



Alarms reference (legacy system)

StorageGRID

NetApp
June 10, 2022

Table of Contents

Alarms reference (legacy system) 1
 Alarms that generate SNMP notifications (legacy system) 25

Alarms reference (legacy system)

The following table lists all of the legacy Default alarms. If an alarm is triggered, you can look up the alarm code in this table to find the recommended actions.



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

Code	Name	Service	Recommended action
ABRL	Available Attribute Relays	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	<p>Restore connectivity to a service (an ADC service) running an Attribute Relay Service as soon as possible. If there are no connected attribute relays, the grid node cannot report attribute values to the NMS service. Thus, the NMS service can no longer monitor the status of the service, or update attributes for the service.</p> <p>If the problem persists, contact technical support.</p>
ACMS	Available Metadata Services	BARC, BLDR, BCMN	<p>An alarm is triggered when an LDR or ARC service loses connection to a DDS service. If this occurs, ingest or retrieve transactions cannot be processed. If the unavailability of DDS services is only a brief transient issue, transactions can be delayed.</p> <p>Check and restore connections to a DDS service to clear this alarm and return the service to full functionality.</p>
ACTS	Cloud Tiering Service Status	ARC	<p>Only available for Archive Nodes with a Target Type of Cloud Tiering - Simple Storage Service (S3).</p> <p>If the ACTS attribute for the Archive Node is set to Read-Only Enabled or Read-Write Disabled, you must set the attribute to Read-Write Enabled.</p> <p>If a major alarm is triggered due to an authentication failure, verify the credentials associated with destination bucket and update values, if necessary.</p> <p>If a major alarm is triggered due to any other reason, contact technical support.</p>
ADCA	ADC Status	ADC	<p>If an alarm is triggered, select SUPPORT > Tools > Grid topology. Then select <i>site > grid node > ADC > Overview > Main</i> and ADC > Alarms > Main to determine the cause of the alarm.</p> <p>If the problem persists, contact technical support.</p>

Code	Name	Service	Recommended action
ADCE	ADC State	ADC	<p>If the value of ADC State is Standby, continue monitoring the service and if the problem persists, contact technical support.</p> <p>If the value of ADC State is Offline, restart the service. If the problem persists, contact technical support.</p>
AITE	Retrieve State	BARC	<p>Only available for Archive Node's with a Target Type of Tivoli Storage Manager (TSM).</p> <p>If the value of Retrieve State is Waiting for Target, check the TSM middleware server and ensure that it is operating correctly. If the Archive Node has just been added to the StorageGRID system, ensure that the Archive Node's connection to the targeted external archival storage system is configured correctly.</p> <p>If the value of Archive Retrieve State is Offline, attempt to update the state to Online. Select SUPPORT > Tools > Grid topology. Then select site > grid node > ARC > Retrieve > Configuration > Main, select Archive Retrieve State > Online, and click Apply Changes.</p> <p>If the problem persists, contact technical support.</p>
AITU	Retrieve Status	BARC	<p>If the value of Retrieve Status is Target Error, check the targeted external archival storage system for errors.</p> <p>If the value of Archive Retrieve Status is Session Lost, check the targeted external archival storage system to ensure it is online and operating correctly. Check the network connection with the target.</p> <p>If the value of Archive Retrieve Status is Unknown Error, contact technical support.</p>
ALIS	Inbound Attribute Sessions	ADC	<p>If the number of inbound attribute sessions on an attribute relay grows too large, it can be an indication that the StorageGRID system has become unbalanced. Under normal conditions, attribute sessions should be evenly distributed amongst ADC services. An imbalance can lead to performance issues.</p> <p>If the problem persists, contact technical support.</p>

Code	Name	Service	Recommended action
ALOS	Outbound Attribute Sessions	ADC	The ADC service has a high number of attribute sessions, and is becoming overloaded. If this alarm is triggered, contact technical support.
ALUR	Unreachable Attribute Repositories	ADC	<p>Check network connectivity with the NMS service to ensure that the service can contact the attribute repository.</p> <p>If this alarm is triggered and network connectivity is good, contact technical support.</p>
AMQS	Audit Messages Queued	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	<p>If audit messages cannot be immediately forwarded to an audit relay or repository, the messages are stored in a disk queue. If the disk queue becomes full, outages can occur.</p> <p>To allow you to respond in time to prevent an outage, AMQS alarms are triggered when the number of messages in the disk queue reaches the following thresholds:</p> <ul style="list-style-type: none"> • Notice: More than 100,000 messages • Minor: At least 500,000 messages • Major: At least 2,000,000 messages • Critical: At least 5,000,000 messages <p>If an AMQS alarm is triggered, check the load on the system—if there have been a significant number of transactions, the alarm should resolve itself over time. In this case, you can ignore the alarm.</p> <p>If the alarm persists and increases in severity, view a chart of the queue size. If the number is steadily increasing over hours or days, the audit load has likely exceeded the audit capacity of the system. Reduce the client operation rate or decrease the number of audit messages logged by changing the audit level to Error or Off. See Configure audit messages and log destinations.</p>

