Information you should monitor regularly

StorageGRID 11.5

NetApp
January 04, 2024

Table of Contents

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. This section contains the following sub-sections:

- Monitoring system health
- Monitoring storage capacity
- Monitoring information lifecycle management
- Monitoring performance, networking, and system resources
- Monitoring tenant activity
- Monitoring archival capacity
- Monitoring load balancing operations
- Applying hotfixes or upgrading software if necessary

What to monitor	Frequency
The system health data shown on the Grid Manager DashboardNote 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
Performance, networking, and system resources: • Query latency • Connectivity and networking • 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

Monitoring system health

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

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.

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.

Link	Indicates
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. **Note:** While the legacy alarm system continues to be supported, the alert system offers significant benefits and is easier to use.
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

Setting up email notifications for alerts

Using SNMP monitoring

Monitoring 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 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.

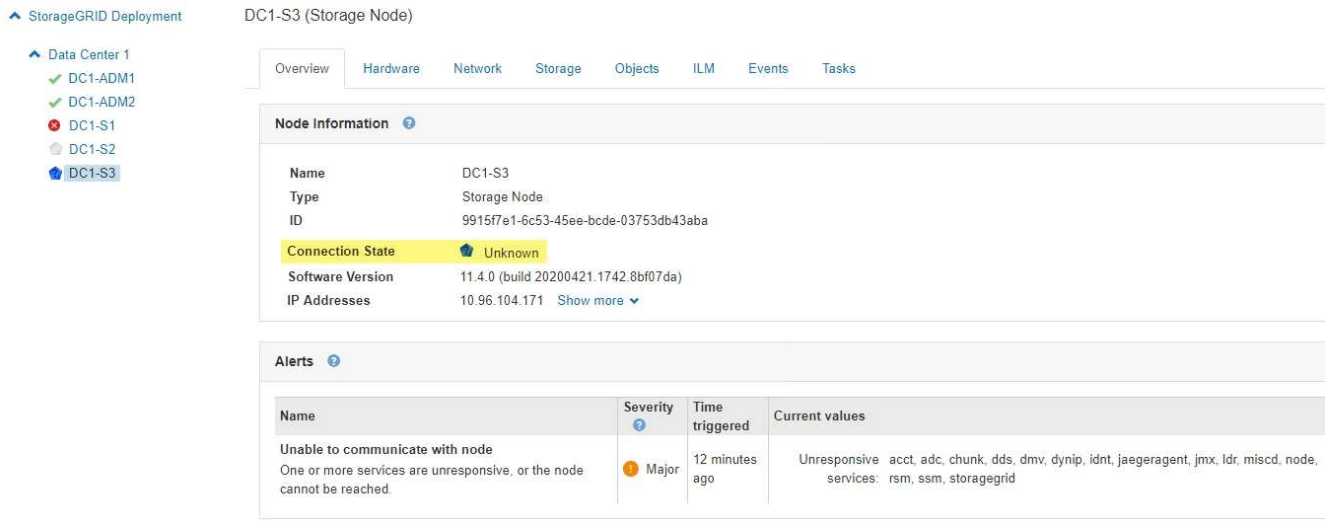
Steps

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

Maintain & recover

Viewing 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.

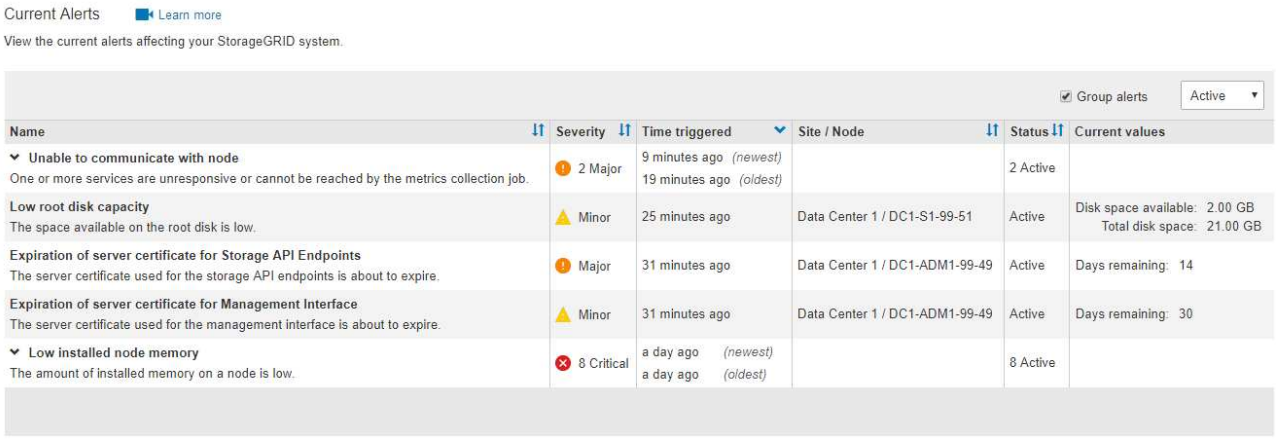
What you'll need

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

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.

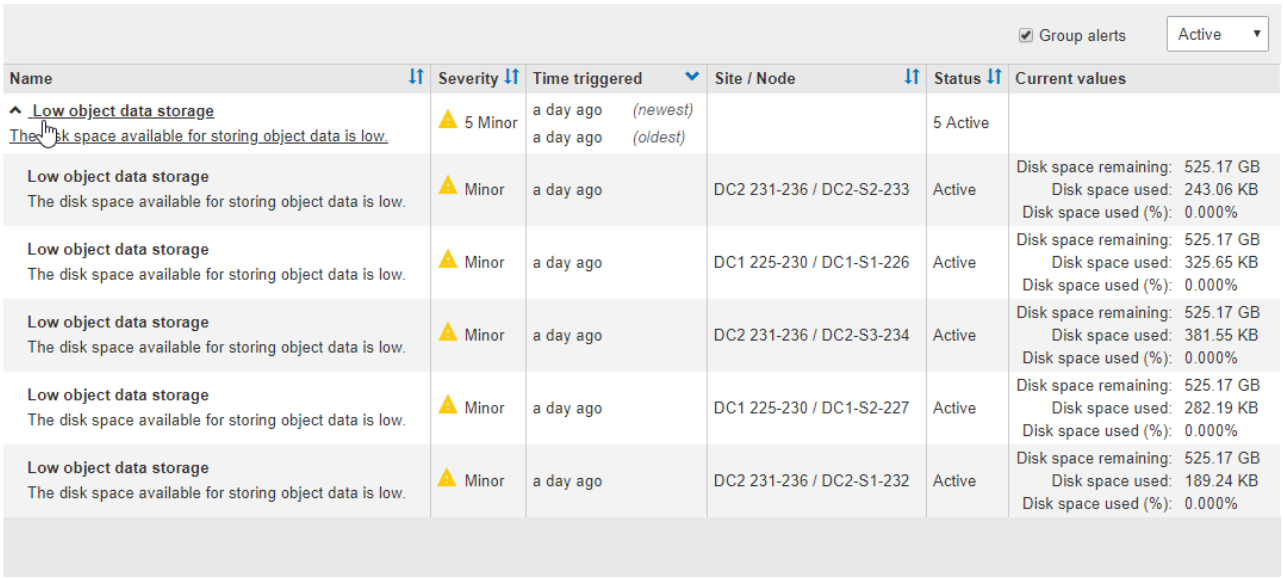
       The Current Alerts page is refreshed every two minutes.

2. Review the information in the table.

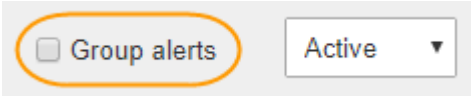
Column header	Description
Name	The name of the alert and its description.

Column header	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. • **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.
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. **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.
7. To view details for a specific alert, select the alert from the table.

   A dialog box for the alert appears. See the instructions for viewing a specific alert.

Related information

Viewing a specific alert

Silencing alert notifications

Viewing resolved alerts

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

What you'll need

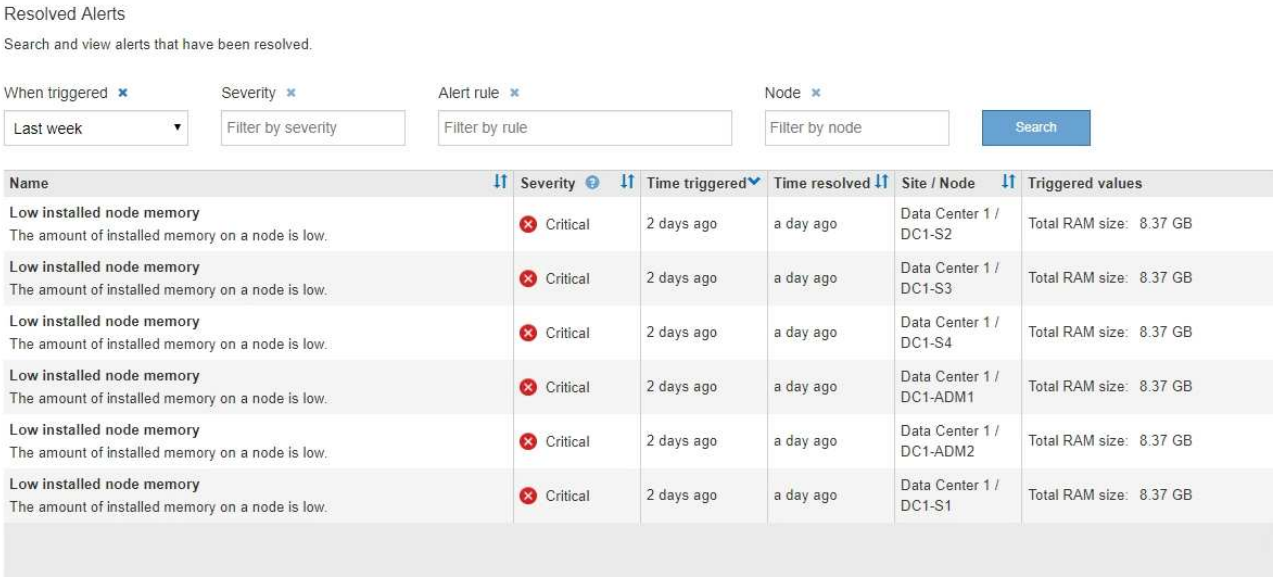
- You must be signed in to the Grid Manager using a supported browser.

