Alerts reference

StorageGRID 11.5

NetApp
August 30, 2024

Table of Contents

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 information about the 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. 1. Replace the battery. The steps to remove and replace a battery are included in the procedure for replacing a storage controller in the appliance installation and maintenance instructions. ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances 2. If this alert persists, contact technical support.
Appliance battery failed	The battery in the appliance's storage controller has failed. 1. Replace the battery. The steps to remove and replace a battery are included in the procedure for replacing a storage controller in the appliance installation and maintenance instructions. ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances 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. 1. Replace the battery. The steps to remove and replace a battery are included in the procedure for replacing a storage controller in the appliance installation and maintenance instructions. ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances 2. If this alert persists, contact technical support.

Alert name	Description and recommended actions
Appliance battery near expiration	The battery in the appliance's storage controller is nearing expiration. 1. Replace the battery soon. The steps to remove and replace a battery are included in the procedure for replacing a storage controller in the appliance installation and maintenance instructions. ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances 2. If this alert persists, contact technical support.
Appliance battery removed	The battery in the appliance's storage controller is missing. 1. Install a battery. The steps to remove and replace a battery are included in the procedure for replacing a storage controller in the appliance installation and maintenance instructions. ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances 2. If this alert persists, contact technical support.
Appliance battery too hot	The battery in the appliance's storage controller is overheated. 1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert. 2. Investigate possible reasons for the temperature increase, such as a fan or HVAC failure. 3. If this alert persists, contact technical support.

Alert name	Description and recommended actions
Appliance BMC communication error	Communication with the baseboard management controller (BMC) has been lost. 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. 2. Attempt to restore BMC communications by placing the node into maintenance mode and then powering the appliance off and back on. See the installation and maintenance instructions for your appliance. ◦ SG6000 storage appliances ◦ SG100 & SG1000 services appliances 3. If this alert persists, contact technical support.
Appliance cache backup device failed	A persistent cache backup device has failed. 1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert. 2. Contact technical support.
Appliance cache backup device insufficient capacity	There is insufficient cache backup device capacity.Contact technical support.
Appliance cache backup device write-protected	A cache backup device is write-protected.Contact technical support.
Appliance cache memory size mismatch	The two controllers in the appliance have different cache sizes.Contact technical support.

Alert name	Description and recommended actions
Appliance compute controller chassis temperature too high	The temperature of the compute controller in a StorageGRID appliance has exceeded a nominal threshold. 1. Check the hardware components for overheating conditions, and follow the recommended actions: ◦ If you have an SG100, SG1000, or SG6000, use the BMC. ◦ If you have an SG5600 or SG5700, use SANtricity System Manager. 2. If necessary, replace the component. See the installation and maintenance instructions for your appliance hardware: ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances ◦ SG100 & SG1000 services 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. 1. Check the hardware components for overheating conditions, and follow the recommended actions: ◦ If you have an SG100, SG1000, or SG6000, use the BMC. ◦ If you have an SG5600 or SG5700, use SANtricity System Manager. 2. If necessary, replace the component. See the installation and maintenance instructions for your appliance hardware: ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances ◦ SG100 & SG1000 services 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. 1. Check the hardware components for errors, and follow the recommended actions: ◦ If you have an SG100, SG1000, or SG6000, use the BMC. ◦ If you have an SG5600 or SG5700, use SANtricity System Manager. 2. If necessary, replace the component. See the installation and maintenance instructions for your appliance hardware: ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances ◦ SG100 & SG1000 services 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. 1. Check the hardware components for errors, and follow the recommended actions: ◦ If you have an SG100, SG1000, or SG6000, use the BMC. ◦ If you have an SG5600 or SG5700, use SANtricity System Manager. 2. If necessary, replace the component. See the installation and maintenance instructions for your appliance hardware: ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances ◦ SG100 & SG1000 services 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.This alert might indicate that the power supply has failed or that it has a problem providing power. 1. Check the hardware components for errors, and follow the recommended actions: ◦ If you have an SG100, SG1000, or SG6000, use the BMC. ◦ If you have an SG5600 or SG5700, use SANtricity System Manager. 2. If necessary, replace the component. See the installation and maintenance instructions for your appliance hardware: ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances ◦ SG100 & SG1000 services appliances
Appliance compute hardware monitor service stalled	The service that monitors storage hardware status has stopped reporting data. 1. Check the status of the eos-system-status service in the base-os. 2. If the service is in a stopped or error state, restart the service. 3. If this alert persists, contact technical support.

