresses for all nodes in grid

If you need to change the Grid Network IP address for all nodes in the grid, you must follow this special procedure. You cannot do a grid-wide Grid Network IP change using the procedure to change individual nodes.

**What you'll need**

- You must have the `Passwords.txt` file.

To ensure that the grid starts up successfully, you must make all the changes at once.

> This procedure applies to the Grid Network only. You cannot use this procedure to change IP addresses on the Admin or Client Networks.

If you want to change the IP addresses and MTU for the nodes at one site only, follow the Change node network configuration instructions.

**Steps**

1. Plan ahead for changes that you need to make outside of the Change IP tool, such as changes to DNS or NTP, and changes to the single sign-on (SSO) configuration, if used.

   > If the existing NTP servers will not be accessible to the grid on the new IP addresses, add the new NTP servers before you perform the change-ip procedure.

> If the existing DNS servers will not be accessible to the grid on the new IP addresses, add the new DNS servers before you perform the change-ip procedure.

> If SSO is enabled for your StorageGRID system and any relying party trusts were configured using Admin Node IP addresses (instead of fully qualified domain names, as recommended), be prepared to update or reconfigure these relying party trusts in Active Directory Federation Services (AD FS) immediately after you change IP addresses. See the instructions for administering StorageGRID.

> If necessary, add the new subnet for the new IP addresses.

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

      When you are logged in as root, the prompt changes from `$` to `#`.
3. Start the Change IP tool by entering the following command: `change-ip`
4. Enter the provisioning passphrase at the prompt.

   The main menu appears. By default, the `Selected nodes` field is set to `all`.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

5. On the main menu, select **2** to edit IP/subnet mask, gateway, and MTU information for all the nodes.
   a. Select **1** to make changes to the Grid Network.

      After you make your selection, the prompt shows the node names, Grid Network name, data type (IP/mask, Gateway, or MTU), and current values.

      Editing the IP address, prefix length, gateway, or MTU of a DHCP-configured interface will change the interface to static. A warning is displayed before each interface configured by DHCP.

      Interfaces configured as `fixed` cannot be edited.

b. To set a new value, enter it in the format shown for the current value.

c. After editing all nodes you want to change, enter **q** to return to the main menu.

   Your changes are held until cleared or applied.

6. Review your changes by selecting one of the following options:
   - **5**: Shows edits in output that is isolated to show only the changed item. Changes are highlighted in green (additions) or red (deletions), as shown in the example output:

```
==============================================================================
Site: RTP
==============================================================================
username-x Grid   IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid   MTU     [               1400 ]: 9000
username-x Grid   MTU     [               1400 ]: 9000
username-x Grid   MTU     [               1400 ]: 9000
username-x Grid   MTU     [               1400 ]: 9000
username-x Grid   MTU     [               1400 ]: 9000
username-x Grid   MTU     [               1400 ]: 9000
username-x Grid   MTU     [               1400 ]: 9000
username-x Admin  IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin  IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin  IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin  IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin  IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin  IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin  Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin  Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin  Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin  Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin  Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin  Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin  MTU     [               1400 ]: 0
username-x Admin  MTU     [               1400 ]: 0
username-x Admin  MTU     [               1400 ]: 0
username-x Admin  MTU     [               1400 ]: 0
username-x Admin  MTU     [               1400 ]: 0
username-x Admin  MTU     [               1400 ]: 0
Press Enter to continue
```

   - **6**: Shows edits in output that displays the full configuration. Changes are highlighted in green (additions) or red (deletions).

> Certain command line interfaces might show additions and deletions using strikethrough formatting. Proper display depends on your terminal client supporting the necessary VT100 escape sequences.

7. Select option **7** to validate all changes.

   This validation ensures that the rules for the Grid Network, such as not using overlapping subnets, are not violated.

   In this example, validation returned errors.

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

In this example, validation passed.

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

8. Once validation passes, select **10** to apply the new network configuration.
9. Select **stage** to apply the changes the next time the nodes are restarted.

> You must select **stage**. Do not perform a rolling restart, either manually or by selecting **apply** instead of **stage**; the grid will not start up successfully.

10. After your changes are complete, select **0** to exit the Change IP tool.
11. Shut down all nodes simultaneously.

> The entire grid must be shut down at once, so that all nodes are down at the same time.

12. Make the physical or virtual networking changes that are required.
13. Verify that all grid nodes are down.
14. Power on all nodes.
15. Once the grid starts up successfully:
    a. If you added new NTP servers, delete the old NTP server values.
    b. If you added new DNS servers, delete the old DNS server values.
16. Download the new Recovery Package from the Grid Manager.
    a. Select **MAINTENANCE** > **System** > **Recovery package**.
    b. Enter the provisioning passphrase.

**Related information**

Administer StorageGRID

Add to or change subnet lists on Grid Network

Shut down grid node

**Add interfaces to existing node**

#### Linux: Add Admin or Client interfaces to an existing node

## Use these steps to add an interface on the Admin Network or the Client Network to a Linux node after it has been installed.

If you did not configure ADMIN_NETWORK_TARGET or CLIENT_NETWORK_TARGET in the node configuration file on the Linux host during installation, use this procedure to add the interface. For more information about the node configuration file, see the instructions for your Linux operating system:

- Install Red Hat Enterprise Linux or CentOS
- Install Ubuntu or Debian

You perform this procedure on the Linux server hosting the node that needs the new network assignment, not inside the node. This procedure only adds the interface to the node; a validation error occurs if you attempt to specify any other network parameters.

To provide addressing information, you must use the Change IP tool. See Change node network configuration.

**Steps**

1. Log in to the Linux server hosting the node.
2. Edit the node configuration file: `/etc/storagegrid/nodes/node-name.conf`.

   > Do not specify any other network parameters, or a validation error will result.

   a. Add an entry for the new network target. For example:

   ```
   CLIENT_NETWORK_TARGET = bond0.3206
   ```

   b. Optional: Add an entry for the MAC address. For example:

   ```
   CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
   ```

3. Run the node validate command:

   ```
   sudo storagegrid node validate node-name
   ```

4. Resolve all validation errors.
5. Run the node reload command:

   ```
   sudo storagegrid node reload node-name
   ```

#### Linux: Add trunk or access interfaces to a node

## You can add extra trunk or access interfaces to a Linux node after it has been installed. The interfaces you add are displayed on the VLAN interfaces page and the HA groups page.

**What you'll need**

- You have access to the instructions for installing StorageGRID on your Linux platform.
  - Install Red Hat Enterprise Linux or CentOS

- Install Ubuntu or Debian

- You have the `Passwords.txt` file.
- You have specific access permissions.

> Do not attempt to add interfaces to a node while a software upgrade, recovery procedure, or expansion procedure is active.

**About this task**

Use these steps to add one or more extra interfaces to a Linux node after the node has been installed. For example, you might want to add a trunk interface to an Admin or Gateway Node, so you can use VLAN interfaces to segregate the traffic belonging to different applications or tenants. Or, you might want to add an access interface to use in a high availability (HA) group.

If you add a trunk interface, you must configure a VLAN interface in StorageGRID. If you add an access interface, you can add the interface directly to an HA group; you do not need to configure a VLAN interface.

The node is unavailable for a brief time when you add interfaces. You should perform this procedure on one node at a time.

**Steps**

1. Log in to the Linux server hosting the node.
2. Using a text editor such as vim or pico, edit the node configuration file:

   ```
   /etc/storagegrid/nodes/node-name.conf
   ```

3. Add an entry to the file to specify the name and, optionally, the description of each extra interface you want to add to the node. Use this format.

   ```
   INTERFACES_TARGET_nnnn=value
   ```

   For *nnnn*, specify a unique number for each `INTERFACES_TARGET` entry you are adding.

   For *value*, specify the name of the physical interface on the bare-metal host. Then, optionally, add a comma and provide a description of the interface, which is displayed on the VLAN interfaces page and the HA groups page.

   For example:

   ```
   INTERFACES_TARGET_01=ens256, Trunk
   ```

   > Do not specify any other network parameters, or a validation error will result.

4. Run the following command to validate your changes to the node configuration file:

   ```
   sudo storagegrid node validate node-name
   ```

   Address any errors or warnings before proceeding to the next step.

5. Run the following command to update the node's configuration:

   ```
   sudo storagegrid node reload node-name
   ```

### After you finish

- If you added one or more trunk interfaces, go to configure VLAN interfaces to configure one or more VLAN interfaces for each new parent interface.
- If you added one or more access interfaces, go to configure high availability groups to add the new interfaces directly to HA groups.

#### VMware: Add trunk or access interfaces to a node

You can add a trunk or access interface to a VM node after the node has been installed. The interfaces you add are displayed on the VLAN interfaces page and the HA groups page.

### What you'll need

- You have access to the instructions for installing StorageGRID on your VMware platform.

Install VMware

- You have configured StorageGRID 11.6.
- You have Admin Node and Gateway Node VMware virtual machines.
- You have a network subnet that is not being used as Grid, Admin, or Client network.
- You have the `Passwords.txt` file.
- You have specific access permissions.

> Do not attempt to add interfaces to a node while a software upgrade, recovery procedure, or expansion procedure is active.

### About this task

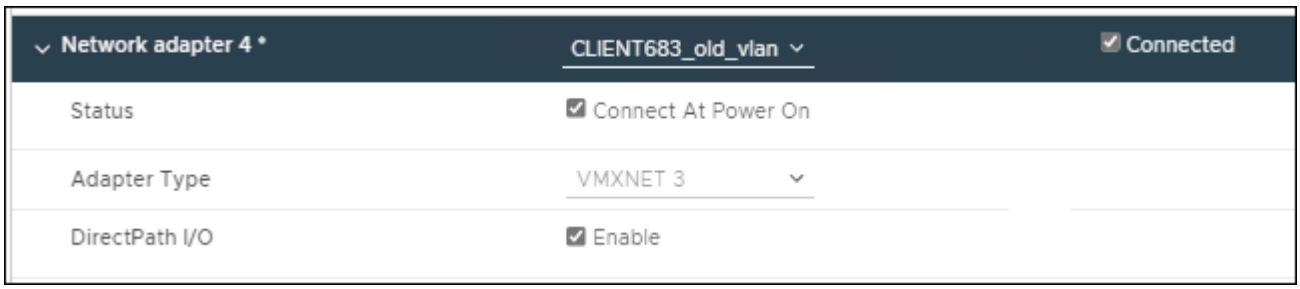
Use these steps to add one or more extra interfaces to a VMware node after the node has been installed. For example, you might want to add a trunk interface to an Admin or Gateway Node, so you can use VLAN interfaces to segregate the traffic belonging to different applications or tenants. Or you might want to add an access interface to use in a high availability (HA) group.

If you add a trunk interface, you must configure a VLAN interface in StorageGRID. If you add an access interface, you can add the interface directly to an HA group; you do not need to configure a VLAN interface.

The node might be unavailable for a brief time when you add interfaces.

### Steps

1. In vCenter, add a new network adapter (type VMXNET3) to an Admin Node and Gateway Node VM. Select **Connected** and **Connect At Power On** check boxes.



2. Use SSH to log in to the Admin Node or Gateway Node.
3. Use `ip link show` to confirm the new network interface ens256 is detected.

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT
group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

#### After you finish

- If you added one or more trunk interfaces, go to configure VLAN interfaces to configure one or more VLAN interfaces for each new parent interface.
- If you added one or more access interfaces, go to configure high availability groups to add the new interfaces directly to HA groups.

### Configure DNS servers

You can add, remove, and update domain name system (DNS) servers, so that you can use fully qualified domain name (FQDN) hostnames rather than IP addresses.

#### What you'll need

- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Maintenance or Root Access permission.
- You must have the IP addresses of the DNS servers to configure.

Specifying DNS server information allows you to use fully qualified domain name (FQDN) hostnames rather than IP addresses for email or SNMP notifications and AutoSupport. Specifying at least two DNS servers is recommended.

> Provide between two to six IP addresses for DNS servers. In general, select DNS servers that each site can access locally in the event of network islanding. This is to ensure an islanded site continues to have access to the DNS service. After configuring the grid-wide DNS server list, you can further customize the DNS server list for each node.

If the DNS server information is omitted or incorrectly configured, a DNST alarm is triggered on each grid node's SSM service. The alarm clears when DNS is configured correctly and the new server information has

reached all grid nodes.

**Steps**

1. Select **MAINTENANCE** > **Network** > **DNS servers**.
2. In the Servers section, add update, or remove DNS server entries, as necessary.

   The best practice is to specify at least two DNS servers per site. You can specify up to six DNS servers.

3. Click **Save**.

#### Modify DNS configuration for single grid node

## Rather than configure the Domain Name System (DNS) globally for the entire deployment, you can run a script to configure DNS differently for each grid node.

In general, you should use the **MAINTENANCE** > **Network** > **DNS servers** option on the Grid Manager to configure DNS servers. Only use the following script if you need to use different DNS servers for different grid nodes.

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.

   e. Add the SSH private key to the SSH agent. Enter: `ssh-add`
   f. Enter the SSH Access Password listed in the `Passwords.txt` file.
2. Log in to the node you want to update with a custom DNS configuration: `ssh node_IP_address`
3. Run the DNS setup script: `setup_resolv.rb.`

   The script responds with the list of supported commands.

```
Tool to modify external name servers

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


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

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

4. Add the IPv4 address of a server that provides domain name service for your network: `add <nameserver IP_address>`
5. Repeat the `add nameserver` command to add name servers.
6. Follow instructions as prompted for other commands.
7. Save your changes and exit the application: `save`
8. Close the command shell on the server: `exit`
9. For each grid node, repeat the steps from logging into the node through closing the command shell.
10. When you no longer require passwordless access to other servers, remove the private key from the SSH

agent. Enter: `ssh-add -D`

### Configure NTP servers

You can add, update, or remove network time protocol (NTP) servers to ensure that data is synchronized accurately between grid nodes in your StorageGRID system.

#### What you'll need

- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Maintenance or Root Access permission.
- You must have the provisioning passphrase.
- You must have the IPv4 addresses of the NTP servers to configure.

#### About this task

The StorageGRID system uses the network time protocol (NTP) to synchronize time between all grid nodes in the grid.

At each site, at least two nodes in the StorageGRID system are assigned the primary NTP role. They synchronize to a suggested minimum of four, and a maximum of six, external time sources and with each other. Every node in the StorageGRID system that is not a primary NTP node acts as an NTP client and synchronizes with these primary NTP nodes.

The external NTP servers connect to the nodes to which you previously assigned Primary NTP roles. For this reason, specifying at least two nodes with Primary NTP roles is recommended.

> Make sure that at least two nodes at each site can access at least four external NTP sources. If only one node at a site can reach the NTP sources, timing issues will occur if that node goes down. In addition, designating two nodes per site as primary NTP sources ensures accurate timing if a site is isolated from the rest of the grid.

The specified external NTP servers must use the NTP protocol. You must specify NTP server references of Stratum 3 or better to prevent issues with time drift.

> When specifying the external NTP source for a production-level StorageGRID installation, do not use the Windows Time (W32Time) service on a version of Windows earlier than Windows Server 2016. The time service on earlier versions of Windows is not sufficiently accurate and is not supported by Microsoft for use in high-accuracy environments, such as StorageGRID.

Support boundary to configure the Windows Time service for high-accuracy environments

If you encounter problems with the stability or availability of the NTP servers originally specified during installation, you can update the list of external NTP sources that the StorageGRID system uses by adding additional servers, or updating or removing existing servers.

#### Steps

1. Select **MAINTENANCE** > **Network** > **NTP servers**.
2. In the Servers section, add update, or remove NTP server entries, as necessary.

   You should include at least 4 NTP servers, and you can specify up to 6 servers.

3. In the **Provisioning Passphrase** text box, enter the provisioning passphrase for your StorageGRID

system and click **Save**.

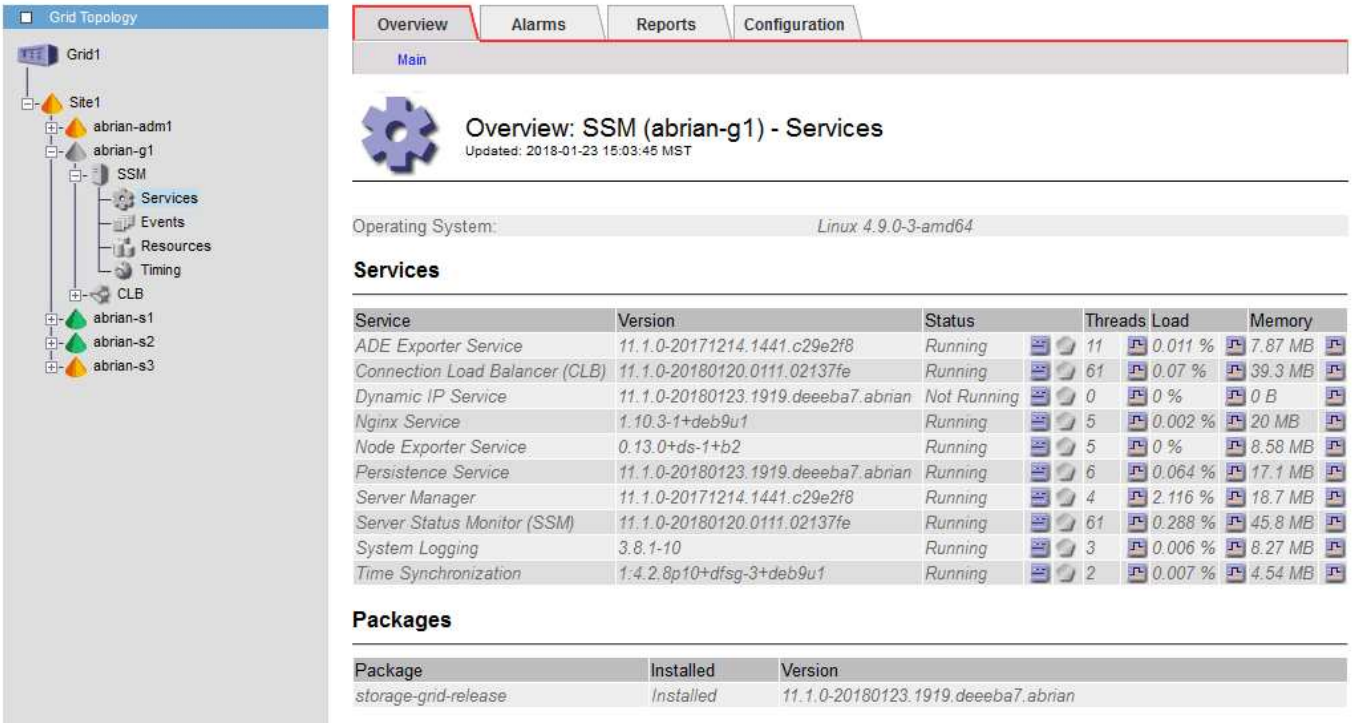
The status of the procedure is displayed at the top of the page. The page is disabled until the configuration updates are complete.

> If all of your NTP servers fail the connection test after you save the new NTP servers, do not proceed. Contact technical support.

### Restore network connectivity for isolated nodes

Under certain circumstances, such as site- or grid-wide IP address changes, one or more groups of nodes might not be able to contact the rest of the grid.

In the Grid Manager (**SUPPORT** > **Tools** > **Grid topology**), if a node is gray, or if a node is blue with many of its services showing a status other than Running, you should check for node isolation.




Some of the consequences of having isolated nodes include the following:

- If multiple nodes are isolated, you might not be able to sign in to or access the Grid Manager.
- If multiple nodes are isolated, the storage usage and quota values shown on the Dashboard for the Tenant Manager might be out of date. The totals will be updated when network connectivity is restored.

To resolve the isolation issue, you run a command line utility on each isolated node or on one node in a group (all nodes in a subnet that does not contain the primary Admin Node) that is isolated from the grid. The utility provides the nodes with the IP address of a non-isolated node in the grid, which allows the isolated node or group of nodes to contact the entire grid again.

> If the multicast Domain Name System (mDNS) is disabled in the networks, the command line utility might have to be run on each isolated node.

1. Access the node and check `/var/local/log/dynip.log` for isolation messages.

   For example:

   ```
   [2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
   no contact with other nodes.
   If this warning persists, manual action may be required.
   ```

   If you are using the VMware console, it will contain a message that the node might be isolated.

   On Linux deployments, isolation messages would appear in `/var/log/storagegrid/node/<nodename>.log` files.

2. If the isolation messages are recurring and persistent, run the following command:

   ```
   add_node_ip.py <address>
   ```

   where `<address>` is the IP address of a remote node that is connected to the grid.

   ```
   # /usr/sbin/add_node_ip.py  10.224.4.210

   Retrieving local host information
   Validating remote node at address 10.224.4.210
   Sending node IP hint for 10.224.4.210 to local node
   Local node found on remote node. Update complete.
   ```

3. Verify the following for each node that was previously isolated:
   - The node's services have started.
   - The status of the Dynamic IP Service is "Running" after you run the `storagegrid-status` command.
   - In the Grid Topology tree, the node no longer appears disconnected from the rest of the grid.

> If running the `add_node_ip.py` command does not solve the problem, there could be other networking issues that need to be resolved.

## Host-level and middleware procedures

Some maintenance procedures are specific to Linux or VMware deployments of StorageGRID, or are specific to other components of the StorageGRID solution.

### Linux: Migrate grid node to new host

You can migrate StorageGRID nodes from one Linux host to another to perform host maintenance (such as OS patching and reboot) without impacting the functionality or availability of your grid.

You migrate one or more nodes from one Linux host (the “source host”) to another Linux host (the “target host”). The target host must have previously been prepared for StorageGRID use.

> You can use this procedure only if you planned your StorageGRID deployment to include migration support.

To migrate a grid node to a new host, both of the following conditions must be true:

- Shared storage is used for all per-node storage volumes
- Network interfaces have consistent names across hosts

> In a production deployment, do not run more than one Storage Node on a single host. Using a dedicated host for each Storage Node provides an isolated failure domain.

Other types of nodes, such as Admin Nodes or Gateway Nodes, can be deployed on the same host. However, if you have multiple nodes of the same type (two Gateway Nodes, for example), do not install all instances on the same host.

For more information, see “Node migration requirements” in the StorageGRID installation instructions for your Linux operating system.

**Related information**

Deploy new Linux hosts

Install Red Hat Enterprise Linux or CentOS

Install Ubuntu or Debian

#### Linux: Export node from source host

### Shut down the grid node and export it from the source Linux host.

Run the following command on the source Linux host.

1. Obtain the status of all nodes currently running on the source host.

   ```
   sudo storagegrid node status all
   ```

   ```
   Name Config-State Run-State

   DC1-ADM1 Configured Running

   DC1-ARC1 Configured Running

   DC1-GW1 Configured Running

   DC1-S1 Configured Running

   DC1-S2 Configured Running

   DC1-S3 Configured Running
   ```

2. Identify the name of the node you want to migrate, and stop it if its Run-State is `Running`.

```
sudo storagegrid node stop DC1-S3
```

```
Stopping node DC1-S3

Waiting up to 630 seconds for node shutdown
```

3. Export the node from the source host.

```
sudo storagegrid node export DC1-S3
```

```
Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.

Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you

want to import it again.
```

4. Take note of the `import command suggested in the output of the `export` command.

   You will run this command on the target host in the next step.

#### Linux: Import node on target host

After exporting the node from the source host, you import and validate the node on the target Linux host. Validation confirms that the node has access to the same block storage and network interface devices as it had on the source host.

Run the following command on the target Linux host.

1. Import the node on the target host.

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

```
Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.

You should run 'storagegrid node validate DC1-S3'
```

2. Validate the node configuration on the new host.

```
sudo storagegrid node validate DC1-S3
```

```
Confirming existence of node DC1-S3... PASSED

Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node DC1-
```

```
S3... PASSED

Checking for duplication of unique values... PASSED
```

3. If any validation errors occur, address them before starting the migrated node.

   For troubleshooting information, see the StorageGRID installation instructions for your Linux operating system.

**Related information**

Install Red Hat Enterprise Linux or CentOS

Install Ubuntu or Debian

#### Linux: Start migrated node

After you validate the migrated node, you start the node by running a command on the target Linux host.

**Steps**

1. Start the node on the new host.