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. • **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.
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 the instructions for viewing a specific alert.

Related information

Viewing a specific alert

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

Steps

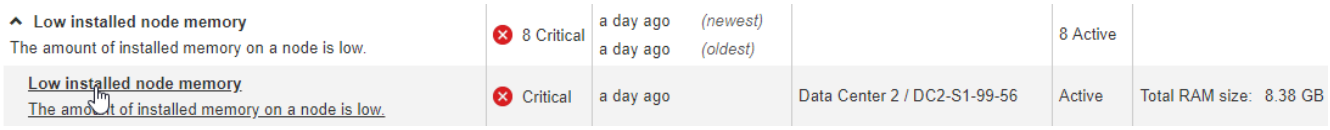
1. Do one of the following, based on whether you want to view a current or resolved alert:

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. • Select **Alerts** > **Current**. • 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.

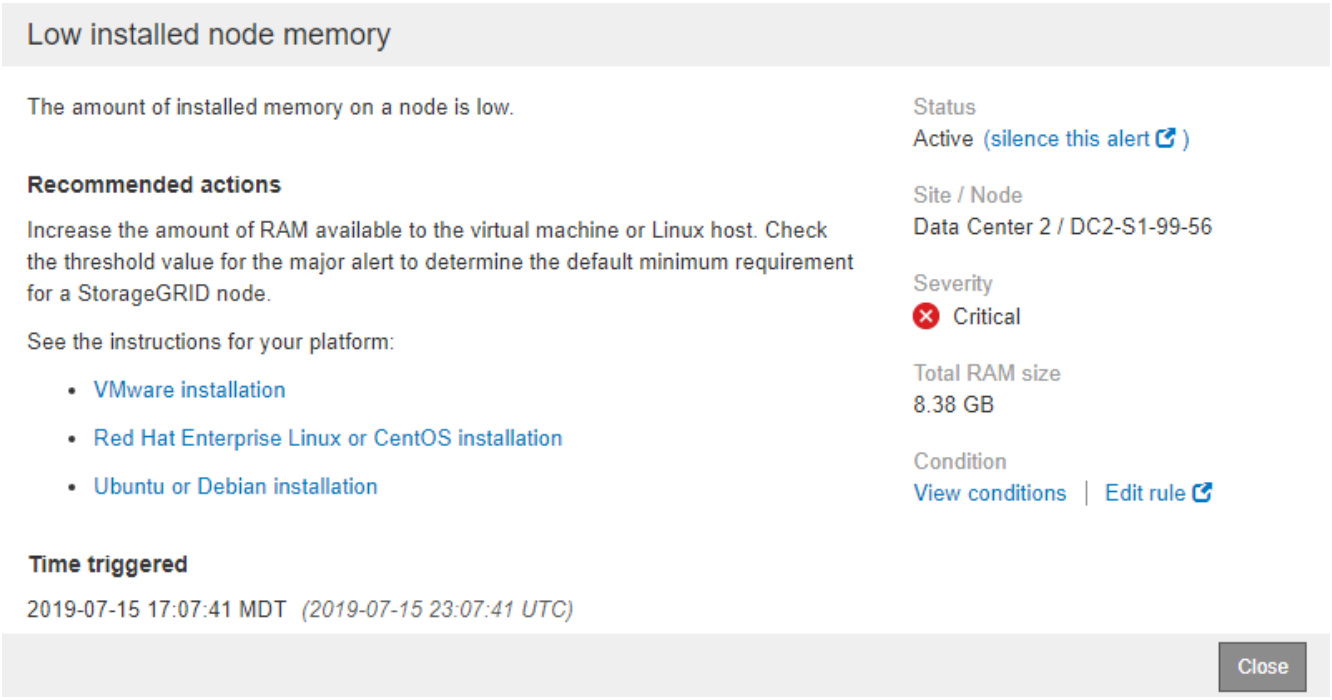
Column header	Description
Resolved alert	• From the Health panel on the Dashboard, click the **Recently resolved alerts** link. (This link appears only if one or more alerts were triggered in the past week and are now resolved. This link is hidden if no alerts were triggered and resolved in the last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

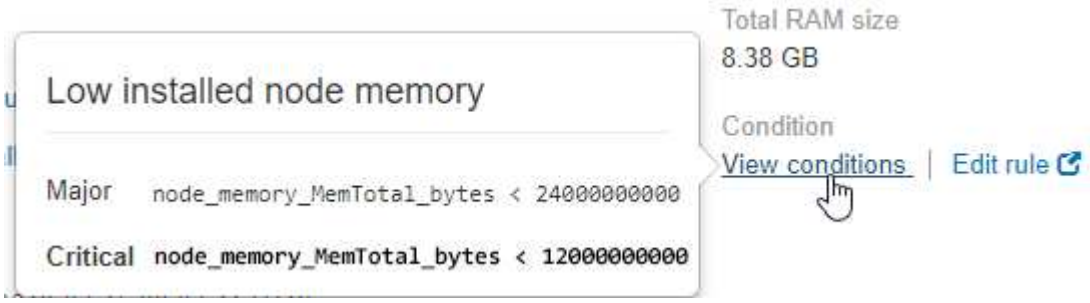
4. Optionally, click **silence this alert** to silence the alert rule that caused this alert to be triggered.

   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**.

Related information

Silencing alert notifications

Editing an alert rule

Viewing legacy alarms

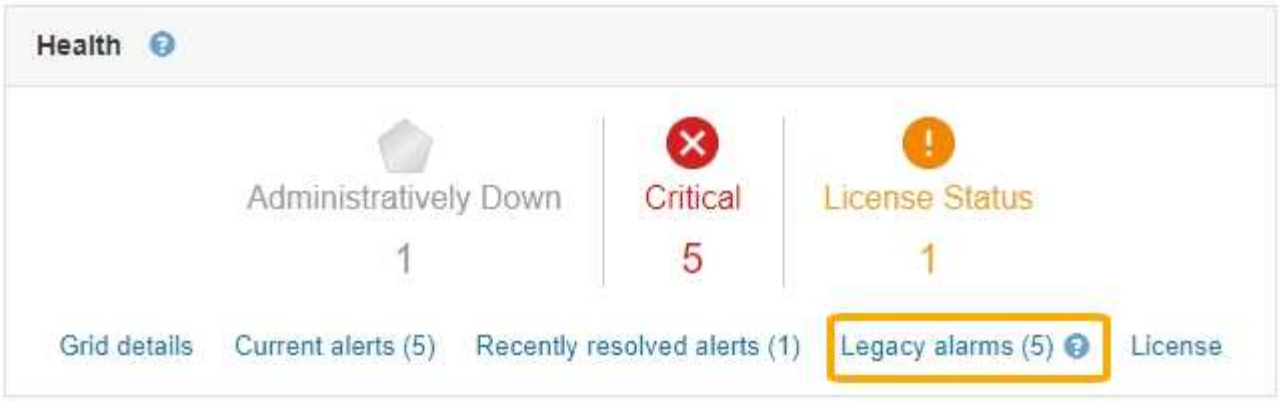
Alarms (legacy system) are triggered when system attributes reach alarm threshold values. You can view the currently active alarms from the Dashboard or the Current Alarms page.

What you'll need

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

About this task

If one or more of the legacy alarms are currently active, the Health panel on the Dashboard includes a **Legacy alarms** link. The number in parentheses indicates how many alarms are currently active.



The **Legacy alarms** count on the Dashboard is incremented whenever a legacy alarm is triggered. This count is incremented even if you have disabled alarm email notifications. You can typically ignore this number (since alerts provide a better view of the system), or you can view the alarms that are currently active.

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

Steps

1. To view the legacy alarms that are currently active, do one of the following:
   - From the Health panel on the Dashboard, click **Legacy alarms**. This link appears only if at least one alarm is currently active.
   - Select **Support** > **Alarms (legacy)** > **Current Alarms**. The Current Alarms page appears.

