# Contents

**Understanding the StorageGRID Webscale system** ......................... 8  
What the StorageGRID Webscale system is ................................................ 8  
Working with the StorageGRID Webscale system ........................................... 9  
  - Signing in to the StorageGRID Webscale system ................................... 11  
  - Signing out of the StorageGRID Webscale system ................................. 13  
  - Changing your password ........................................................................ 13  
  - Changing the browser session timeout period ....................................... 13  
  - Viewing StorageGRID Webscale license information ............................ 14  
  - Updating StorageGRID Webscale license information ........................... 14  
  - Understanding the StorageGRID Webscale Management API .................. 15  

**Managing storage tenant accounts** ....................................................... 19  
  - Managing S3 tenant accounts ................................................................. 19  
  - Creating tenant accounts for S3 ............................................................ 19  
  - Editing tenant accounts for S3 ............................................................... 20  
  - Editing group policies for S3 tenant accounts ....................................... 21  
  - Editing S3 root keys for S3 tenant accounts ......................................... 26  
  - Managing Swift tenant accounts ............................................................ 27  
  - Creating tenant accounts for Swift ....................................................... 27  
  - Editing tenant accounts for Swift .......................................................... 28  
  - Editing group policies for Swift tenant accounts .................................... 29  
  - Deleting tenant accounts ....................................................................... 29  
  - Configuring LDAP for identity federation .............................................. 30  
  - OpenLDAP server configuration guidelines .......................................... 31  
  - Disabling LDAP for identity federation ................................................ 31  
  - Manually forcing synchronization with the LDAP server ........................ 32  
  - Managing federated user S3 credentials ................................................ 32  

**Monitoring the StorageGRID Webscale system** ................................... 34  
  - About alarms and email notifications ..................................................... 34  
  - Alarm notification types ......................................................................... 34  
  - Notification status and queues ............................................................... 35  
  - Configuring notifications ....................................................................... 35  
  - Suppressing email notifications for a mailing list .................................. 42  
  - Suppressing email notifications system wide ....................................... 42  
  - Selecting a preferred sender ................................................................. 43  
  - Alarms management ............................................................................. 44  
  - Alarm class types .................................................................................. 44  
  - Alarm triggering logic ............................................................................ 47  
  - Creating custom service or component alarms ..................................... 50  
  - Creating custom global alarms .............................................................. 52  
  - Disabling alarms ................................................................................... 54  
  - Alarms and tables .................................................................................. 55
Disabling default alarms for services ............................................................  55
Disabling a default alarm system wide .........................................................  56
Disabling global custom alarms for services .................................................  57
Disabling global custom alarms system wide ..............................................  58
Clearing triggered alarms ..............................................................................  59

What AutoSupport is ................................................................................................. 60
Triggering AutoSupport messages ................................................................  60
Disabling weekly AutoSupport messages .....................................................  61
Troubleshooting AutoSupport ....................................................................... 62

Monitoring servers and grid nodes ............................................................... 62
What is the SSM service .............................................................................  62
Monitoring StorageGRID Webscale Appliance Storage Nodes ............... 64

Managing objects through information lifecycle management ...............  70
What an information lifecycle management policy is ........................................  70
What an information lifecycle management rule is .........................................  71
How object storage locations are determined ...........................................  71
How object data is protected from loss .......................................................  71
How ILM rules filter objects .........................................................................  73
What dual commit is .....................................................................................  75

Configuring information lifecycle management rules and policy .............  76
Creating and assigning storage grades .......................................................  76
Configuring storage pools ...........................................................................  78
Configuring Erasure Coding profiles .........................................................  81
Specifying time values for time based metadata ........................................  83
Creating an ILM rule ....................................................................................  83
Configuring and activating an ILM policy ...................................................  87
Working with ILM rules and ILM polices .....................................................  93

Managing disk storage ..................................................................................... 101
What a Storage Node is ..................................................................................... 101
What the LDR service is .............................................................................  101
What the DDS service is ...........................................................................  101
CMS service .................................................................................................  103
ADC service ...............................................................................................  103
What the nodetool repair operation is ........................................................  104

Managing Storage Nodes ............................................................................. 104
Object stores .................................................................................................  104
Monitoring Storage Node capacity ............................................................. 104
Watermarks .................................................................................................  106
Storage Node configuration settings ............................................................ 107
Managing full Storage Nodes ..................................................................... 110

Monitoring storage ............................................................................................ 111
Monitoring storage capacity system-wide ............................................... 111
Monitoring storage capacity per Storage Node ........................................... 111