```
sudo storagegrid node start DC1-S3
Starting node DC1-S3
```

2. In the Grid Manager, verify that the status of the node is green with no alarms raised against it.

   > Verifying that the status of the node is green ensures that the migrated node has fully restarted and rejoined the grid. If the status is not green, do not migrate any additional nodes so that you will not have more than one node out of service.

   If you are unable to access the Grid Manager, wait for 10 minutes, then run the following command:

   `sudo storagegrid node status` ***`node-name`***

   Confirm that the migrated node has a Run-State of `Running`.

### Archive Node maintenance for TSM middleware

Archive Nodes might be configured to target either tape through a TSM middleware server or the cloud through the S3 API. Once configured, an Archive Node's target cannot be changed.

If the server hosting the Archive Node fails, replace the server and follow the appropriate recovery procedure.

#### Fault with archival storage devices

If you determine that there is a fault with the archival storage device that the Archive Node is accessing through Tivoli Storage Manager (TSM), take the Archive Node offline to limit the number of alarms displayed in the StorageGRID system. You can then use the administrative tools of the TSM server or the storage device,

or both, to further diagnose and resolve the problem.

### Take the Target component offline

Before undertaking any maintenance of the TSM middleware server that might result in it becoming unavailable to the Archive Node, take the Target component offline to limit the number of alarms that are triggered if the TSM middleware server becomes unavailable.

#### What you'll need

You must be signed in to the Grid Manager using a supported web browser.

#### Steps

1. Select **SUPPORT** > **Tools** > **Grid topology**.
2. Select **Archive Node** > **ARC** > **Target** > **Configuration** > **Main**.
3. Change the value of Tivoli Storage Manager State to **Offline**, and click **Apply Changes**.
4. After maintenance is complete, change the value of Tivoli Storage Manager State to **Online**, and click **Apply Changes**.

#### Tivoli Storage Manager administrative tools

The dsmadmc tool is the administrative console for the TSM middleware server that is installed on the Archive Node. You can access the tool by typing `dsmadmc` at the command line of the server. Log in to the administrative console using the same administrative user name and password that is configured for the ARC service.

The `tsmquery.rb` script was created to generate status information from dsmadmc in a more readable form. You can run this script by entering the following command at the command line of the Archive Node:
`/usr/local/arc/tsmquery.rb status`

For more information about the TSM administrative console dsmadmc, see the *Tivoli Storage Manager for Linux: Administrator's Reference*.

#### Object permanently unavailable

When the Archive Node requests an object from the Tivoli Storage Manager (TSM) server and the retrieval fails, the Archive Node retries the request after an interval of 10 seconds. If the object is permanently unavailable (for example, because the object is corrupted on tape), the TSM API has no way to indicate this to the Archive Node, so the Archive Node continues to retry the request.

When this situation occurs, an alarm is triggered, and the value continues to increase. To see the alarm, select **SUPPORT** > **Tools** > **Grid topology**. Then, select **Archive Node** > **ARC** > **Retrieve** > **Request Failures**.

If the object is permanently unavailable, you must identify the object and then manually cancel the Archive Node's request as described in the procedure, Determining if objects are permanently unavailable.

A retrieval can also fail if the object is temporarily unavailable. In this case, subsequent retrieval requests should eventually succeed.

If the StorageGRID system is configured to use an ILM rule that creates a single object copy and that copy cannot be retrieved, the object is lost and cannot be recovered. However, you must still follow the procedure to determine if the object is permanently unavailable to "clean up" the StorageGRID system, to cancel the Archive Node's request, and to purge metadata for the lost object.

### Determining if objects are permanently unavailable

You can determine if objects are permanently unavailable by making a request using the TSM administrative console.

#### What you'll need

- You must have specific access permissions.
- You must have the `Passwords.txt` file.
- You must know the IP address of an Admin Node.

#### About this task

This example is provided for your information only; this procedure cannot help you identify all failure conditions that might result in unavailable objects or tape volumes. For information about TSM administration, see TSM Server documentation.

#### Steps

1. Log in to an Admin Node:
   a. Enter the following command: `ssh admin@Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
2. Identify the object or objects that could not be retrieved by the Archive Node:
   a. Go to the directory containing the audit log files: `cd /var/local/audit/export`

      The active audit log file is named audit.log. Once a day, the active `audit.log` file is saved, and a new `audit.log` file is started. The name of the saved file indicates when it was saved, in the format `yyyy-mm-dd.txt`. After a day, the saved file is compressed and renamed, in the format `yyyy-mm-dd.txt.gz`, which preserves the original date.

   b. Search the relevant audit log file for messages indicating that an archived object could not be retrieved. For example, enter: `grep ARCE audit.log | less -n`

      When an object cannot be retrieved from an Archive Node, the ARCE audit message (Archive Object Retrieve End) displays ARUN (archive middleware unavailable) or GERR (general error) in the result field. The following example line from the audit log shows that the ARCE message terminated with the result ARUN for CBID 498D8A1F681F05B3.

      ```
      [AUDT:[CBID(UI64):0x498D8A1F681F05B3][VLID(UI64):□20091127][RSLT(FC32
      ):ARUN][AVER(UI32):7]
      [ATIM(UI64):1350613602969243][ATYP(FC32):ARCE][ANID(UI32):13959984][A
      MID(FC32):ARCI]
      [ATID(UI64):4560349751312520631]]
      ```

      For more information see the instructions for understanding audit messages.

   c. Record the CBID of each object that had a request failure.

      You might also want to record the following additional information used by the TSM to identify objects saved by the Archive Node:

- **File Space Name**: Equivalent to the Archive Node ID. To find the Archive Node ID, select **SUPPORT** > **Tools** > **Grid topology**. Then, select **Archive Node** > **ARC** > **Target** > **Overview**.
- **High Level Name**: Equivalent to the volume ID assigned to the object by the Archive Node. The volume ID takes the form of a date (for example, `20091127`), and is recorded as the VLID of the object in archive audit messages.
- **Low Level Name**: Equivalent to the CBID assigned to an object by the StorageGRID system.

d. Log out of the command shell: `exit`

3. Check the TSM server to see if the objects identified in step 2 are permanently unavailable:

a. Log in to the administrative console of the TSM server: `dsmadmc`

Use the administrative user name and password that are configured for the ARC service. Enter the user name and password in the Grid Manager. (To see the user name, select **SUPPORT** > **Tools** > **Grid topology**. Then, select **Archive Node** > **ARC** > **Target** > **Configuration**.)

b. Determine if the object is permanently unavailable.

For example, you might search the TSM activity log for a data integrity error for that object. The following example shows a search of the activity log for the past day for an object with CBID `498D8A1F681F05B3`.

```
> query actlog begindate=-1 search=276C14E94082CC69
12/21/2008 05:39:15 ANR0548W Retrieve or restore
failed for session 9139359 for node DEV-ARC-20 (Bycast ARC)
processing file space /19130020 4 for file /20081002/
498D8A1F681F05B3 stored as Archive - data
integrity error detected. (SESSION: 9139359)
>
```

Depending on the nature of the error, the CBID might not be recorded in the TSM activity log. You might need to search the log for other TSM errors around the time of the request failure.

c. If an entire tape is permanently unavailable, identify the CBIDs for all objects stored on that volume: `query content TSM_Volume_Name`

where `TSM_Volume_Name` is the TSM name for the unavailable tape. The following is an example of the output for this command:

```
 > query content TSM-Volume-Name
Node Name     Type Filespace  FSID Client's Name for File Name
------------- ---- ---------- ---- ----------------------------
DEV-ARC-20    Arch /19130020  216  /20081201/ C1D172940E6C7E12
DEV-ARC-20    Arch /19130020  216  /20081201/ F1D7FBC2B4B0779E
```

The `Client's Name for File Name` is the same as the Archive Node volume ID (or TSM “high level name”) followed by the object’s CBID (or TSM “low level name”). That is, the `Client's Name for File Name` takes the form `/Archive Node volume ID /CBID`. In the first line of the

example output, the `Client's Name for File Name` is `/20081201/ C1D172940E6C7E12`.

Recall also that the `Filespace` is the node ID of the Archive Node.

You will need the CBID of each object stored on the volume and the node ID of the Archive Node to cancel the retrieval request.

4. For each object that is permanently unavailable, cancel the retrieval request and issue a command to inform the StorageGRID system that the object copy was lost:

> Use the ADE Console with caution. If the console is used improperly, it is possible to interrupt system operations and corrupt data. Enter commands carefully, and only use the commands documented in this procedure.

   a. If you are not already logged in to the Archive Node, log in as follows:
      i. Enter the following command: `ssh admin@grid_node_IP`
      ii. Enter the password listed in the `Passwords.txt` file.
      iii. Enter the following command to switch to root: `su -`
      iv. Enter the password listed in the `Passwords.txt` file.
   b. Access the ADE console of the ARC service: `telnet localhost 1409`
   c. Cancel the request for the object: `/proc/BRTR/cancel -c CBID`

      where `CBID` is the identifier of the object that cannot be retrieved from the TSM.

      If the only copies of the object are on tape, the “bulk retrieval” request is canceled with a message, “1 requests canceled”. If copies of the object exist elsewhere in the system, the object retrieval is processed by a different module so the response to the message is “0 requests canceled”.

   d. Issue a command to notify the StorageGRID system that an object copy has been lost and that an additional copy must be made: `/proc/CMSI/Object_Lost CBID node_ID`

      where `CBID` is the identifier of the object that cannot be retrieved from the TSM server, and `node_ID` is the node ID of the Archive Node where the retrieval failed.

      You must enter a separate command for each lost object copy: entering a range of CBIDs is not supported.

      In most cases, the StorageGRID system immediately begins to make additional copies of object data to ensure that the system’s ILM policy is followed.

      However, if the ILM rule for the object specified that only one copy be made and that copy has now been lost, the object cannot be recovered. In this case running the `Object_Lost` command purges the lost object’s metadata from the StorageGRID system.

      When the `Object_Lost` command completes successfully, the following message is returned:

```
CLOC_LOST_ANS returned result 'SUCS'
```

> The `/proc/CMSI/Object_Lost` command is only valid for lost objects that are stored on Archive Nodes.

e. Exit the ADE Console: `exit`

f. Log out of the Archive Node: `exit`

5. Reset the value of Request Failures in the StorageGRID system:
   a. Go to **Archive Node** > **ARC** > **Retrieve** > **Configuration**, and select **Reset Request Failure Count**.
   b. Click **Apply Changes**.

**Related information**

Administer StorageGRID

Review audit logs

#### VMware: Configure virtual machine for automatic restart

If the virtual machine does not restart after VMware vSphere Hypervisor is restarted, you might need to configure the virtual machine for automatic restart.

You should perform this procedure if you notice that a virtual machine does not restart while you are recovering a grid node or performing another maintenance procedure.

**Steps**

1. In the VMware vSphere Client tree, select the virtual machine that is not started.
2. Right-click the virtual machine, and select **Power on**.
3. Configure VMware vSphere Hypervisor to restart the virtual machine automatically in future.

## Grid node procedures

You might need to perform procedures on a specific grid node. While you can perform a few of these procedures from Grid Manager, most of the procedures require you to access Server Manager from the node's command line.

Server Manager runs on every grid node to supervise the starting and stopping of services and to ensure that services gracefully join and leave the StorageGRID system. Server Manager also monitors the services on every grid node and will automatically attempt to restart any services that report faults.

> You should access Server Manager only if technical support has directed you to do so.

> You must close the current command shell session and log out after you are finished with Server Manager. Enter: `exit`

#### View Server Manager status and version

For each grid node, you can view the current status and version of Server Manager running on that grid node. You can also obtain the current status of all services running on that grid node.

#### What you'll need

You must have the `Passwords.txt` file.

#### Steps

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. View the current status of Server Manager running on the grid node: **`service servermanager status`**

   The current status of Server Manager running on the grid node is reported (running or not). If Server Manager's status is `running`, the time it has been running since last it was started is listed. For example:

   ```
   servermanager running for 1d, 13h, 0m, 30s
   ```

3. View the current version of Server Manager running on a grid node: **`service servermanager version`**

   The current version is listed. For example:

   ```
   11.1.0-20180425.1905.39c9493
   ```

4. Log out of the command shell: **`exit`**

### View current status of all services

You can view the current status of all services running on a grid node at any time.

#### What you'll need

You must have the `Passwords.txt` file.

#### Steps

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. View the status of all services running on the grid node: `storagegrid-status`

   For example, the output for the primary Admin Node shows the current status of the AMS, CMN, and NMS services as Running. This output is updated immediately if the status of a service changes.

```
Host Name                      190-ADM1
IP Address
Operating System Kernel        4.9.0          Verified
Operating System Environment   Debian 9.4     Verified
StorageGRID Webscale Release   11.1.0         Verified
Networking                                    Verified
Storage Subsystem                             Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.1.0         Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.1.0         Running
cmn                            11.1.0         Running
nms                            11.1.0         Running
ssm                            11.1.0         Running
mi                             11.1.0         Running
dynip                          11.1.0         Running
nginx                          1.10.3         Running
tomcat                         8.5.14         Running
grafana                        4.2.0          Running
mgmt api                       11.1.0         Running
prometheus                     1.5.2+ds       Running
persistence                    11.1.0         Running
ade exporter                   11.1.0         Running
attrDownPurge                  11.1.0         Running
attrDownSamp1                  11.1.0         Running
attrDownSamp2                  11.1.0         Running
node exporter                  0.13.0+ds      Running
```

3. Return to the command line, press **Ctrl+C**.
4. Optionally, view a static report for all services running on the grid node: `/usr/local/servermanager/reader.rb`

   This report includes the same information as the continuously updated report, but it is not updated if the status of a service changes.

5. Log out of the command shell: `exit`

### Start Server Manager and all services

You might need to start Server Manager, which also starts all services on the grid node.

#### What you'll need

You must have the `Passwords.txt` file.

#### About this task

Starting Server Manager on a grid node where it is already running results in a restart of Server Manager and all services on the grid node.

#### Steps

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@grid_node_IP`

b. Enter the password listed in the `Passwords.txt` file.

c. Enter the following command to switch to root: `su -`

d. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

2. Start Server Manager: `service servermanager start`
3. Log out of the command shell: `exit`

#### Restart Server Manager and all services

You might need to restart server manager and all services running on a grid node.

**What you'll need**

You must have the `Passwords.txt` file.

**Steps**

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@`*`grid_node_IP`*

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Restart Server Manager and all services on the grid node: `service servermanager restart`

   Server Manager and all services on the grid node are stopped and then restarted.

   > Using the `restart` command is the same as using the `stop` command followed by the `start` command.

3. Log out of the command shell: `exit`

#### Stop Server Manager and all services

Server Manager is intended to run at all times, but you might need to stop Server Manager and all services running on a grid node.

**What you'll need**

You must have the `Passwords.txt` file.

**Steps**

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@`*`grid_node_IP`*

   b. Enter the password listed in the `Passwords.txt` file.

c. Enter the following command to switch to root: `su -`

d. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

2. Stop Server manager and all services running on the grid node: `service servermanager stop`

   Server Manager and all services running on the grid node are gracefully terminated. Services can take up to 15 minutes to shut down.

3. Log out of the command shell: `exit`

#### View current status of service

You can view the current status of a services running on a grid node at any time.

##### What you'll need

You must have the `Passwords.txt` file.

##### Steps

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. View the current status of a service running on a grid node: `**service *servicename* status** The current status of the requested service running on the grid node is reported (running or not). For example:

```
cmn running for 1d, 14h, 21m, 2s
```

3. Log out of the command shell: **`exit`**

#### Stop service

Some maintenance procedures require you to stop a single service while keeping other services on the grid node running. Only stop individual services when directed to do so by a maintenance procedure.

##### What you'll need

You must have the `Passwords.txt` file.

##### About this task

When you use these steps to "administratively stop" a service, Server Manager will not automatically restart the service. You must either start the single service manually or restart Server Manager.

If you need to stop the LDR service on a Storage Node, be aware that it might take a while to stop the service if there are active connections.

**Steps**

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Stop an individual service: `service servicename stop`

   For example:

   ```
   service ldr stop
   ```

   Services can take up to 11 minutes to stop.

3. Log out of the command shell: `exit`

**Related information**

Force service to terminate

### Place appliance into maintenance mode

You must place the appliance into maintenance mode before performing specific maintenance procedures.

**What you'll need**

- You are signed in to the Grid Manager using a supported web browser.
- You have the Maintenance or Root access permission. For details, see the instructions for administering StorageGRID.

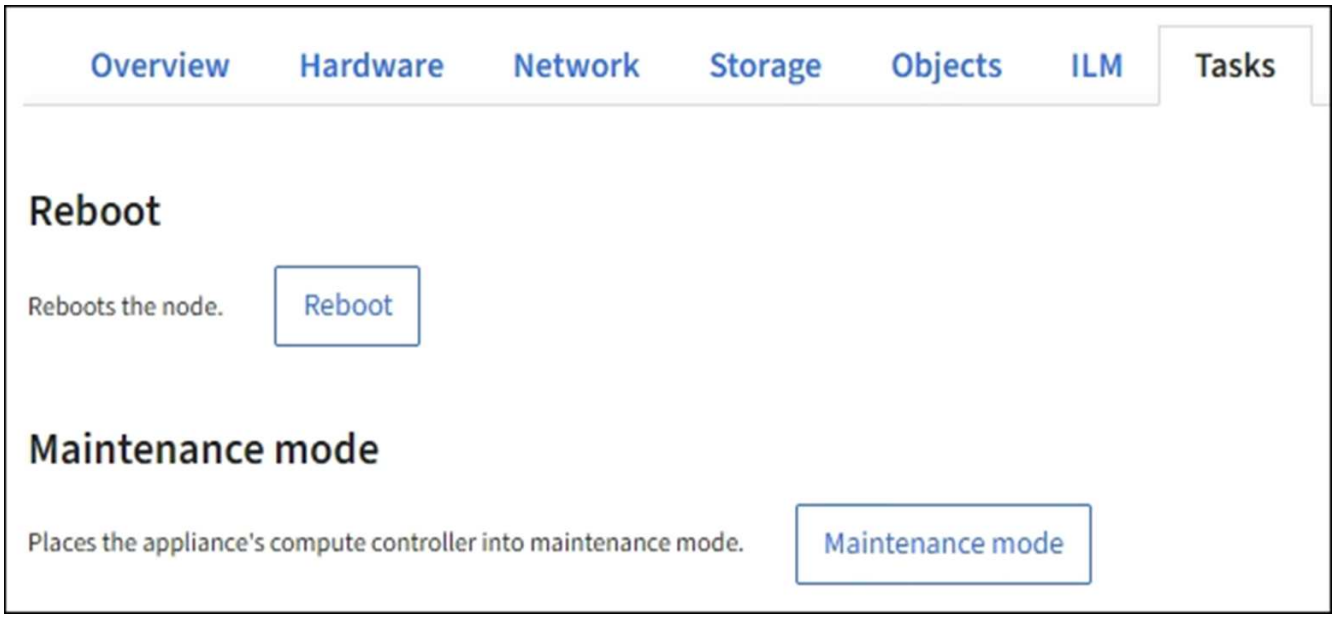
**About this task**

In rare instances, placing a StorageGRID appliance into maintenance mode might make the appliance unavailable for remote access.

The admin account password and SSH host keys for a StorageGRID appliance in maintenance mode remain the same as they were when the appliance was in service.

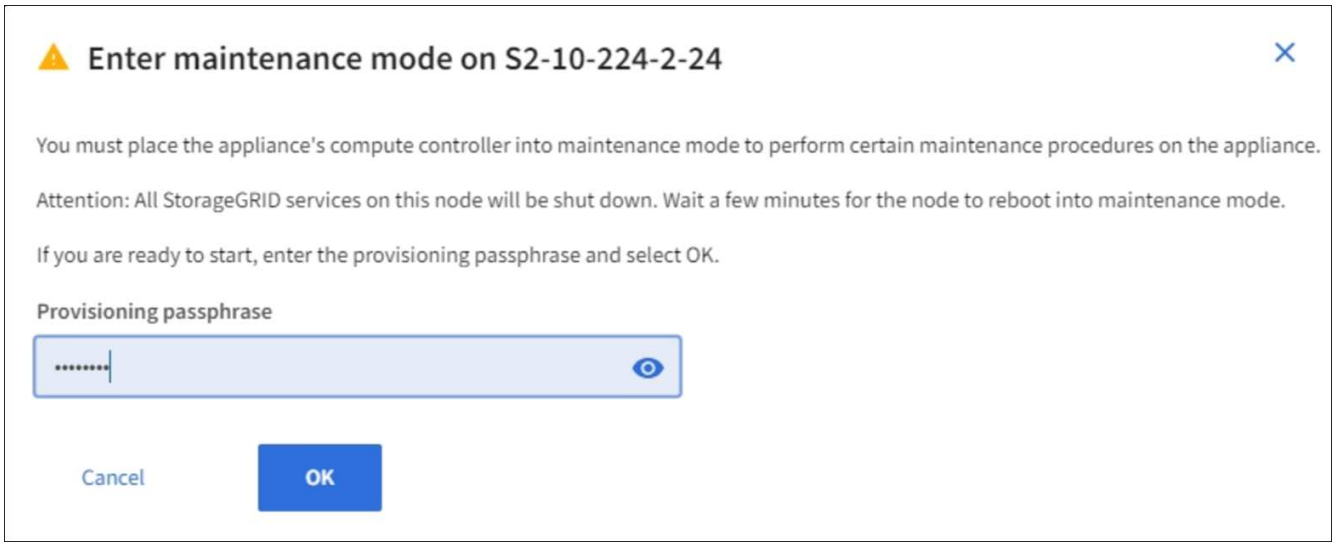
**Steps**

1. From the Grid Manager, select **NODES**.
2. From the tree view of the Nodes page, select the appliance Storage Node.
3. Select **Tasks**.



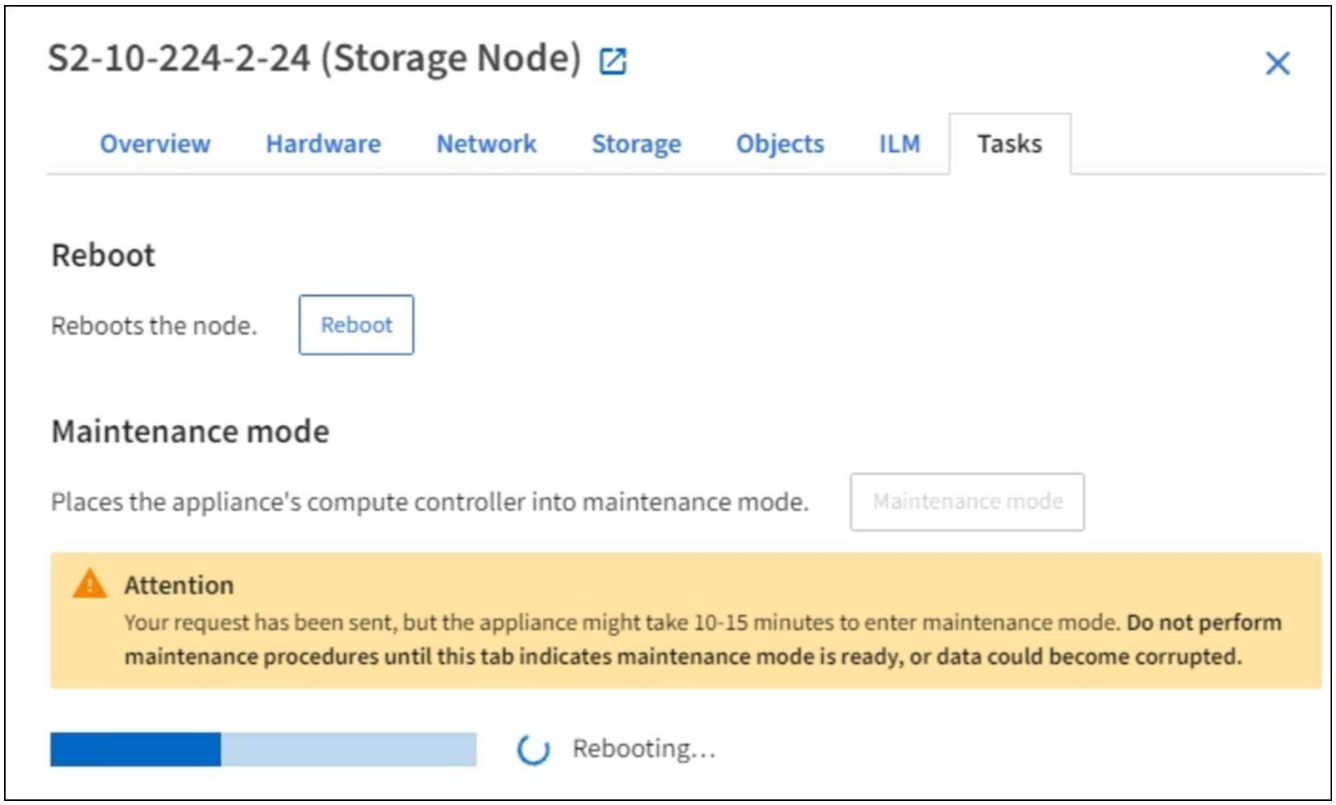

4. Select **Maintenance mode**.

   A confirmation dialog box appears.

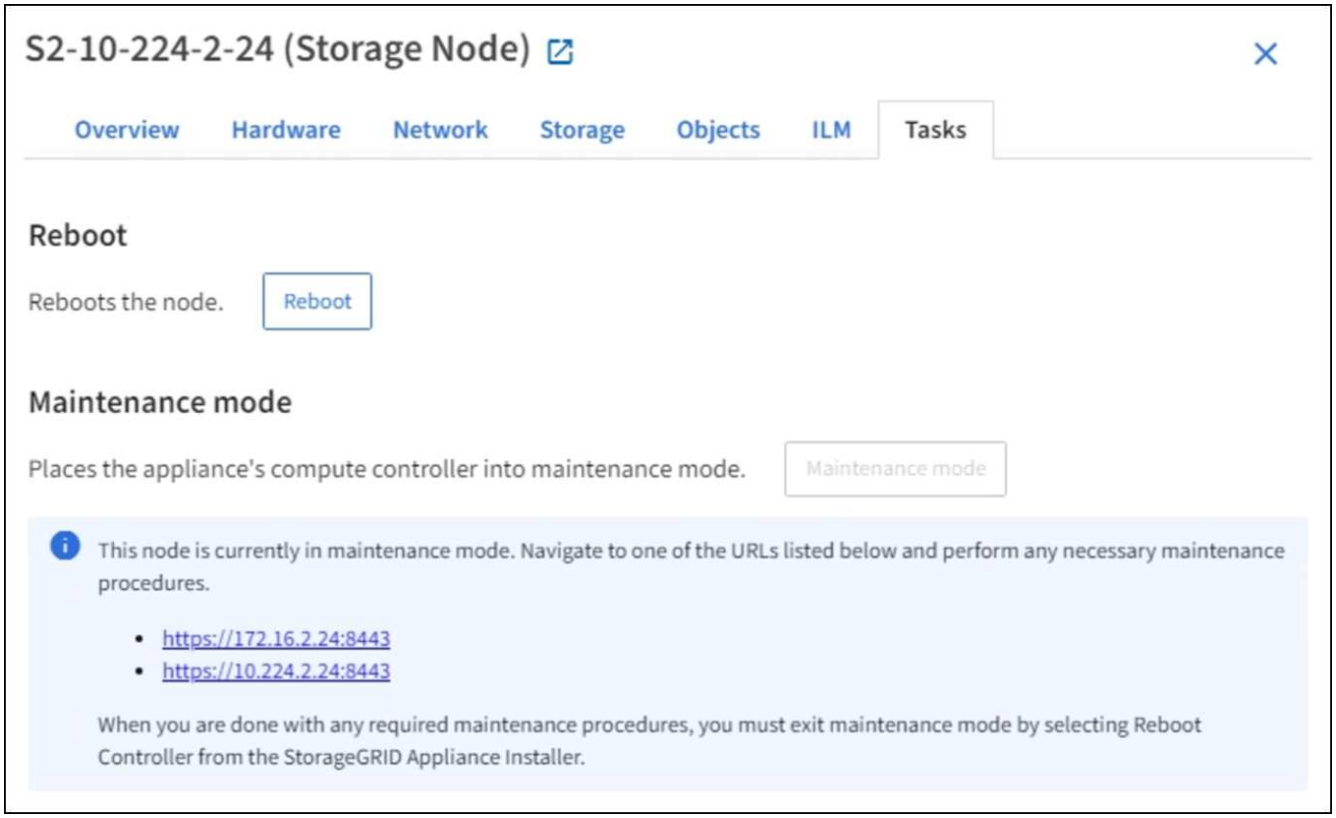



5. Enter the provisioning passphrase, and select **OK**.

   A progress bar and a series of messages, including "Request Sent","Stopping StorageGRID", and "Rebooting", indicate that the appliance is completing the steps for entering maintenance mode.




When the appliance is in maintenance mode, a confirmation message lists the URLs you can use to access the StorageGRID Appliance Installer.



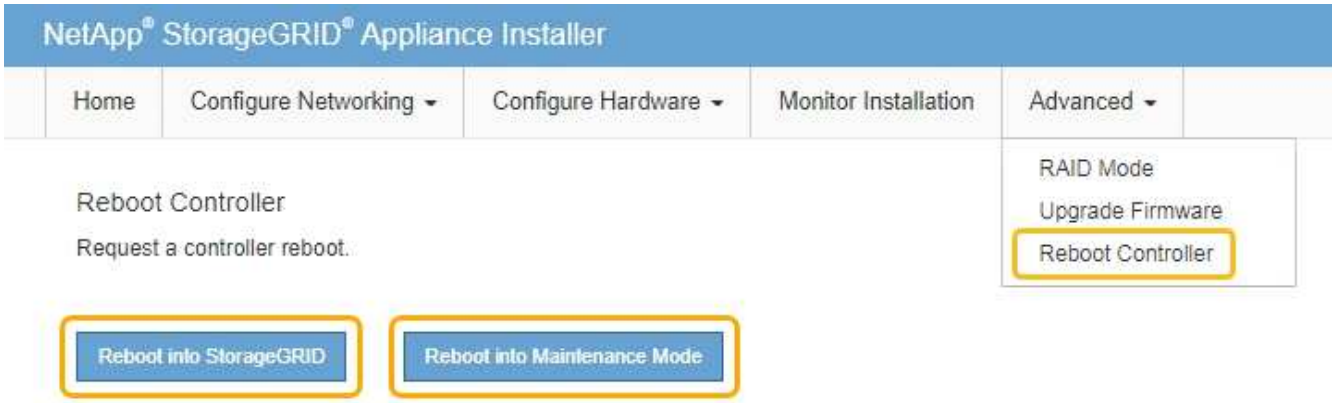

6. To access the StorageGRID Appliance Installer, browse to any of the URLs displayed.

   If possible, use the URL containing the IP address of the appliance's Admin Network port.

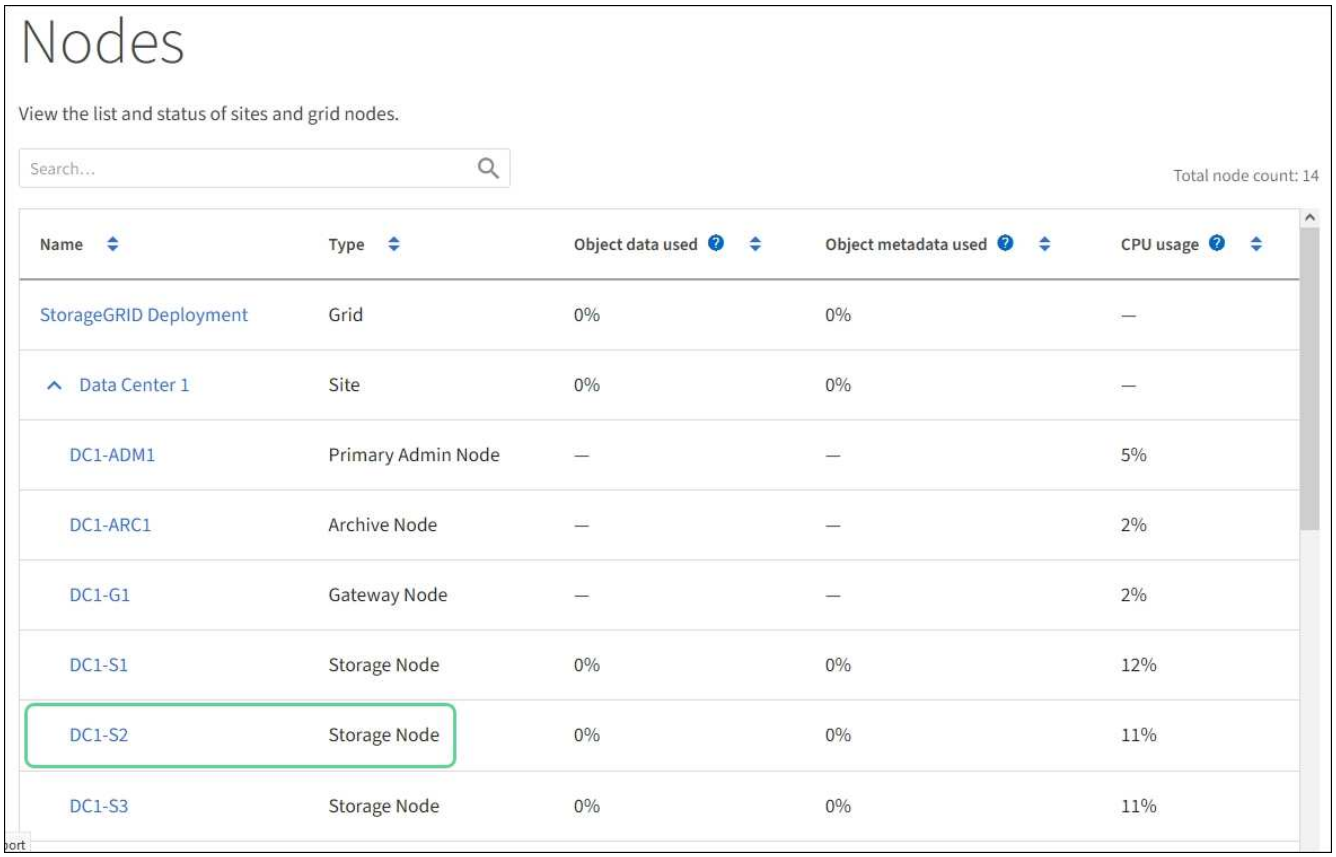
> Accessing `https://169.254.0.1:8443` requires a direct connection to the local management port.

7. From the StorageGRID Appliance Installer, confirm that the appliance is in maintenance mode.

8. Perform any required maintenance tasks.
9. After completing maintenance tasks, exit maintenance mode and resume normal node operation. From the StorageGRID Appliance Installer, select **Advanced** > **Reboot Controller**, and then select **Reboot into StorageGRID**.




It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **Nodes** page should display a normal status (no icons to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.




### Force service to terminate

If you need to stop a service immediately, you can use the `force-stop` command.

#### What you'll need

You must have the `Passwords.txt` file.

#### Steps

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@`*`grid_node_IP`*

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Manually force the service to terminate: `service` *`servicename`* `force-stop`

   For example:

   ```
   service ldr force-stop
   ```

   The system waits 30 seconds before terminating the service.

3. Log out of the command shell: `exit`

#### Start or restart service

You might need to start a service that has been stopped, or you might need to stop and restart a service.

#### What you'll need

You must have the `Passwords.txt` file.

#### Steps

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Decide which command to issue, based on whether the service is currently running or stopped.

   - If the service is currently stopped, use the `start` command to start the service manually: `service servicename start`

     For example:

     ```
     service ldr start
     ```

   - If the service is currently running, use the `restart` command to stop the service and then restart it: `service servicename restart`

     For example:

     ```
     service ldr restart
     ```

     > Using the `restart` command is the same as using the `stop` command followed by the `start` command. You can issue `restart` even if the service is currently stopped.

3. Log out of the command shell: `exit`

#### Remove port remaps

If you want to configure an endpoint for the Load Balancer service, and you want to use a port that has already been configured as the Mapped-To Port of a port remap, you must first remove the existing port remap, or the endpoint will not be effective. You must run a script on each Admin Node and Gateway Node that has conflicting remapped ports to

remove all of the node's port remaps.

> **About this task**
>
> This procedure removes all port remaps. If you need to keep some of the remaps, contact technical support.

For information about configuring load balancer endpoints, see the instructions for administering StorageGRID.

> If the port remap provides client access, the client should be reconfigured to use a different port configured as an load balancer endpoint if possible, to avoid loss of service, Otherwise, removing the port mapping will result in loss of client access and should be scheduled appropriately.

> This procedure does not work for a StorageGRID system deployed as a container on bare metal hosts. See the instructions for removing port remaps on bare metal hosts.

**Steps**

1. Log in to the node.
   a. Enter the following command: `ssh -p 8022 admin@node_IP`

      Port 8022 is the SSH port of the base OS, while port 22 is the SSH port of the container engine running StorageGRID.

   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.

2. Run the following script: `remove-port-remap.sh`
3. Reboot the node.

   Follow the instructions for rebooting a grid node.

4. Repeat these steps on each Admin Node and Gateway Node that has conflicting remapped ports.

**Related information**

Administer StorageGRID

**Remove port remaps on bare metal hosts**

If you want to configure an endpoint for the Load Balancer service, and you want to use a port that has already been configured as the Mapped-To Port of a port remap, you must first remove the existing port remap, or the endpoint will not be effective. If you are running StorageGRID on bare metal hosts, follow this procedure instead of the general procedure for removing port remaps. You must edit the node configuration file for each Admin Node and Gateway Node that has conflicting remapped ports to remove all of the node's port remaps and restart the node.

**About this task**

This procedure removes all port remaps. If you need to keep some of the remaps, contact technical support.

For information about configuring load balancer endpoints, see the instructions for administering StorageGRID.

This procedure can result in temporary loss of service as nodes are restarted.

**Steps**

1. Log in to the host supporting the node. Log in as root or with an account that has sudo permission.
2. Run the following command to temporarily disable the node: `sudo storagegrid node stop node-name`
3. Using a text editor such as vim or pico, edit the node configuration file for the node.

   The node configuration file can be found at `/etc/storagegrid/nodes/node-name.conf`.

4. Locate the section of the node configuration file that contains the port remaps.

   See the last two lines in the following example.