Code	Name	Service	Recommended action
AOTE	Store State	BARC	<p>Only available for Archive Node's with a Target Type of Tivoli Storage Manager (TSM).</p> <p>If the value of Store State is Waiting for Target, check the external archival storage system and ensure that it is operating correctly. If the Archive Node has just been added to the StorageGRID system, ensure that the Archive Node's connection to the targeted external archival storage system is configured correctly.</p> <p>If the value of Store State is Offline, check the value of Store Status. Correct any problems before moving the Store State back to Online.</p>
AOTU	Store Status	BARC	<p>If the value of Store Status is Session Lost check that the external archival storage system is connected and online.</p> <p>If the value of Target Error, check the external archival storage system for errors.</p> <p>If the value of Store Status is Unknown Error, contact technical support.</p>
APMS	Storage Multipath Connectivity	SSM	<p>If the multipath state alarm appears as "Degraded" (select SUPPORT > Tools > Grid topology, then select site > grid node > SSM > Events), do the following:</p> <ol style="list-style-type: none"> 1. Plug in or replace the cable that does not display any indicator lights. 2. Wait one to five minutes. <p>Do not unplug the other cable until at least five minutes after you plug in the first one. Unplugging too early can cause the root volume to become read-only, which requires that the hardware be restarted.</p> <ol style="list-style-type: none"> 3. Return to the SSM > Resources page, and verify that the "Degraded" Multipath status has changed to "Nominal" in the Storage Hardware section.

Code	Name	Service	Recommended action
ARCE	ARC State	ARC	<p>The ARC service has a state of Standby until all ARC components (Replication, Store, Retrieve, Target) have started. It then transitions to Online.</p> <p>If the value of ARC State does not transition from Standby to Online, check the status of the ARC components.</p> <p>If the value of ARC State is Offline, restart the service. If the problem persists, contact technical support.</p>
AROQ	Objects Queued	ARC	<p>This alarm can be triggered if the removable storage device is running slowly due to problems with the targeted external archival storage system, or if it encounters multiple read errors. Check the external archival storage system for errors, and ensure that it is operating correctly.</p> <p>In some cases, this error can occur as a result of a high rate of data requests. Monitor the number of objects queued as system activity declines.</p>
ARRF	Request Failures	ARC	<p>If a retrieval from the targeted external archival storage system fails, the Archive Node retries the retrieval as the failure can be due to a transient issue. However, if the object data is corrupt or has been marked as being permanently unavailable, the retrieval does not fail. Instead, the Archive Node continuously retries the retrieval and the value for Request Failures continues to increase.</p> <p>This alarm can indicate that the storage media holding the requested data is corrupt. Check the external archival storage system to further diagnose the problem.</p> <p>If you determine that the object data is no longer in the archive, the object will have to be removed from the StorageGRID system. For more information, contact technical support.</p> <p>Once the problem that triggered this alarm is addressed, reset the failures count. Select SUPPORT > Tools > Grid topology. Then select <i>site</i> > <i>grid node</i> > ARC > Retrieve > Configuration > Main, select Reset Request Failure Count and click Apply Changes.</p>

Code	Name	Service	Recommended action
ARRV	Verification Failures	ARC	<p>To diagnose and correct this problem, contact technical support.</p> <p>Once the problem that triggered this alarm is addressed, reset the failures count. Select SUPPORT > Tools > Grid topology. Then select <i>site > grid node > ARC > Retrieve > Configuration > Main</i>, select Reset Verification Failure Count and click Apply Changes.</p>
ARVF	Store Failures	ARC	<p>This alarm can occur as a result of errors with the targeted external archival storage system. Check the external archival storage system for errors, and ensure that it is operating correctly.</p> <p>Once the problem that triggered this alarm is addressed, reset the failures count. Select SUPPORT > Tools > Grid topology. Then select <i>site > grid node > ARC > Retrieve > Configuration > Main</i>, select Reset Store Failure Count, and click Apply Changes.</p>
ASXP	Audit Shares	AMS	<p>An alarm is triggered if the value of Audit Shares is Unknown. This alarm can indicate a problem with the installation or configuration of the Admin Node.</p> <p>If the problem persists, contact technical support.</p>
AUMA	AMS Status	AMS	<p>If the value of AMS Status is DB Connectivity Error, restart the grid node.</p> <p>If the problem persists, contact technical support.</p>
AUME	AMS State	AMS	<p>If the value of AMS State is Standby, continue monitoring the StorageGRID system. If the problem persists, contact technical support.</p> <p>If the value of AMS State is Offline, restart the service. If the problem persists, contact technical support.</p>
AUXS	Audit Export Status	AMS	<p>If an alarm is triggered, correct the underlying problem, and then restart the AMS service.</p> <p>If the problem persists, contact technical support.</p>
BADD	Storage Controller Failed Drive Count	SSM	<p>This alarm is triggered when one or more drives in a StorageGRID appliance has failed or is not optimal. Replace the drives as required.</p>