Alert name	Description and recommended actions
Appliance Fibre Channel fault detected	There is a problem with the Fibre Channel connection between the storage and compute controllers in the appliance. 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: a. Verify that the Fibre Channel cables between controllers are completely connected. b. Ensure that the Fibre Channel cables are free of excessive bends. c. Confirm that the SFP+ modules are properly seated. **Note:** If this problem persists, the StorageGRID system might take the problematic connection offline automatically. 2. If necessary, replace components. See the installation and maintenance instructions for your appliance.
Appliance Fibre Channel HBA port failure	A Fibre Channel HBA port is failing or has failed.Contact technical support.
Appliance flash cache drives non-optimal	The drives used for the SSD cache are non-optimal. 1. Replace the SSD cache drives. See the appliance installation and maintenance instructions. ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances 2. If this alert persists, contact technical support.
Appliance interconnect/battery canister removed	The interconnect/battery canister is missing. 1. Replace the battery. The steps to remove and replace a battery are included in the procedure for replacing a storage controller in the appliance installation and maintenance instructions. ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances 2. If this alert persists, contact technical support.

Alert name	Description and recommended actions
Appliance LACP port missing	A port on a StorageGRID appliance is not participating in the LACP bond. 1. Check the configuration for the switch. Ensure the interface is configured in the correct link aggregation group. 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. 1. Check the status of power supply A and B to determine which power supply is operating abnormally, and follow the recommended actions: ◦ If you have an SG100, SG1000, or SG6000, use the BMC. ◦ If you have an SG5600 or SG5700, use SANtricity System Manager. 2. If necessary, replace the component. See the installation and maintenance instructions for your appliance hardware: ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances ◦ SG100 & SG1000 services appliances
Appliance storage controller A failure	Storage controller A in a StorageGRID appliance has failed. 1. Use SANtricity System Manager to check hardware components, and follow the recommended actions. 2. If necessary, replace the component. See the installation and maintenance instructions for your appliance hardware: ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances

Alert name	Description and recommended actions
Appliance storage controller B failure	Storage controller B in a StorageGRID appliance has failed. 1. Use SANtricity System Manager to check hardware components, and follow the recommended actions. 2. If necessary, replace the component. See the installation and maintenance instructions for your appliance hardware: ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances
Appliance storage controller drive failure	One or more drives in a StorageGRID appliance has failed or is not optimal. 1. Use SANtricity System Manager to check hardware components, and follow the recommended actions. 2. If necessary, replace the component. See the installation and maintenance instructions for your appliance hardware: ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances
Appliance storage controller hardware issue	SANtricity software is reporting "Needs attention" for a component in a StorageGRID appliance. 1. Use SANtricity System Manager to check hardware components, and follow the recommended actions. 2. If necessary, replace the component. See the installation and maintenance instructions for your appliance hardware: ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances

Alert name	Description and recommended actions
Appliance storage controller power supply A failure	Power supply A in a StorageGRID appliance has deviated from the recommended operating voltage. 1. Use SANtricity System Manager to check hardware components, and follow the recommended actions. 2. If necessary, replace the component. See the installation and maintenance instructions for your appliance hardware: ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances
Appliance storage controller power supply B failure	Power supply B in a StorageGRID appliance has deviated from the recommended operating voltage. 1. Use SANtricity System Manager to check hardware components, and follow the recommended actions. 2. If necessary, replace the component. See the installation and maintenance instructions for your appliance hardware: ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances
Appliance storage hardware monitor service stalled	The service that monitors storage hardware status has stopped reporting data. 1. Check the status of the eos-system-status service in the base-os. 2. If the service is in a stopped or error state, restart the service. 3. If this alert persists, contact technical support.