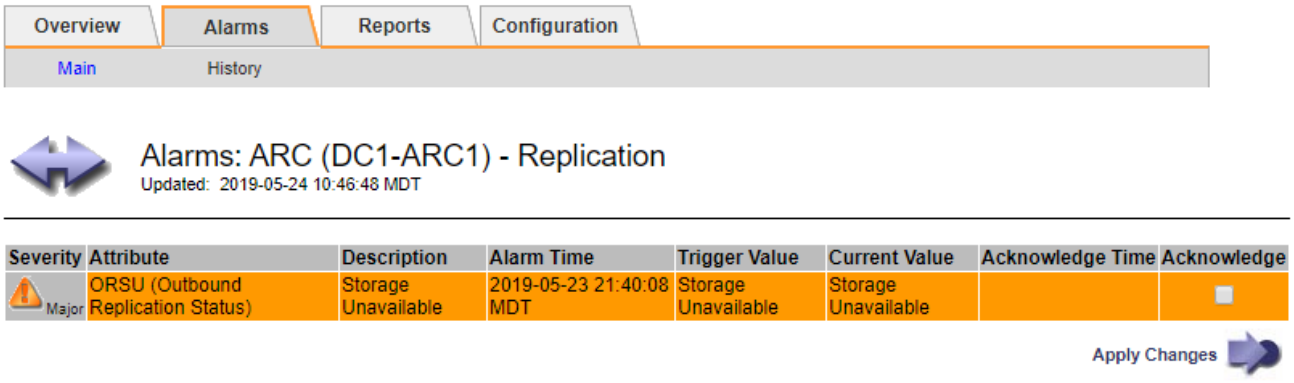
The alarm icon indicates the severity of each alarm, as follows:

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.

Icon	Color	Alarm severity	Meaning
	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)

Acknowledging current alarms (legacy system)

Disabling alarms (legacy system)

Monitoring storage capacity

You must monitor the total usable space available on Storage Nodes 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.

Related information

Viewing the Storage tab

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

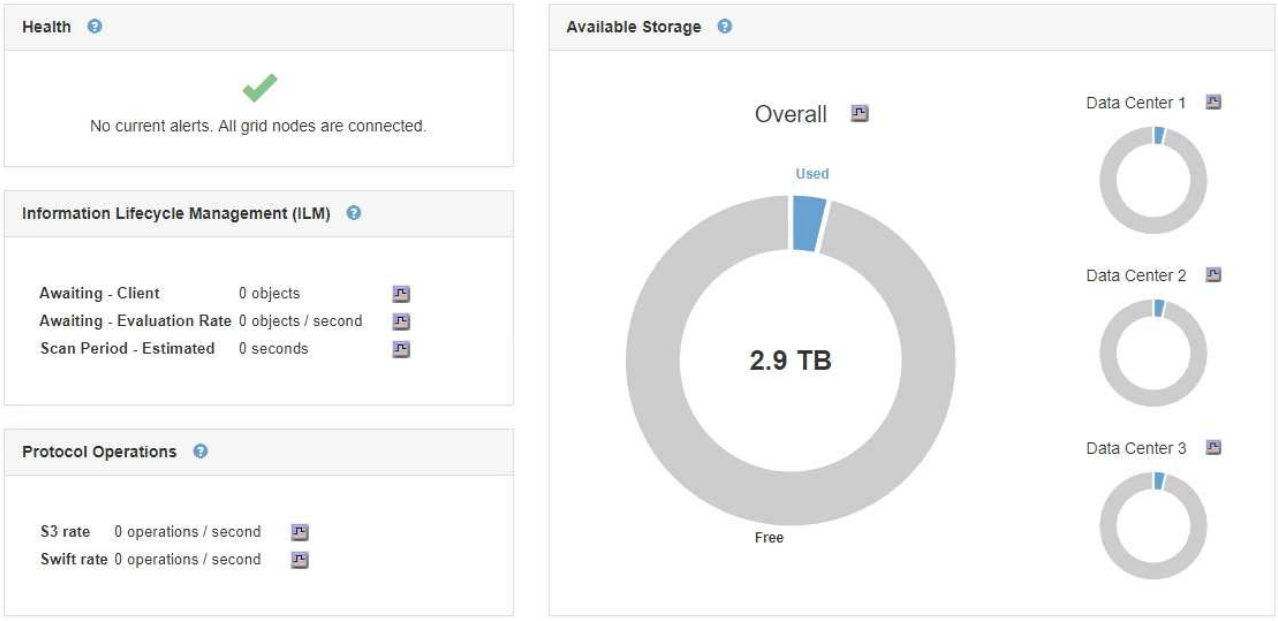
About this task

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.

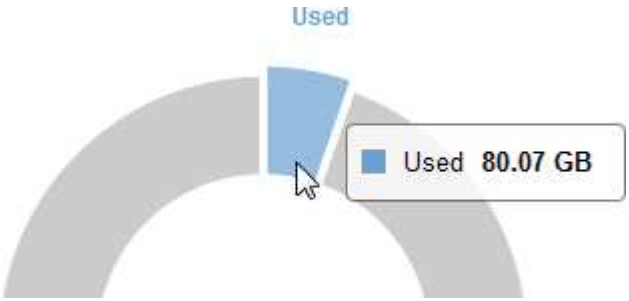
Steps

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.

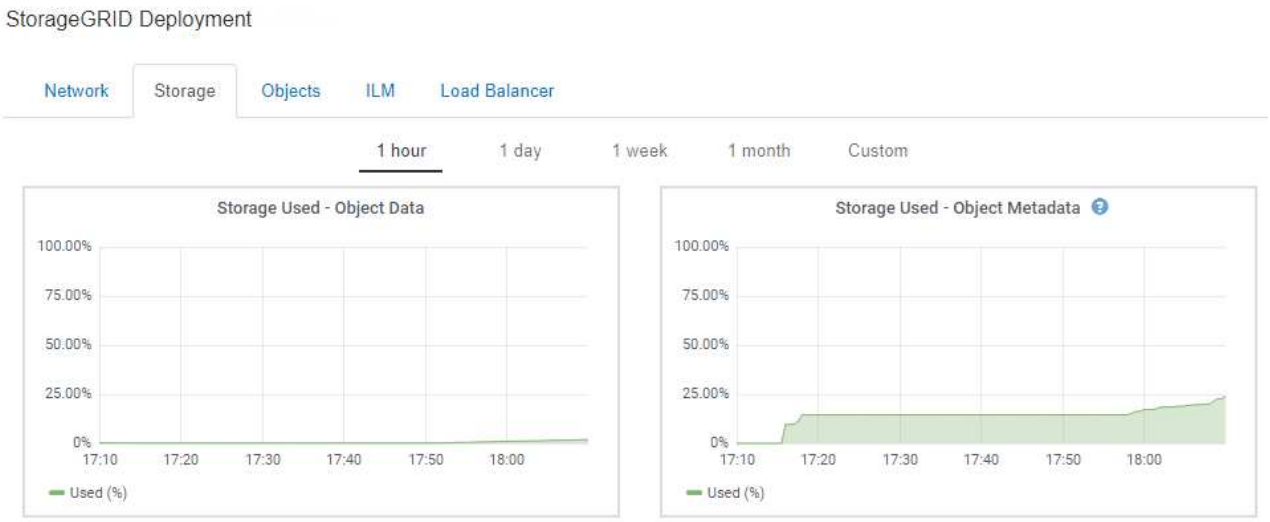
e. Click the chart icon for the overall chart or for an individual data center to view a graph showing capacity usage over time.

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**.

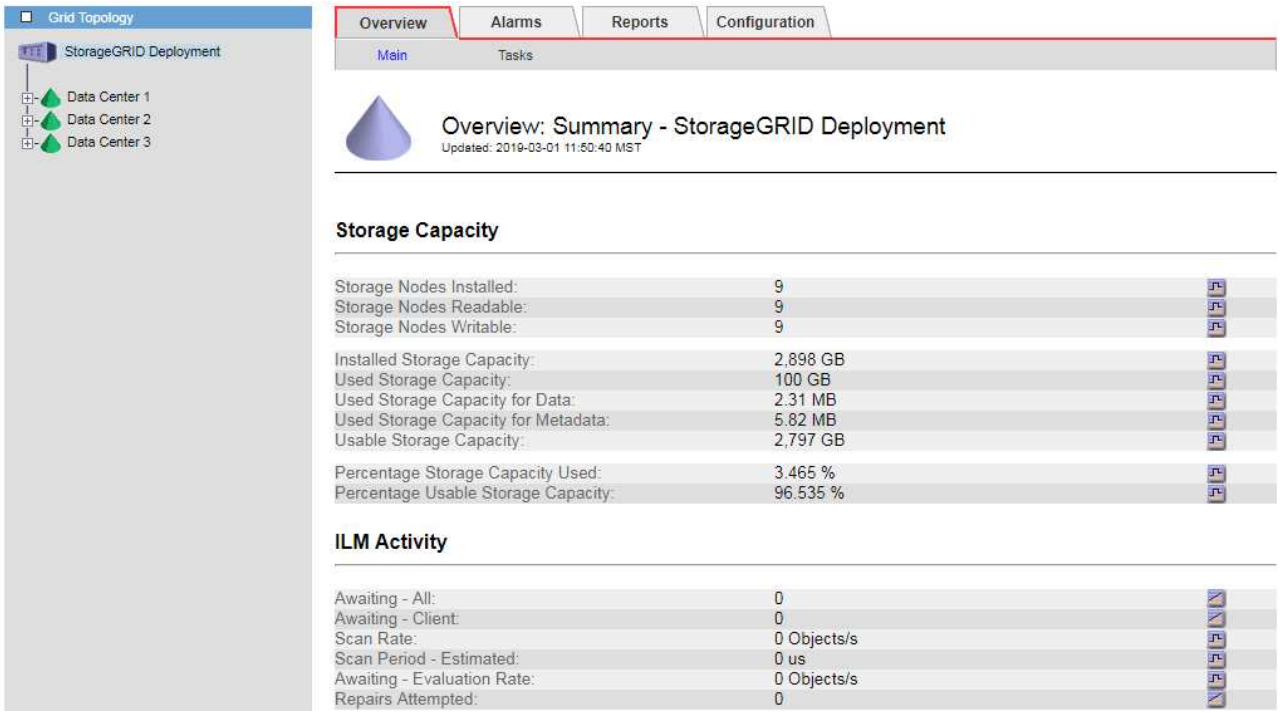
b. Select ***grid*** > **Storage**.



