■ NetApp

Monitor operations

StorageGRID

NetApp
May 03, 2022

Table of Contents

Monitor operations

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.

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. (The screenshot shows a system named StorageGRID Deployment.)
- 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.

Tabs for the Nodes page

The tabs at the top of the Nodes page are based on what you select from the tree at the left.

Tab name	Description	Included for
Overview	• Provides basic information about each node. • Shows any active alerts affecting the node.	All nodes
Hardware	• Displays CPU utilization and memory usage for each node • For appliance nodes, provides additional hardware information.	All nodes
Network	Displays a graph showing the network traffic received and sent across the network interfaces. The view for a single node shows additional information for the node.	All nodes, each site, and the entire grid

Tab name	Description	Included for
Storage	• Provides details for the disk devices and volumes on each node. • For Storage Nodes, each site, and the entire grid, includes graphs showing object data storage and metadata storage used over time.	All nodes, each site, and the entire grid
Objects	• Provides information about S3 and Swift ingest and retrieve rates. • For Storage Nodes, provides object counts and information about metadata store queries and background verification.	Storage Nodes, each site, and the entire grid
ILM	Provides information about Information Lifecycle Management (ILM) operations. • For Storage Nodes, provides details about ILM evaluation and background verification for erasure coded objects. • For each site and the entire grid, shows a graph of the ILM queue over time. • For the entire grid, provides the estimated time to complete a full ILM scan of all objects.	Storage Nodes, each site, and the entire grid
Load balancer	Includes performance and diagnostic graphs related to the Load Balancer service. • For each site, provides an aggregate summary of the statistics for all nodes at that site. • For the entire grid, provides an aggregate summary of the statistics for all sites.	Admin Nodes and Gateway Nodes, each site, and the entire grid
Platform services	Provides information about any S3 platform service operations at a site.	Each site
SANtricity System Manager	Provides access to SANtricity System Manager. From SANtricity System Manager, you can review hardware diagnostic and environmental information for the storage controller, as well as issues related to the drives.	Storage appliance nodes **Note**: The SANtricity System Manager tab will not appear if the controller firmware on the storage appliance is earlier than 8.70.

Prometheus metrics

The Prometheus service on Admin Nodes collects time series metrics from the services on all nodes.

3

The metrics collected by Prometheus are used in a number of places in the Grid Manager:

- **Nodes page**: The graphs and charts on the tabs available from the Nodes page use the Grafana visualization tool to display the time-series metrics collected by Prometheus. Grafana displays time-series data in graph and chart formats, while Prometheus serves as the backend data source.

- **Alerts**: Alerts are triggered at specific severity levels when alert rule conditions that use Prometheus metrics evaluate as true.

- **Grid Management API**: You can use Prometheus metrics in custom alert rules or with external automation tools to monitor your StorageGRID system. A complete list of Prometheus metrics is available from the Grid Management API. (From the top of the Grid Manager, select the help icon and select **API Documentation** > **metrics**.) While more than a thousand metrics are available, only a relatively small number are required to monitor the most critical StorageGRID operations.

  > ⓘ Metrics that include *private* in their names are intended for internal use only and are subject to change between StorageGRID releases without notice.

- The **SUPPORT** > **Tools** > **Diagnostics** page and the **SUPPORT** > **Tools** > **Metrics** page: These pages, which are primarily intended for use by technical support, provide a number of tools and charts that use the values of Prometheus metrics.

  > ⓘ Some features and menu items within the Metrics page are intentionally non-functional and are subject to change.

StorageGRID attributes

Attributes report values and statuses for many of the functions of the StorageGRID system. Attribute values are available for each grid node, each site, and the entire grid.

StorageGRID attributes are used in a number of places in the Grid Manager:

- **Nodes page**: Many of the values shown on the Nodes page are StorageGRID attributes. (Prometheus metrics are also shown on the Nodes pages.)

- **Alarms**: When attributes reach defined threshold values, StorageGRID alarms (legacy system) are triggered at specific severity levels.

- **Grid Topology tree**: Attribute values are shown in the Grid Topology tree (**SUPPORT** > **Tools** > **Grid topology**).

- **Events**: System events occur when certain attributes record an error or fault condition for a node, including errors such as network errors.