Alert name	Description and recommended actions
Appliance storage shelves degraded	The status of one of the components in the storage shelf for a storage appliance is degraded. 1. Use SANtricity System Manager to check hardware components, and follow the recommended actions. 2. If necessary, replace the component. See the installation and maintenance instructions for your appliance hardware: ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances
Appliance temperature exceeded	The nominal or maximum temperature for the appliance's storage controller has been exceeded. 1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert. 2. Investigate possible reasons for the temperature increase, such as a fan or HVAC failure. 3. If this alert persists, contact technical support.
Appliance temperature sensor removed	A temperature sensor has been removed. Contact technical support.
Cassandra auto-compactor error	The Cassandra auto-compactor has experienced an error.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. 1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert. 2. Contact technical support.

Alert name	Description and recommended actions
Cassandra auto-compactor metrics out of date	The metrics that describe the Cassandra auto-compactor are out of date. 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. 1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert. 2. Contact technical support.
Cassandra communication error	The nodes that run the Cassandra service are having trouble communicating with each other.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. 1. Determine if there is another alert affecting one or more Storage Nodes. This alert might be resolved when you resolve the other alert. 2. Check for a network issue that might be affecting one or more Storage Nodes. 3. Select **Support** > **Tools** > **Grid Topology**. 4. For each Storage Node in your system, select **SSM** > **Services**. Ensure that the status of the Cassandra service is"` Running.`" 5. If Cassandra is not running, follow the steps for starting or restarting a service in the recovery and maintenance instructions. 6. If all instances of the Cassandra service are now running and the alert is not resolved, contact technical support. Maintain & recover

Alert name	Description and recommended actions
Cassandra compactions overloaded	The Cassandra compaction process is overloaded.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. 1. Restart the Cassandra service by following the steps for restarting a service in the recovery and maintenance instructions. 2. If this alert persists, contact technical support. Maintain & recover
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. 1. Reboot the node. From the Grid Manager, go to **Nodes**, select the node, and select the Tasks tab. 2. If this alert persists, contact technical support.
Cassandra repair progress slow	The progress of Cassandra database repairs is slow.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. 1. Confirm that all Storage Nodes are online and there are no networking-related alerts. 2. Monitor this alert for up to 2 days to see if the issue resolves on its own. 3. If database repairs continue to proceed slowly, contact technical support.

Alert name	Description and recommended actions
Cassandra repair service not available	The Cassandra repair service is not available.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. 1. Select **Support** > **Tools** > **Grid Topology**. 2. For each Storage Node in your system, select **SSM** > **Services**. Ensure that the status of the Cassandra Reaper service is "Running." 3. If Cassandra Reaper is not running, follow the steps for starting or restarting a service in the recovery and maintenance instructions. 4. If all instances of the Cassandra Reaper service are now running and the alert is not resolved, contact technical support. Maintain & recover
Cloud Storage Pool connectivity error	The health check for Cloud Storage Pools detected one or more new errors. 1. Go to the Cloud Storage Pools section of the Storage Pools page. 2. Look at the Last Error column to determine which Cloud Storage Pool has an error. 3. See the instructions for managing objects with information lifecycle management. Manage objects with ILM
DHCP lease expired	The DHCP lease on a network interface has expired.If the DHCP lease has expired, follow the recommended actions: 1. Ensure there is connectivity between this node and the DHCP server on the affected interface. 2. Ensure there are IP addresses available to assign in the affected subnet on the DHCP server. 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. Maintain & recover

Alert name	Description and recommended actions
DHCP lease expiring soon	The DHCP lease on a network interface is expiring soon.To prevent the DHCP lease from expiring, follow the recommended actions: 1. Ensure there is connectivity between this node and the DHCP server on the affected interface. 2. Ensure there are IP addresses available to assign in the affected subnet on the DHCP server. 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. Maintain & recover
DHCP server unavailable	The DHCP server is unavailable.The StorageGRID node is unable to contact your DHCP server. The DHCP lease for the node's IP address cannot be validated. 1. Ensure there is connectivity between this node and the DHCP server on the affected interface. 2. Ensure there are IP addresses available to assign in the affected subnet on the DHCP server. 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. Maintain & recover

Alert name	Description and recommended actions
Disk I/O is very slow	Very slow disk I/O might be impacting StorageGRID performance. 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. 2. Examine the storage system that hosts this node's volumes to determine, and correct, the root cause of the slow I/O. 3. If this alert persists, contact technical support. 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.