Code	Name	Service	Recommended action
BASF	Available Object Identifiers	CMN	<p>When a StorageGRID system is provisioned, the CMN service is allocated a fixed number of object identifiers. This alarm is triggered when the StorageGRID system begins to exhaust its supply of object identifiers.</p> <p>To allocate more identifiers, contact technical support.</p>
BASS	Identifier Block Allocation Status	CMN	<p>By default, an alarm is triggered when object identifiers cannot be allocated because ADC quorum cannot be reached.</p> <p>Identifier block allocation on the CMN service requires a quorum (50% + 1) of the ADC services to be online and connected. If quorum is unavailable, the CMN service is unable to allocate new identifier blocks until ADC quorum is re-established. If ADC quorum is lost, there is generally no immediate impact on the StorageGRID system (clients can still ingest and retrieve content), as approximately one month's supply of identifiers are cached elsewhere in the grid; however, if the condition continues, the StorageGRID system will lose the ability to ingest new content.</p> <p>If an alarm is triggered, investigate the reason for the loss of ADC quorum (for example, it can be a network or Storage Node failure) and take corrective action.</p> <p>If the problem persists, contact technical support.</p>
BRDT	Compute Controller Chassis Temperature	SSM	<p>An alarm is triggered if the temperature of the compute controller in a StorageGRID appliance exceeds a nominal threshold.</p> <p>Check hardware components and environmental issues for overheated condition. If necessary, replace the component.</p>
BTOF	Offset	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	<p>An alarm is triggered if the service time (seconds) differs significantly from the operating system time. Under normal conditions, the service should resynchronize itself. If the service time drifts too far from the operating system time, system operations can be affected. Confirm that the StorageGRID system's time source is correct.</p> <p>If the problem persists, contact technical support.</p>

Code	Name	Service	Recommended action
BTSE	Clock State	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	<p>An alarm is triggered if the service's time is not synchronized with the time tracked by the operating system. Under normal conditions, the service should resynchronize itself. If the time drifts too far from operating system time, system operations can be affected. Confirm that the StorageGRID system's time source is correct.</p> <p>If the problem persists, contact technical support.</p>
CAHP	Java Heap Usage Percent	DDS	<p>An alarm is triggered if Java is unable to perform garbage collection at a rate that allows enough heap space for the system to properly function. An alarm might indicate a user workload that exceeds the resources available across the system for the DDS metadata store. Check the ILM Activity in the Dashboard, or select SUPPORT > Tools > Grid topology, then select <i>site</i> > <i>grid node</i> > DDS > Resources > Overview > Main.</p> <p>If the problem persists, contact technical support.</p>
CAIH	Number Available Ingest Destinations	CLB	This alarm is deprecated.
CAQH	Number Available Destinations	CLB	<p>This alarm clears when underlying issues of available LDR services are corrected. Ensure that the HTTP component of LDR services are online and running normally.</p> <p>If the problem persists, contact technical support.</p>

Code	Name	Service	Recommended action
CASA	Data Store Status	DDS	<p>An alarm is raised if the Cassandra metadata store becomes unavailable.</p> <p>Check the status of Cassandra:</p> <ol style="list-style-type: none"> 1. At the Storage Node, log in as admin and <code>su</code> to root using the password listed in the <code>Passwords.txt</code> file. 2. Enter: <code>service cassandra status</code> 3. If Cassandra is not running, restart it: <code>service cassandra restart</code> <p>This alarm might also indicate that the metadata store (Cassandra database) for a Storage Node requires rebuilding.</p> <p>See information about troubleshooting the Services: Status - Cassandra (SVST) alarm in Troubleshoot metadata issues.</p> <p>If the problem persists, contact technical support.</p>
CASE	Data Store State	DDS	<p>This alarm is triggered during installation or expansion to indicate a new data store is joining the grid.</p>
CCES	Incoming Sessions - Established	CLB	<p>This alarm is triggered if there are 20,000 or more HTTP sessions currently active (open) on the Gateway Node. If a client has too many connections, you might see connection failures. You should reduce the workload.</p>
CCNA	Compute Hardware	SSM	<p>This alarm is triggered if the status of the compute controller hardware in a StorageGRID appliance is Needs Attention.</p>

Code	Name	Service	Recommended action
CDLP	Metadata Used Space (Percent)	DDS	<p>This alarm is triggered when the Metadata Effective Space (CEMS) reaches 70% full (minor alarm), 90% full (major alarm), and 100% full (critical alarm).</p> <p>If this alarm reaches the 90% threshold, a warning appears on the Dashboard in the Grid Manager. You must perform an expansion procedure to add new Storage Nodes as soon as possible. See Expand your grid.</p> <p>If this alarm reaches the 100% threshold, you must stop ingesting objects and add Storage Nodes immediately. Cassandra requires a certain amount of space to perform essential operations such as compaction and repair. These operations will be impacted if object metadata uses more than 100% of the allowed space. Undesirable results can occur.</p> <p>Note: Contact technical support if you are unable to add Storage Nodes.</p> <p>After new Storage Nodes are added, the system automatically rebalances object metadata across all Storage Nodes, and the alarm clears.</p> <p>Also see information about troubleshooting the Low metadata storage alert in Troubleshoot metadata issues.</p>
CLBA	CLB Status	CLB	<p>If an alarm is triggered, select SUPPORT > Tools > Grid topology, then select <i>site > grid node > CLB > Overview > Main</i> and CLB > Alarms > Main to determine the cause of the alarm and to troubleshoot the problem.</p> <p>If the problem persists, contact technical support.</p>
CLBE	CLB State	CLB	<p>If the value of CLB State is Standby, continue monitoring the situation and if the problem persists, contact technical support.</p> <p>If the state is Offline and there are no known server hardware issues (for example, the server is unplugged) or scheduled downtime, restart the service. If the problem persists, contact technical support.</p>