```
ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = Interface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = Interface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = Interface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443
```

5. Edit the PORT_REMAP and PORT_REMAP_INBOUND entries to remove port remaps.

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. Run the following command to validate your changes to the node configuration file for the node: `sudo storagegrid node validate node-name`

   Address any errors or warnings before proceeding to the next step.

7. Run the following command to restart the node without port remaps: `sudo storagegrid node start node-name`
8. Log in to the node as admin using the password listed in the `Passwords.txt` file.
9. Verify that the services start correctly.
   a. View a listing of the statuses of all services on the server:`sudo storagegrid-status`

      The status is updated automatically.

b. Wait until all services have a status of either Running or Verified.

c. Exit the status screen:`Ctrl+C`

10. Repeat these steps on each Admin Node and Gateway Node that has conflicting remapped ports.

## Reboot grid node

You can reboot a grid node from the Grid Manager or from the node's command shell.

### About this task

When you reboot a grid node, the node shuts down and restarts. All services are restarted automatically.

If you plan to reboot Storage Nodes, note the following:

- If an ILM rule specifies an ingest behavior of Dual commit or the rule specifies Balanced and it is not possible to immediately create all required copies, StorageGRID immediately commits any newly ingested objects to two Storage Nodes on the same site and evaluates ILM later. If you want to reboot two or more Storage Nodes on a given site, you might not be able to access these objects for the duration of the reboot.
- To ensure you can access all objects while a Storage Node is rebooting, stop ingesting objects at a site for approximately one hour before rebooting the node.

### Related information

Administer StorageGRID

#### Reboot grid node from Grid Manager

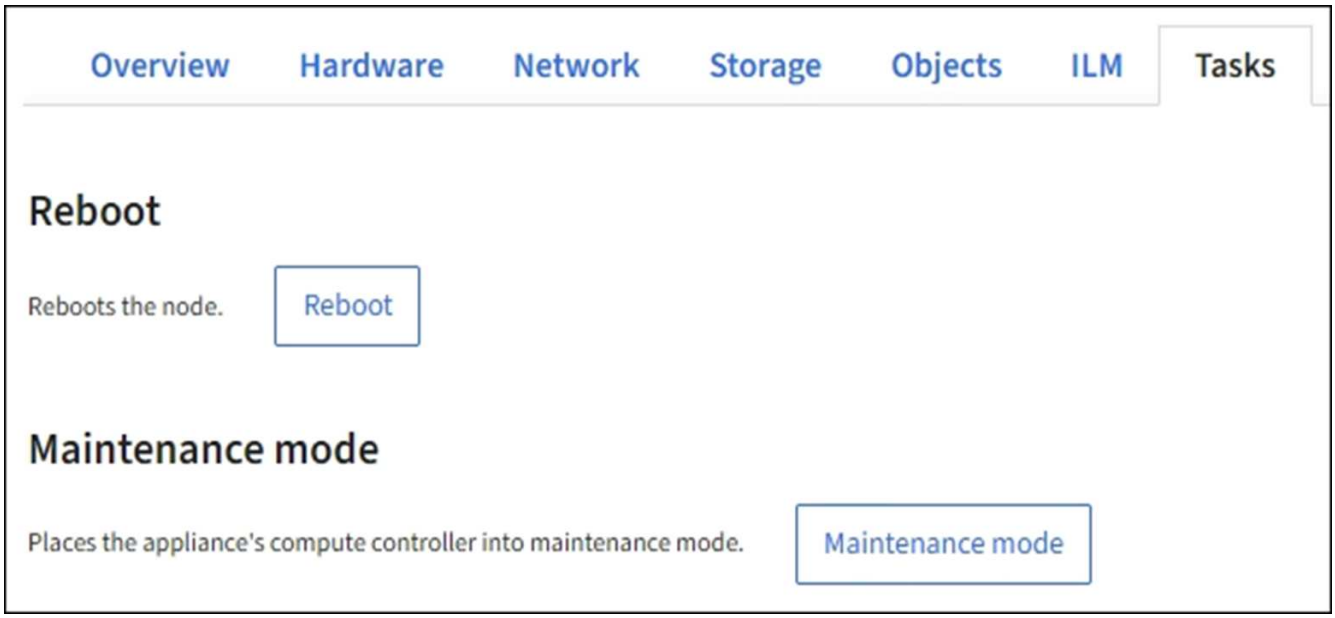
Rebooting a grid node from the Grid Manager issues the `reboot` command on the target node.

### What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have the Maintenance or Root access permission.
- You have the provisioning passphrase.

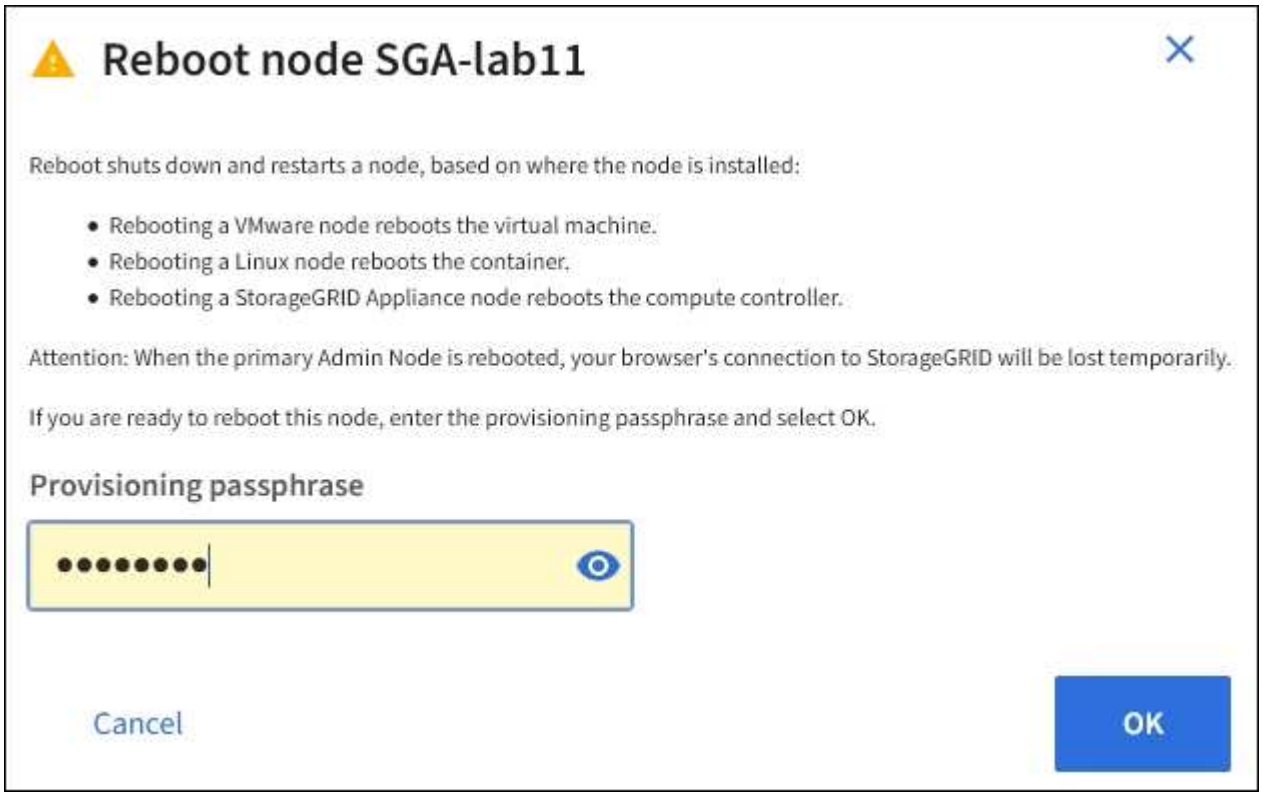
### Steps

1. Select **NODES**.
2. Select the grid node you want to reboot.
3. Select the **Tasks** tab.




4. Select **Reboot**.

   A confirmation dialog box appears.




> If you are rebooting the primary Admin Node, the confirmation dialog box reminds you that your browser's connection to the Grid Manager will be lost temporarily when services are stopped.

5. Enter the provisioning passphrase, and click **OK**.
6. Wait for the node to reboot.

It might take some time for services to shut down.

When the node is rebooting, the gray icon (Administratively Down) appears on the left side of the **Nodes** page. When all services have started again and the node is successfully connected to the grid, the **Nodes** page should display a normal status (no icons to the left of the node name), indicating that no alerts are active and the node is connected to the grid.

#### Reboot grid node from command shell

If you need to monitor the reboot operation more closely or if you are unable to access the Grid Manager, you can log into the grid node and run the Server Manager reboot command from the command shell.

You must have the `Passwords.txt` file.

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@`*`grid_node_IP`*

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Optionally, stop services: `service servermanager stop`

   Stopping services is an optional, but recommended step. Services can take up to 15 minutes to shut down, and you might want to log in to the system remotely to monitor the shutdown process before you reboot the node in the next step.

3. Reboot the grid node: `reboot`

4. Log out of the command shell: `exit`

### Shut down grid node

You can shut down a grid node from the node's command shell.

#### What you'll need

- You must have the `Passwords.txt` file.

#### About this task

Before performing this procedure, review these considerations:

- In general, you should not shut down more than one node at a time to avoid disruptions.
- Do not shut down a node during a maintenance procedure unless explicitly instructed to do so by the documentation or by technical support.
- The shutdown process is based on where the node is installed, as follows:
  - Shutting down a VMware node shuts down the virtual machine.

- Shutting down a Linux node shuts down the container.
- Shutting down a StorageGRID appliance node shuts down the compute controller.

- If you plan to shut down more than one Storage Node at a site, stop ingesting objects at that site for approximately one hour before shutting down the nodes.

  If any ILM rule uses the **Dual commit** ingest option (or if a rule uses the **Balanced** option and all required copies cannot be created immediately), StorageGRID immediately commits any newly ingested objects to two Storage Nodes on the same site and evaluates ILM later. If more than one Storage Node at a site is shut down, you might not be able to access newly ingested objects for the duration of the shutdown. Write operations might also fail if too few Storage Nodes remain available at the site.

**Steps**

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Stop all services: `service servermanager stop`

   Services can take up to 15 minutes to shut down, and you might want to log in to the system remotely to monitor the shutdown process.

3. If the node is running on a VMware virtual machine or it is an appliance node, issue the shutdown command: `shutdown -h now`

   Perform this step regardless of the outcome of the `service servermanager stop` command.

   > After you issue the `shutdown -h now` command on an appliance node, you must power cycle the appliance to restart the node.

   For the appliance, this command shuts down the controller, but the appliance is still powered on. You must complete the next step.

4. If you are powering down an appliance node:
   - For the SG100 or SG1000 services appliance
     i. Turn off the power to the appliance.
     ii. Wait for the blue power LED to turn off.
   - For the SG6000 appliance
     i. Wait for the green Cache Active LED on the back of the storage controllers to turn off.

        This LED is on when cached data needs to be written to the drives. You must wait for this LED to turn off before you turn off power.

     ii. Turn off the power to the appliance, and wait for the blue power LED to turn off.

- For the SG5700 appliance
  i. Wait for the green Cache Active LED on the back of the storage controller to turn off.

     This LED is on when cached data needs to be written to the drives. You must wait for this LED to turn off before you turn off power.

  ii. Turn off the power to the appliance, and wait for all LED and seven-segment display activity to stop.

**Related information**

Administer StorageGRID

### Power down host

Before you power down a host, you must stop services on all grid nodes on that host.

**Steps**

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Stop all services running on the node: `service servermanager stop`

   Services can take up to 15 minutes to shut down, and you might want to log in to the system remotely to monitor the shutdown process.

3. Repeat steps 1 and 2 for each node on the host.
4. If you have a Linux host:

   a. Log in to the host operating system.

   b. Stop the node: `storagegrid node stop`

   c. Shut down the host operating system.

5. If the node is running on a VMware virtual machine or it is an appliance node, issue the shutdown command: `shutdown -h now`

   Perform this step regardless of the outcome of the `service servermanager stop` command.

   > After you issue the `shutdown -h now` command on an appliance node, you must power cycle the appliance to restart the node.

   For the appliance, this command shuts down the controller, but the appliance is still powered on. You must complete the next step.

6. If you are powering down an appliance node:
   - For the SG100 or SG1000 services appliance

    i. Turn off the power to the appliance.
    ii. Wait for the blue power LED to turn off.
  - For the SG6000 appliance
    i. Wait for the green Cache Active LED on the back of the storage controllers to turn off.

       This LED is on when cached data needs to be written to the drives. You must wait for this LED to turn off before you turn off power.

    ii. Turn off the power to the appliance, and wait for the blue power LED to turn off.
  - For the SG5700 appliance
    i. Wait for the green Cache Active LED on the back of the storage controller to turn off.

       This LED is on when cached data needs to be written to the drives. You must wait for this LED to turn off before you turn off power.

    ii. Turn off the power to the appliance, and wait for all LED and seven-segment display activity to stop.
7. Log out of the command shell: `exit`

**Related information**

SG100 and SG1000 services appliances

SG6000 storage appliances

SG5700 storage appliances

### Power off and on all nodes in grid

You might need to shut down your entire StorageGRID system, for example, if you are moving a data center. These steps provide a high-level overview of the recommended sequence for performing a controlled shutdown and startup.

When you power off all nodes in a site or grid, you will not be able to access ingested objects while the Storage Nodes are offline.

#### Stop services and shut down grid nodes

Before you can power off a StorageGRID system, you must stop all services running on each grid node, and then shut down all VMware virtual machines, container engines, and StorageGRID appliances.

**About this task**

Stop services on Admin Nodes and API Gateway Nodes first, and then stop services on Storage Nodes.

This approach allows you to use the primary Admin Node to monitor the status of the other grid nodes for as long as possible.

> If a single host includes more than one grid node, do not shut down the host until you have stopped all of the nodes on that host. If the host includes the primary Admin Node, shut down that host last.

> If required, you can migrate nodes from one Linux host to another to perform host maintenance without impacting the functionality or availability of your grid.

**Steps**

1. Stop all client applications from accessing the grid.
2. Log in to each Gateway Node:
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.
3. Stop all services running on the node: `service servermanager stop`

   Services can take up to 15 minutes to shut down, and you might want to log in to the system remotely to monitor the shutdown process.
4. Repeat the previous two steps to stop the services on all Storage Nodes, Archive Nodes, and non-primary Admin Nodes.

   You can stop the services on these nodes in any order.

   > If you issue the `service servermanager stop` command to stop the services on an appliance Storage Node, you must power cycle the appliance to restart the node.
5. For the primary Admin Node, repeat the steps for logging into the node and stopping all services on the node.
6. For nodes that are running on Linux hosts:
   a. Log in to the host operating system.
   b. Stop the node: `storagegrid node stop`
   c. Shut down the host operating system.
7. For nodes that are running on VMware virtual machines and for appliance Storage Nodes, issue the shutdown command: `shutdown -h now`

   Perform this step regardless of the outcome of the `service servermanager stop` command.

   For the appliance, this command shuts down the compute controller, but the appliance is still powered on. You must complete the next step.
8. If you have appliance nodes:
   - For the SG100 or SG1000 services appliance
     i. Turn off the power to the appliance.
     ii. Wait for the blue power LED to turn off.
   - For the SG6000 appliance

i. Wait for the green Cache Active LED on the back of the storage controllers to turn off.

   This LED is on when cached data needs to be written to the drives. You must wait for this LED to turn off before you turn off power.

ii. Turn off the power to the appliance, and wait for the blue power LED to turn off.

- For the SG5700 appliance

  i. Wait for the green Cache Active LED on the back of the storage controller to turn off.

     This LED is on when cached data needs to be written to the drives. You must wait for this LED to turn off before you turn off power.

  ii. Turn off the power to the appliance, and wait for all LED and seven-segment display activity to stop.

9. If required, log out of the command shell: `exit`

   The StorageGRID grid has now been shut down.

**Related information**

SG100 and SG1000 services appliances

SG6000 storage appliances

SG5700 storage appliances

#### Start up grid nodes

## Follow this sequence to start up the grid nodes after a complete shutdown.

**What you'll need**

If the entire grid has been shut down for more than 15 days, you must contact technical support before starting up any grid nodes. Do not attempt the recovery procedures that rebuild Cassandra data. Doing so might result in data loss.

**About this task**

If possible, you should power on the grid nodes in this order:

- Apply power to Admin Nodes first.
- Apply power to Gateway Nodes last.

If a host includes multiple grid nodes, the nodes will come back online automatically when you power on the host.

**Steps**

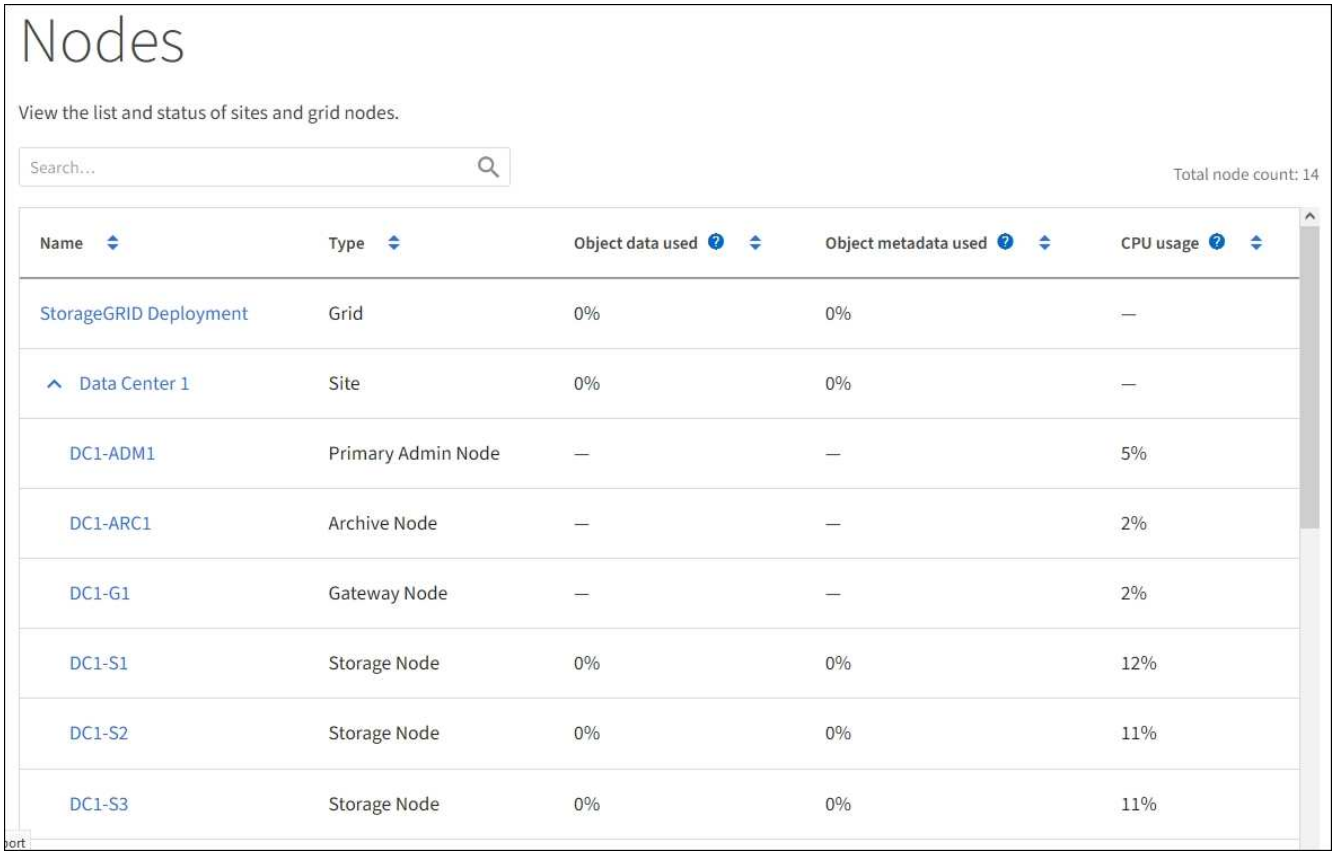
1. Power on the hosts for the primary Admin Node and any non-primary Admin Nodes.

   You will not be able to log in to the Admin Nodes until the Storage Nodes have been restarted.

2. Power on the hosts for all Archive Nodes and Storage Nodes.

You can power on these nodes in any order.

3. Power on the hosts for all Gateway Nodes.
4. Sign in to the Grid Manager.
5. Select **NODES** and monitor the status of the grid nodes. Verify that there are no alert icons next to the node names.




### Use a DoNotStart file

If you are performing various maintenance or configuration procedures under the direction of technical support, you might be asked to use a DoNotStart file to prevent services from starting when Server Manager is started or restarted.

> You should add or remove a DoNotStart file only if technical support has directed you to do so.

To prevent a service from starting, place a DoNotStart file in the directory of the service you want to prevent from starting. At start-up, Server Manager looks for the DoNotStart file. If the file is present, the service (and any services dependent on it) is prevented from starting. When the DoNotStart file is removed, the previously stopped service will start on the next start or restart of Server Manager. Services are not automatically started when the DoNotStart file is removed.

The most efficient way to prevent all services from restarting is to prevent the NTP service from starting. All services are dependent on the NTP service and cannot run if the NTP service is not running.

#### Add DoNotStart file for service

## You can prevent an individual service from starting by adding a DoNotStart file to that service's directory on a grid node.

### What you'll need

You must have the `Passwords.txt` file.

### Steps

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Add a DoNotStart file: `touch /etc/sv/service/DoNotStart`

   where `service` is the name of the service to be prevented from starting. For example,

   ```
   touch /etc/sv/ldr/DoNotStart
   ```

   A DoNotStart file is created. No file content is needed.

   When Server Manager or the grid node is restarted, Server Manager restarts, but the service does not.

3. Log out of the command shell: `exit`

#### Remove DoNotStart file for service

## When you remove a DoNotStart file that is preventing a service from starting, you must start that service.

### What you'll need

You must have the `Passwords.txt` file.

### Steps

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@grid_node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Remove the DoNotStart file from the service directory: `rm /etc/sv/service/DoNotStart`

   where `service` is the name of the service. For example,

   ```
   rm /etc/sv/ldr/DoNotStart
   ```

3. Start the service: `service servicename start`
4. Log out of the command shell: `exit`

## Troubleshoot Server Manager

### Access Server Manager log file

If a problem arises when using Server Manager, check its log file.

Error messages related to Server Manager are captured in the Server Manager log file, which is located at: `/var/local/log/servermanager.log`

Check this file for error messages regarding failures. Escalate the issue to technical support if required. You might be asked to forward log files to technical support.

### Service with an error state

If you detect that a service has entered an error state, attempt to restart the service.

#### What you'll need

You must have the `Passwords.txt` file.

#### About this task

Server Manager monitors services and restarts any that have stopped unexpectedly. If a service fails, Server Manager attempts to restart it. If there are three failed attempts to start a service within five minutes, the service enters an error state. Server Manager does not attempt another restart.

#### Steps

1. Log in to the grid node:

   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Confirm the error state of the service: `service servicename status`

   For example:

```
service ldr status
```

If the service is in an error state, the following message is returned: *servicename* `in error state`. For example:

```
ldr in error state
```

> If the service status is `disabled`, see the instructions for removing a DoNotStart file for a service.

3. Attempt to remove the error state by restarting the service: `service` *servicename* `restart`

   If the service fails to restart, contact technical support.

4. Log out of the command shell: `exit`

## Appliance node cloning

You can clone an appliance node in StorageGRID to use an appliance of newer design or increased capabilities. Cloning transfers all information on the existing node to the new appliance, provides a hardware-upgrade process that is easy to perform, and provides an alternative to decommissioning and expansion for replacing appliances.

### How appliance node cloning works

Appliance node cloning lets you easily replace an existing appliance node (source) in your grid with a compatible appliance (target) that is part of the same logical StorageGRID site. The process transfers all data to the new appliance, placing it in service to replace the old appliance node and leaving the old appliance in a pre-install state.

#### Why clone an appliance node?

You can clone an appliance node if you need to:

- Replace appliances that are reaching end-of-life.
- Upgrade existing nodes to take advantage of improved appliance technology.
- Increase grid storage capacity without changing the number of Storage Nodes in your StorageGRID system.
- Improve storage efficiency, such as by changing the RAID mode from DDP-8 to DDP-16, or to RAID-6.
- Efficiently implement node encryption to allow the use of external key management servers (KMS).

#### Which StorageGRID network is used?

Cloning transfers data from the source node directly to the target appliance over any of the three StorageGRID networks. The Grid Network is typically used, but you can also use the Admin Network or the Client Network if

the source appliance is connected to these networks. Choose the network to use for cloning traffic that provides the best data-transfer performance without degrading StorageGRID network performance or data availability.

When you install the replacement appliance, you must specify temporary IP addresses for StorageGRID connection and data transfer. Since the replacement appliance will be part of the same networks as the appliance node it replaces, you must specify temporary IP addresses for each of these networks on the replacement appliance.

#### Target appliance compatibility

Replacement appliances must be the same type as the source node they are replacing and both must be part of the same logical StorageGRID site.

- A replacement services appliance can be different than the Admin Node or Gateway Node it is replacing.
  - You can clone an SG100 source node appliance to an SG1000 services target appliance to give the Admin Node or Gateway Node greater capability.
  - You can clone an SG1000 source node appliance to an SG100 services target appliance to redeploy the SG1000 for a more demanding application.

    For example, if an SG1000 source node appliance is being used as an Admin Node and you want to use it as a dedicated load-balancing node.

  - Replacing an SG1000 source node appliance with an SG100 services target appliance reduces the maximum speed of the network ports from 100-GbE to 25-GbE.
  - The SG100 and SG1000 appliances have different network connectors. Changing the appliance type might require replacing the cables or SFP modules.
- A replacement storage appliance must have equal or greater capacity than the Storage Node it is replacing.
  - If the target storage appliance has the same number of drives as the source node, the drives in the target appliance must have greater capacity (in TB).
  - If you plan to use the same RAID mode on the target node as was used on the source node, or a less storage efficient RAID mode (for example, switching from RAID6 to DDP), the drives in the target appliance must be larger (in TB) than the drives in the source appliance.
  - If the number of standard drives installed in a target storage appliance is less than the number of drives in the source node, due to installation of solid-state drives (SSDs), the overall storage capacity of the standard drives in the target appliance (in TB) must meet or exceed the total functional drive capacity of all drives in the source Storage Node.

    For example, when cloning an SG5660 source Storage Node appliance with 60 drives to an SG6060 or SG6060X target appliance with 58 standard drives, larger drives should be installed in the SG6060 or SG6060X target appliance before cloning to maintain storage capacity. (The two drive slots containing SSDs in the target appliance are not included in the total appliance-storage capacity.)

    However, if a 60-drive SG5660 source node appliance is configured with SANtricity Dynamic Disk Pools DDP-8, configuring a 58-drive same-size-drive SG6060 or SG6060X target appliance with DDP-16 might make the SG6060 or SG6060X appliance a valid clone target due to its improved storage efficiency.

    You can view information about the current RAID mode of the source appliance node on the **NODES** page in Grid Manager. Select the **Storage** tab for the appliance.

#### What information is not cloned?

The following appliance configurations do not transfer to the replacement appliance during cloning. You must configure them during initial set up of the replacement appliance.

- BMC interface
- Network links
- Node encryption status
- SANtricity System Manager (for Storage Nodes)
- RAID mode (for Storage Nodes)

#### What issues prevent cloning?

If any of the following issues are encountered while cloning, the cloning process halts and an error message is generated:

- Wrong network configuration
- Lack of connectivity between the source and target appliances
- Source and target appliance incompatibility
- For Storage Nodes, a replacement appliance of insufficient capacity

You must resolve each issue for cloning to continue.

### Considerations and requirements for appliance node cloning

## Before cloning an appliance node, you must understand the considerations and requirements.

#### Hardware requirements for the replacement appliance

Ensure that the replacement appliance meets the following criteria:

- The source node (appliance being replaced) and the target (new) appliance must be the same type of appliance:
  - You can only clone an Admin Node appliance or a Gateway Node appliance to a new services appliance.
  - You can only clone a Storage Node appliance to a new storage appliance.
- For Admin Node or Gateway Node appliances, the source node appliance and the target appliance do not need to be the same type of appliance; however, changing the appliance type might require replacing the cables or SFP modules.

  For example, you can replace a SG1000 node appliance with a SG100 or replace a SG100 appliance with a SG1000 appliance.

- For Storage Node appliances, the source node appliance and the target appliance do not need to be the same type of appliance; however, the target appliance must have greater storage capacity than the source appliance.

  For example, you can replace a SG5600 node appliance with a SG5700 or a SG6000 appliance.

Contact your StorageGRID sales representative for help choosing compatible replacement appliances to clone specific appliance nodes in your StorageGRID installation.

#### Prepare to clone an appliance node

You must have the following information before you clone an appliance node:

- Obtain a temporary IP address for the Grid Network from your network administrator for use with the target appliance during initial installation. If the source node belongs to an Admin Network or Client Network, obtain temporary IP addresses for these networks.

  Temporary IP addresses are normally on the same subnet as the source node appliance being cloned and are not needed after cloning completes. The source and target appliances must both connect to the primary Admin Node of your StorageGRID to establish a cloning connection.

- Determine which network to use for cloning data-transfer traffic that provides the best data-transfer performance without degrading StorageGRID network performance or data availability.

  Using the 1-GbE Admin Network for clone data transfer results in slower cloning.

- Determine if node encryption using a key management server (KMS) will be used on the target appliance, so that you can enable node encryption during initial target appliance installation before cloning. You can check if node encryption is enabled on the source appliance node as described in appliance installation.

  The source node and target appliance can have different node-encryption settings. Data decryption and encryption is performed automatically during data transfer and when the target node restarts and joins the grid.

  - SG100 and SG1000 services appliances
  - SG5600 storage appliances
  - SG5700 storage appliances
  - SG6000 storage appliances

- Determine if the RAID mode on the target appliance should be changed from its default setting, so you can specify this information during initial target appliance installation before cloning. You can view information about the current RAID mode of the source appliance node on the **NODES** page in Grid Manager. Select the **Storage** tab for the appliance.

  The source node and target appliance can have different RAID settings.

- Plan for sufficient time to complete the node cloning process. Several days might be required to transfer data from an operational Storage Node to a target appliance. Schedule cloning at a time that minimizes the impact to your business.
- You should only clone one appliance node at a time. Cloning can prevent you from performing other StorageGRID maintenance functions at the same time.
- After you have cloned an appliance node, you can use the source appliance that was returned to a pre-install state as the target to clone another compatible node appliance.

#### Clone appliance node

The cloning process might take several days to transfer data between the source node (appliance being replaced) and the target (new) appliance.

**What you'll need**

- You have installed the compatible target appliance into a cabinet or rack, connected all cables, and applied power.
- You have verified that the StorageGRID Appliance Installer version on the replacement appliance matches the software version of your StorageGRID system, upgrading the StorageGRID Appliance Installer firmware, if necessary.
- You have configured the target appliance, including configuring StorageGRID connections, SANtricity System Manager (storage appliances only), and the BMC interface.
  - When configuring StorageGRID connections, use the temporary IP addresses.
  - When configuring network links, use the final link configuration.

> Leave the StorageGRID Appliance Installer open after you complete initial target appliance configuration. You will return to the target appliance's installer page after you start the node cloning process.

- You have optionally enabled node encryption for the target appliance.
- You have optionally set the RAID mode for the target appliance (storage appliances only).
- Considerations and requirements for appliance node cloning

  SG100 and SG1000 services appliances

  SG5600 storage appliances

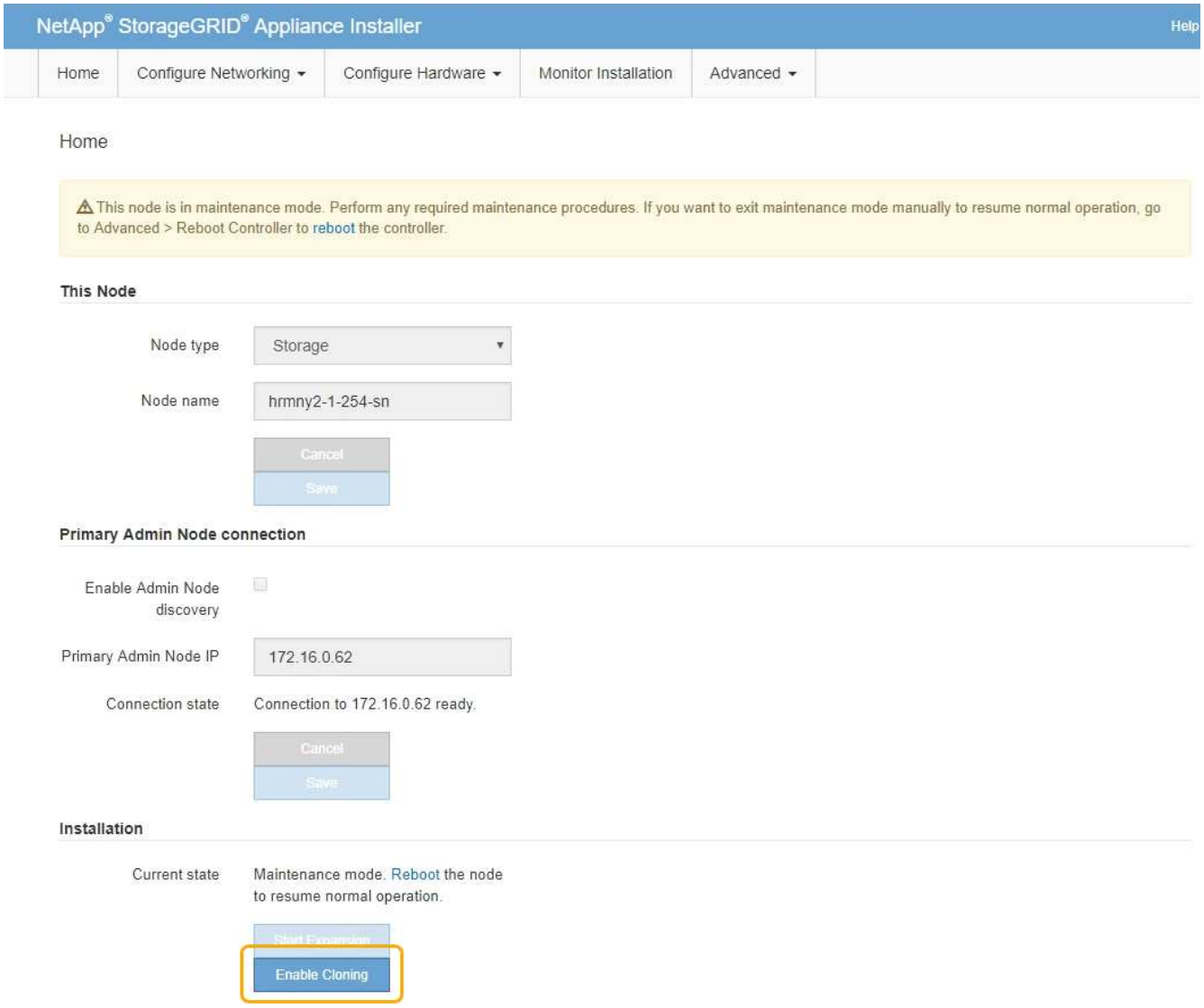
  SG5700 storage appliances

  SG6000 storage appliances

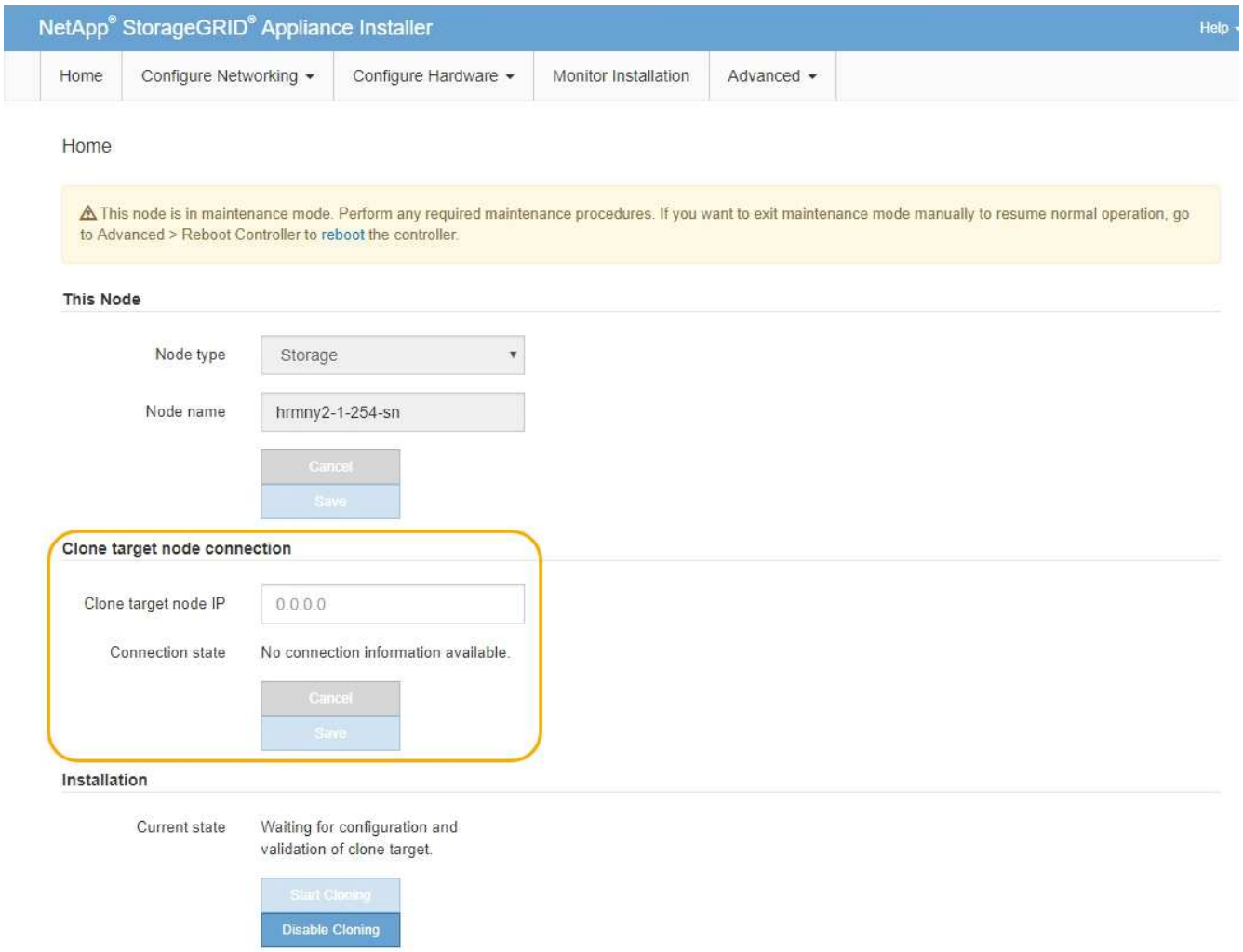
You should clone only one appliance node at a time to maintain StorageGRID network performance and data availability.

**Steps**

1. Place the source node you are cloning into maintenance mode.
2. From the StorageGRID Appliance Installer on the source node, in the Installation section of the Home page, select **Enable Cloning**.




The Primary Admin Node connection section is replaced with the Clone target node connection section.

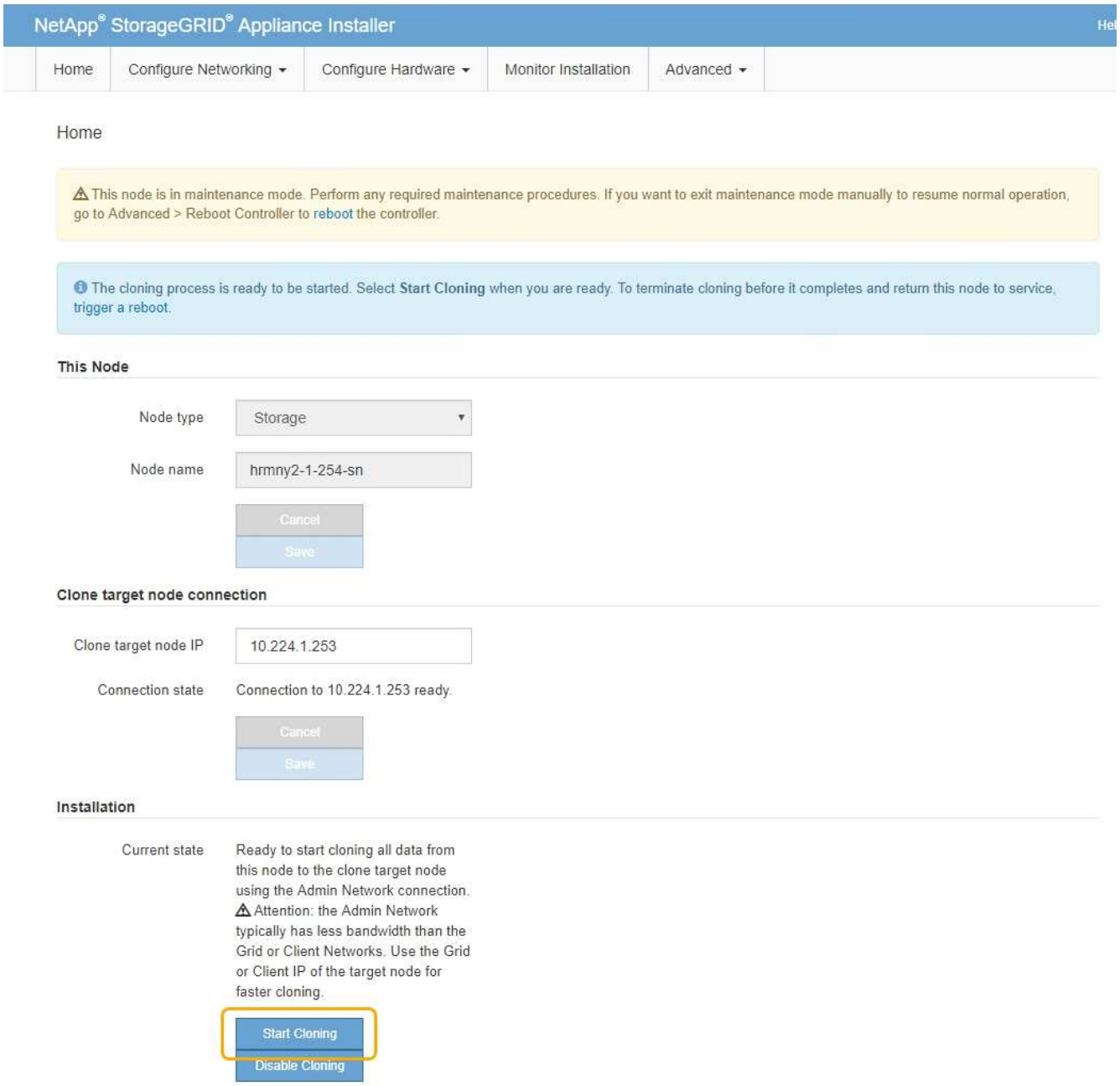



3. For **Clone target node IP**, enter the temporary IP address assigned to the target node for the network to use for clone data-transfer traffic, and then select **Save**.

   Typically, you enter the IP address for the Grid Network, but if you need to use a different network for clone data-transfer traffic, enter the IP address of the target node on that network.

   > Using the 1-GbE Admin Network for clone data transfer results in slower cloning.

   After the target appliance is configured and validated, in the Installation section, **Start Cloning** is enabled on the source node.



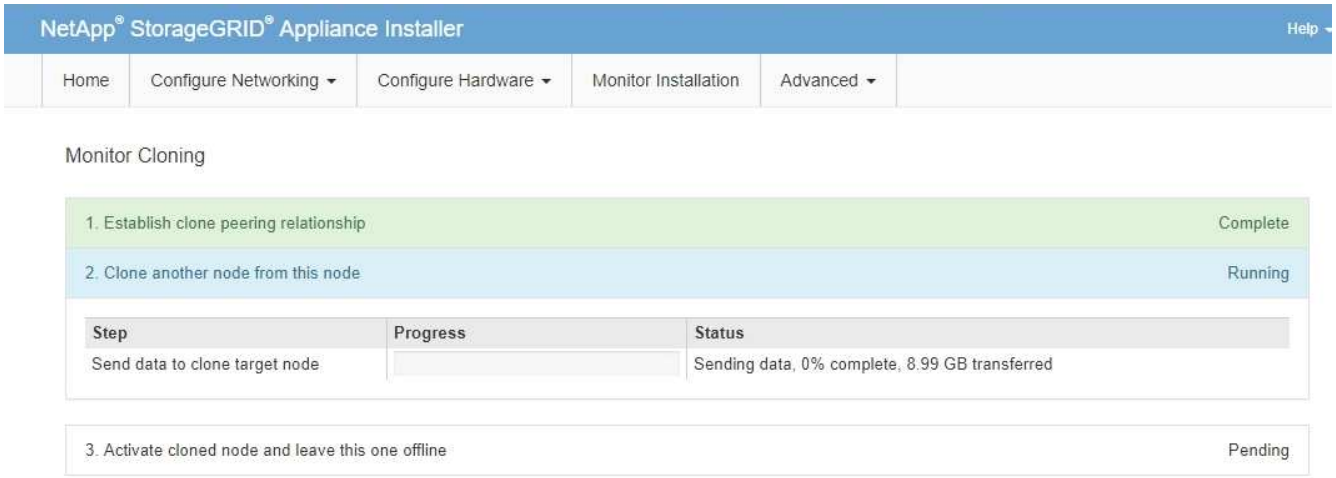

If issues exist that prevent cloning, **Start Cloning** is not enabled and issues that you must resolve are listed as the **Connection state**. These issues are listed on the StorageGRID Appliance Installer Home page of both the source node and the target appliance. Only one issue displays at a time and the state automatically updates as conditions change. Resolve all cloning issues to enable **Start Cloning**.

When **Start Cloning** is enabled, the **Current state** indicates the StorageGRID network that was selected for cloning traffic, along with information about using that network connection.

Considerations and requirements for appliance node cloning

4. Select **Start Cloning** on the source node.
5. Monitor the cloning progress using the StorageGRID Appliance Installer on either the source or target node.

   The StorageGRID Appliance Installer on both the source and target nodes indicates the same status.




The Monitor Cloning page provides detailed progress for each stage of the cloning process:

- **Establish clone peering relationship** shows the progress of cloning set up and configuration.
- **Clone another node from this node** shows the progress of data transfer. (This part of the cloning process can take several days to complete.)
- **Activate cloned node and leave this one offline** shows the progress of transferring control to the target node and placing the source node in a pre-install state, after data transfer is complete.

6. If you need to terminate the cloning process and return the source node to service before cloning is complete, on the source node go to the StorageGRID Appliance Installer Home page and select **Advanced** > **Reboot Controller**, and then select **Reboot into StorageGRID**.

   If the cloning process is terminated:

   - The source node exits maintenance mode and rejoins StorageGRID.
   - The target node remains in the pre-install state. To restart cloning the source node, start the cloning process again from step 1.

When cloning successfully completes:

- The source and target nodes swap IP addresses:
  - The target node now uses the IP addresses originally assigned to the source node for the Grid, Admin, and Client Networks.
  - The source node now uses the temporary IP address initially assigned to the target node.
- The target node exits maintenance mode and joins StorageGRID, replacing the source node.
- The source appliance is in a pre-installed state, as if you had prepared it for reinstallation.

> If the appliance does not rejoin the grid, go to the StorageGRID Appliance Installer Home page for the source node, select **Advanced** > **Reboot Controller**, and then select **Reboot into Maintenance Mode**. After the source node reboots in maintenance mode, repeat the node cloning procedure.

User data remains on the source appliance as a recovery option if an unexpected issue occurs with the target node. After the target node has successfully rejoined StorageGRID, user data on the source appliance is outdated and is no longer needed. If desired, ask StorageGRID Support to clear the source appliance to destroy this data.

You can:

- Use the source appliance as a target for additional cloning operations: no additional configuration is required. This appliance already has the temporary IP address assigned that were originally specified for the first clone target.
- Install and set up the source appliance as a new appliance node.
- Discard the source appliance if it is no longer of use with StorageGRID.

# Review audit logs

## Review audit logs: Overview

These instructions contain information about the structure and content of StorageGRID audit messages and audit logs. You can use this information to read and analyze the audit trail of system activity.

These instructions are for administrators responsible for producing reports of system activity and usage that require analysis of the StorageGRID system's audit messages.

To use the text log file, you must have access to the configured audit share on the Admin Node.

For information on configuring audit message levels and using an external syslog server, see Configure audit messages and log destinations.

#### Related information

- Administer StorageGRID

### Audit message flow and retention

All StorageGRID services generate audit messages during normal system operation. You should understand how these audit messages move through the StorageGRID system to the `audit.log` file.

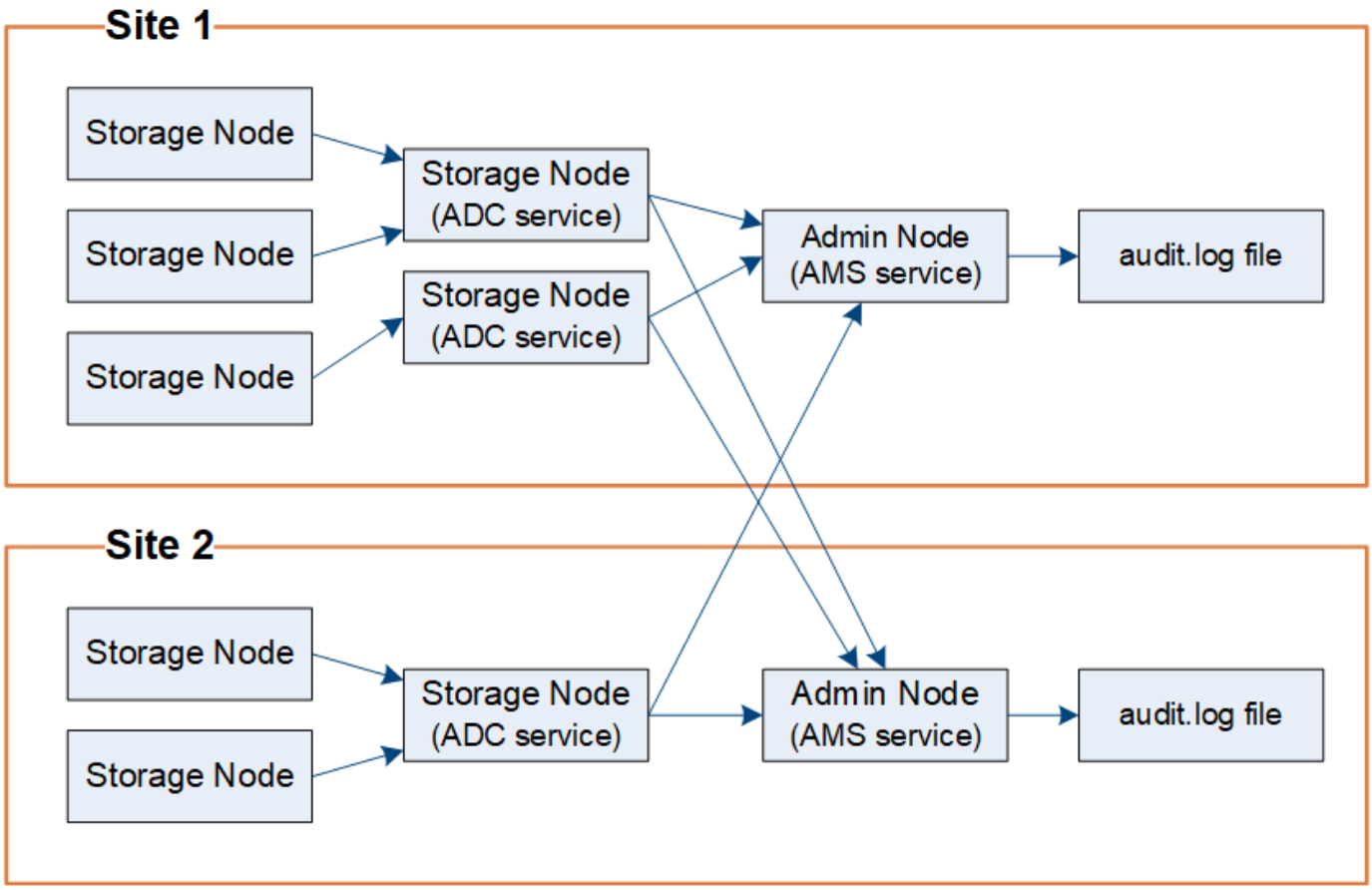
#### Audit message flow

Audit messages are processed by Admin Nodes and by those Storage Nodes that have an Administrative Domain Controller (ADC) service.

As shown in the audit message flow diagram, each StorageGRID node sends its audit messages to one of the ADC services at the data center site. The ADC service is automatically enabled for the first three Storage Nodes installed at each site.

In turn, each ADC service acts as a relay and sends its collection of audit messages to every Admin Node in the StorageGRID system, which gives each Admin Node a complete record of system activity.

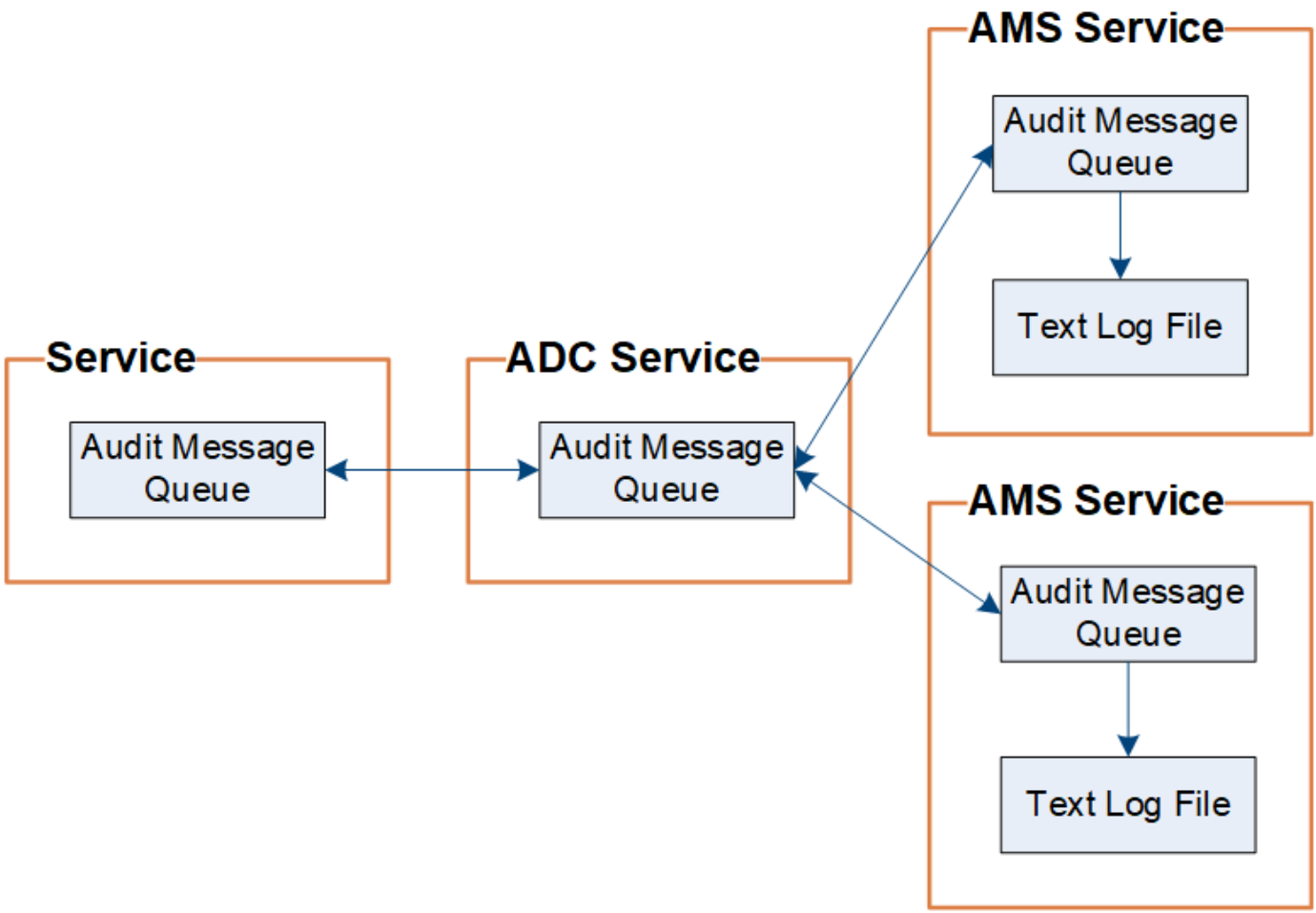
Each Admin Node stores audit messages in text log files; the active log file is named `audit.log`.




**Audit message retention**

StorageGRID uses a copy-and-delete process to ensure that no audit messages are lost before they can be written to the audit log.

When a node generates or relays an audit message, the message is stored in an audit message queue on the system disk of the grid node. A copy of the message is always held in an audit message queue until the message is written to the audit log file in the Admin Node's `/var/local/audit/export` directory. This helps prevent loss of an audit message during transport.




The audit message queue can temporarily increase due to network connectivity issues or insufficient audit capacity. As the queues increase, they consume more of the available space in each node's `/var/local/` directory. If the issue persists and a node's audit message directory becomes too full, the individual nodes will prioritize processing their backlog and become temporarily unavailable for new messages.

Specifically, you might see the following behaviors:

- If the `/var/local/audit/export` directory used by an Admin Node becomes full, the Admin Node will be flagged as unavailable to new audit messages until the directory is no longer full. S3 and Swift client requests are not affected. The XAMS (Unreachable Audit Repositories) alarm is triggered when an audit repository is unreachable.
- If the `/var/local/` directory used by a Storage Node with the ADC service becomes 92% full, the node will be flagged as unavailable to audit messages until the directory is only 87% full. S3 and Swift client requests to other nodes are not affected. The NRLY (Available Audit Relays) alarm is triggered when audit relays are unreachable.

  > If there are no available Storage Nodes with the ADC service, the Storage Nodes store the audit messages locally in the `/var/local/log/localaudit.log` file.

- If the `/var/local/` directory used by a Storage Node becomes 85% full, the node will start refusing S3 and Swift client requests with `503 Service Unavailable`.

The following types of issues can cause audit message queues to grow very large:

- The outage of an Admin Node or a Storage Node with the ADC service. If one of the system's nodes is down, the remaining nodes might become backlogged.
- A sustained activity rate that exceeds the audit capacity of the system.
- The `/var/local/` space on an ADC Storage Node becoming full for reasons unrelated to audit messages. When this happens, the node stops accepting new audit messages and prioritizes its current backlog, which can cause backlogs on other nodes.

#### Large audit queue alert and Audit Messages Queued (AMQS) alarm

To help you monitor the size of audit message queues over time, the **Large audit queue** alert and the legacy AMQS alarm are triggered when the number of messages in a Storage Node queue or Admin Node queue reaches certain thresholds.

If the **Large audit queue** alert or the legacy AMQS alarm is triggered, start by checking the load on the system—if there have been a significant number of recent transactions, the alert and the alarm should resolve over time and can be ignored.

If the alert or alarm persists and increases in severity, view a chart of the queue size. If the number is steadily increasing over hours or days, the audit load has likely exceeded the audit capacity of the system. Reduce the client operation rate or decrease the number of audit messages logged by changing the audit level for Client Writes and Client Reads to Error or Off. See "Configure audit messages and log destinations."

#### Duplicate messages

The StorageGRID system takes a conservative approach if a network or node failure occurs. For this reason, duplicate messages might exist in the audit log.

#### Access audit log file

The audit share contains the active `audit.log` file and any compressed audit log files. For easy access to audit logs, you can configure client access to audit shares for both NFS and CIFS (CIFS is deprecated). You can also access audit log files directly from the command line of the Admin Node.

##### What you'll need

- You must have specific access permissions.
- You must have the `Passwords.txt` file.
- You must know the IP address of an Admin Node.

##### Steps

1. Log in to an Admin Node:
   a. Enter the following command: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Enter the password listed in the `Passwords.txt` file.
2. Go to the directory containing the audit log files:

   ```
   cd /var/local/audit/export
   ```

3. View the current or a saved audit log file, as required.

**Related information**

Administer StorageGRID

### Audit log file rotation

Audit logs files are saved to an Admin Node's `/var/local/audit/export` directory. The active audit log files are named `audit.log`.

> Optionally, you can change the destination of audit logs and send audit information to an external syslog server. Local logs of audit records continue to be generated and stored when an external syslog server is configured. See Configure audit messages and log destinations.

Once a day, the active `audit.log` file is saved, and a new `audit.log` file is started. The name of the saved file indicates when it was saved, in the format *`yyyy-mm-dd.txt`*. If more than one audit log is created in a single day, the file names use the date the file was saved, appended by a number, in the format *`yyyy-mm-dd.txt.n`*. For example, `2018-04-15.txt` and `2018-04-15.txt.1` are the first and second log files created and saved on 15 April 2018.

After a day, the saved file is compressed and renamed, in the format *`yyyy-mm-dd.txt.gz`*, which preserves the original date. Over time, this results in the consumption of storage allocated for audit logs on the Admin Node. A script monitors the audit log space consumption and deletes log files as necessary to free space in the `/var/local/audit/export` directory. Audit logs are deleted based on the date they were created, with the oldest being deleted first. You can monitor the script's actions in the following file: `/var/local/log/manage-audit.log`.

This example shows the active `audit.log` file, the previous day's file (`2018-04-15.txt`), and the compressed file for the prior day (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

## Audit log file and message formats

You can use audit logs to gather information about your system and troubleshoot issues. You should understand the format of the audit log file and the general format used for audit messages.

### Audit log file format

The audit log files are found on every Admin Node and contain a collection of individual audit messages.

Each audit message contains the following:

- The Coordinated Universal Time (UTC) of the event that triggered the audit message (ATIM) in ISO 8601 format, followed by a space:

  *`YYYY-MM-DDTHH:MM:SS.UUUUUU`*, where *`UUUUUU`* are microseconds.

- The audit message itself, enclosed within square brackets and beginning with `AUDT`.

The following example shows three audit messages in an audit log file (line breaks added for readability). These messages were generated when a tenant created an S3 bucket and added two objects to that bucket.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

In their default format, the audit messages in the audit log files are not easy to read or interpret. You can use the `audit-explain` tool to obtain simplified summaries of the audit messages in the audit log. You can use the `audit-sum` tool to summarize how many write, read, and delete operations were logged and how long these operations took.

**Related information**

Use audit-explain tool

Use audit-sum tool

#### Use audit-explain tool

## You can use the `audit-explain` tool to translate the audit messages in the audit log into an easy-to-read format.

**What you'll need**

- You must have specific access permissions.
- You must have the `Passwords.txt` file.
- You must know the IP address of the primary Admin Node.

**About this task**

The `audit-explain` tool, available on the primary Admin Node, provides simplified summaries of the audit messages in an audit log.

> The `audit-explain` tool is primarily intended for use by technical support during troubleshooting operations. Processing `audit-explain` queries can consume a large amount of CPU power, which might impact StorageGRID operations.

This example shows typical output from the `audit-explain` tool. These four SPUT audit messages were generated when the S3 tenant with account ID 92484777680322627870 used S3 PUT requests to create a bucket named "bucket1" and add three objects to that bucket.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

The `audit-explain` tool can process plain or compressed audit logs. For example:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

The `audit-explain` tool can also process multiple files at once. For example:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

Finally, the `audit-explain` tool can accept input from a pipe, which allows you to filter and preprocess the input using the `grep` command or other means. For example:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Since audit logs can be very large and slow to parse, you can save time by filtering parts that you want to look at and running `audit-explain` on the parts, instead of the entire file.

> The `audit-explain` tool does not accept compressed files as piped input. To process compressed files, provide their file names as command-line arguments, or use the `zcat` tool to decompress the files first. For example:

```
zcat audit.log.gz | audit-explain
```

Use the `help (-h)` option to see the available options. For example:

```
$ audit-explain -h
```

**Steps**

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Enter the password listed in the `Passwords.txt` file.
2. Enter the following command, where `/var/local/audit/export/audit.log` represents the name and the location of the file or files you want to analyze:

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   The `audit-explain` tool prints human-readable interpretations of all messages in the specified file or files.

   > To reduce line lengths and to aid readability, timestamps are not shown by default. If you want to see the timestamps, use the timestamp (`-t`) option.

**Related information**

SPUT: S3 PUT

#### Use audit-sum tool

You can use the `audit-sum` tool to count the write, read, head, and delete audit messages and to see the minimum, maximum, and average time (or size) for each operation type.

**What you'll need**

- You must have specific access permissions.
- You must have the `Passwords.txt` file.
- You must know the IP address of the primary Admin Node.

**About this task**

The `audit-sum` tool, available on the primary Admin Node, summarizes how many write, read, and delete operations were logged and how long these operations took.

> The `audit-sum` tool is primarily intended for use by technical support during troubleshooting operations. Processing `audit-sum` queries can consume a large amount of CPU power, which might impact StorageGRID operations.

This example shows typical output from the `audit-sum` tool. This example shows how long protocol operations took.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                  1771398        0.011        1770.563
0.487
```

The `audit-sum` tool provides counts and times for the following S3, Swift, and ILM audit messages in an audit log:

| Code | Description | Refer to |
|---|---|---|
| ARCT | Archive Retrieve from Cloud-Tier | ARCT: Archive Retrieve from Cloud-Tier |

| Code | Description | Refer to |
|---|---|---|
| ASCT | Archive Store Cloud-Tier | ASCT: Archive Store Cloud-Tier |
| IDEL | ILM Initiated Delete: Logs when ILM starts the process of deleting an object. | IDEL: ILM Initiated Delete |
| SDEL | S3 DELETE: Logs a successful transaction to delete an object or bucket. | SDEL: S3 DELETE |
| SGET | S3 GET: Logs a successful transaction to retrieve an object or list the objects in a bucket. | SGET: S3 GET |
| SHEA | S3 HEAD: Logs a successful transaction to check for the existence of an object or bucket. | SHEA: S3 HEAD |
| SPUT | S3 PUT: Logs a successful transaction to create a new object or bucket. | SPUT: S3 PUT |
| WDEL | Swift DELETE: Logs a successful transaction to delete an object or container. | WDEL: Swift DELETE |
| WGET | Swift GET: Logs a successful transaction to retrieve an object or list the objects in a container. | WGET: Swift GET |
| WHEA | Swift HEAD: Logs a successful transaction to check for the existence of an object or container. | WHEA: Swift HEAD |
| WPUT | Swift PUT: Logs a successful transaction to create a new object or container. | WPUT: Swift PUT |

The `audit-sum` tool can process plain or compressed audit logs. For example:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

The `audit-sum` tool can also process multiple files at once. For example:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

Finally, the `audit-sum` tool can also accept input from a pipe, which allows you to filter and preprocess the input using the `grep` command or other means. For example:

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```

> This tool does not accept compressed files as piped input. To process compressed files, provide their file names as command-line arguments, or use the `zcat` tool to decompress the files first. For example:

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

You can use command-line options to summarize operations on buckets separately from operations on objects or to group message summaries by bucket name, by time period, or by target type. By default, the summaries show the minimum, maximum, and average operation time, but you can use the `size (-s)` option to look at object size instead.

Use the `help (-h)` option to see the available options. For example:

```
$ audit-sum -h
```

**Steps**

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Enter the password listed in the `Passwords.txt` file.
2. If you want to analyze all messages related to write, read, head, and delete operations, follow these steps:
   a. Enter the following command, where `/var/local/audit/export/audit.log` represents the name and the location of the file or files you want to analyze:

   ```
   $ audit-sum /var/local/audit/export/audit.log
   ```

This example shows typical output from the `audit-sum` tool. This example shows how long protocol operations took.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                  1771398        0.011        1770.563
0.487
```

In this example, SGET (S3 GET) operations are the slowest on average at 1.13 seconds, but SGET and SPUT (S3 PUT) operations both show long worst-case times of about 1,770 seconds.

b. To show the slowest 10 retrieval operations, use the grep command to select only SGET messages and add the long output option (`-l`) to include object paths: `grep SGET audit.log | audit-sum -l`

   The results include the type (object or bucket) and path, which allows you to grep the audit log for other messages relating to these particular objects.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== =============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

From this example output, you can see that the three slowest S3 GET requests were for objects about 5 GB in size, which is much larger than the other objects. The large size accounts for the slow worst-case retrieval times.

3. If you want to determine what sizes of objects are being ingested into and retrieved from your grid, use the size option (`-s`):

```
audit-sum -s audit.log
```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                    213371        0.000          10.504
1.695
  SGET                    201906        0.000        5000.000
14.920
  SHEA                     22716        0.001          10.504
2.967
  SPUT                   1771398        0.000        5000.000
2.495
```

In this example, the average object size for SPUT is under 2.5 MB, but the average size for SGET is much larger. The number of SPUT messages is much higher than the number of SGET messages, indicating that most objects are never retrieved.

4. If you want to determine if retrievals were slow yesterday:
   a. Issue the command on the appropriate audit log and use the group-by-time option (`-gt`), followed by the time period (for example, 15M, 1H, 10S):

```
grep SGET audit.log | audit-sum -gt 1H
```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

These results show that S3 GET traffic spiked between 06:00 and 07:00. The max and average times are both considerably higher at these times as well, and they did not ramp up gradually as the count increased. This suggests that capacity was exceeded somewhere, perhaps in the network or in the grid's ability to process requests.

b. To determine what size objects were being retrieved each hour yesterday, add the size option (`-s`) to the command:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

These results indicate that some very large retrievals occurred when the overall retrieval traffic was at its maximum.

c. To see more detail, use the `audit-explain` tool to review all the SGET operations during that hour:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

If the output of the grep command is expected to be many lines, add the `less` command to show the contents of the audit log file one page (one screen) at a time.

5. If you want to determine if SPUT operations on buckets are slower than SPUT operations for objects:

a. Start by using the `-go` option, which groups messages for object and bucket operations separately:

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

The results show that SPUT operations for buckets have different performance characteristics than SPUT operations for objects.

b. To determine which buckets have the slowest SPUT operations, use the `-gb` option, which groups messages by bucket:

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. To determine which buckets have the largest SPUT object size, use both the `-gb` and the `-s` options:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

**Related information**

Use audit-explain tool

**Audit message format**

## Audit messages exchanged within the StorageGRID system include standard information common to all messages and specific content describing the event or activity being reported.

If the summary information provided by the `audit-explain` and `audit-sum` tools is insufficient, refer to this section to understand the general format of all audit messages.

The following is an example audit message as it might appear in the audit log file:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Each audit message contains a string of attribute elements. The entire string is enclosed in brackets (`[ ]`), and each attribute element in the string has the following characteristics:

- Enclosed in brackets `[ ]`
- Introduced by the string `AUDT`, which indicates an audit message
- Without delimiters (no commas or spaces) before or after
- Terminated by a line feed character `\n`

Each element includes an attribute code, a data type, and a value that are reported in this format:

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

The number of attribute elements in the message depends on the event type of the message. The attribute elements are not listed in any particular order.

The following list describes the attribute elements:

- `ATTR` is a four-character code for the attribute being reported. There are some attributes that are common to all audit messages and others that are event-specific.
- `type` is a four-character identifier of the programming data type of the value, such as UI64, FC32, and so on. The type is enclosed in parentheses `( )`.
- `value` is the content of the attribute, typically a numeric or text value. Values always follow a colon (`:`). Values of data type CSTR are surrounded by double quotes `" "`.

**Related information**

Use audit-explain tool

Use audit-sum tool

Audit messages

Common elements in audit messages

Data types

Audit message examples

#### Data types

Different data types are used to store information in audit messages.

| Type | Description |
|---|---|
| UI32 | Unsigned long integer (32 bits); it can store the numbers 0 to 4,294,967,295. |
| UI64 | Unsigned double long integer (64 bits); it can store the numbers 0 to 18,446,744,073,709,551,615. |
| FC32 | Four-character constant; a 32-bit unsigned integer value represented as four ASCII characters such as "ABCD." |
| IPAD | Used for IP addresses. |

| Type | Description |
| --- | --- |
| CSTR | A variable-length array of UTF-8 characters. Characters can be escaped with the following conventions:<br>• Backslash is \\.<br>• Carriage return is \r.<br>• Double quotes is \".<br>• Line feed (new line) is \n.<br>• Characters can be replaced by their hexadecimal equivalents (in the format \xHH, where HH is the hexadecimal value representing the character). |

#### Event-specific data

Each audit message in the audit log records data specific to a system event.