Alert name	Description and recommended actions
Email notification failure	The email notification for an alert could not be sent.This alert is triggered when an alert email notification fails or a test email (sent from the **Alerts** > **Email Setup** page) cannot be delivered. 1. Sign in to Grid Manager from the Admin Node listed in the **Site/Node** column of the alert. 2. Go to the **Alerts** > **Email Setup** page, check the settings, and change them if required. 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. 4. If the test email could not be sent, confirm your email server is online. 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. 6. Extract the downloaded archive, and review the contents of `prometheus.log` (`_/GID<gid><time_stamp>/<site_node>/<time_stamp>/metrics/prometheus.log`). 7. If you are unable to resolve the problem, contact technical support.
Expiration of certificates configured on Client Certificates page	One or more certificates configured on the Client Certificates page are about to expire. 1. Select **Configuration** > **Access Control** > **Client Certificates**. 2. Select a certificate that will expire soon. 3. Select **Edit** to upload or generate a new certificate. 4. Repeat these steps for each certificate that will expire soon. Administer StorageGRID

Alert name	Description and recommended actions
Expiration of load balancer endpoint certificate	One or more load balancer endpoint certificates are about to expire. 1. Select **Configuration** > **Network Settings** > **Load Balancer Endpoints**. 2. Select an endpoint that has a certificate that will expire soon. 3. Select **Edit endpoint** to upload or generate a new certificate. 4. Repeat these steps for each endpoint that has an expired certificate or one that will expire soon. For more information about managing load balancer endpoints, see the instructions for administering StorageGRID. Administer StorageGRID
Expiration of server certificate for Management Interface	The server certificate used for the management interface is about to expire. 1. Select **Configuration** > **Network Settings** > **Server Certificates**. 2. In the Management Interface Server Certificate section, upload a new certificate. Administer StorageGRID
Expiration of server certificate for Storage API Endpoints	The server certificate used for accessing storage API endpoints is about to expire. 1. Select **Configuration** > **Network Settings** > **Server Certificates**. 2. In the Object Storage API Service Endpoints Server Certificate section, upload a new certificate. Administer StorageGRID

Alert name	Description and recommended actions
Grid Network MTU mismatch	The maximum transmission unit (MTU) setting for the Grid Network interface (eth0) differs significantly across nodes in the grid.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. Troubleshooting the Grid Network MTU mismatch alert
High Java heap use	A high percentage of Java heap space is being used.If the Java heap becomes full, metadata services can become unavailable and client requests can fail. 1. Review the ILM activity on the Dashboard. This alert might resolve on its own when the ILM workload decreases. 2. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert. 3. If this alert persists, contact technical support.
High latency for metadata queries	The average time for Cassandra metadata queries is too long.An increase in query latency can be caused by a hardware change, such as replacing a disk, or a workload change, such as a sudden increase in ingests. 1. Determine if there were any hardware or workload changes around the time the query latency increased. 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. 1. Confirm that the configured LDAP server is online and available. 2. Review the settings on the Identity Federation page. Confirm that all values are current. See “Configuring a federated identity source” in the instructions for administering StorageGRID. 3. Click **Test Connection** to validate the settings for the LDAP server. 4. If you cannot resolve the issue, contact technical support. Administer StorageGRID
ILM placement unachievable	A placement instruction in an ILM rule cannot be achieved for certain objects.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. 1. Ensure that all nodes are online. 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. 3. As required, update rule settings and activate a new policy. It might take up to 1 day for the alert to clear. 4. If the problem persists, contact technical support. 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. Manage objects with ILM