Code	Name	Service	Recommended action
CMNA	CMN Status	CMN	<p>If the value of CMN Status is Error, select SUPPORT > Tools > Grid topology, then select <i>site > grid node > CMN > Overview > Main</i> and CMN > Alarms > Main to determine the cause of the error and to troubleshoot the problem.</p> <p>An alarm is triggered and the value of CMN Status is No Online CMN during a hardware refresh of the primary Admin Node when the CMNs are switched (the value of the old CMN State is Standby and the new is Online).</p> <p>If the problem persists, contact technical support.</p>
CPRC	Remaining Capacity	NMS	<p>An alarm is triggered if the remaining capacity (number of available connections that can be opened to the NMS database) falls below the configured alarm severity.</p> <p>If an alarm is triggered, contact technical support.</p>
CPSA	Compute Controller Power Supply A	SSM	<p>An alarm is triggered if there is an issue with power supply A in the compute controller for a StorageGRID appliance.</p> <p>If necessary, replace the component.</p>
CPSB	Compute Controller Power Supply B	SSM	<p>An alarm is triggered if there is an issue with power supply B in the compute controller for a StorageGRID appliance.</p> <p>If necessary, replace the component.</p>
CPUT	Compute Controller CPU Temperature	SSM	<p>An alarm is triggered if the temperature of the CPU in the compute controller in a StorageGRID appliance exceeds a nominal threshold.</p> <p>If the Storage Node is a StorageGRID appliance, the StorageGRID system indicates that the controller needs attention.</p> <p>Check hardware components and environment issues for overheated condition. If necessary, replace the component.</p>
DNST	DNS Status	SSM	<p>After installation completes, a DNST alarm is triggered in the SSM service. After the DNS is configured and the new server information reaches all grid nodes, the alarm is canceled.</p>

Code	Name	Service	Recommended action
ECCD	Corrupt Fragments Detected	LDR	<p>An alarm is triggered when the background verification process detects a corrupt erasure coded fragment. If a corrupt fragment is detected, an attempt is made to rebuild the fragment. Reset the Corrupt Fragments Detected and Copies Lost attributes to zero and monitor them to see if counts go up again. If counts do go up, there may be a problem with the Storage Node's underlying storage. A copy of erasure coded object data is not considered missing until such time that the number of lost or corrupt fragments breaches the erasure code's fault tolerance; therefore, it is possible to have corrupt fragment and to still be able to retrieve the object.</p> <p>If the problem persists, contact technical support.</p>
ECST	Verification Status	LDR	<p>This alarm indicates the current status of the background verification process for erasure coded object data on this Storage Node.</p> <p>A major alarm is triggered if there is an error in the background verification process.</p>
FOPN	Open File Descriptors	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	<p>FOPN can become large during peak activity. If it does not diminish during periods of slow activity, contact technical support.</p>
HSTE	HTTP State	BLDR	<p>See recommended actions for HSTU.</p>

Code	Name	Service	Recommended action
HSTU	HTTP Status	BLDR	<p>HSTE and HSTU are related to the HTTP protocol for all LDR traffic, including S3, Swift, and other internal StorageGRID traffic. An alarm indicates that one of the following situations has occurred:</p> <ul style="list-style-type: none"> • The HTTP protocol has been taken offline manually. • The Auto-Start HTTP attribute has been disabled. • The LDR service is shutting down. <p>The Auto-Start HTTP attribute is enabled by default. If this setting is changed, HTTP could remain offline after a restart.</p> <p>If necessary, wait for the LDR service to restart.</p> <p>Select SUPPORT > Tools > Grid topology. Then select Storage Node > LDR > Configuration. If the HTTP protocol is offline, place it online. Verify that the Auto-Start HTTP attribute is enabled.</p> <p>If the HTTP protocol remains offline, contact technical support.</p>
HTAS	Auto-Start HTTP	LDR	<p>Specifies whether to start HTTP services automatically on start-up. This is a user-specified configuration option.</p>
IRSU	Inbound Replication Status	BLDR, BARC	<p>An alarm indicates that inbound replication has been disabled. Confirm configuration settings: Select SUPPORT > Tools > Grid topology. Then select site > grid node > LDR > Replication > Configuration > Main.</p>
LATA	Average Latency	NMS	<p>Check for connectivity issues.</p> <p>Check system activity to confirm that there is an increase in system activity. An increase in system activity will result in an increase to attribute data activity. This increased activity will result in a delay to the processing of attribute data. This can be normal system activity and will subside.</p> <p>Check for multiple alarms. An increase in average latency times can be indicated by an excessive number of triggered alarms.</p> <p>If the problem persists, contact technical support.</p>