Following the opening `[AUDT:` container that identifies the message itself, the next set of attributes provide information about the event or action described by the audit message. These attributes are highlighted in the following example:

```
2018-12-05T08:24:45.921845 [AUDT:*\[RSLT\(FC32\):SUCS\]*
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025621595611246499"\]
\[SACC\(CSTR\):"account"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRs
KJA=="\] \[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"account"\]\[S3BK\(CSTR\):"bucket"\]
\[S3KY\(CSTR\):"object"\]\[CBID\(UI64\):0xCC128B9B9E428347\] \[UUID\(CSTR\):"B975D2CE-E4DA-
4D14-8A23-1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][AMID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

The `ATYP` element (underlined in the example) identifies which event generated the message. This example message includes the SHEA message code ([ATYP(FC32):SHEA]), indicating it was generated by a successful S3 HEAD request.

#### Related information

Common elements in audit messages

Audit messages

#### Common elements in audit messages

All audit messages contain the common elements.

| Code | Type | Description |
|---|---|---|
| AMID | FC32 | Module ID: A four-character identifier of the module ID that generated the message. This indicates the code segment within which the audit message was generated. |
| ANID | UI32 | Node ID: The grid node ID assigned to the service that generated the message. Each service is allocated a unique identifier at the time the StorageGRID system is configured and installed. This ID cannot be changed. |
| ASES | UI64 | Audit Session Identifier: In previous releases, this element indicated the time at which the audit system was initialized after the service started up. This time value was measured in microseconds since the operating system epoch (00:00:00 UTC on 1 January, 1970).<br><br>**Note:** This element is obsolete and no longer appears in audit messages. |
| ASQN | UI64 | Sequence Count: In previous releases, this counter was incremented for each generated audit message on the grid node (ANID) and reset to zero at service restart.<br><br>**Note:** This element is obsolete and no longer appears in audit messages. |
| ATID | UI64 | Trace ID: An identifier that is shared by the set of messages that were triggered by a single event. |
| ATIM | UI64 | Timestamp: The time the event was generated that triggered the audit message, measured in microseconds since the operating system epoch (00:00:00 UTC on 1 January, 1970). Note that most available tools for converting the timestamp to local date and time are based on milliseconds.<br><br>Rounding or truncation of the logged timestamp might be required. The human-readable time that appears at the beginning of the audit message in the `audit.log` file is the ATIM attribute in ISO 8601 format. The date and time are represented as *`YYYY-MMDDTHH:MM:SS.UUUUUU`*, where the `T` is a literal string character indicating the beginning of the time segment of the date. *`UUUUUU`* are microseconds. |
| ATYP | FC32 | Event Type: A four-character identifier of the event being logged. This governs the "payload" content of the message: the attributes that are included. |
| AVER | UI32 | Version: The version of the audit message. As the StorageGRID software evolves, new versions of services might incorporate new features in audit reporting. This field enables backward compatibility in the AMS service to process messages from older versions of services. |
| RSLT | FC32 | Result: The result of event, process, or transaction. If is not relevant for a message, NONE is used rather than SUCS so that the message is not accidentally filtered. |

#### Audit message examples

## You can find detailed information in each audit message. All audit messages use the same format.

The following is a sample audit message as it might appear in the `audit.log` file:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

The audit message contains information about the event being recorded, as well as information about the audit message itself.

To identify which event is recorded by the audit message, look for the ATYP attribute (highlighted below):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP\(FC32\):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

The value of the ATYP attribute is SPUT. SPUT represents an S3 PUT transaction, which logs the ingest of an object to a bucket.

The following audit message also shows the bucket to which the object is associated:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

To discover when the PUT event occurred, note the Universal Coordinated Time (UTC) timestamp at the

beginning of the audit message. This value is a human-readable version of the ATIM attribute of the audit message itself:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM records the time, in microseconds, since the beginning of the UNIX epoch. In the example, the value `1405631878959669` translates to Thursday, 17-Jul-2014 21:17:59 UTC.

**Related information**

SPUT: S3 PUT

Common elements in audit messages

## Audit messages and the object lifecycle

Audit messages are generated each time an object is ingested, retrieved, or deleted. You can identify these transactions in the audit log by locating API-specific (S3 or Swift) audit messages.

Audit messages are linked through identifiers specific to each protocol.

| Protocol | Code |
|---|---|
| Linking S3 operations | S3BK (S3 Bucket) and/or S3KY (S3 Key) |
| Linking Swift operations | WCON (Swift Container) and/or WOBJ (Swift Object) |
| Linking internal operations | CBID (Object's Internal Identifier) |

### Timing of audit messages

Because of factors such as timing differences between grid nodes, object size, and network delays, the order of audit messages generated by the different services can vary from that shown in the examples in this section.

### Information lifecycle management policy configuration

With the default ILM policy (Baseline 2 Copy), object data is copied once for a total of two copies. If the ILM policy requires more than two copies, there will be an additional set of CBRE, CBSE, and SCMT messages for each extra copy. For more information about ILM policies, see information about managing objects with information lifecycle management.

### Archive Nodes

The series of audit messages generated when an Archive Node sends object data to an external archival storage system is similar to that for Storage Nodes except that there is no SCMT (Store Object Commit) message, and the ATCE (Archive Object Store Begin) and ASCE (Archive Object Store End) messages are generated for each archived copy of object data.

The series of audit messages generated when an Archive Node retrieves object data from an external archival storage system is similar to that for Storage Nodes except that the ARCB (Archive Object Retrieve Begin) and ARCE (Archive Object Retrieve End) messages are generated for each retrieved copy of object data.

The series of audit messages generated when an Archive Node deletes object data from an external archival storage system is similar to that for Storage Nodes except that there is no SREM (Object Store Remove) message, and there is an AREM (Archive Object Remove) message for each delete request.

#### Related information

Manage objects with ILM

### Object ingest transactions

You can identify client ingest transactions in the audit log by locating API-specific (S3 or Swift) audit messages.

Not all audit messages generated during an ingest transaction are listed in the following tables. Only the messages required to trace the ingest transaction are included.

#### S3 ingest audit messages

| Code | Name | Description | Trace | See |
|---|---|---|---|---|
| SPUT | S3 PUT transaction | An S3 PUT ingest transaction has completed successfully. | CBID, S3BK, S3KY | SPUT: S3 PUT |
| ORLM | Object Rules Met | The ILM policy has been satisfied for this object. | CBID | ORLM: Object Rules Met |

#### Swift ingest audit messages

| Code | Name | Description | Trace | See |
|---|---|---|---|---|
| WPUT | Swift PUT transaction | A Swift PUT ingest transaction has successfully completed. | CBID, WCON, WOBJ | WPUT: Swift PUT |
| ORLM | Object Rules Met | The ILM policy has been satisfied for this object. | CBID | ORLM: Object Rules Met |

#### Example: S3 object ingest

The series of audit messages below is an example of the audit messages generated and saved to the audit log when an S3 client ingests an object to a Storage Node (LDR service).

In this example, the active ILM policy includes the stock ILM rule, Make 2 Copies.

> Not all audit messages generated during a transaction are listed in the example below. Only those related to the S3 ingest transaction (SPUT) are listed.

This example assumes that an S3 bucket has been previously created.

**SPUT: S3 PUT**

The SPUT message is generated to indicate that an S3 PUT transaction has been issued to create an object in a specific bucket.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

**ORLM: Object Rules Met**

The ORLM message indicates that the ILM policy has been satisfied for this object. The message includes the object's CBID and the name of the ILM rule that was applied.

For replicated objects, the LOCS field includes the LDR node ID and volume ID of the object locations.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

For erasure-coded objects, the LOCS field includes the Erasure Coding profile ID and the Erasure Coding group ID

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

The PATH field includes S3 bucket and key information or Swift container and object information, depending on which API was used.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

#### Object delete transactions

You can identify object delete transactions in the audit log by locating API-specific (S3 and Swift) audit messages.

Not all audit messages generated during a delete transaction are listed in the following tables. Only messages required to trace the delete transaction are included.

##### S3 delete audit messages

| Code | Name | Description | Trace | See |
|---|---|---|---|---|
| SDEL | S3 Delete | Request made to delete the object from a bucket. | CBID, S3KY | SDEL: S3 DELETE |

##### Swift delete audit messages

| Code | Name | Description | Trace | See |
|---|---|---|---|---|
| WDEL | Swift Delete | Request made to delete the object from a container, or the container. | CBID, WOBJ | WDEL: Swift DELETE |

#### Example: S3 object deletion

When an S3 client deletes an object from a Storage Node (LDR service), an audit message is generated and saved to the audit log.

> Not all audit messages generated during a delete transaction are listed in the example below. Only those related to the S3 delete transaction (SDEL) are listed.

**SDEL: S3 Delete**

Object deletion begins when the client sends a DELETE Object request to an LDR service. The message contains the bucket from which to delete the object and the object's S3 Key, which is used to identify the object.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

#### Object retrieve transactions

You can identify object retrieve transactions in the audit log by locating API-specific (S3 and Swift) audit messages.

Not all audit messages generated during a retrieve transaction are listed in the following tables. Only messages required to trace the retrieve transaction are included.

**S3 retrieval audit messages**

| Code | Name | Description | Trace | See |
|---|---|---|---|---|
| SGET | S3 GET | Request made to retrieve an object from a bucket. | CBID, S3BK, S3KY | SGET: S3 GET |

**Swift retrieval audit messages**

| Code | Name | Description | Trace | See |
|---|---|---|---|---|
| WGET | Swift GET | Request made to retrieve an object from a container. | CBID, WCON, WOBJ | WGET: Swift GET |

#### Example: S3 object retrieval

## When an S3 client retrieves an object from a Storage Node (LDR service), an audit message is generated and saved to the audit log.

Note that not all audit messages generated during a transaction are listed in the example below. Only those related to the S3 retrieval transaction (SGET) are listed.

**SGET: S3 GET**

Object retrieval begins when the client sends a GET Object request to an LDR service. The message contains the bucket from which to retrieve the object and the object's S3 Key, which is used to identify the object.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

If the bucket policy allows, a client can anonymously retrieve objects, or can retrieve objects from a bucket that is owned by a different tenant account. The audit message contains information about the bucket owner's tenant account so that you can track these anonymous and cross-account requests.

In the following example message, the client sends a GET Object request for an object stored in a bucket that they do not own. The values for SBAI and SBAC record the bucket owner's tenant account ID and name, which differs from the tenant account ID and name of the client recorded in S3AI and SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

#### Example: S3 Select on an object

## When an S3 client issues an S3 Select query on an object, audit messages are generated and saved to the audit log.

Note that not all audit messages generated during a transaction are listed in the example below. Only those related to the S3 Select transaction (SelectObjectContent) are listed.

Each query results in two audit messages: one that performs the authorization of the S3 Select request (the S3SR field is set to “select”) and a subsequent standard GET operation that retrieves the data from storage during processing.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):13630097093968959 85]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

#### Metadata update messages

Audit messages are generated when an S3 client updates an object’s metadata.

##### S3 metadata update audit messages

| Code | Name | Description | Trace | See |
|---|---|---|---|---|
| SUPD | S3 Metadata Updated | Generated when an S3 client updates the metadata for an ingested object. | CBID, S3KY, HTRH | SUPD: S3 Metadata Updated |

#### Example: S3 metadata update

The example shows a successful transaction to update the metadata for an existing S3 object.

#### SUPD: S3 Metadata Update

The S3 client makes a request (SUPD) to update the specified metadata (`x-amz-meta-\*`) for the S3 object (S3KY). In this example, request headers are included in the field HTRH because it has been configured as an audit protocol header (**CONFIGURATION** > **Monitoring** > **Audit and syslog server**).

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

#### Related information

Configure audit messages and log destinations

## Audit messages

Detailed descriptions of audit messages returned by the system are listed in the following sections. Each audit message is first listed in a table that groups related messages by the class of activity that the message represents. These groupings are useful both for understanding the types of activities that are audited, and for selecting the desired type of audit message filtering.

The audit messages are also listed alphabetically by their four-character codes. This alphabetic listing enables you to find information about specific messages.

The four-character codes used throughout this chapter are the ATYP values found in the audit messages as shown in the following sample message:

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

For information on setting audit message levels, changing log destinations, and using an external syslog server for your audit information, see Configure audit messages and log destinations

### Audit message categories

You should be familiar with the various categories within which audit messages are grouped. These groups are organized based on the class of activity that the message represents.

#### System audit messages

You should be familiar with audit messages belonging to the system audit category. These are events related to the auditing system itself, grid node states, system-wide task activity (grid tasks), and service backup operations, so that you can address potential issues.

| Code | Message title and description | See |
|---|---|---|
| ECMC | Missing Erasure Coded Data Fragment: Indicates that a missing erasure coded data fragment has been detected. | ECMC: Missing Erasure Coded Data Fragment |
| ECOC | Corrupt Erasure Coded Data Fragment: Indicates that a corrupt erasure coded data fragment has been detected. | ECOC: Corrupt Erasure Coded Data Fragment |
| ETAF | Security Authentication Failed: A connection attempt using Transport Layer Security (TLS) failed. | ETAF: Security Authentication Failed |
| GNRG | GNDS Registration: A service updated or registered information about itself in the StorageGRID system. | GNRG: GNDS Registration |
| GNUR | GNDS Unregistration: A service has unregistered itself from the StorageGRID system. | GNUR: GNDS Unregistration |

| Code | Message title and description | See |
| --- | --- | --- |
| GTED | Grid Task Ended: The CMN service finished processing the grid task. | GTED: Grid Task Ended |
| GTST | Grid Task Started: The CMN service started to process the grid task. | GTST: Grid Task Started |
| GTSU | Grid Task Submitted: A grid task was submitted to the CMN service. | GTSU: Grid Task Submitted |
| IDEL | ILM Initiated Delete: This audit message is generated when ILM starts the process of deleting an object. | IDEL: ILM Initiated Delete |
| LKCU | Overwritten Object Cleanup. This audit message is generated when an overwritten object is automatically removed to free up storage space. | LKCU: Overwritten Object Cleanup |
| LLST | Location Lost: This audit message is generated when a location is lost. | LLST: Location Lost |
| OLST | Object Lost: A requested object cannot be located within the StorageGRID system. | OLST: System Detected Lost Object |
| ORLM | Object Rules Met: Object data is stored as specified by the ILM rules. | ORLM: Object Rules Met |
| SADD | Security Audit Disable: Audit message logging was turned off. | SADD: Security Audit Disable |
| SADE | Security Audit Enable: Audit message logging has been restored. | SADE: Security Audit Enable |
| SVRF | Object Store Verify Fail: A content block failed verification checks. | SVRF: Object Store Verify Fail |
| SVRU | Object Store Verify Unknown: Unexpected object data detected in the object store. | SVRU: Object Store Verify Unknown |

| Code | Message title and description | See |
|---|---|---|
| SYSD | Node Stop: A shutdown was requested. | SYSD: Node Stop |
| SYST | Node Stopping: A service initiated a graceful stop. | SYST: Node Stopping |
| SYSU | Node Start: A service started; the nature of the previous shutdown is indicated in the message. | SYSU: Node Start |
| VLST | User Initiated Volume Lost: The `/proc/CMSI/Volume_Lost` command was run. | VLST: User Initiated Volume Lost |

**Related information**

LKCU: Overwritten Object Cleanup

#### Object storage audit messages

You should be familiar with audit messages belonging to the object storage audit category. These are events related to the storage and management of objects within the StorageGRID system. These include object storage and retrievals, grid-node to grid-node transfers, and verifications.

| Code | Description | See |
|---|---|---|
| APCT | Archive Purge from Cloud-Tier: Archived object data is deleted from an external archival storage system, which connects to the StorageGRID through the S3 API. | APCT: Archive Purge from Cloud-Tier |
| ARCB | Archive Object Retrieve Begin: The ARC service begins the retrieval of object data from the external archival storage system. | ARCB: Archive Object Retrieve Begin |
| ARCE | Archive Object Retrieve End: Object data has been retrieved from an external archival storage system, and the ARC service reports the status of the retrieval operation. | ARCE: Archive Object Retrieve End |

| Code | Description | See |
| --- | --- | --- |
| ARCT | Archive Retrieve from Cloud-Tier: Archived object data is retrieved from an external archival storage system, which connects to the StorageGRID through the S3 API. | ARCT: Archive Retrieve from Cloud-Tier |
| AREM | Archive Object Remove: A content block was successfully or unsuccessfully deleted from the external archival storage system. | AREM: Archive Object Remove |
| ASCE | Archive Object Store End: A content block has been written to the external archival storage system, and the ARC service reports the status of the write operation. | ASCE: Archive Object Store End |
| ASCT | Archive Store Cloud-Tier: Object data is stored to an external archival storage system, which connects to the StorageGRID through the S3 API. | ASCT: Archive Store Cloud-Tier |
| ATCE | Archive Object Store Begin: Writing a content block to an external archival storage has started. | ATCE: Archive Object Store Begin |
| AVCC | Archive Validate Cloud-Tier Configuration: The account and bucket settings provided were successfully or unsuccessfully validated. | AVCC: Archive Validate Cloud-Tier Configuration |
| CBSE | Object Send End: The source entity completed a grid-node to grid-node data transfer operation. | CBSE: Object Send End |
| CBRE | Object Receive End: The destination entity completed a grid-node to grid-node data transfer operation. | CBRE: Object Receive End |
| SCMT | Object Store Commit: A content block was completely stored and verified, and can now be requested. | SCMT: Object Store Commit |

| Code | Description | See |
| --- | --- | --- |
| SREM | Object Store Remove: A content block was deleted from a grid node, and can no longer be requested directly. | SREM: Object Store Remove |

#### Client read audit messages

Client read audit messages are logged when an S3 or Swift client application makes a request to retrieve an object.

| Code | Description | Used by | See |
| --- | --- | --- | --- |
| SGET | S3 GET: Logs a successful transaction to retrieve an object or list the objects in a bucket.<br><br>**Note:** If the transaction operates on a subresource, the audit message will include the field S3SR. | S3 client | SGET: S3 GET |
| SHEA | S3 HEAD: Logs a successful transaction to check for the existence of an object or bucket. | S3 client | SHEA: S3 HEAD |
| WGET | Swift GET: Logs a successful transaction to retrieve an object or list the objects in a container. | Swift client | WGET: Swift GET |
| WHEA | Swift HEAD: Logs a successful transaction to check for the existence of an object or container. | Swift client | WHEA: Swift HEAD |

#### Client write audit messages

Client write audit messages are logged when an S3 or Swift client application makes a request to create or modify an object.

| Code | Description | Used by | See |
| --- | --- | --- | --- |
| OVWR | Object Overwrite: Logs a transaction to overwrite one object with another object. | S3 clients<br><br>Swift clients | OVWR: Object Overwrite |
| SDEL | S3 DELETE: Logs a successful transaction to delete an object or bucket.<br><br>**Note:** If the transaction operates on a subresource, the audit message will include the field S3SR. | S3 client | SDEL: S3 DELETE |
| SPOS | S3 POST: Logs a successful transaction to restore an object from AWS Glacier storage to a Cloud Storage Pool. | S3 client | SPOS: S3 POST |
| SPUT | S3 PUT: Logs a successful transaction to create a new object or bucket.<br><br>**Note:** If the transaction operates on a subresource, the audit message will include the field S3SR. | S3 client | SPUT: S3 PUT |
| SUPD | S3 Metadata Updated: Logs a successful transaction to update the metadata for an existing object or bucket. | S3 client | SUPD: S3 Metadata Updated |
| WDEL | Swift DELETE: Logs a successful transaction to delete an object or container. | Swift client | WDEL: Swift DELETE |
| WPUT | Swift PUT: Logs a successful transaction to create a new object or container. | Swift client | WPUT: Swift PUT |

#### Management audit message

The Management category logs user requests to the Management API.

| Code | Message title and description | See |
|---|---|---|
| MGAU | Management API audit message: A log of user requests. | MGAU: Management audit message |

### Audit message reference

#### APCT: Archive Purge from Cloud-Tier

This message is generated when archived object data is deleted from an external archival storage system, which connects to the StorageGRID through the S3 API.

| Code | Field | Description |
|---|---|---|
| CBID | Content Block ID | The unique identifier for the content block that was deleted. |
| CSIZ | Content Size | The size of the object in bytes. Always returns 0. |
| RSLT | Result Code | Returns successful (SUCS) or the error reported by the backend. |
| SUID | Storage Unique Identifier | Unique identifier (UUID) of the cloud-tier from which the object was deleted. |

#### ARCB: Archive Object Retrieve Begin

This message is generated when a request is made to retrieve archived object data and the retrieval process begins. Retrieval requests are processed immediately, but can be reordered to improve efficiency of retrieval from linear media such as tape.

| Code | Field | Description |
|---|---|---|
| CBID | Content Block ID | The unique identifier of the Content Block to be retrieved from the external archival storage system. |
| RSLT | Result | Indicates the result of starting the archive retrieval process. Currently defined value is:SUCS: The content request was received and queued for retrieval. |

This audit message marks the time of an archive retrieval. It allows you to match the message with a corresponding ARCE end message to determine the duration of archive retrieval, and whether the operation was successful.

#### ARCE: Archive Object Retrieve End

This message is generated when an attempt by the Archive Node to retrieve object data from an external archival storage system completes. If successful, the message indicates that the requested object data has been completely read from the archive location, and was successfully verified. After the object data has been retrieved and verified, it is delivered to the requesting service.

| Code | Field | Description |
|---|---|---|
| CBID | Content Block ID | The unique identifier of the Content Block to be retrieved from the external archival storage system. |
| VLID | Volume Identifier | The identifier of the volume on which the data was archived.If an archive location for the content is not found, a Volume ID of 0 is returned. |
| RSLT | Retrieval Result | The completion status of the archive retrieval process:<br>• SUCS: successful<br>• VRFL: failed (object verification failure)<br>• ARUN: failed (external archival storage system unavailable)<br>• CANC: failed (retrieval operation canceled)<br>• GERR: failed (general error) |

Matching this message with the corresponding ARCB message can indicate the time taken to perform the archive retrieval. This message indicates whether the retrieval was successful, and in the case of failure, the cause of the failure to retrieve the content block.

#### ARCT: Archive Retrieve from Cloud-Tier

This message is generated when archived object data is retrieved from an external archival storage system, which connects to the StorageGRID through the S3 API.

| Code | Field | Description |
|---|---|---|
| CBID | Content Block ID | The unique identifier for the content block that was retrieved. |

| Code | Field | Description |
| --- | --- | --- |
| CSIZ | Content Size | The size of the object in bytes. The value is only accurate for successful retrieves. |
| RSLT | Result Code | Returns successful (SUCS) or the error reported by the backend. |
| SUID | Storage Unique Identifier | Unique identifier (UUID) of the external archival storage system. |
| TIME | Time | Total processing time for the request in microseconds. |

#### AREM: Archive Object Remove

The Archive Object Remove audit message indicates that a content block was successfully or unsuccessfully deleted from an Archive Node. If the result is successful, the Archive Node has successfully informed the external archival storage system that StorageGRID has released an object location. Whether the object is removed from the external archive storage system depends on the type of system and its configuration.

| Code | Field | Description |
| --- | --- | --- |
| CBID | Content Block ID | The unique identifier of the Content Block to be retrieved from the external archival media system. |
| VLID | Volume Identifier | The identifier of the volume on which the object data was archived. |
| RSLT | Result | The completion status of the archive removal process:<br>• SUCS: successful<br>• ARUN: failed (external archival storage system unavailable)<br>• GERR: failed (general error) |

#### ASCE: Archive Object Store End

This message indicates that writing a content block to an external archival storage system has ended.

| Code | Field | Description |
| --- | --- | --- |
| CBID | Content Block Identifier | The identifier of the content block stored on the external archival storage system. |
| VLID | Volume Identifier | The unique identifier of the archive volume to which the object data is written. |
| VREN | Verification Enabled | Indicates if verification is performed for content blocks. Currently defined values are:<br>• VENA: verification is enabled<br>• VDSA: verification is disabled |
| MCLS | Management Class | A string identifying the TSM Management Class to which the content block is assigned if applicable. |
| RSLT | Result | Indicates the result of the archive process. Currently defined values are:<br>• SUCS: successful (archiving process succeeded)<br>• OFFL: failed (archiving is offline)<br>• VRFL: failed (object verification failed)<br>• ARUN: failed (external archival storage system unavailable)<br>• GERR: failed (general error) |

This audit message means that the specified content block has been written to the external archival storage system. If the write fails, the result provides basic troubleshooting information about where the failure occurred. More detailed information about archive failures can be found by examining Archive Node attributes in the StorageGRID system.

#### ASCT: Archive Store Cloud-Tier

This message is generated when archived object data is stored to an external archival storage system, which connects to StorageGRID through the S3 API.

| Code | Field | Description |
| --- | --- | --- |
| CBID | Content Block ID | The unique identifier for the content block that was retrieved. |
| CSIZ | Content Size | The size of the object in bytes. |
| RSLT | Result Code | Returns successful (SUCS) or the error reported by the backend. |
| SUID | Storage Unique Identifier | Unique identifier (UUID) of the cloud-tier the content was stored to. |
| TIME | Time | Total processing time for the request in microseconds. |

#### ATCE: Archive Object Store Begin

This message indicates that writing a content block to an external archival storage has started.

| Code | Field | Description |
| --- | --- | --- |
| CBID | Content Block ID | The unique identifier of the content block to be archived. |
| VLID | Volume Identifier | The unique identifier of the volume to which the content block is written. If the operation fails, a volume ID of 0 is returned. |
| RSLT | Result | Indicates the result of the transfer of the content block. Currently defined values are:<br>• SUCS: success (content block stored successfully)<br>• EXIS: ignored (content block was already stored)<br>• ISFD: failed (insufficient disk space)<br>• STER: failed (error storing the CBID)<br>• OFFL: failed (archiving is offline)<br>• GERR: failed (general error) |

#### AVCC: Archive Validate Cloud-Tier Configuration

This message is generated when the configuration settings are validated for a Cloud Tiering - Simple Storage Service (S3) target type.

| Code | Field | Description |
|---|---|---|
| RSLT | Result Code | Returns successful (SUCS) or the error reported by the backend. |
| SUID | Storage Unique Identifier | UUID associated with the external archival storage system being validated. |

#### CBRB: Object Receive Begin

During normal system operations, content blocks are continuously transferred between different nodes as data is accessed, replicated and retained. When transfer of a content block from one node to another is initiated, this message is issued by the destination entity.

| Code | Field | Description |
|---|---|---|
| CNID | Connection Identifier | The unique identifier of the node-to-node session/connection. |
| CBID | Content Block Identifier | The unique identifier of the content block being transferred. |