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. As directed by technical support, view additional details about the storage capacity for your grid.
   a. Select **Support** > **Tools** > **Grid Topology**.
   b. Select ***grid*** > **Overview** > **Main**.



4. 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.

Related information

Expand your grid

Monitoring storage capacity for each Storage Node

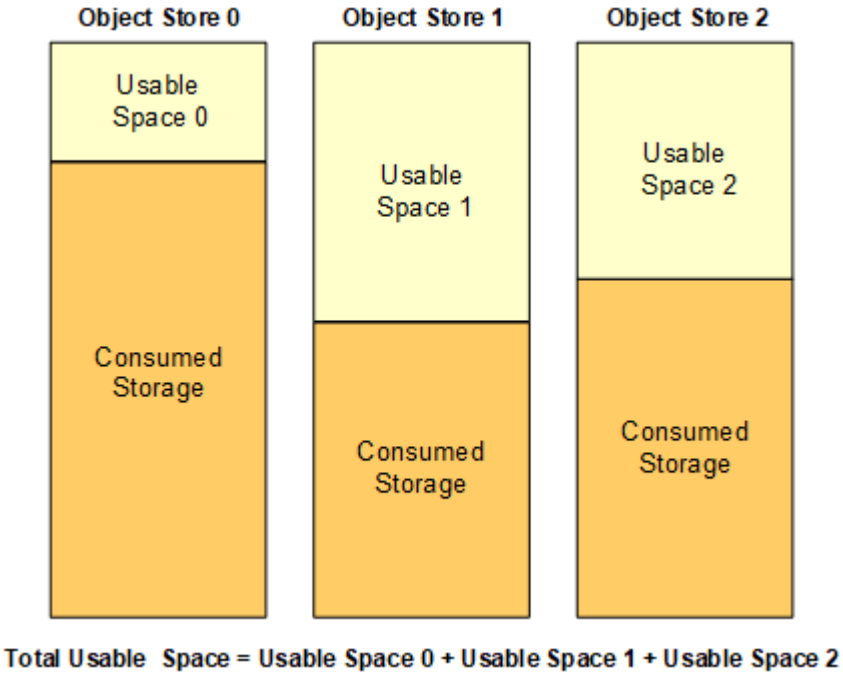
You must monitor the total usable space for each Storage Node to ensure that the node has enough space for new object data.

What you'll need

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

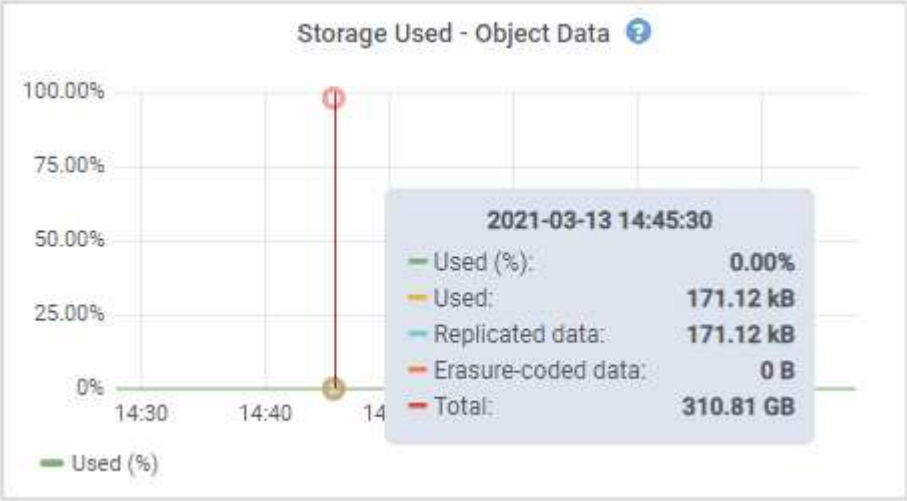
1. Select **Nodes** > ***Storage Node*** > **Storage**.

   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	0.03%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.85%	0 bytes/s	58 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	81 bytes/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	14.90 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.10 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 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	96.45 GB	250.90 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 and the legacy Storage Status (SSTS) alarm are triggered when insufficient space remains for storing object data on a Storage Node.

Related information

Administer StorageGRID

Troubleshooting the Low object data storage alert

Expand your grid

Monitoring object metadata capacity for each Storage Node

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

About this task

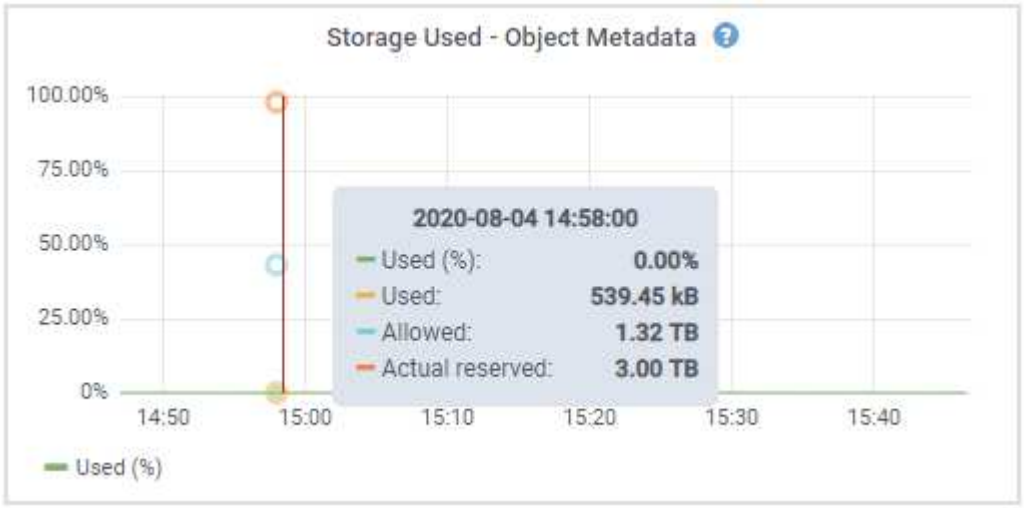
StorageGRID maintains three copies of object metadata at each site to provide redundancy and to protect object metadata from loss. The three copies are evenly distributed across all Storage Nodes at each site using the space reserved for metadata on storage volume 0 of each Storage Node.

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`

Value	Description	Prometheus metric
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.	`storagegrid_storage_utilization_metadata_reserved_bytes`

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.

Related information

Troubleshooting the Low metadata storage alert

Administer StorageGRID

Expand your grid

Monitoring 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 browser.

About this task

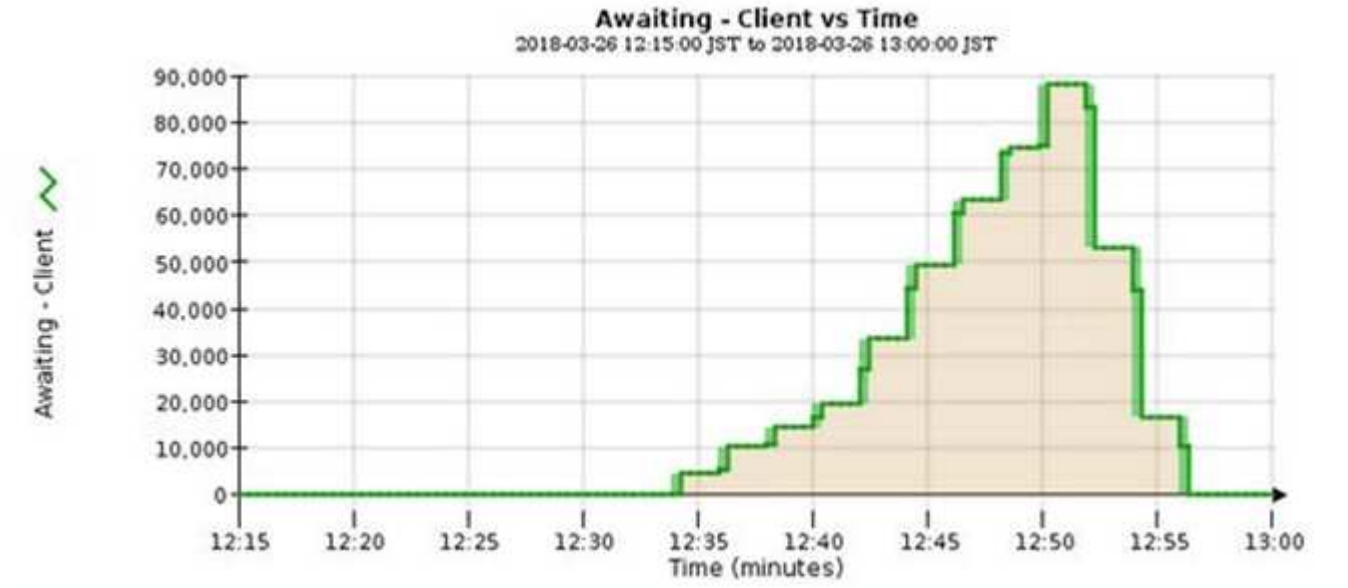
The StorageGRID system manages objects by applying the active ILM policy. The ILM policy and associated ILM rules determine how many copies are made, the type of copies that are created, where copies are placed, and the length of time each copy is retained.