Code	Name	Service	Recommended action
LDRE	LDR State	LDR	<p>If the value of LDR State is Standby, continue monitoring the situation and if the problem persists, contact technical support.</p> <p>If the value of LDR State is Offline, restart the service. If the problem persists, contact technical support.</p>
LOST	Lost Objects	DDS, LDR	<p>Triggered when the StorageGRID system fails to retrieve a copy of the requested object from anywhere in the system. Before a LOST (Lost Objects) alarm is triggered, the system attempts to retrieve and replace a missing object from elsewhere in the system.</p> <p>Lost objects represent a loss of data. The Lost Objects attribute is incremented whenever the number of locations for an object drops to zero without the DDS service purposely purging the content to satisfy the ILM policy.</p> <p>Investigate LOST (LOST Object) alarms immediately. If the problem persists, contact technical support.</p> <p>Troubleshoot lost and missing object data</p>
MCEP	Management Interface Certificate Expiry	CMN	<p>Triggered when the certificate used for accessing the management interface is about to expire.</p> <ol style="list-style-type: none"> 1. From the Grid Manager, select CONFIGURATION > Security > Certificates. 2. On the Global tab, select Management interface certificate. 3. Upload a new management interface certificate.
MINQ	E-mail Notifications Queued	NMS	<p>Check the network connections of the servers hosting the NMS service and the external mail server. Also confirm that the email server configuration is correct.</p> <p>Configure email server settings for alarms (legacy system)</p>
MINS	E-mail Notifications Status	BNMS	<p>A minor alarm is triggered if the NMS service is unable to connect to the mail server. Check the network connections of the servers hosting the NMS service and the external mail server. Also confirm that the email server configuration is correct.</p> <p>Configure email server settings for alarms (legacy system)</p>

Code	Name	Service	Recommended action
MISS	NMS Interface Engine Status	BNMS	An alarm is triggered if the NMS interface engine on the Admin Node that gathers and generates interface content is disconnected from the system. Check Server Manager to determine if the server individual application is down.
NANG	Network Auto Negotiate Setting	SSM	<p>Check the network adapter configuration. The setting must match preferences of your network routers and switches.</p> <p>An incorrect setting can have a severe impact on system performance.</p>
NDUP	Network Duplex Setting	SSM	<p>Check the network adapter configuration. The setting must match preferences of your network routers and switches.</p> <p>An incorrect setting can have a severe impact on system performance.</p>
NLNK	Network Link Detect	SSM	<p>Check the network cable connections on the port and at the switch.</p> <p>Check the network router, switch, and adapter configurations.</p> <p>Restart the server.</p> <p>If the problem persists, contact technical support.</p>
NRER	Receive Errors	SSM	<p>The following can be causes of NRER alarms:</p> <ul style="list-style-type: none"> • Forward error correction (FEC) mismatch • Switch port and NIC MTU mismatch • High link error rates • NIC ring buffer overrun <p>See information about troubleshooting the Network Receive Error (NRER) alarm in Troubleshoot network, hardware, and platform issues.</p>

Code	Name	Service	Recommended action
NRLY	Available Audit Relays	BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	<p>If audit relays are not connected to ADC services, audit events cannot be reported. They are queued and unavailable to users until the connection is restored.</p> <p>Restore connectivity to an ADC service as soon as possible.</p> <p>If the problem persists, contact technical support.</p>
NSCA	NMS Status	NMS	<p>If the value of NMS Status is DB Connectivity Error, restart the service. If the problem persists, contact technical support.</p>
NSCE	NMS State	NMS	<p>If the value of NMS State is Standby, continue monitoring and if the problem persists, contact technical support.</p> <p>If the value of NMS State is Offline, restart the service. If the problem persists, contact technical support.</p>
NSPD	Speed	SSM	<p>This can be caused by network connectivity or driver compatibility issues. If the problem persists, contact technical support.</p>
NTBR	Free Tablespace	NMS	<p>If an alarm is triggered, check how fast database usage has been changing. A sudden drop (as opposed to a gradual change over time) indicates an error condition. If the problem persists, contact technical support.</p> <p>Adjusting the alarm threshold allows you to proactively manage when additional storage needs to be allocated.</p> <p>If the available space reaches a low threshold (see alarm threshold), contact technical support to change the database allocation.</p>


Code	Name	Service	Recommended action
NTER	Transmit Errors	SSM	<p>These errors can clear without being manually reset. If they do not clear, check network hardware. Check that the adapter hardware and driver are correctly installed and configured to work with your network routers and switches.</p> <p>When the underlying problem is resolved, reset the counter. Select SUPPORT > Tools > Grid topology. Then select <i>site</i> > <i>grid node</i> > SSM > Resources > Configuration > Main, select Reset Transmit Error Count, and click Apply Changes.</p>
NTFQ	NTP Frequency Offset	SSM	<p>If the frequency offset exceeds the configured threshold, there is likely a hardware problem with the local clock. If the problem persists, contact technical support to arrange a replacement.</p>
NTLK	NTP Lock	SSM	<p>If the NTP daemon is not locked to an external time source, check network connectivity to the designated external time sources, their availability, and their stability.</p>
NTOF	NTP Time Offset	SSM	<p>If the time offset exceeds the configured threshold, there is likely a hardware problem with the oscillator of the local clock. If the problem persists, contact technical support to arrange a replacement.</p>
NTSJ	Chosen Time Source Jitter	SSM	<p>This value indicates the reliability and stability of the time source that NTP on the local server is using as its reference.</p> <p>If an alarm is triggered, it can be an indication that the time source's oscillator is defective, or that there is a problem with the WAN link to the time source.</p>
NTSU	NTP Status	SSM	<p>If the value of NTP Status is Not Running, contact technical support.</p>
OPST	Overall Power Status	SSM	<p>An alarm is triggered if the power of a StorageGRID appliance deviates from the recommended operating voltage.</p> <p>Check the status of Power Supply A or B to determine which power supply is operating abnormally.</p> <p>If necessary, replace the power supply.</p>