| CTDR | Transfer Direction | Indicates if the CBID transfer was push-initiated or pull-initiated:<br><br>PUSH: The transfer operation was requested by the sending entity.<br><br>PULL: The transfer operation was requested by the receiving entity. |
| CTSR | Source Entity | The node ID of the source (sender) of the CBID transfer. |
| CTDS | Destination Entity | The node ID of the destination (receiver) of the CBID transfer. |
| CTSS | Start Sequence Count | Indicates the first sequence count requested. If successful, the transfer begins from this sequence count. |

| Code | Field | Description |
| --- | --- | --- |
| CTES | Expected End Sequence Count | Indicates the last sequence count requested. If successful, the transfer is considered complete when this sequence count has been received. |
| RSLT | Transfer Start Status | Status at the time the transfer was started:<br><br>SUCS: Transfer started successfully. |

This audit message means a node-to-node data transfer operation was initiated on a single piece of content, as identified by its Content Block Identifier. The operation requests data from "Start Sequence Count" to "Expected End Sequence Count". Sending and receiving nodes are identified by their node IDs. This information can be used to track system data flow, and when combined with storage audit messages, to verify replica counts.

#### CBRE: Object Receive End

When transfer of a content block from one node to another is completed, this message is issued by the destination entity.

| Code | Field | Description |
| --- | --- | --- |
| CNID | Connection Identifier | The unique identifier of the node-to-node session/connection. |
| CBID | Content Block Identifier | The unique identifier of the content block being transferred. |
| CTDR | Transfer Direction | Indicates if the CBID transfer was push-initiated or pull-initiated:<br><br>PUSH: The transfer operation was requested by the sending entity.<br><br>PULL: The transfer operation was requested by the receiving entity. |
| CTSR | Source Entity | The node ID of the source (sender) of the CBID transfer. |
| CTDS | Destination Entity | The node ID of the destination (receiver) of the CBID transfer. |
| CTSS | Start Sequence Count | Indicates the sequence count on which the transfer started. |

| Code | Field | Description |
| --- | --- | --- |
| CTAS | Actual End Sequence Count | Indicates the last sequence count successfully transferred. If the Actual End Sequence Count is the same as the Start Sequence Count, and the Transfer Result was not successful, no data was exchanged. |
| RSLT | Transfer Result | The result of the transfer operation (from the perspective of the sending entity):<br><br>SUCS: transfer successfully completed; all requested sequence counts were sent.<br><br>CONL: connection lost during transfer<br><br>CTMO: connection timed-out during establishment or transfer<br><br>UNRE: destination node ID unreachable<br><br>CRPT: transfer ended due to reception of corrupt or invalid data (might indicate tampering) |

This audit message means a node-to-node data transfer operation was completed. If the Transfer Result was successful, the operation transferred data from "Start Sequence Count" to "Actual End Sequence Count". Sending and receiving nodes are identified by their node IDs. This information can be used to track system data flow and to locate, tabulate, and analyze errors. When combined with storage audit messages, it can also be used to verify replica counts.

#### CBSB: Object Send Begin

During normal system operations, content blocks are continuously transferred between different nodes as data is accessed, replicated and retained. When transfer of a content block from one node to another is initiated, this message is issued by the source entity.

| Code | Field | Description |
| --- | --- | --- |
| CNID | Connection Identifier | The unique identifier of the node-to-node session/connection. |
| CBID | Content Block Identifier | The unique identifier of the content block being transferred. |

| Code | Field | Description |
|---|---|---|
| CTDR | Transfer Direction | Indicates if the CBID transfer was push-initiated or pull-initiated:<br><br>PUSH: The transfer operation was requested by the sending entity.<br><br>PULL: The transfer operation was requested by the receiving entity. |
| CTSR | Source Entity | The node ID of the source (sender) of the CBID transfer. |
| CTDS | Destination Entity | The node ID of the destination (receiver) of the CBID transfer. |
| CTSS | Start Sequence Count | Indicates the first sequence count requested. If successful, the transfer begins from this sequence count. |
| CTES | Expected End Sequence Count | Indicates the last sequence count requested. If successful, the transfer is considered complete when this sequence count has been received. |
| RSLT | Transfer Start Status | Status at the time the transfer was started:<br><br>SUCS: transfer started successfully. |

This audit message means a node-to-node data transfer operation was initiated on a single piece of content, as identified by its Content Block Identifier. The operation requests data from "Start Sequence Count" to "Expected End Sequence Count". Sending and receiving nodes are identified by their node IDs. This information can be used to track system data flow, and when combined with storage audit messages, to verify replica counts.

#### CBSE: Object Send End

When transfer of a content block from one node to another is completed, this message is issued by the source entity.

| Code | Field | Description |
|---|---|---|
| CNID | Connection Identifier | The unique identifier of the node-to-node session/connection. |

| Code | Field | Description |
| --- | --- | --- |
| CBID | Content Block Identifier | The unique identifier of the content block being transferred. |
| CTDR | Transfer Direction | Indicates if the CBID transfer was push-initiated or pull-initiated:<br><br>PUSH: The transfer operation was requested by the sending entity.<br><br>PULL: The transfer operation was requested by the receiving entity. |
| CTSR | Source Entity | The node ID of the source (sender) of the CBID transfer. |
| CTDS | Destination Entity | The node ID of the destination (receiver) of the CBID transfer. |
| CTSS | Start Sequence Count | Indicates the sequence count on which the transfer started. |
| CTAS | Actual End Sequence Count | Indicates the last sequence count successfully transferred. If the Actual End Sequence Count is the same as the Start Sequence Count, and the Transfer Result was not successful, no data was exchanged. |
| RSLT | Transfer Result | The result of the transfer operation (from the perspective of the sending entity):<br><br>SUCS: Transfer successfully completed; all requested sequence counts were sent.<br><br>CONL: connection lost during transfer<br><br>CTMO: connection timed-out during establishment or transfer<br><br>UNRE: destination node ID unreachable<br><br>CRPT: transfer ended due to reception of corrupt or invalid data (might indicate tampering) |

This audit message means a node-to-node data transfer operation was completed. If the Transfer Result was successful, the operation transferred data from "Start Sequence Count" to "Actual End Sequence Count". Sending and receiving nodes are identified by their node IDs. This information can be used to track system data flow and to locate, tabulate, and analyze errors. When combined with storage audit messages, it can also be used to verify replica counts.

#### ECMC: Missing Erasure Coded Data Fragment

This audit message indicates that the system has detected a missing erasure-coded data fragment.

| Code | Field | Description |
|---|---|---|
| VCMC | VCS ID | The name of the VCS that contains the missing chunk. |
| MCID | Chunk ID | The identifier of the missing erasure-coded fragment. |
| RSLT | Result | This field has the value 'NONE'. RSLT is a mandatory message field, but is not relevant for this particular message. 'NONE' is used rather than 'SUCS' so that this message is not filtered. |

#### ECOC: Corrupt Erasure Coded Data Fragment

This audit message indicates that the system has detected a corrupt erasure-coded data fragment.

| Code | Field | Description |
|---|---|---|
| VCCO | VCS ID | The name of the VCS that contains the corrupt chunk. |
| VLID | Volume ID | The RangeDB Volume that contains the corrupt erasure-coded fragment. |
| CCID | Chunk ID | The identifier of the corrupt erasure-coded fragment. |
| RSLT | Result | This field has the value 'NONE'. RSLT is a mandatory message field, but is not relevant for this particular message. 'NONE' is used rather than 'SUCS' so that this message is not filtered. |

**ETAF: Security Authentication Failed**

This message is generated when a connection attempt using Transport Layer Security (TLS) has failed.

| Code | Field | Description |
|---|---|---|
| CNID | Connection Identifier | The unique system identifier for the TCP/IP connection over which the authentication failed. |
| RUID | User Identity | A service dependent identifier representing the identity of the remote user. |
| RSLT | Reason Code | The reason for the failure:<br><br>SCNI: Secure connection establishment failed.<br><br>CERM: Certificate was missing.<br><br>CERT: Certificate was invalid.<br><br>CERE: Certificate was expired.<br><br>CERR: Certificate was revoked.<br><br>CSGN: Certificate signature was invalid.<br><br>CSGU: Certificate signer was unknown.<br><br>UCRM: User credentials were missing.<br><br>UCRI: User credentials were invalid.<br><br>UCRU: User credentials were disallowed.<br><br>TOUT: Authentication timed out. |

When a connection is established to a secure service that uses TLS, the credentials of the remote entity are verified using the TLS profile and additional logic built into the service. If this authentication fails due to invalid, unexpected, or disallowed certificates or credentials, an audit message is logged. This enables queries for unauthorized access attempts and other security-related connection problems.

The message could result from a remote entity having an incorrect configuration, or from attempts to present invalid or disallowed credentials to the system. This audit message should be monitored to detect attempts to gain unauthorized access to the system.

#### GNRG: GNDS Registration

The CMN service generates this audit message when a service has updated or registered information about itself in the StorageGRID system.

| Code | Field | Description |
|---|---|---|
| RSLT | Result | The result of the update request:<br>• SUCS: Successful<br>• SUNV: Service Unavailable<br>• GERR: Other failure |
| GNID | Node ID | The node ID of the service that initiated the update request. |
| GNTP | Device Type | The grid node's device type (for example, BLDR for an LDR service). |
| GNDV | Device Model version | The string identifying the grid node's device model version in the DMDL bundle. |
| GNGP | Group | The group to which the grid node belongs (in the context of link costs and service-query ranking). |
| GNIA | IP Address | The grid node's IP address. |

This message is generated whenever a grid node updates its entry in the Grid Nodes Bundle.

#### GNUR: GNDS Unregistration

The CMN service generates this audit message when a service has unregistered information about itself from the StorageGRID system.

| Code | Field | Description |
|---|---|---|
| RSLT | Result | The result of the update request:<br>• SUCS: Successful<br>• SUNV: Service Unavailable<br>• GERR: Other failure |
| GNID | Node ID | The node ID of the service that initiated the update request. |

#### GTED: Grid Task Ended

This audit message indicates that the CMN service has finished processing the specified grid task and has moved the task to the Historical table. If the result is SUCS, ABRT, or ROLF, there will be a corresponding Grid Task Started audit message. The other results indicate that processing of this grid task never started.

| Code | Field | Description |
|---|---|---|
| TSID | Task ID | This field uniquely identifies a generated grid task and allows the grid task to be managed over its lifecycle.<br><br>**Note:** The Task ID is assigned at the time that a grid task is generated, not the time that it is submitted. It is possible for a given grid task to be submitted multiple times, and in this case the Task ID field is not sufficient to uniquely link the Submitted, Started, and Ended audit messages. |
| RSLT | Result | The final status result of the grid task:<br><br>• SUCS: The grid task completed successfully.<br>• ABRT: The grid task was aborted without a rollback error.<br>• ROLF: The grid task was aborted and was unable to complete the rollback process.<br>• CANC: The grid task was canceled by the user before it was started.<br>• EXPR: The grid task expired before it was started.<br>• IVLD: The grid task was invalid.<br>• AUTH: The grid task was unauthorized.<br>• DUPL: The grid task was rejected as a duplicate. |

#### GTST: Grid Task Started

This audit message indicates that the CMN service has started to process the specified grid task. The audit message immediately follows the Grid Task Submitted message for

grid tasks initiated by the internal Grid Task Submission service and selected for automatic activation. For grid tasks submitted into the Pending table, this message is generated when the user starts the grid task.

| Code | Field | Description |
|---|---|---|
| TSID | Task ID | This field uniquely identifies a generated grid task and allows the task to be managed over its lifecycle.<br><br>**Note:** The Task ID is assigned at the time that a grid task is generated, not the time that it is submitted. It is possible for a given grid task to be submitted multiple times, and in this case the Task ID field is not sufficient to uniquely link the Submitted, Started, and Ended audit messages. |
| RSLT | Result | The result. This field has only one value:<br><br>• SUCS: The grid task was started successfully. |

#### GTSU: Grid Task Submitted

This audit message indicates that a grid task has been submitted to the CMN service.

| Code | Field | Description |
|---|---|---|
| TSID | Task ID | Uniquely identifies a generated grid task and allows the task to be managed over its lifecycle.<br><br>**Note:** The Task ID is assigned at the time that a grid task is generated, not the time that it is submitted. It is possible for a given grid task to be submitted multiple times, and in this case the Task ID field is not sufficient to uniquely link the Submitted, Started, and Ended audit messages. |
| TTYP | Task Type | The type of grid task. |
| TVER | Task Version | A number indicating the version of the grid task. |

| Code | Field | Description |
| --- | --- | --- |
| TDSC | Task Description | A human-readable description of the grid task. |
| VATS | Valid After Timestamp | The earliest time (UINT64 microseconds from January 1, 1970 - UNIX time) at which the grid task is valid. |
| VBTS | Valid Before Timestamp | The latest time (UINT64 microseconds from January 1, 1970 - UNIX time) at which the grid task is valid. |
| TSRC | Source | The source of the task:<br>• TXTB: The grid task was submitted through the StorageGRID system as a signed text block.<br>• GRID: The grid task was submitted through the internal Grid Task Submission Service. |
| ACTV | Activation Type | The type of activation:<br>• AUTO: The grid task was submitted for automatic activation.<br>• PEND: The grid task was submitted into the pending table. This is the only possibility for the TXTB source. |
| RSLT | Result | The result of the submission:<br>• SUCS: The grid task was submitted successfully.<br>• FAIL: The task has been moved directly to the historical table. |

#### IDEL: ILM Initiated Delete

This message is generated when ILM starts the process of deleting an object.

The IDEL message is generated in either of these situations:

- **For objects in compliant S3 buckets**: This message is generated when ILM starts the process of auto-

deleting an object because its retention period has expired (assuming the auto-delete setting is enabled and legal hold is off).

- **For objects in non-compliant S3 buckets or Swift containers**. This message is generated when ILM starts the process of deleting an object because no placement instructions in the active ILM policy currently apply to the object.

| Code | Field | Description |
|---|---|---|
| CBID | Content Block Identifier | The CBID of the object. |
| CMPA | Compliance: Auto delete | For objects in compliant S3 buckets only. 0 (false) or 1 (true), indicating whether a compliant object should be deleted automatically when its retention period ends, unless the bucket is under a legal hold. |
| CMPL | Compliance: Legal hold | For objects in compliant S3 buckets only. 0 (false) or 1 (true), indicating whether the bucket is currently under a legal hold. |
| CMPR | Compliance: Retention period | For objects in compliant S3 buckets only. The length of the object's retention period in minutes. |
| CTME | Compliance: Ingest time | For objects in compliant S3 buckets only. The object's ingest time. You can add the retention period in minutes to this value to determine when the object can be deleted from the bucket. |
| DMRK | Delete Marker Version ID | The version ID of the delete marker created when deleting an object from a versioned bucket. Operations on buckets do not include this field. |
| CSIZ | Content size | The size of the object in bytes. |
| LOCS | Locations | The storage location of object data within the StorageGRID system. The value for LOCS is "" if the object has no locations (for example, it has been deleted).<br><br>CLEC: for erasure-coded objects, the erasure coding profile ID and the erasure coding group ID that is applied to the object's data.<br><br>CLDI: for replicated objects, the LDR node ID and the volume ID of the object's location.<br><br>CLNL: ARC node ID of the object's location if the object data is archived. |
| PATH | S3 Bucket/Key or Swift Container/Object ID | The S3 bucket name and S3 key name, or the Swift container name and Swift object identifier. |
| RSLT | Result | The result of the ILM operation.<br><br>SUCS: The ILM operation was successful. |

| Code | Field | Description |
|---|---|---|
| RULE | Rules Label | • If an object in a compliant S3 bucket is being deleted automatically because its retention period has expired, this field is blank.<br>• If the object is being deleted because there are no more placement instructions that currently apply to the object, this field shows the human-readable label of the last ILM rule that applied to the object. |
| SGRP | Site (Group) | If present, the object was deleted at the site specified, which is not the site where the object was ingested. |
| UUID | Universally Unique Identifier | The identifier of the object within the StorageGRID system. |
| VSID | Version ID | The version ID of the specific version of an object that was deleted. Operations on buckets and objects in unversioned buckets do not include this field. |

#### LKCU: Overwritten Object Cleanup

This message is generated when StorageGRID removes an overwritten object that previously required cleanup to free up storage space. An object is overwritten when an S3 or Swift client writes an object to a path already containing a object. The removal process occurs automatically and in the background.

| Code | Field | Description |
|---|---|---|
| CSIZ | Content size | The size of the object in bytes. |
| LTYP | Type of cleanup | *Internal use only.* |
| LUID | Removed Object UUID | The identifier of the object that was removed. |
| PATH | S3 Bucket/Key or Swift Container/Object ID | The S3 bucket name and S3 key name, or the Swift container name and Swift object identifier. |
| SEGC | Container UUID | UUID of the container for the segmented object. This value is available only if the object is segmented. |
| UUID | Universally Unique Identifier | The identifier of the object that still exists. This value is available only if the object has not been deleted. |

#### LLST: Location Lost

This message is generated whenever a location for an object copy (replicated or erasure coded) cannot be found.

| Code | Field | Description |
|---|---|---|
| CBIL | CBID | The affected CBID. |
| NOID | Source Node ID | The node ID on which the locations were lost. |
| UUID | Universally Unique ID | The identifier of the affected object in the StorageGRID system. |
| ECPR | Erasure Coding Profile | For erasure-coded object data. The ID of the Erasure Coding profile used. |
| LTYP | Location Type | CLDI (Online): For replicated object data<br><br>CLEC (Online): For erasure-coded object data<br><br>CLNL (Nearline): For archived replicated object data |
| PCLD | Path to replicated object | The complete path to the disk location of the lost object data. Only returned when LTYP has a value of CLDI (that is, for replicated objects).<br><br>Takes the form `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@` |
| RSLT | Result | Always NONE. RSLT is a mandatory message field, but is not relevant for this message. NONE is used rather than SUCS so that this message is not filtered. |
| TSRC | Triggering Source | USER: User triggered<br><br>SYST: System triggered |

**MGAU: Management audit message**

The Management category logs user requests to the Management API. Every request that is not a GET or HEAD request to the API logs a response with the username, IP, and type of request to the API.

| Code | Field | Description |
|---|---|---|
| MDIP | Destination IP Address | The server (destination) IP address. |
| MDNA | Domain name | The host domain name. |
| MPAT | Request PATH | The request path. |
| MPQP | Request query parameters | The query parameters for the request. |
| MRBD | Request body | The content of the request body. While the response body is logged by default, the request body is logged in certain cases when the response body is empty. Because the following information is not available in the response body, it is taken from the request body for the following POST methods:<br>• Username and account ID in **POST authorize**<br>• New subnets configuration in **POST /grid/grid-networks/update**<br>• New NTP servers in **POST /grid/ntp-servers/update**<br>• Decommissioned server IDs in **POST /grid/servers/decommission**<br>**Note:** Sensitive information is either deleted (for example, an S3 access key) or masked with asterisks (for example, a password). |

| Code | Field | Description |
|---|---|---|
| MRMD | Request method | The HTTP request method:<br>• POST<br>• PUT<br>• DELETE<br>• PATCH |
| MRSC | Response code | The response code. |
| MRSP | Response body | The content of the response (the response body) is logged by default.<br>**Note:** Sensitive information is either deleted (for example, an S3 access key) or masked with asterisks (for example, a password). |
| MSIP | Source IP address | The client (source) IP address. |
| MUUN | User URN | The URN (uniform resource name) of the user who sent the request. |
| RSLT | Result | Returns successful (SUCS) or the error reported by the backend. |

#### OLST: System Detected Lost Object

This message is generated when the DDS service cannot locate any copies of an object within the StorageGRID system.

| Code | Field | Description |
|---|---|---|
| CBID | Content Block Identifier | The CBID of the lost object. |
| NOID | Node ID | If available, the last known direct or nearline location of the lost object. It is possible to have just the Node ID without a Volume ID if the volume information is not available. |
| PATH | S3 Bucket/Key or Swift Container/Object ID | If available, the S3 bucket name and S3 key name, or the Swift container name and Swift object identifier. |

| Code | Field | Description |
| --- | --- | --- |
| RSLT | Result | This field has the value NONE. RSLT is a mandatory message field, but is not relevant for this message. NONE is used rather than SUCS so that this message is not filtered. |
| UUID | Universally Unique ID | The identifier of the lost object within the StorageGRID system. |
| VOLI | Volume ID | If available, the Volume ID of the Storage Node or Archive Node for the last known location of the lost object. |

#### ORLM: Object Rules Met

This message is generated when the object is successfully stored and copied as specified by the ILM rules.

> The ORLM message is not generated when an object is successfully stored by the default Make 2 Copies rule if another rule in the policy uses the Object Size advanced filter.

| Code | Field | Description |
| --- | --- | --- |
| BUID | Bucket Header | Bucket ID field. Used for internal operations. Appears only if STAT is PRGD. |
| CBID | Content Block Identifier | The CBID of the object. |
| CSIZ | Content size | The size of the object in bytes. |
| LOCS | Locations | The storage location of object data within the StorageGRID system. The value for LOCS is "" if the object has no locations (for example, it has been deleted).<br><br>CLEC: for erasure-coded objects, the erasure coding profile ID and the erasure coding group ID that is applied to the object's data.<br><br>CLDI: for replicated objects, the LDR node ID and the volume ID of the object's location.<br><br>CLNL: ARC node ID of the object's location if the object data is archived. |

| Code | Field | Description |
| --- | --- | --- |
| PATH | S3 Bucket/Key or Swift Container/Object ID | The S3 bucket name and S3 key name, or the Swift container name and Swift object identifier. |
| RSLT | Result | The result of the ILM operation.<br><br>SUCS: The ILM operation was successful. |
| RULE | Rules Label | The human-readable label given to the ILM rule applied to this object. |
| SEGC | Container UUID | UUID of the container for the segmented object. This value is available only if the object is segmented. |
| SGCB | Container CBID | CBID of the container for the segmented object. This value is available only for segmented and multipart objects. |
| STAT | Status | The status of ILM operation.<br><br>DONE: ILM operations against the object have completed.<br><br>DFER: The object has been marked for future ILM re-evaluation.<br><br>PRGD: The object has been deleted from the StorageGRID system.<br><br>NLOC: The object data can no longer be found in the StorageGRID system. This status might indicate that all copies of object data are missing or damaged. |
| UUID | Universally Unique Identifier | The identifier of the object within the StorageGRID system. |

The ORLM audit message can be issued a number of times for a single object. For instance, it is issued whenever one of the following events take place:

- ILM rules for the object are satisfied forever.
- ILM rules for the object are satisfied for this epoch.
- ILM rules have deleted the object.
- The background verification process detects that a copy of replicated object data is corrupt. The StorageGRID system performs an ILM evaluation to replace the corrupt object.

**Related information**

- Object ingest transactions
- Object delete transactions

#### OVWR: Object Overwrite

This message is generated when an external (client-requested) operation causes one object to be overwritten by another object.

| Code | Field | Description |
|---|---|---|
| CBID | Content Block Identifier (new) | The CBID for the new object. |
| CSIZ | Previous Object Size | The size, in bytes, of the object being overwritten. |
| OCBD | Content Block Identifier (previous) | The CBID for the previous object. |
| UUID | Universally Unique ID (new) | The identifier of the new object within the StorageGRID system. |
| OUID | Universally Unique ID (previous) | The identifier for the previous object within the StorageGRID system. |
| PATH | S3 or Swift Object Path | The S3 or Swift object path used for both the previous and new object |
| RSLT | Result Code | Result of the Object Overwrite transaction. Result is always:<br><br>SUCS: Successful |
| SGRP | Site (Group) | If present, the overwritten object was deleted at the site specified, which is not the site where the overwritten object was ingested. |

#### SADD: Security Audit Disable

This message indicates that the originating service (node ID) has turned off audit message logging; audit messages are no longer being collected or delivered.

| Code | Field | Description |
|---|---|---|
| AETM | Enable Method | The method used to disable the audit. |
| AEUN | User Name | The user name that executed the command to disable audit logging. |

| Code | Field | Description |
|---|---|---|
| RSLT | Result | This field has the value NONE. RSLT is a mandatory message field, but is not relevant for this message. NONE is used rather than SUCS so that this message is not filtered. |

The message implies that logging was previously enabled, but has now been disabled. This is typically used only during bulk ingest to improve system performance. Following the bulk activity, auditing is restored (SADE) and the capability to disable auditing is then permanently blocked.

#### SADE: Security Audit Enable

This message indicates that the originating service (node ID) has restored audit message logging; audit messages are again being collected and delivered.

| Code | Field | Description |
|---|---|---|
| AETM | Enable Method | The method used to enable the audit. |
| AEUN | User Name | The user name that executed the command to enable audit logging. |
| RSLT | Result | This field has the value NONE. RSLT is a mandatory message field, but is not relevant for this message. NONE is used rather than SUCS so that this message is not filtered. |

The message implies that logging was previously disabled (SADD), but has now been restored. This is typically only used during bulk ingest to improve system performance. Following the bulk activity, auditing is restored and the capability to disable auditing is then permanently blocked.

#### SCMT: Object Store Commit

Grid content is not made available or recognized as stored until it has been committed (meaning it has been stored persistently). Persistently stored content has been completely written to disk, and has passed related integrity checks. This message is issued when a content block is committed to storage.

| Code | Field | Description |
|---|---|---|
| CBID | Content Block Identifier | The unique identifier of the content block committed to permanent storage. |

| Code | Field | Description |
|---|---|---|
| RSLT | Result Code | Status at the time the object was stored to disk:<br><br>SUCS: Object successfully stored. |

This message means a given content block has been completely stored and verified, and can now be requested. It can be used to track data flow within the system.

#### SDEL: S3 DELETE

When an S3 client issues a DELETE transaction, a request is made to remove the specified object or bucket. This message is issued by the server if the transaction is successful.

| Code | Field | Description |
|---|---|---|
| CBID | Content Block Identifier | The unique identifier of the content block requested. If the CBID is unknown, this field is set to 0. Operations on buckets do not include this field. |
| CNCH | Consistency Control Header | The value of the Consistency-Control HTTP request header, if present in the request. |
| CNID | Connection Identifier | The unique system identifier for the TCP/IP connection. |
| CSIZ | Content Size | The size of the deleted object in bytes. Operations on buckets do not include this field. |
| DMRK | Delete Marker Version ID | The version ID of the delete marker created when deleting an object from a versioned bucket. Operations on buckets do not include this field. |
| HTRH | HTTP Request Header | List of logged HTTP request header names and values as selected during configuration.<br><br>**Note:** `X-Forwarded-For` is automatically included if it is present in the request and if the `X-Forwarded-For` value is different from the request sender IP address (SAIP audit field). |
| MTME | Last Modified Time | The Unix timestamp, in microseconds, indicating when the object was last modified. |
| RSLT | Result Code | Result of the DELETE transaction. Result is always:<br><br>SUCS: Successful |

| Code | Field | Description |
| --- | --- | --- |
| S3AI | S3 tenant account ID (request sender) | The tenant account ID of the user who sent the request. An empty value indicates anonymous access. |
| S3AK | S3 Access Key ID (request sender) | The hashed S3 access key ID for the user that sent the request. An empty value indicates anonymous access. |
| S3BK | S3 Bucket | The S3 bucket name. |
| S3KY | S3 Key | The S3 key name, not including the bucket name. Operations on buckets do not include this field. |
| S3SR | S3 Subresource | The bucket or object subresource being operated on, if applicable. |
| SACC | S3 tenant account name (request sender) | The name of the tenant account for the user who sent the request. Empty for anonymous requests. |