Alert name	Description and recommended actions
ILM scan period too long	The time required to scan, evaluate objects, and apply ILM is too long.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. 1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert. 2. Confirm that all Storage Nodes are online. 3. Temporarily reduce the amount of client traffic. For example, from the Grid Manager, select **Configuration** > **Network Settings** > **Traffic Classification**, and create a policy that limits bandwidth or the number of requests. 4. If disk I/O or CPU are overloaded, try to reduce the load or increase the resource. 5. If necessary, update ILM rules to use synchronous placement (default for rules created after StorageGRID 11.3). 6. If this alert persists, contact technical support. Administer StorageGRID
ILM scan rate low	The ILM scan rate is set to less than 100 objects/second.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. 1. Determine if a temporary change was made to the ILM scan rate as part of an ongoing support investigation. 2. Contact technical support. 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. 1. Using the KMS software, update the CA certificate for the key management server. 2. From the Grid Manager, select **Configuration** > **System Settings** > **Key Management Server**. 3. Select the KMS that has a certificate status warning. 4. Select **Edit**. 5. Select **Next** to go to Step 2 (Upload Server Certificate). 6. Select **Browse** to upload the new certificate. 7. Select **Save**. Administer StorageGRID
KMS client certificate expiration	The client certificate for a key management server is about to expire. 1. From the Grid Manager, select **Configuration** > **System Settings** > **Key Management Server**. 2. Select the KMS that has a certificate status warning. 3. Select **Edit**. 4. Select **Next** to go to Step 3 (Upload Client Certificates). 5. Select **Browse** to upload the new certificate. 6. Select **Browse** to upload the new private key. 7. Select **Save**. Administer StorageGRID
KMS configuration failed to load	The configuration for the key management server exists but failed to load. 1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert. 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. 1. From the Grid Manager, select **Configuration** > **System Settings** > **Key Management Server**. 2. Confirm that the port and hostname entries are correct. 3. Confirm that the server certificate, client certificate, and the client certificate private key are correct and not expired. 4. Ensure that firewall settings allow the appliance node to communicate with the specified KMS. 5. Correct any networking or DNS issues. 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. 1. Confirm that the KMS assigned to the site is using the correct name for the encryption key and any prior versions. 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. 1. From the Grid Manager, select **Configuration** > **System Settings** > **Key Management Server**. 2. Add a KMS for this site or add a default KMS. Administer StorageGRID

Alert name	Description and recommended actions
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. 1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert. 2. Ensure that the key management server (KMS) has the configured encryption key and any previous key versions. 3. If you need assistance or this alert persists, contact technical support.
KMS server certificate expiration	The server certificate used by the key management server (KMS) is about to expire. 1. Using the KMS software, update the server certificate for the key management server. 2. If you need assistance or this alert persists, contact technical support. Administer StorageGRID
Large audit queue	The disk queue for audit messages is full. 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. 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. 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**). Review audit logs
Low audit log disk capacity	The space available for audit logs is low. 1. Monitor this alert to see if the issue resolves on its own and the disk space becomes available again. 2. Contact technical support if the available space continues to decrease.

Alert name	Description and recommended actions
Low available node memory	The amount of RAM available on a node is low.Low available RAM could indicate a change in the workload or a memory leak with one or more nodes. 1. Monitor this alert to see if the issue resolves on its own. 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. 1. Select **ILM** > **Storage Pools**. 2. Select the storage pool listed in the alert, and select **View details**. 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. 4. Perform an expansion procedure to increase storage capacity. Expand your grid
Low installed node memory	The amount of installed memory on a node is low.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: • Install Red Hat Enterprise Linux or CentOS • Install Ubuntu or Debian • Install VMware

Alert name	Description and recommended actions
Low metadata storage	The space available for storing object metadata is low.**Critical alert** 1. Stop ingesting objects. 2. Immediately add Storage Nodes in an expansion procedure. **Major alert** Immediately add Storage Nodes in an expansion procedure. **Minor alert** 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. 2. Add Storage Nodes in an expansion procedure as soon as possible. Once new Storage Nodes are added, the system automatically rebalances object metadata across all Storage Nodes, and the alarm clears. Troubleshooting the Low metadata storage alert Expand your grid
Low metrics disk capacity	The space available for the metrics database is low. 1. Monitor this alert to see if the issue resolves on its own and the disk space becomes available again. 2. Contact technical support if the available space continues to decrease.
Low object data storage	The space available for storing object data is low.Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes. Troubleshooting the Low object data storage alert Expand your grid