Code	Name	Service	Recommended action
OQRT	Objects Quarantined	LDR	<p>After the objects are automatically restored by the StorageGRID system, the quarantined objects can be removed from the quarantine directory.</p> <ol style="list-style-type: none"> 1. Select SUPPORT > Tools > Grid topology. 2. Select site > Storage Node > LDR > Verification > Configuration > Main. 3. Select Delete Quarantined Objects. 4. Click Apply Changes. <p>The quarantined objects are removed, and the count is reset to zero.</p>
ORSU	Outbound Replication Status	BLDR, BARC	<p>An alarm indicates that outbound replication is not possible: storage is in a state where objects cannot be retrieved. An alarm is triggered if outbound replication is disabled manually. Select SUPPORT > Tools > Grid topology. Then select site > grid node > LDR > Replication > Configuration.</p> <p>An alarm is triggered if the LDR service is unavailable for replication. Select SUPPORT > Tools > Grid topology. Then select site > grid node > LDR > Storage.</p>
OSLF	Shelf Status	SSM	<p>An alarm is triggered if the status of one of the components in the storage shelf for a storage appliance is degraded. Storage shelf components include the IOMs, fans, power supplies, and drive drawers. If this alarm is triggered, see the maintenance instructions for your appliance.</p>
PMEM	Service Memory Usage (Percent)	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	<p>Can have a value of Over Y% RAM, where Y represents the percentage of memory being used by the server.</p> <p>Figures under 80% are normal. Over 90% is considered a problem.</p> <p>If memory usage is high for a single service, monitor the situation and investigate.</p> <p>If the problem persists, contact technical support.</p>
PSAS	Power Supply A Status	SSM	<p>An alarm is triggered if power supply A in a StorageGRID appliance deviates from the recommended operating voltage.</p> <p>If necessary, replace power supply A.</p>

Code	Name	Service	Recommended action
PSBS	Power Supply B Status	SSM	<p>An alarm is triggered if power supply B in a StorageGRID appliance deviates from the recommended operating voltage.</p> <p>If necessary, replace the power supply B.</p>
RDTE	Tivoli Storage Manager State	BARC	<p>Only available for Archive Nodes with a Target Type of Tivoli Storage Manager (TSM).</p> <p>If the value of Tivoli Storage Manager State is Offline, check Tivoli Storage Manager Status and resolve any problems.</p> <p>Bring the component back online. Select SUPPORT > Tools > Grid topology. Then select <i>site</i> > grid node > ARC > Target > Configuration > Main, select Tivoli Storage Manager State > Online, and click Apply Changes.</p>
RDTU	Tivoli Storage Manager Status	BARC	<p>Only available for Archive Nodes with a Target Type of Tivoli Storage Manager (TSM).</p> <p>If the value of Tivoli Storage Manager Status is Configuration Error and the Archive Node has just been added to the StorageGRID system, ensure that the TSM middleware server is correctly configured.</p> <p>If the value of Tivoli Storage Manager Status is Connection Failure, or Connection Failure, Retrying, check the network configuration on the TSM middleware server, and the network connection between the TSM middleware server and the StorageGRID system.</p> <p>If the value of Tivoli Storage Manager Status is Authentication Failure, or Authentication Failure, Reconnecting, the StorageGRID system can connect to the TSM middleware server, but cannot authenticate the connection. Check that the TSM middleware server is configured with the correct user, password, and permissions, and restart the service.</p> <p>If the value of Tivoli Storage Manager Status is Session Failure, an established session has been lost unexpectedly. Check the network connection between the TSM middleware server and the StorageGRID system. Check the middleware server for errors.</p> <p>If the value of Tivoli Storage Manager Status is Unknown Error, contact technical support.</p>

Code	Name	Service	Recommended action
RIRF	Inbound Replications — Failed	BLDR, BARC	<p>An Inbound Replications — Failed alarm can occur during periods of high load or temporary network disruptions. After system activity reduces, this alarm should clear. If the count of failed replications continues to increase, look for network problems and verify that the source and destination LDR and ARC services are online and available.</p> <p>To reset the count, select SUPPORT > Tools > Grid topology, then select <i>site</i> > <i>grid node</i> > LDR > Replication > Configuration > Main. Select Reset Inbound Replication Failure Count, and click Apply Changes.</p>
RIRQ	Inbound Replications — Queued	BLDR, BARC	<p>Alarms can occur during periods of high load or temporary network disruption. After system activity reduces, this alarm should clear. If the count for queued replications continues to increase, look for network problems and verify that the source and destination LDR and ARC services are online and available.</p>
RORQ	Outbound Replications — Queued	BLDR, BARC	<p>The outbound replication queue contains object data being copied to satisfy ILM rules and objects requested by clients.</p> <p>An alarm can occur as a result of a system overload. Wait to see if the alarm clears when system activity declines. If the alarm recurs, add capacity by adding Storage Nodes.</p>
SAVP	Total Usable Space (Percent)	LDR	<p>If usable space reaches a low threshold, options include expanding the StorageGRID system or move object data to archive through an Archive Node.</p>