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.

Monitoring performance, networking, and system resources

You should monitor performance, networking, and system resources to determine whether StorageGRID can handle its current load and to ensure that client performance does not degrade over time.

Monitoring query latency

Client actions such as storing, retrieving, or deleting objects create queries to the grid's distributed database of object metadata. You should monitor trends in query latency to ensure that grid resources are adequate for the current load.

What you'll need

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

About this task

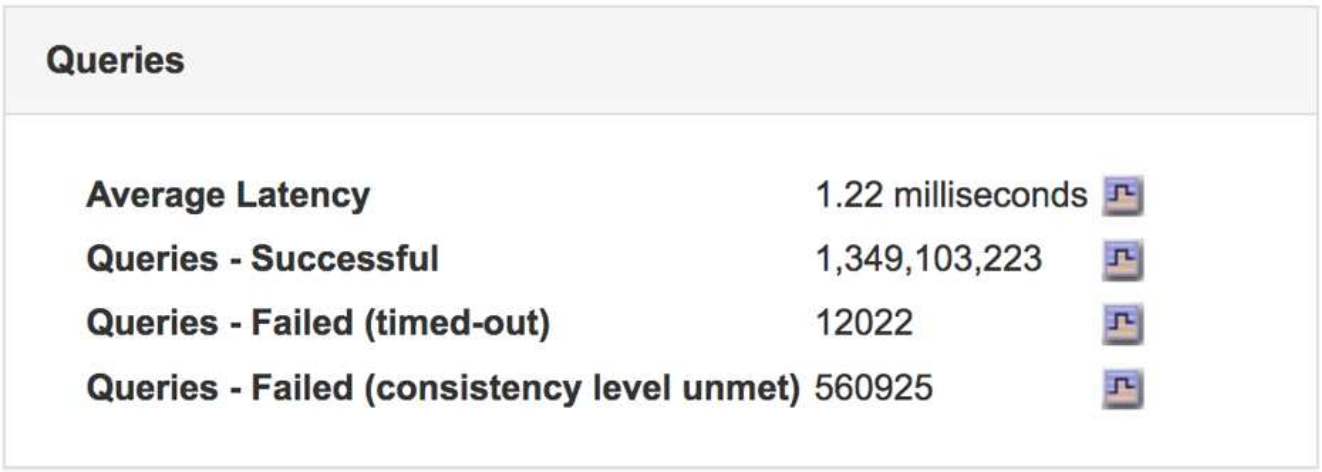
Temporary increases in query latency are normal and can be caused by a sudden increase in ingest requests. Failed queries are also normal and can result from transient network issues or nodes that are temporarily unavailable. However, if the average time to perform a query increases, overall grid performance declines.

If you notice that query latency is increasing over time, you should consider adding additional Storage Nodes in an expansion procedure to satisfy future workloads.

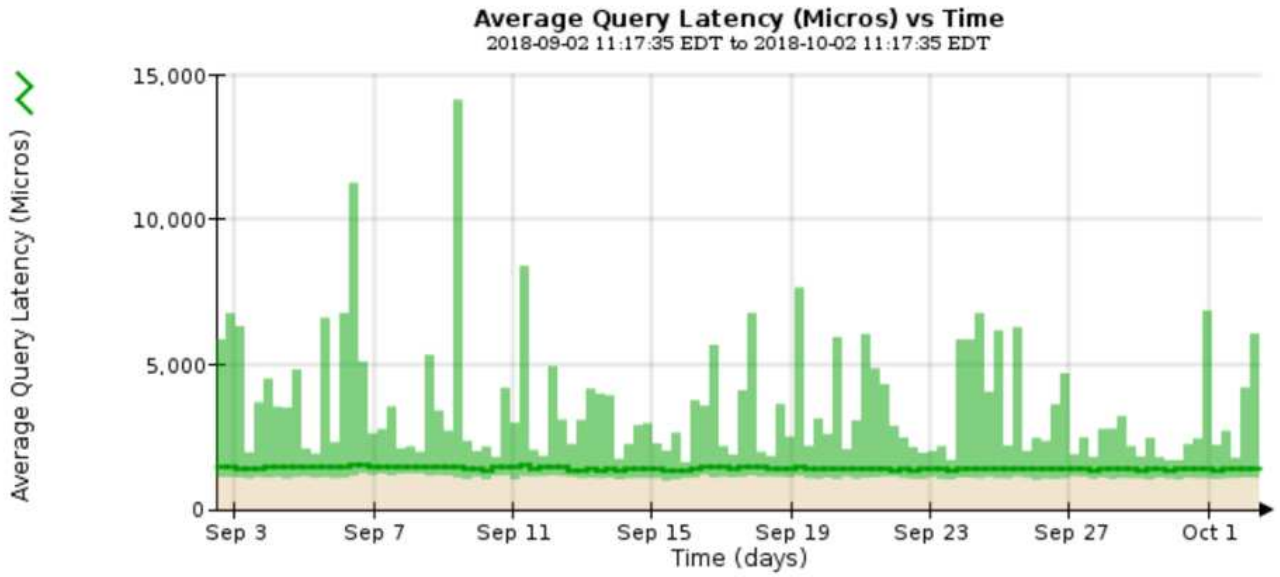
The **High latency for metadata queries** alert is triggered if the average time for queries is too long.

Steps

1. Select **Nodes** > ***Storage Node*** > **Objects**.
2. Scroll down to the Queries table and view the value for Average Latency.



3. Click the chart icon to chart the value over time.



The example chart shows spikes in query latency during normal grid operation.

Related information

Expand your grid

Monitoring 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 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.

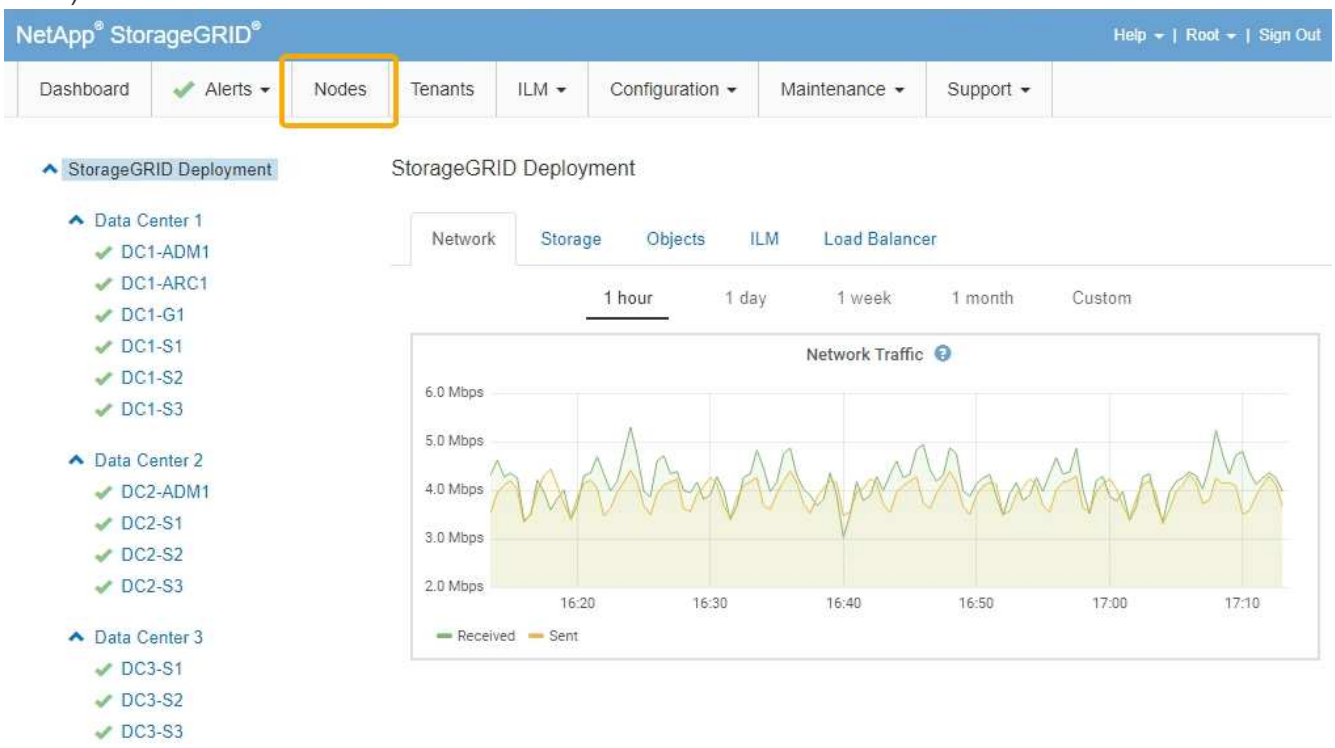
You can use the Grid Manager to monitor connectivity and network performance, so you can address any issues promptly.