| SAIP | IP address (request sender) | The IP address of the client application that made the request. |
| SBAC | S3 tenant account name (bucket owner) | The tenant account name for the bucket owner. Used to identify cross-account or anonymous access. |
| SBAI | S3 tenant account ID (bucket owner) | The tenant account ID of the owner of the target bucket. Used to identify cross-account or anonymous access. |
| SGRP | Site (Group) | If present, the object was deleted at the site specified, which is not the site where the object was ingested. |
| SUSR | S3 User URN (request sender) | The tenant account ID and the user name of the user making the request. The user can either be a local user or an LDAP user. For example: `urn:sgws:identity::03393893651506583485:root`<br><br>Empty for anonymous requests. |
| TIME | Time | Total processing time for the request in microseconds. |
| TLIP | Trusted Load Balancer IP Address | If the request was routed by a trusted Layer 7 load balancer, the IP address of the load balancer. |

| Code | Field | Description |
|---|---|---|
| UUID | Universally Unique Identifier | The identifier of the object within the StorageGRID system. |
| VSID | Version ID | The version ID of the specific version of an object that was deleted. Operations on buckets and objects in unversioned buckets do not include this field. |

#### SGET: S3 GET

When an S3 client issues a GET transaction, a request is made to retrieve an object or list the objects in a bucket. This message is issued by the server if the transaction is successful.

| Code | Field | Description |
|---|---|---|
| CBID | Content Block Identifier | The unique identifier of the content block requested. If the CBID is unknown, this field is set to 0. Operations on buckets do not include this field. |
| CNCH | Consistency Control Header | The value of the Consistency-Control HTTP request header, if present in the request. |
| CNID | Connection Identifier | The unique system identifier for the TCP/IP connection. |
| CSIZ | Content Size | The size of the retrieved object in bytes. Operations on buckets do not include this field. |
| HTRH | HTTP Request Header | List of logged HTTP request header names and values as selected during configuration.<br><br>**Note:** `X-Forwarded-For` is automatically included if it is present in the request and if the `X-Forwarded-For` value is different from the request sender IP address (SAIP audit field). |

| Code | Field | Description |
| --- | --- | --- |
| RANG | Range Read | For range read operations only. Indicates the range of bytes that was read by this request. The value after the slash (/) shows the size of the entire object. |
| RSLT | Result Code | Result of the GET transaction. Result is always:<br><br>SUCS: Successful |
| S3AI | S3 tenant account ID (request sender) | The tenant account ID of the user who sent the request. An empty value indicates anonymous access. |
| S3AK | S3 Access Key ID (request sender) | The hashed S3 access key ID for the user that sent the request. An empty value indicates anonymous access. |
| S3BK | S3 Bucket | The S3 bucket name. |
| S3KY | S3 Key | The S3 key name, not including the bucket name. Operations on buckets do not include this field. |
| S3SR | S3 Subresource | The bucket or object subresource being operated on, if applicable. |
| SACC | S3 tenant account name (request sender) | The name of the tenant account for the user who sent the request. Empty for anonymous requests. |
| SAIP | IP address (request sender) | The IP address of the client application that made the request. |
| SBAC | S3 tenant account name (bucket owner) | The tenant account name for the bucket owner. Used to identify cross-account or anonymous access. |
| SBAI | S3 tenant account ID (bucket owner) | The tenant account ID of the owner of the target bucket. Used to identify cross-account or anonymous access. |

| Code | Field | Description |
| --- | --- | --- |
| SUSR | S3 User URN (request sender) | The tenant account ID and the user name of the user making the request. The user can either be a local user or an LDAP user. For example: `urn:sgws:identity::03393893651506583485:root`<br><br>Empty for anonymous requests. |
| TIME | Time | Total processing time for the request in microseconds. |
| TLIP | Trusted Load Balancer IP Address | If the request was routed by a trusted Layer 7 load balancer, the IP address of the load balancer. |
| UUID | Universally Unique Identifier | The identifier of the object within the StorageGRID system. |
| VSID | Version ID | The version ID of the specific version of an object that was requested. Operations on buckets and objects in unversioned buckets do not include this field. |

#### SHEA: S3 HEAD

When an S3 client issues a HEAD transaction, a request is made to check for the existence of an object or bucket and retrieve the metadata about an object. This message is issued by the server if the transaction is successful.

| Code | Field | Description |
| --- | --- | --- |
| CBID | Content Block Identifier | The unique identifier of the content block requested. If the CBID is unknown, this field is set to 0. Operations on buckets do not include this field. |
| CNID | Connection Identifier | The unique system identifier for the TCP/IP connection. |
| CSIZ | Content Size | The size of the checked object in bytes. Operations on buckets do not include this field. |

| Code | Field | Description |
| --- | --- | --- |
| HTRH | HTTP Request Header | List of logged HTTP request header names and values as selected during configuration.<br><br>**Note:** `X-Forwarded-For` is automatically included if it is present in the request and if the `X-Forwarded-For` value is different from the request sender IP address (SAIP audit field). |
| RSLT | Result Code | Result of the GET transaction. Result is always:<br><br>SUCS: Successful |
| S3AI | S3 tenant account ID (request sender) | The tenant account ID of the user who sent the request. An empty value indicates anonymous access. |
| S3AK | S3 Access Key ID (request sender) | The hashed S3 access key ID for the user that sent the request. An empty value indicates anonymous access. |
| S3BK | S3 Bucket | The S3 bucket name. |
| S3KY | S3 Key | The S3 key name, not including the bucket name. Operations on buckets do not include this field. |
| SACC | S3 tenant account name (request sender) | The name of the tenant account for the user who sent the request. Empty for anonymous requests. |
| SAIP | IP address (request sender) | The IP address of the client application that made the request. |
| SBAC | S3 tenant account name (bucket owner) | The tenant account name for the bucket owner. Used to identify cross-account or anonymous access. |
| SBAI | S3 tenant account ID (bucket owner) | The tenant account ID of the owner of the target bucket. Used to identify cross-account or anonymous access. |

| Code | Field | Description |
| --- | --- | --- |
| SUSR | S3 User URN (request sender) | The tenant account ID and the user name of the user making the request. The user can either be a local user or an LDAP user. For example: `urn:sgws:identity::03393893651506583485:root`<br><br>Empty for anonymous requests. |
| TIME | Time | Total processing time for the request in microseconds. |
| TLIP | Trusted Load Balancer IP Address | If the request was routed by a trusted Layer 7 load balancer, the IP address of the load balancer. |
| UUID | Universally Unique Identifier | The identifier of the object within the StorageGRID system. |
| VSID | Version ID | The version ID of the specific version of an object that was requested. Operations on buckets and objects in unversioned buckets do not include this field. |

#### SPOS: S3 POST

When an S3 client issues a POST Object request, this message is issued by the server if the transaction is successful.

| Code | Field | Description |
| --- | --- | --- |
| CBID | Content Block Identifier | The unique identifier of the content block requested. If the CBID is unknown, this field is set to 0. |
| CNCH | Consistency Control Header | The value of the Consistency-Control HTTP request header, if present in the request. |
| CNID | Connection Identifier | The unique system identifier for the TCP/IP connection. |
| CSIZ | Content Size | The size of the retrieved object in bytes. |

| Code | Field | Description |
| --- | --- | --- |
| HTRH | HTTP Request Header | List of logged HTTP request header names and values as selected during configuration.<br><br>**Note:** `X-Forwarded-For` is automatically included if it is present in the request and if the `X-Forwarded-For` value is different from the request sender IP address (SAIP audit field). |
| RSLT | Result Code | Result of the POST Object restore request. Result is always:<br><br>SUCS: Successful |
| S3AI | S3 tenant account ID (request sender) | The tenant account ID of the user who sent the request. An empty value indicates anonymous access. |
| S3AK | S3 Access Key ID (request sender) | The hashed S3 access key ID for the user that sent the request. An empty value indicates anonymous access. |
| S3BK | S3 Bucket | The S3 bucket name. |
| S3KY | S3 Key | The S3 key name, not including the bucket name. Operations on buckets do not include this field. |
| S3SR | S3 Subresource | The bucket or object subresource being operated on, if applicable.<br><br>Set to “select” for an S3 Select operation. |
| SACC | S3 tenant account name (request sender) | The name of the tenant account for the user who sent the request. Empty for anonymous requests. |
| SAIP | IP address (request sender) | The IP address of the client application that made the request. |
| SBAC | S3 tenant account name (bucket owner) | The tenant account name for the bucket owner. Used to identify cross-account or anonymous access. |

| Code | Field | Description |
| --- | --- | --- |
| SBAI | S3 tenant account ID (bucket owner) | The tenant account ID of the owner of the target bucket. Used to identify cross-account or anonymous access. |
| SRCF | Subresource Configuration | Restore information. |
| SUSR | S3 User URN (request sender) | The tenant account ID and the user name of the user making the request. The user can either be a local user or an LDAP user. For example: `urn:sgws:identity::03393893651506583485:root`<br><br>Empty for anonymous requests. |
| TIME | Time | Total processing time for the request in microseconds. |
| TLIP | Trusted Load Balancer IP Address | If the request was routed by a trusted Layer 7 load balancer, the IP address of the load balancer. |
| UUID | Universally Unique Identifier | The identifier of the object within the StorageGRID system. |
| VSID | Version ID | The version ID of the specific version of an object that was requested. Operations on buckets and objects in unversioned buckets do not include this field. |

#### SPUT: S3 PUT

When an S3 client issues a PUT transaction, a request is made to create a new object or bucket. This message is issued by the server if the transaction is successful.

| Code | Field | Description |
| --- | --- | --- |
| CBID | Content Block Identifier | The unique identifier of the content block requested. If the CBID is unknown, this field is set to 0. Operations on buckets do not include this field. |

| Code | Field | Description |
| --- | --- | --- |
| CMPS | Compliance Settings | The compliance settings used when creating the bucket, if present in the PUT Bucket request (truncated to the first 1024 characters) |
| CNCH | Consistency Control Header | The value of the Consistency-Control HTTP request header, if present in the request. |
| CNID | Connection Identifier | The unique system identifier for the TCP/IP connection. |
| CSIZ | Content Size | The size of the retrieved object in bytes. Operations on buckets do not include this field. |
| HTRH | HTTP Request Header | List of logged HTTP request header names and values as selected during configuration.<br><br>**Note:** `X-Forwarded-For` is automatically included if it is present in the request and if the `X-Forwarded-For` value is different from the request sender IP address (SAIP audit field). |
| LKEN | Object Lock Enabled | Value of the request header `x-amz-bucket-object-lock-enabled`, if present in the PUT Bucket request. |
| LKLH | Object Lock Legal Hold | Value of the request header `x-amz-object-lock-legal-hold`, if present in the PUT Object request. |
| LKMD | Object Lock Retention Mode | Value of the request header `x-amz-object-lock-mode`, if present in the PUT Object request. |
| LKRU | Object Lock Retain Until Date | Value of the request header `x-amz-object-lock-retain-until-date`, if present in the PUT Object request. |

| Code | Field | Description |
| --- | --- | --- |
| MTME | Last Modified Time | The Unix timestamp, in microseconds, indicating when the object was last modified. |
| RSLT | Result Code | Result of the PUT transaction. Result is always:<br><br>SUCS: Successful |
| S3AI | S3 tenant account ID (request sender) | The tenant account ID of the user who sent the request. An empty value indicates anonymous access. |
| S3AK | S3 Access Key ID (request sender) | The hashed S3 access key ID for the user that sent the request. An empty value indicates anonymous access. |
| S3BK | S3 Bucket | The S3 bucket name. |
| S3KY | S3KY | The S3 key name, not including the bucket name. Operations on buckets do not include this field. |
| S3SR | S3 Subresource | The bucket or object subresource being operated on, if applicable. |
| SACC | S3 tenant account name (request sender) | The name of the tenant account for the user who sent the request. Empty for anonymous requests. |
| SAIP | IP address (request sender) | The IP address of the client application that made the request. |
| SBAC | S3 tenant account name (bucket owner) | The tenant account name for the bucket owner. Used to identify cross-account or anonymous access. |
| SBAI | S3 tenant account ID (bucket owner) | The tenant account ID of the owner of the target bucket. Used to identify cross-account or anonymous access. |
| SRCF | Subresource Configuration | The new subresource configuration (truncated to the first 1024 characters). |

| Code | Field | Description |
| --- | --- | --- |
| SUSR | S3 User URN (request sender) | The tenant account ID and the user name of the user making the request. The user can either be a local user or an LDAP user. For example: `urn:sgws:identity::03393893651506583485:root`<br><br>Empty for anonymous requests. |
| TIME | Time | Total processing time for the request in microseconds. |
| TLIP | Trusted Load Balancer IP Address | If the request was routed by a trusted Layer 7 load balancer, the IP address of the load balancer. |
| ULID | Upload ID | Included only in SPUT messages for Complete Multipart Upload operations. Indicates that all parts have been uploaded and assembled. |
| UUID | Universally Unique Identifier | The identifier of the object within the StorageGRID system. |
| VSID | Version ID | The version ID of a new object created in a versioned bucket. Operations on buckets and objects in unversioned buckets do not include this field. |
| VSST | Versioning State | The new versioning state of a bucket. Two states are used: "enabled" or "suspended." Operations on objects do not include this field. |

#### SREM: Object Store Remove

This message is issued when content is removed from persistent storage and is no longer accessible through regular APIs.

| Code | Field | Description |
| --- | --- | --- |
| CBID | Content Block Identifier | The unique identifier of the content block deleted from permanent storage. |

| Code | Field | Description |
|---|---|---|
| RSLT | Result Code | Indicates the result of the content removal operations. The only defined value is:<br><br>SUCS: Content removed from persistent storage |

This audit message means a given content block has been deleted from a node and can no longer be requested directly. The message can be used to track the flow of deleted content within the system.

#### SUPD: S3 Metadata Updated

This message is generated by the S3 API when an S3 client updates the metadata for an ingested object. The message is issued by the server if the metadata update is successful.

| Code | Field | Description |
|---|---|---|
| CBID | Content Block Identifier | The unique identifier of the content block requested. If the CBID is unknown, this field is set to 0. Operations on buckets do not include this field. |
| CNCH | Consistency Control Header | The value of the Consistency-Control HTTP request header, if present in the request, when updating a bucket's compliance settings. |
| CNID | Connection Identifier | The unique system identifier for the TCP/IP connection. |
| CSIZ | Content Size | The size of the retrieved object in bytes. Operations on buckets do not include this field. |
| HTRH | HTTP Request Header | List of logged HTTP request header names and values as selected during configuration.<br><br>**Note:** `X-Forwarded-For` is automatically included if it is present in the request and if the `X-Forwarded-For` value is different from the request sender IP address (SAIP audit field). |

| Code | Field | Description |
| --- | --- | --- |
| RSLT | Result Code | Result of the GET transaction. Result is always:<br><br>SUCS: successful |
| S3AI | S3 tenant account ID (request sender) | The tenant account ID of the user who sent the request. An empty value indicates anonymous access. |
| S3AK | S3 Access Key ID (request sender) | The hashed S3 access key ID for the user that sent the request. An empty value indicates anonymous access. |
| S3BK | S3 Bucket | The S3 bucket name. |
| S3KY | S3 Key | The S3 key name, not including the bucket name. Operations on buckets do not include this field. |
| SACC | S3 tenant account name (request sender) | The name of the tenant account for the user who sent the request. Empty for anonymous requests. |
| SAIP | IP address (request sender) | The IP address of the client application that made the request. |
| SBAC | S3 tenant account name (bucket owner) | The tenant account name for the bucket owner. Used to identify cross-account or anonymous access. |
| SBAI | S3 tenant account ID (bucket owner) | The tenant account ID of the owner of the target bucket. Used to identify cross-account or anonymous access. |
| SUSR | S3 User URN (request sender) | The tenant account ID and the user name of the user making the request. The user can either be a local user or an LDAP user. For example:<br>`urn:sgws:identity::03393893651506583485:root`<br><br>Empty for anonymous requests. |

| Code | Field | Description |
| --- | --- | --- |
| TIME | Time | Total processing time for the request in microseconds. |
| TLIP | Trusted Load Balancer IP Address | If the request was routed by a trusted Layer 7 load balancer, the IP address of the load balancer. |
| UUID | Universally Unique Identifier | The identifier of the object within the StorageGRID system. |
| VSID | Version ID | The version ID of the specific version of an object whose metadata was updated. Operations on buckets and objects in unversioned buckets do not include this field. |

#### SVRF: Object Store Verify Fail

This message is issued whenever a content block fails the verification process. Each time replicated object data is read from or written to disk, several verification and integrity checks are performed to ensure the data sent to the requesting user is identical to the data originally ingested into the system. If any of these checks fail, the system automatically quarantines the corrupt replicated object data to prevent it from being retrieved again.

| Code | Field | Description |
| --- | --- | --- |
| CBID | Content Block Identifier | The unique identifier of the content block which failed verification. |

| Code | Field | Description |
|---|---|---|
| RSLT | Result Code | Verification failure type:<br><br>CRCF: Cyclic redundancy check (CRC) failed.<br><br>HMAC: Hash-based message authentication code (HMAC) check failed.<br><br>EHSH: Unexpected encrypted content hash.<br><br>PHSH: Unexpected original content hash.<br><br>SEQC: Incorrect data sequence on disk.<br><br>PERR: Invalid structure of disk file.<br><br>DERR: Disk error.<br><br>FNAM: Bad file name. |

**Note:** This message should be monitored closely. Content verification failures can indicate attempts to tamper with content or impending hardware failures.

To determine what operation triggered the message, see the value of the AMID (Module ID) field. For example, an SVFY value indicates that the message was generated by the Storage Verifier module, that is, background verification, and STOR indicates that the message was triggered by content retrieval.

#### SVRU: Object Store Verify Unknown

The LDR service's Storage component continuously scans all copies of replicated object data in the object store. This message is issued when an unknown or unexpected copy of replicated object data is detected in the object store and moved to the quarantine directory.

| Code | Field | Description |
|---|---|---|
| FPTH | File Path | The file path of the unexpected object copy. |
| RSLT | Result | This field has the value 'NONE'. RSLT is a mandatory message field, but is not relevant for this message. 'NONE' is used rather than 'SUCS' so that this message is not filtered. |

**Note:** The SVRU: Object Store Verify Unknown audit message should be monitored closely. It means unexpected copies of object data were detected in the object store. This situation should be investigated immediately to determine how theses copies were created, because it can indicate attempts to tamper with content or impending hardware failures.

#### SYSD: Node Stop

When a service is stopped gracefully, this message is generated to indicate the shutdown was requested. Typically this message is sent only after a subsequent restart, because the audit message queue is not cleared prior to shutdown. Look for the SYST message, sent at the beginning of the shutdown sequence, if the service has not restarted.

| Code | Field | Description |
|---|---|---|
| RSLT | Clean Shutdown | The nature of the shutdown:<br><br>SUCS: System was cleanly shutdown. |

The message does not indicate if the host server is being stopped, only the reporting service. The RSLT of a SYSD cannot indicate a "dirty" shutdown, because the message is generated only by "clean" shutdowns.

#### SYST: Node Stopping

When a service is gracefully stopped, this message is generated to indicate the shutdown was requested and that the service has initiated its shutdown sequence. SYST can be used to determine if the shutdown was requested, before the service is restarted (unlike SYSD, which is typically sent after the service restarts.)

| Code | Field | Description |
|---|---|---|
| RSLT | Clean Shutdown | The nature of the shutdown:<br><br>SUCS: System was cleanly shutdown. |

The message does not indicate if the host server is being stopped, only the reporting service. The RSLT code of a SYST message cannot indicate a "dirty" shutdown, because the message is generated only by "clean" shutdowns.

#### SYSU: Node Start

When a service is restarted, this message is generated to indicate if the previous shutdown was clean (commanded) or disorderly (unexpected).

| Code | Field | Description |
|---|---|---|
| RSLT | Clean Shutdown | The nature of the shutdown:<br><br>SUCS: System was cleanly shut down.<br><br>DSDN: System was not cleanly shut down.<br><br>VRGN: System was started for the first time after server installation (or re-installation). |

The message does not indicate if the host server was started, only the reporting service. This message can be used to:

- Detect discontinuity in the audit trail.
- Determine if a service is failing during operation (as the distributed nature of the StorageGRID system can mask these failures). Server Manager restarts a failed service automatically.

#### VLST: User Initiated Volume Lost

This message is issued whenever the `/proc/CMSI/Volume_Lost` command is run.

| Code | Field | Description |
|---|---|---|
| VOLL | Volume Identifier Lower | The lower end of the affected volume range or a single volume. |
| VOLU | Volume Identifier Upper | The upper end of the affected volume range. Equal to VOLL if a single volume. |
| NOID | Source Node ID | The node ID on which the locations were lost. |
| LTYP | Location Type | 'CLDI' (Online) or 'CLNL' (Nearline). If not specified, defaults to 'CLDI'. |
| RSLT | Result | Always 'NONE'. RSLT is a mandatory message field, but is not relevant for this message. 'NONE' is used rather than 'SUCS' so that this message is not filtered. |

#### WDEL: Swift DELETE

When a Swift client issues a DELETE transaction, a request is made to remove the

specified object or container. This message is issued by the server if the transaction is successful.

| Code | Field | Description |
|---|---|---|
| CBID | Content Block Identifier | The unique identifier of the content block requested. If the CBID is unknown, this field is set to 0. Operations on containers do not include this field. |
| CSIZ | Content Size | The size of the deleted object in bytes. Operations on containers do not include this field. |
| HTRH | HTTP Request Header | List of logged HTTP request header names and values as selected during configuration.<br><br>**Note:** `X-Forwarded-For` is automatically included if it is present in the request and if the `X-Forwarded-For` value is different from the request sender IP address (SAIP audit field). |
| MTME | Last Modified Time | The Unix timestamp, in microseconds, indicating when the object was last modified. |
| RSLT | Result Code | Result of the DELETE transaction. Result is always:<br><br>SUCS: Successful |
| SAIP | IP address of requesting client | The IP address of the client application that made the request. |
| SGRP | Site (Group) | If present, the object was deleted at the site specified, which is not the site where the object was ingested. |
| TIME | Time | Total processing time for the request in microseconds. |
| TLIP | Trusted Load Balancer IP Address | If the request was routed by a trusted Layer 7 load balancer, the IP address of the load balancer. |
| UUID | Universally Unique Identifier | The identifier of the object within the StorageGRID system. |
| WACC | Swift Account ID | The unique account ID as specified by the StorageGRID system. |
| WCON | Swift Container | The Swift container name. |
| WOBJ | Swift Object | The Swift object identifier. Operations on containers do not include this field. |

| Code | Field | Description |
| --- | --- | --- |
| WUSR | Swift Account User | The Swift account username that uniquely identifies the client performing the transaction. |

#### WGET: Swift GET

When a Swift client issues a GET transaction, a request is made to retrieve an object, list the objects in a container, or list the containers in an account. This message is issued by the server if the transaction is successful.

| Code | Field | Description |
| --- | --- | --- |
| CBID | Content Block Identifier | The unique identifier of the content block requested. If the CBID is unknown, this field is set to 0. Operations on accounts and containers do not include this field. |
| CSIZ | Content Size | The size of the retrieved object in bytes. Operations on accounts and containers do not include this field. |
| HTRH | HTTP Request Header | List of logged HTTP request header names and values as selected during configuration.<br><br>**Note:** `X-Forwarded-For` is automatically included if it is present in the request and if the `X-Forwarded-For` value is different from the request sender IP address (SAIP audit field). |
| RSLT | Result Code | Result of the GET transaction. Result is always<br><br>SUCS: successful |
| SAIP | IP address of requesting client | The IP address of the client application that made the request. |
| TIME | Time | Total processing time for the request in microseconds. |
| TLIP | Trusted Load Balancer IP Address | If the request was routed by a trusted Layer 7 load balancer, the IP address of the load balancer. |

| Code | Field | Description |
| --- | --- | --- |
| UUID | Universally Unique Identifier | The identifier of the object within the StorageGRID system. |
| WACC | Swift Account ID | The unique account ID as specified by the StorageGRID system. |
| WCON | Swift Container | The Swift container name. Operations on accounts do not include this field. |
| WOBJ | Swift Object | The Swift object identifier. Operations on accounts and containers do not include this field. |
| WUSR | Swift Account User | The Swift account username that uniquely identifies the client performing the transaction. |

#### WHEA: Swift HEAD

When a Swift client issues a HEAD transaction, a request is made to check for the existence of an account, container, or object, and retrieve any relevant metadata. This message is issued by the server if the transaction is successful.

| Code | Field | Description |
| --- | --- | --- |
| CBID | Content Block Identifier | The unique identifier of the content block requested. If the CBID is unknown, this field is set to 0. Operations on accounts and containers do not include this field. |
| CSIZ | Content Size | The size of the retrieved object in bytes. Operations on accounts and containers do not include this field. |
| HTRH | HTTP Request Header | List of logged HTTP request header names and values as selected during configuration.<br><br>**Note:** `X-Forwarded-For` is automatically included if it is present in the request and if the `X-Forwarded-For` value is different from the request sender IP address (SAIP audit field). |

| Code | Field | Description |
| --- | --- | --- |
| RSLT | Result Code | Result of the HEAD transaction. Result is always:<br><br>SUCS: successful |
| SAIP | IP address of requesting client | The IP address of the client application that made the request. |
| TIME | Time | Total processing time for the request in microseconds. |
| TLIP | Trusted Load Balancer IP Address | If the request was routed by a trusted Layer 7 load balancer, the IP address of the load balancer. |
| UUID | Universally Unique Identifier | The identifier of the object within the StorageGRID system. |
| WACC | Swift Account ID | The unique account ID as specified by the StorageGRID system. |
| WCON | Swift Container | The Swift container name. Operations on accounts do not include this field. |
| WOBJ | Swift Object | The Swift object identifier. Operations on accounts and containers do not include this field. |
| WUSR | Swift Account User | The Swift account username that uniquely identifies the client performing the transaction. |

#### WPUT: Swift PUT

When a Swift client issues a PUT transaction, a request is made to create a new object or container. This message is issued by the server if the transaction is successful.

| Code | Field | Description |
| --- | --- | --- |
| CBID | Content Block Identifier | The unique identifier of the content block requested. If the CBID is unknown, this field is set to 0. Operations on containers do not include this field. |

| Code | Field | Description |
| --- | --- | --- |
| CSIZ | Content Size | The size of the retrieved object in bytes. Operations on containers do not include this field. |
| HTRH | HTTP Request Header | List of logged HTTP request header names and values as selected during configuration.<br><br>**Note:** `X-Forwarded-For` is automatically included if it is present in the request and if the `X-Forwarded-For` value is different from the request sender IP address (SAIP audit field). |
| MTME | Last Modified Time | The Unix timestamp, in microseconds, indicating when the object was last modified. |
| RSLT | Result Code | Result of the PUT transaction. Result is always:<br><br>SUCS: successful |
| SAIP | IP address of requesting client | The IP address of the client application that made the request. |
| TIME | Time | Total processing time for the request in microseconds. |
| TLIP | Trusted Load Balancer IP Address | If the request was routed by a trusted Layer 7 load balancer, the IP address of the load balancer. |
| UUID | Universally Unique Identifier | The identifier of the object within the StorageGRID system. |
| WACC | Swift Account ID | The unique account ID as specified by the StorageGRID system. |
| WCON | Swift Container | The Swift container name. |
| WOBJ | Swift Object | The Swift object identifier. Operations on containers do not include this field. |

| Code | Field | Description |
| --- | --- | --- |
| WUSR | Swift Account User | The Swift account username that uniquely identifies the client performing the transaction. |

**Copyright information**

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

**Trademark information**

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.