Code	Name	Service	Recommended action
SCAS	Status	CMN	<p>If the value of Status for the active grid task is Error, look up the grid task message. Select SUPPORT > Tools > Grid topology. Then select <i>site > grid node > CMN > Grid Tasks > Overview > Main</i>. The grid task message displays information about the error (for example, “check failed on node 12130011”).</p> <p>After you have investigated and corrected the problem, restart the grid task. Select SUPPORT > Tools > Grid topology. Then select <i>site > grid node > CMN > Grid Tasks > Configuration > Main</i>, and select Actions > Run.</p> <p>If the value of Status for a grid task being aborted is Error, retry aborting the grid task.</p> <p>If the problem persists, contact technical support.</p>
SCEP	Storage API Service Endpoints Certificate Expiry	CMN	<p>Triggered when the certificate used for accessing storage API endpoints is about to expire.</p> <ol style="list-style-type: none"> 1. Select CONFIGURATION > Security > Certificates. 2. On the Global tab, select S3 and Swift API certificate. 3. Upload a new S3 and Swift API certificate.
SCHR	Status	CMN	<p>If the value of Status for the historical grid task is Aborted, investigate the reason and run the task again if required.</p> <p>If the problem persists, contact technical support.</p>
SCSA	Storage Controller A	SSM	<p>An alarm is triggered if there is an issue with storage controller A in a StorageGRID appliance.</p> <p>If necessary, replace the component.</p>
SCSB	Storage Controller B	SSM	<p>An alarm is triggered if there is an issue with storage controller B in a StorageGRID appliance.</p> <p>If necessary, replace the component.</p> <p>Some appliance models do not have a storage controller B.</p>

Code	Name	Service	Recommended action
SHLH	Health	LDR	<p>If the value of Health for an object store is Error, check and correct:</p> <ul style="list-style-type: none"> • problems with the volume being mounted • file system errors
SLSA	CPU Load Average	SSM	<p>The higher the value the busier the system.</p> <p>If the CPU Load Average persists at a high value, the number of transactions in the system should be investigated to determine whether this is due to heavy load at the time. View a chart of the CPU load average: Select SUPPORT > Tools > Grid topology. Then select <i>site</i> > <i>grid node</i> > SSM > Resources > Reports > Charts.</p> <p>If the load on the system is not heavy and the problem persists, contact technical support.</p>
SMST	Log Monitor State	SSM	<p>If the value of Log Monitor State is not Connected for a persistent period of time, contact technical support.</p>
SMTT	Total Events	SSM	<p>If the value of Total Events is greater than zero, check if there are known events (such as network failures) that can be the cause. Unless these errors have been cleared (that is, the count has been reset to 0), Total Events alarms can be triggered.</p> <p>When an issue is resolved, reset the counter to clear the alarm. Select NODES > site > grid node > Events > Reset event counts.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  To reset event counts, you must have the Grid Topology Page Configuration permission. </div> <p>If the value of Total Events is zero, or the number increases and the problem persists, contact technical support.</p>
SNST	Status	CMN	<p>An alarm indicates that there is a problem storing the grid task bundles. If the value of Status is Checkpoint Error or Quorum Not Reached, confirm that a majority of ADC services are connected to the StorageGRID system (50 percent plus one) and then wait a few minutes.</p> <p>If the problem persists, contact technical support.</p>

Code	Name	Service	Recommended action
SOSS	Storage Operating System Status	SSM	<p>An alarm is triggered if SANtricity software indicates that there is a “Needs attention” issue with a component in a StorageGRID appliance.</p> <p>Select NODES. Then select appliance Storage Node > Hardware. Scroll down to view the status of each component. In SANtricity software, check other appliance components to isolate the issue.</p>
SSMA	SSM Status	SSM	<p>If the value of SSM Status is Error, select SUPPORT > Tools > Grid topology, then select site > grid node > SSM > Overview > Main and SSM > Overview > Alarms to determine the cause of the alarm.</p> <p>If the problem persists, contact technical support.</p>
SSME	SSM State	SSM	<p>If the value of SSM State is Standby, continue monitoring, and if the problem persists, contact technical support.</p> <p>If the value of SSM State is Offline, restart the service. If the problem persists, contact technical support.</p>
SSTS	Storage Status	BLDR	<p>If the value of Storage Status is Insufficient Usable Space, there is no more available storage on the Storage Node and data ingests are redirected to other available Storage Node. Retrieval requests can continue to be delivered from this grid node.</p> <p>Additional storage should be added. It is not impacting end user functionality, but the alarm persists until additional storage is added.</p> <p>If the value of Storage Status is Volume(s) Unavailable, a part of the storage is unavailable. Storage and retrieval from these volumes is not possible. Check the volume’s Health for more information: Select SUPPORT > Tools > Grid topology. Then select site > grid node > LDR > Storage > Overview > Main. The volume’s Health is listed under Object Stores.</p> <p>If the value of Storage Status is Error, contact technical support.</p> <p>Troubleshoot the Storage Status (SSTS) alarm</p>