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

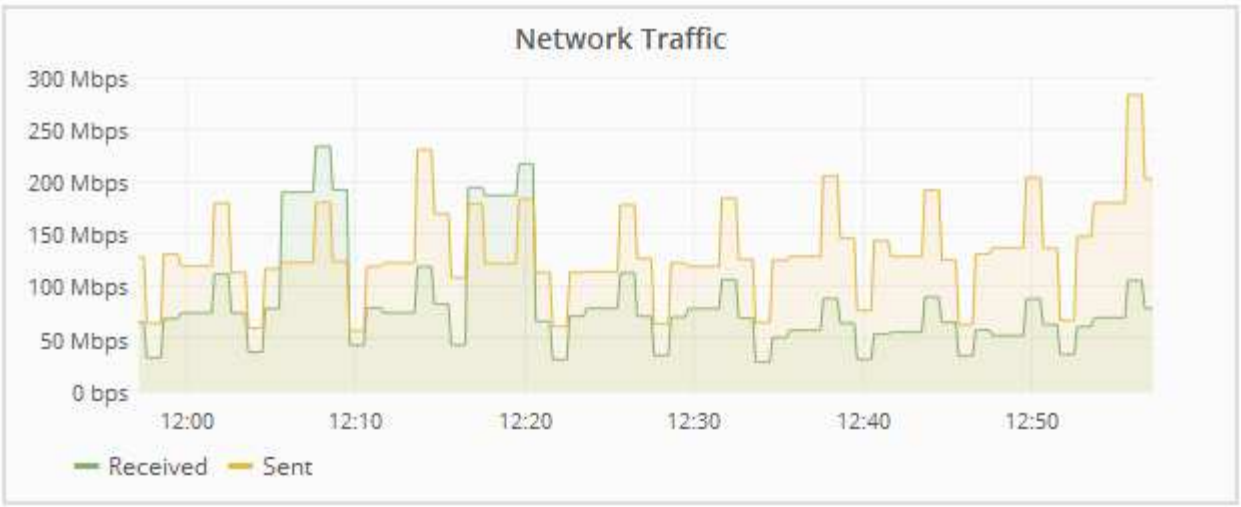
1. Select **Nodes**.

   The Nodes page appears. The node icons indicate at a glance which nodes are connected (green checkmark icon) and which nodes are disconnected (blue or gray icons).



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.

Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
eth0	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
eth1	D8:C4:97:2A:E4:9E	Gigabit	Full	Off	Up
eth2	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
hic1	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic2	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic3	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic4	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
mtc1	D8:C4:97:2A:E4:9E	Gigabit	Full	On	Up
mtc2	D8:C4:97:2A:E4:9F	Gigabit	Full	On	Up

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

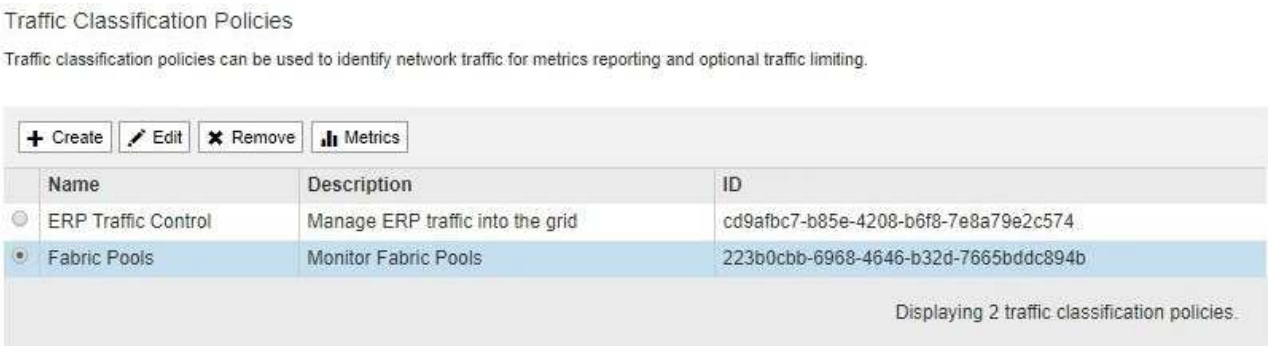
Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	3.250 TB	5,610,578,144	0	8,327	0	0
eth1	1.205 GB	9,828,095	0	32,049	0	0
eth2	849.829 GB	186,349,407	0	10,269	0	0
hic1	114.864 GB	303,443,393	0	0	0	0
hic2	2.315 TB	5,351,180,956	0	305	0	0
hic3	1.690 TB	1,793,580,230	0	0	0	0
hic4	194.283 GB	331,640,075	0	0	0	0
mtc1	1.205 GB	9,828,096	0	0	0	0
mtc2	1.168 GB	9,564,173	0	32,050	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	5.759 TB	5,789,638,626	0	0	0	0
eth1	4.563 MB	41,520	0	0	0	0
eth2	855.404 GB	139,975,194	0	0	0	0
hic1	289.248 GB	326,321,151	5	0	0	5
hic2	1.636 TB	2,640,416,419	18	0	0	18
hic3	3.219 TB	4,571,516,003	33	0	0	33
hic4	1.687 TB	1,658,180,262	22	0	0	22
mtc1	4.563 MB	41,520	0	0	0	0
mtc2	49.678 KB	609	0	0	0	0

3. Use the metrics associated with your traffic classification policies to monitor network traffic.
   a. Select **Configuration** > **Network Settings** > **Traffic Classification**.

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



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

Viewing the Network tab

Monitoring node connection states

Administer StorageGRID

Monitoring node-level resources

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

What you'll need

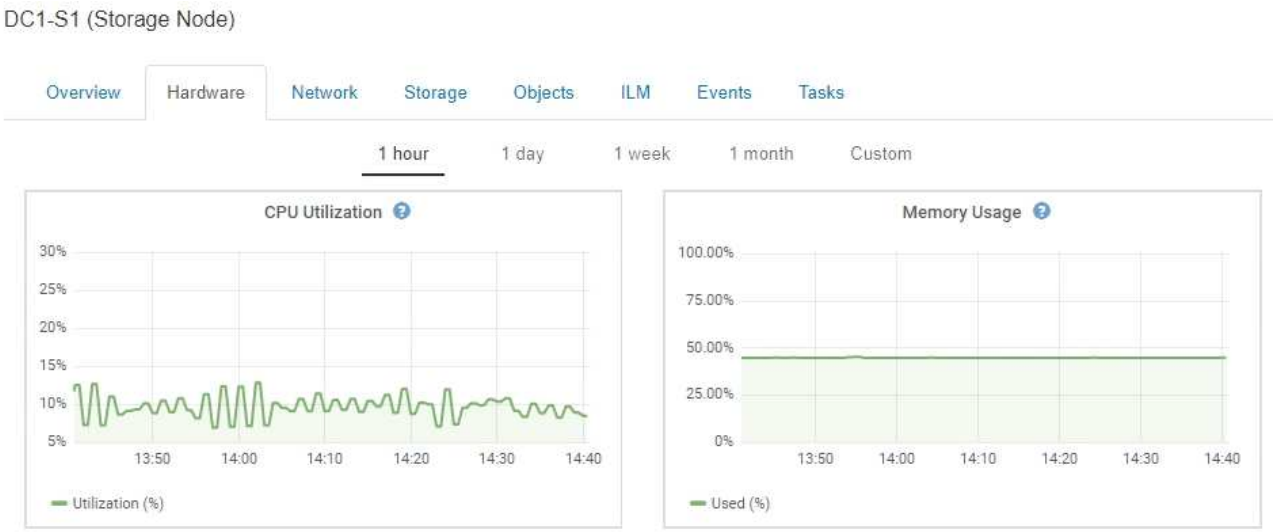
- You must be signed in to the Grid Manager using a supported browser.

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

Viewing information about appliance Storage Nodes

Viewing information about appliance Admin Nodes and Gateway Nodes

Monitoring 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 must be signed in to the Grid Manager using a supported browser.
- You must have the Root Access or Administrator permission.