Attribute values

Attributes are reported on a best-effort basis and are approximately correct. Attribute updates can be lost under some circumstances, such as the crash of a service or the failure and rebuild of a grid node.

In addition, propagation delays might slow the reporting of attributes. Updated values for most attributes are sent to the StorageGRID system at fixed intervals. It can take several minutes before an update is visible in the system, and two attributes that change more or less simultaneously can be reported at slightly different times.

Related information

- Monitor and troubleshoot
- Monitor and manage alerts
- Use StorageGRID support options

Monitor and manage 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 is designed to be your primary tool for monitoring any issues that might occur in your StorageGRID system.

- 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 and Resolved Alerts pages provide a user friendly interface for viewing current and historical 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.

- 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 Current Alerts and Resolved Alerts pages. You can expand and collapse alert groups to show or hide the individual alerts. For example, if several nodes are reporting the **Unable to communicate with node** alert, only one email is sent and the alert is shown as a group on the Current Alerts page.

Current Alerts   Learn more

View the current alerts affecting your StorageGRID system.

				☑ Group alerts Active ▼

Name	Severity	Time triggered ▼	Site / Node	Status	Current values
⌄ Unable to communicate with node One or more services are unresponsive or cannot be reached by the metrics collection job.	⚠ 2 Major	9 minutes ago *(newest)* 19 minutes ago *(oldest)*		2 Active	
Low root disk capacity The space available on the root disk is low.	⚠ Minor	25 minutes ago	Data Center 1 / DC1-S1-99-51	Active	Disk space available: 2.00 GB Total disk space: 21.00 GB
Expiration of server certificate for Storage API Endpoints The server certificate used for the storage API endpoints is about to expire.	⚠ Major	31 minutes ago	Data Center 1 / DC1-ADM1-99-49	Active	Days remaining: 14
Expiration of server certificate for Management Interface The server certificate used for the management interface is about to expire.	⚠ Minor	31 minutes ago	Data Center 1 / DC1-ADM1-99-49	Active	Days remaining: 30
⌄ Low installed node memory The amount of installed memory on a node is low.	❌ 8 Critical	a day ago *(newest)* a day ago *(oldest)*		8 Active	

- Alerts use intuitive names and descriptions to help you understand more quickly what the problem is. 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 email 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 StorageGRID documentation to make it easier to find and access more detailed troubleshooting procedures.

Low installed node memory

The amount of installed memory on a node is low.

Recommended actions

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 instructions for your platform:

- VMware installation

- Red Hat Enterprise Linux or CentOS installation

- Ubuntu or Debian installation

Time triggered

2019-07-15 17:07:41 MDT *(2019-07-15 23:07:41 UTC)*

Status
Active (silence this alert ⤷)

Site / Node
Data Center 2 / DC2-S1-99-56

Severity
❌ Critical

Total RAM size
8.38 GB

Condition
View conditions | Edit rule ⤷

Close

ⓘ The legacy alarm system is deprecated. The user interface and APIs for the legacy alarm system will be removed in a future release. The alert system offers significant benefits and is easier to use.

Manage alerts

All StorageGRID users can view alerts. If you have the Root Access or Manage Alerts permission, you can also manage alerts, as follows:

- 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. You can silence an alert rule for the entire grid, a single site, or a single node.

- 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.

  For example, 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 < 24000000000
```

Related information

Monitor and troubleshoot

Use SNMP monitoring

If you want to monitor StorageGRID using the Simple Network Management Protocol (SNMP), you can use the Grid Manager to configure the SNMP agent.

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. 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. The agent 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.

- Certain alarms (legacy system) are triggered at specified severity levels or higher.

> ℹ️ SNMP notifications are not sent for every alarm or every alarm severity.

Related information

- Monitor and troubleshoot

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. Additionally, each node in your grid stores a limited amount of audit messages in a local log file (localaudit.log).

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 send audit information stored on Admin Nodes and local nodes to an external syslog server. Using an external syslog server can make it easier to manage your audit information and reduce network traffic. See Configure audit messages and log destinations for more information.

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 Configure audit client access.

Related information

- Review audit logs
- Administer StorageGRID