Code	Name	Service	Recommended action
SVST	Status	SSM	<p>This alarm clears when other alarms related to a non-running service are resolved. Track the source service alarms to restore operation.</p> <p>Select SUPPORT > Tools > Grid topology. Then select site > grid node > SSM > Services > Overview > Main. When the status of a service is shown as Not Running, its state is Administratively Down. The service's status can be listed as Not Running for the following reasons:</p> <ul style="list-style-type: none"> • The service has been manually stopped (<code>/etc/init.d/<service> stop</code>). • There is an issue with the MySQL database and Server Manager shuts down the MI service. • A grid node has been added, but not started. • During installation, a grid node has not yet connected to the Admin Node. <p>If a service is listed as Not Running, restart the service (<code>/etc/init.d/<service> restart</code>).</p> <p>This alarm might also indicate that the metadata store (Cassandra database) for a Storage Node requires rebuilding.</p> <p>If the problem persists, contact technical support.</p> <p>Troubleshoot the Services: Status - Cassandra (SVST) alarm</p>
TMEM	Installed Memory	SSM	<p>Nodes running with less than 24 GiB of installed memory can lead to performance problems and system instability. The amount of memory installed on the system should be increased to at least 24 GiB.</p>
TPOP	Pending Operations	ADC	<p>A queue of messages can indicate that the ADC service is overloaded. Too few ADC services can be connected to the StorageGRID system. In a large deployment, the ADC service can require adding computational resources, or the system can require additional ADC services.</p>
UMEM	Available Memory	SSM	<p>If the available RAM gets low, determine whether this is a hardware or software issue. If it is not a hardware issue, or if available memory falls below 50 MB (the default alarm threshold), contact technical support.</p>

Code	Name	Service	Recommended action
VMFI	Entries Available	SSM	This is an indication that additional storage is required. Contact technical support.
VMFR	Space Available	SSM	If the value of Space Available gets too low (see alarm thresholds), it needs to be investigated as to whether there are log files growing out of proportion, or objects taking up too much disk space (see alarm thresholds) that need to be reduced or deleted. If the problem persists, contact technical support.
VMST	Status	SSM	An alarm is triggered if the value of Status for the mounted volume is Unknown. A value of Unknown or Offline can indicate that the volume cannot be mounted or accessed due to a problem with the underlying storage device.
VPRI	Verification Priority	BLDR, BARC	By default, the value of Verification Priority is Adaptive. If Verification Priority is set to High, an alarm is triggered because storage verification can slow normal operations of the service.
VSTU	Object Verification Status	BLDR	Select SUPPORT > Tools > Grid topology . Then select site > grid node > LDR > Storage > Overview > Main . Check the operating system for any signs of block-device or file system errors. If the value of Object Verification Status is Unknown Error, it usually indicates a low-level file system or hardware problem (I/O error) that prevents the Storage Verification task from accessing stored content. Contact technical support.
XAMS	Unreachable Audit Repositories	BADC, BARC, BCLB, BCMN, BLDR, BNMS	Check network connectivity to the server hosting the Admin Node. If the problem persists, contact technical support.

Alarms that generate SNMP notifications (legacy system)

The following table lists the legacy alarms that generate SNMP notifications. Unlike alerts, not all alarms generate SNMP notifications. Only the alarms listed generate SNMP notifications and only at the indicated severity or higher.



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

Code	Name	Severity
ACMS	Available Metadata Services	Critical
AITE	Retrieve State	Minor
AITU	Retrieve Status	Major
AMQS	Audit Messages Queued	Notice
AOTE	Store State	Minor
AOTU	Store Status	Major
AROQ	Objects Queued	Minor
ARRF	Request Failures	Major
ARRV	Verification Failures	Major
ARVF	Store Failures	Major
ASXP	Audit Shares	Minor
AUMA	AMS Status	Minor
AUXS	Audit Export Status	Minor
BTOF	Offset	Notice
CAHP	Java Heap Usage Percent	Major
CAQH	Number Available Destinations	Notice
CASA	Data Store Status	Major
CDLP	Metadata Used Space (Percent)	Major
CLBE	CLB State	Critical
DNST	DNS Status	Critical
ECST	Verification Status	Major
HSTE	HTTP State	Major

Code	Name	Severity
HTAS	Auto-Start HTTP	Notice
LOST	Lost Objects	Major
MINQ	E-mail Notifications Queued	Notice
MINS	E-mail Notifications Status	Minor
NANG	Network Auto Negotiate Setting	Notice
NDUP	Network Duplex Setting	Minor
NLNK	Network Link Detect	Minor
NRER	Receive Errors	Notice
NSPD	Speed	Notice
NTER	Transmit Errors	Notice
NTFQ	NTP Frequency Offset	Minor
NTLK	NTP Lock	Minor
NTOF	NTP Time Offset	Minor
NTSJ	Chosen Time Source Jitter	Minor
NTSU	NTP Status	Major
OPST	Overall Power Status	Major
ORSU	Outbound Replication Status	Notice
PSAS	Power Supply A Status	Major
PSBS	Power Supply B Status	Major
RDTE	Tivoli Storage Manager State	Notice
RDTU	Tivoli Storage Manager Status	Major
SAVP	Total Usable Space (Percent)	Notice

Code	Name	Severity
SHLH	Health	Notice
SLSA	CPU Load Average	Notice
SMTT	Total Events	Notice
SNST	Status	
SOSS	Storage Operating System Status	Notice
SSTS	Storage Status	Notice
SVST	Status	Notice
TMEM	Installed Memory	Minor
UMEM	Available Memory	Minor
VMST	Status	Minor
VPRI	Verification Priority	Notice
VSTU	Object Verification Status	Notice

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.