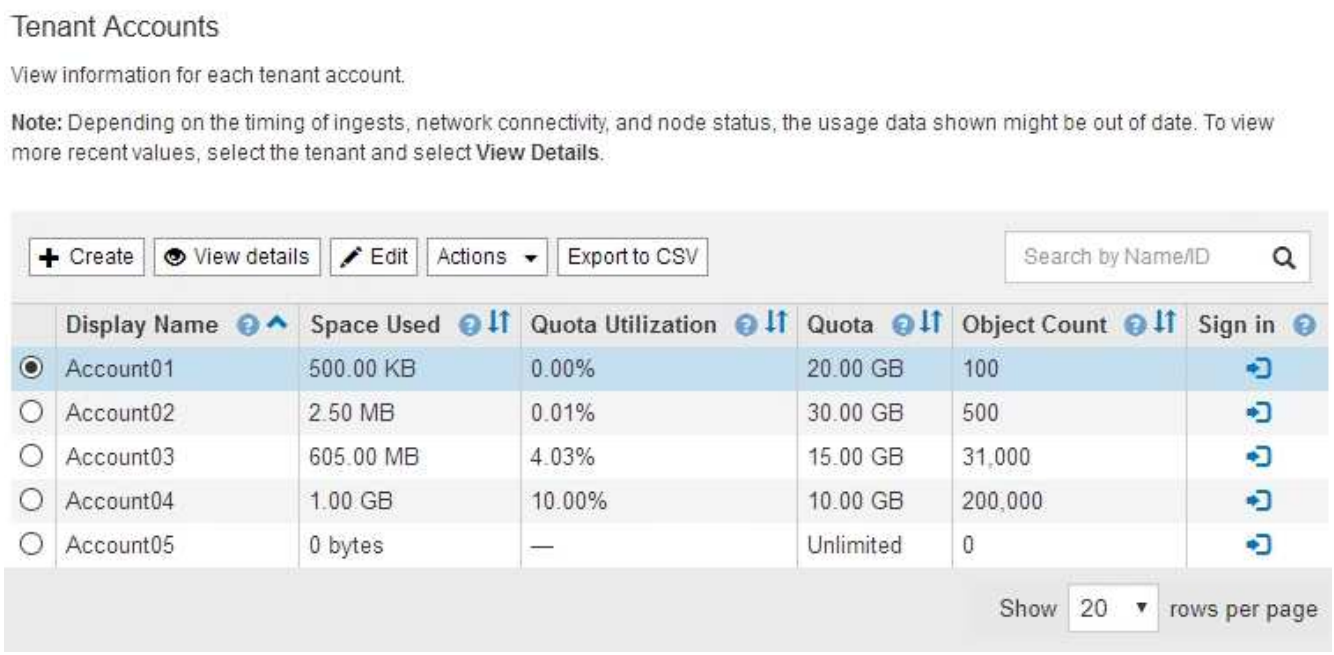
About this task

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 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 field contains a dash (--) and the Quota field indicates “Unlimited.”



If your system includes more than 20 items, you can specify how many rows are shown on each page at one time. Use the search box to search for a tenant account by display name or tenant ID.

You can sign in to a tenant account by selecting the link in the **Sign in** 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.

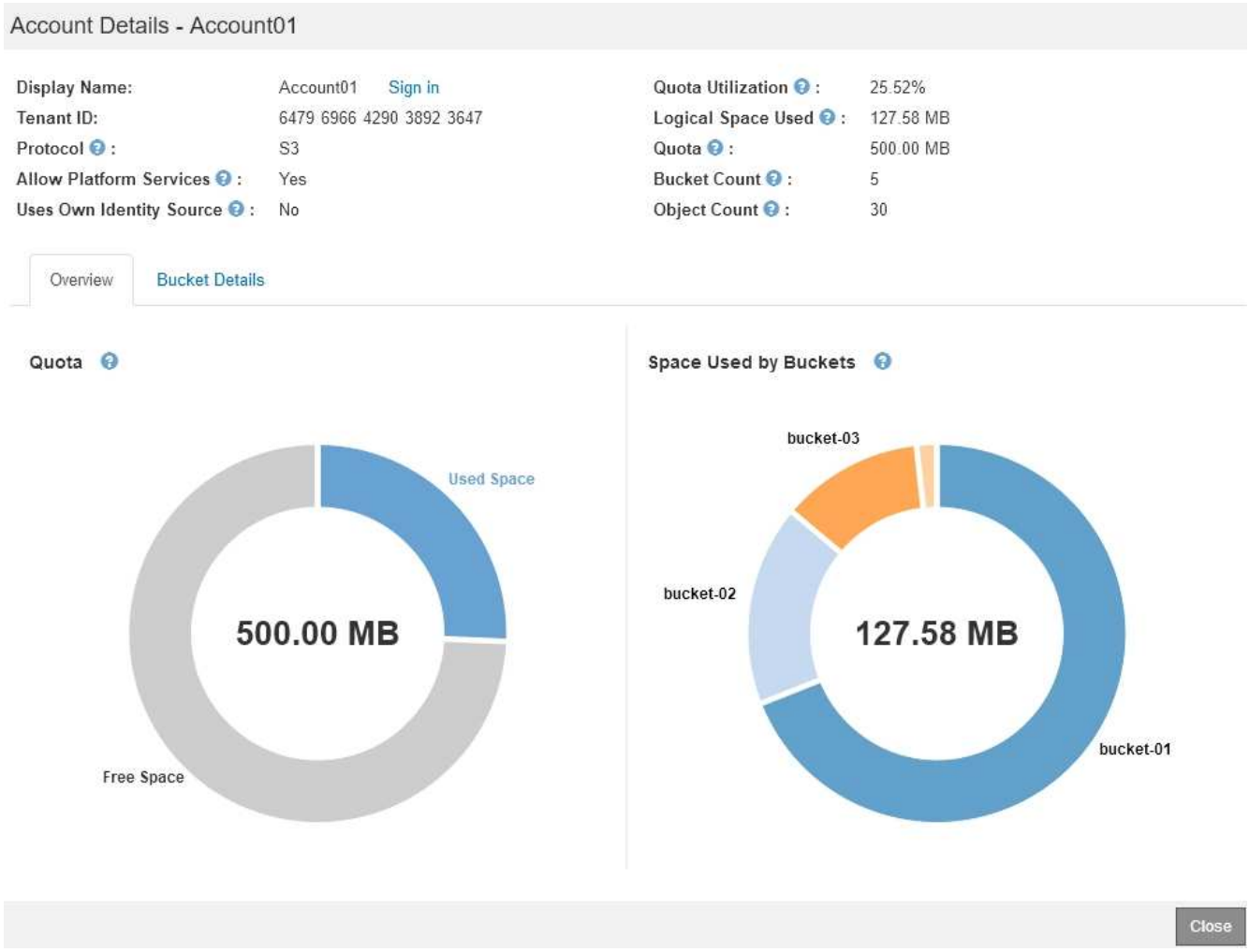
   The contents of a .csv file look like the following example:

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
56243391454153665591	Account01	500000	0	20000000000	100	S3
82457136581801590515	Account02	2500000	0.01	30000000000	500	S3
04489086912300179118	Account03	605000000	4.03	15000000000	31000	S3
26417581662098345719	Account04	1000000000	10	10000000000	200000	S3
78472447501213318575	Account05	0			0	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 from the Tenant Accounts page, and then select **View details**.

   The Account Details page appears and shows summary information, a chart that represents the amount of quota used and remaining, and a chart that represents the amount of object data in buckets (S3) or containers (Swift).



- **Quota**

  If a quota was set for this tenant, the **Quota** chart shows how much of that quota this tenant has used and how much is still available. If no quota was set, the tenant has an unlimited quota, and an informational message is displayed. 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 Used Space segment to see the number of stored objects and the total bytes used. You can place your cursor over the Free Space segment to see how many bytes of storage quota are available.

  > 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.

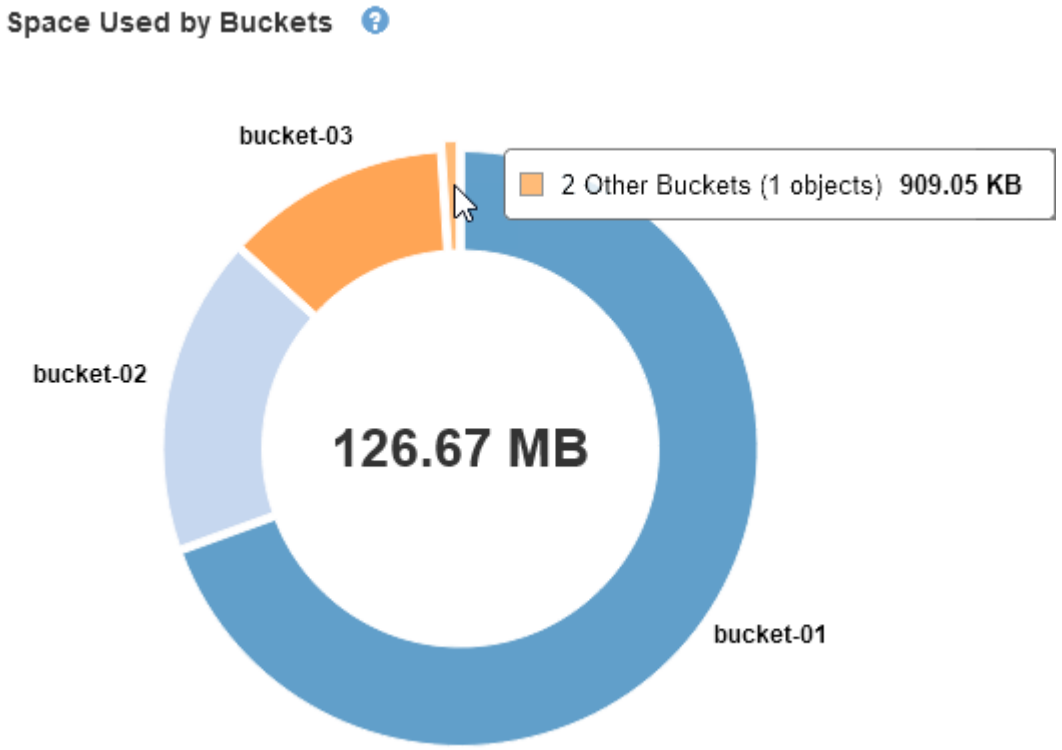
  > A tenant's quota utilization indicates the total amount of object data the tenant has uploaded to StorageGRID (logical size). The quota utilization does not represent the space used to store copies of those objects and their metadata (physical size).