Alert name	Description and recommended actions
Low root disk capacity	The space available for the root disk is low. 1. Monitor this alert to see if the issue resolves on its own and the disk space becomes available again. 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. 1. Monitor this alert to see if the issue resolves on its own and the disk space becomes available again. 2. Contact technical support if the available space continues to decrease.
Node network connectivity error	Errors have occurred while transferring data between nodes.Network connectivity errors might clear without manual intervention. Contact technical support if the errors do not clear. Troubleshooting the Network Receive Error (NRER) alarm
Node network reception frame error	A high percentage of the network frames received by a node had errors.This alert might indicate a hardware issue, such as a bad cable or a failed transceiver on either end of the Ethernet connection. 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. 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. 1. Verify that you have specified at least four external NTP servers, each providing a Stratum 3 or better reference. 2. Check that all NTP servers are operating normally. 3. Verify the connections to the NTP servers. Make sure they are not blocked by a firewall.

Alert name	Description and recommended actions
Node not locked with NTP server	The node is not locked to a network time protocol (NTP) server. 1. Verify that you have specified at least four external NTP servers, each providing a Stratum 3 or better reference. 2. Check that all NTP servers are operating normally. 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. Contact technical support.
Objects lost	One or more objects have been lost from the grid.This alert might indicate that data has been permanently lost and is not retrievable. 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. Troubleshooting lost and missing object data 2. When the underlying problem is resolved, reset the counter: a. Select **Support** > **Tools** > **Grid Topology**. b. For the Storage Node that raised the alert, select ***site*** > ***grid node*** > **LDR** > **Data Store** > **Configuration** > **Main**. 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.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. See “Troubleshooting platform services” in the instructions for administering StorageGRID. Administer StorageGRID

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. 1. Check the cable and physical connection to Admin Network port 1. 2. Address any connection issues. See the installation and maintenance instructions for your appliance hardware. 3. If this port is disconnected on purpose, disable this rule. From the Grid Manager, select **Alerts** > **Alert Rules**, select the rule, and click **Edit rule**. Then, uncheck the **Enabled** check box. ◦ SG100 & SG1000 services appliances ◦ Disabling an alert rule
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. 1. Check the cables, SFPs, and physical connections to the StorageGRID network. 2. Address any connection issues. See the installation and maintenance instructions for your appliance hardware. 3. If this port is disconnected on purpose, disable this rule. From the Grid Manager, select **Alerts** > **Alert Rules**, select the rule, and click **Edit rule**. Then, uncheck the **Enabled** check box. ◦ SG100 & SG1000 services appliances ◦ Disabling an alert rule
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. 1. Check the cables, SFPs, and physical connections to the StorageGRID network. 2. Address any connection issues. See the installation and maintenance instructions for your appliance hardware. 3. If this port is disconnected on purpose, disable this rule. From the Grid Manager, select **Alerts** > **Alert Rules**, select the rule, and click **Edit rule**. Then, uncheck the **Enabled** check box. ◦ SG100 & SG1000 services appliances ◦ Disabling an alert rule

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.Appliance functionality is not impacted, but you should address the issue immediately. If both drives fail, the appliance will no longer function. 1. From the Grid Manager, select **Nodes** > ***services appliance*, and then select the Hardware** tab. 2. Review the message in the **Storage RAID Mode** field. 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. 4. If the message indicates that one of the SSDs has failed, replace the failed drive as soon as possible. For instructions on how to replace a drive in a services appliance, see the SG100 and SG1000 appliances installation and maintenance guide. SG100 & SG1000 services appliances
Storage appliance link down on Admin Network port 1	The Admin Network port 1 on the appliance is down or disconnected. 1. Check the cable and physical connection to Admin Network port 1. 2. Address any connection issues. See the installation and maintenance instructions for your appliance hardware. 3. If this port is disconnected on purpose, disable this rule. From the Grid Manager, select **Alerts** > **Alert Rules**, select the rule, and click **Edit rule**. Then, uncheck the **Enabled** check box. ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances ◦ Disabling an alert rule