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.

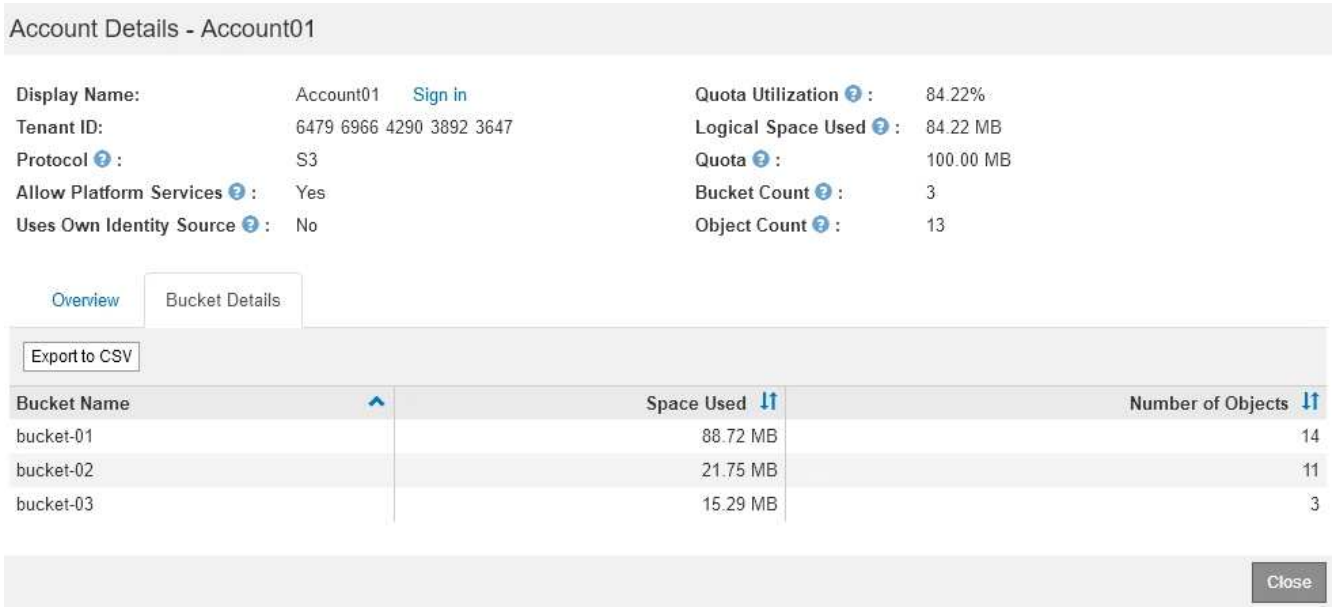
- **Space Used**

  The **Space Used by Buckets** (S3) or **Space Used by Containers** (Swift) chart shows the largest buckets for the tenant. Space used is the total amount of object data in the bucket. This value does not represent the storage space required for ILM copies and object metadata.

  If the tenant has more than nine buckets or containers, they are combined into a segment called Other. Some chart segments might be too small to include a label. You can place your cursor over any of the segments to see the label and obtain more information, including the number of stored objects and total bytes for each bucket or container.



4. Select **Bucket Details** (S3) or **Container Details** (Swift) to view a list of the spaced used and number of objects for each of the tenant's buckets or containers.



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

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

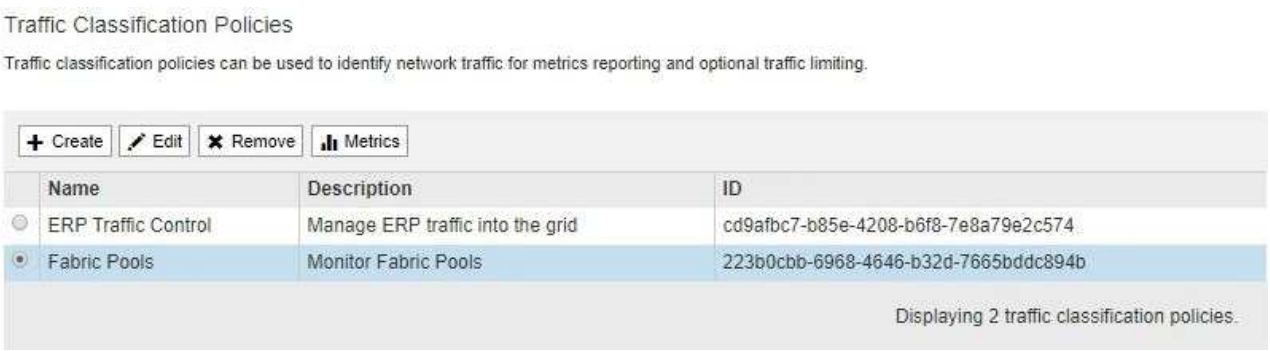
   The contents of an individual S3 tenant's .csv file look like the following example:

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.

6. If traffic classification policies are in place for a tenant, review the network traffic for that tenant.
   a. Select **Configuration** > **Network Settings** > **Traffic Classification**.

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



   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.

7. 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.

8. 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.

   - Select **Help** > **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

Administer StorageGRID

Reviewing support metrics

Monitoring 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 browser.
- You must have specific access permissions.

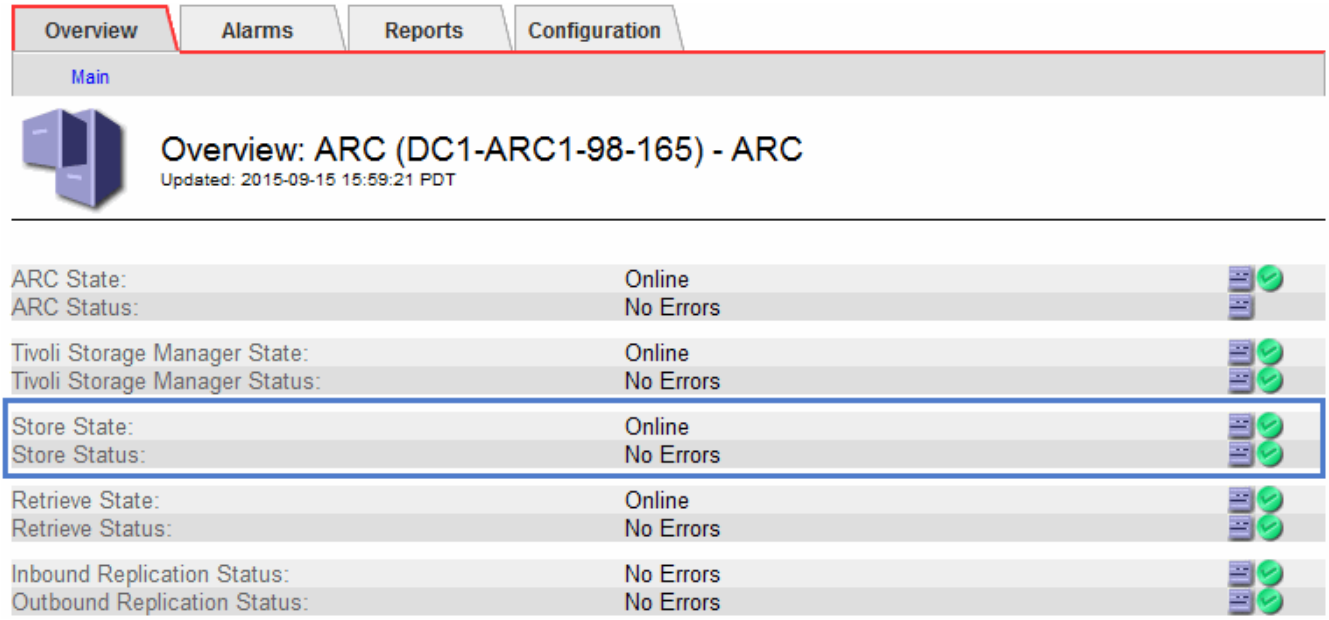
About this task

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.

Related information

Administer StorageGRID

Monitoring 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 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

Viewing the Load Balancer tab

Applying hotfixes or upgrading 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

Maintain & recover

Copyright information

Trademark information