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. 1. Check the cables, SFPs, and physical connections to the StorageGRID network. 2. Address any connection issues. See the installation and maintenance instructions for your appliance hardware. 3. If this port is disconnected on purpose, disable this rule. From the Grid Manager, select **Alerts** > **Alert Rules**, select the rule, and click **Edit rule**. Then, uncheck the **Enabled** check box. ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances ◦ Disabling an alert rule
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. 1. Check the cables, SFPs, and physical connections to the StorageGRID network. 2. Address any connection issues. See the installation and maintenance instructions for your appliance hardware. 3. If this port is disconnected on purpose, disable this rule. From the Grid Manager, select **Alerts** > **Alert Rules**, select the rule, and click **Edit rule**. Then, uncheck the **Enabled** check box. ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ SG5600 storage appliances ◦ Disabling an alert rule

Alert name	Description and recommended actions
Storage appliance storage connectivity degraded	There is a problem with one or more connections between the compute controller and storage controller. 1. Go to the appliance to check the port indicator lights. 2. If a port's lights are off, confirm the cable is properly connected. As needed, replace the cable. 3. Wait up to five minutes. 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. 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.This alert indicates that a volume cannot be mounted or accessed because of a problem with an underlying storage device. 1. Check the status of all storage devices used for the node: ◦ 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. ▪ Install Red Hat Enterprise Linux or CentOS ▪ Install Ubuntu or Debian ▪ Install VMware ◦ If the node is installed on an SG100, SG1000 or SG6000 appliance, use the BMC. ◦ If the node is installed on a SG5600 or SG5700 appliance, use SANtricity System Manager. 2. If necessary, replace the component. See the installation and maintenance instructions for your appliance hardware. ◦ SG6000 storage appliances ◦ SG5700 storage appliances ◦ 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. This alert rule is disabled by default because it might generate a lot of notifications. 1. From the Grid Manager, select **Tenants**. 2. Sort the table by **Quota Utilization**. 3. Select a tenant whose quota utilization is close to 100%. 4. Do either or both of the following: ◦ Select **Edit** to increase the storage quota for the tenant. ◦ 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.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. Monitor this alert to see if the issue resolves on its own. If the issue persists: 1. Determine if there is another alert affecting this node. This alert might be resolved when you resolve the other alert. 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. 3. Ensure that the host for the node is powered on. If it is not, start the host. If more than one host is powered off, see the recovery and maintenance instructions. 4. Determine if there is a network connectivity issue between this node and the Admin Node. 5. If you cannot resolve the alert, contact technical support. Maintain & recover
Unexpected node reboot	A node rebooted unexpectedly within the last 24 hours. 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. 2. If you cannot resolve the alert, there might be a hardware failure. Contact technical support.

Alert name	Description and recommended actions
Unidentified corrupt object detected	A file was found in replicated object storage that could not be identified as a replicated object. 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. 2. After resolving any storage issues, run foreground verification to determine if objects are missing and to replace them if possible. 3. Monitor this alert. The alert will clear after 24 hours, but will be triggered again if the issue has not been fixed. 4. If you cannot resolve the alert, contact technical support. Running foreground verification

Related information

Commonly used Prometheus metrics

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.

The following table lists the most commonly used Prometheus metrics and provides a mapping of each metric to the equivalent attribute (used in the alarm system).

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. For a complete list of metrics, select **Help** > **API Documentation**.

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

Prometheus metrics are retained for 31 days.

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.

Prometheus metric	Description
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.
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. Troubleshooting 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.

Prometheus metric	Description
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.
storagegrid_ilm_scan_period_estimated_minutes	The estimated time to complete a full ILM scan on this node. **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_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.

Prometheus metric	Description
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.
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_load	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_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.

Prometheus metric	Description
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: • 10 = Offline • 15 = Maintenance • 20 = Read-only • 30 = Online
storagegrid_storage_status	The current status of the storage services. Attribute values are: • 0 = No Errors • 10 = In Transition • 20 = Insufficient Free Space • 30 = Volume(s) Unavailable • 40 = Error
storagegrid_storage_utilization_metadata_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_metadata_reserved_bytes	The total space on volume 0 of each Storage Node that is actually reserved for object metadata. For any given Storage Node, the actual reserved space for metadata depends on the size of volume 0 for the node and the system-wide Metadata Reserved Space setting.
storagegrid_storage_utilization_total_space_bytes	The total amount of storage space allocated to all object stores.

Prometheus metric	Description
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.
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.

Copyright information

Trademark information