Configure settings for stored objects .......................................................... 112
Configuring stored object encryption .......................................................... 112
Configuring stored object hashing .............................................................. 113
Configuring stored object compression ....................................................... 114
Deletion protection settings ......................................................................... 115
Mounted storage devices ......................................................................................... 116
What security partitions are ..................................................................................... 116
What object segmentation is ................................................................................... 117
Verifying object integrity ........................................................................................ 118
What background verification is ................................................................. 118
Configuring the background verification rate ............................................... 119
What foreground verification is ................................................................... 120
Running foreground verification ........................................................................ 120
How load balancing works ...................................................................................... 123
Managing archival storage ................................................................................. 124
What an Archive Node is ........................................................................................ 124
What the ARC service is ..................................................................................... 124
About supported archive targets ........................................................................ 125
Managing connections to archival storage ......................................................... 125
Configuring connection settings for S3 API ................................................... 126
Modifying connection settings for S3 API ...................................................... 128
Configuring connections to Tivoli Storage Manager middleware ...................... 129
Managing Archive Nodes .................................................................................. 131
Optimizing Archive Node’s TSM middleware sessions ....................................... 131
Managing an Archive Node when TSM server reaches capacity ...................... 132
Configuring Archive Node replication ............................................................ 133
Configuring retrieve settings ............................................................................. 134
Configuring the archive store ............................................................................ 135
Set custom alarms for the Archive Node ......................................................... 137
What an Admin Node is ...................................................................................... 138
Admin Node redundancy ................................................................................... 139
Alarm acknowledgments .................................................................................... 139
E-mail notifications and AutoSupport messages ............................................... 140
Changing the name of an Admin Node .............................................................. 141
NMS entities .......................................................................................................... 142
Changing an NMS entity name ........................................................................ 143
Managing networking ......................................................................................... 144
Viewing IP addresses ........................................................................................... 145
Modifying the DNS configuration for a single grid node .................................... 145
Configure SNMP monitoring ............................................................................ 146
Management Information Base file .................................................................... 147
Detailed registry ................................................................................................... 147
Link costs ............................................................................................................. 147
Updating link costs ............................................................................................. 148
Changing network transfer encryption ............................................................ 149
Configuring passwordless SSH access ............................................................ 150
Configuring certificates ...................................................................................... 151
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring custom server certificates for the grid management interface</td>
<td>151</td>
</tr>
<tr>
<td>Restoring the default server certificates for the grid management interface</td>
<td>152</td>
</tr>
<tr>
<td>Configuring custom server certificates for storage API endpoints</td>
<td>152</td>
</tr>
<tr>
<td>Restoring the default server certificates for storage API endpoints</td>
<td>153</td>
</tr>
<tr>
<td>Copying the StorageGRID Webscale system’s CA certificate</td>
<td>153</td>
</tr>
<tr>
<td><strong>Configuring audit client access</strong></td>
<td>155</td>
</tr>
<tr>
<td>Configuring audit clients for CIFS</td>
<td>155</td>
</tr>
<tr>
<td>Configuring audit clients for Workgroup</td>
<td>155</td>
</tr>
<tr>
<td>Configuring audit clients for Active Directory</td>
<td>157</td>
</tr>
<tr>
<td>Adding a user or group to a CIFS audit share</td>
<td>160</td>
</tr>
<tr>
<td>Removing a user or group from a CIFS audit share</td>
<td>161</td>
</tr>
<tr>
<td>Changing a CIFS audit share user or group name</td>
<td>162</td>
</tr>
<tr>
<td>Verifying CIFS audit integration</td>
<td>163</td>
</tr>
<tr>
<td>Configuring the audit client for NFS</td>
<td>163</td>
</tr>
<tr>
<td>Adding an NFS audit client to an audit share</td>
<td>164</td>
</tr>
<tr>
<td>Verifying NFS audit integration</td>
<td>166</td>
</tr>
<tr>
<td>Removing an NFS audit client from the audit share</td>
<td>166</td>
</tr>
<tr>
<td>Changing the IP address of an NFS audit client</td>
<td>167</td>
</tr>
<tr>
<td><strong>Controlling system access with administration user accounts and groups</strong></td>
<td>168</td>
</tr>
<tr>
<td>About administration user groups</td>
<td>168</td>
</tr>
<tr>
<td>About admin user accounts</td>
<td>169</td>
</tr>
<tr>
<td>Creating admin groups</td>
<td>170</td>
</tr>
<tr>
<td>Modifying an admin groups account</td>
<td>171</td>
</tr>
<tr>
<td>Deleting an admin groups account</td>
<td>171</td>
</tr>
<tr>
<td>Creating an admin users account</td>
<td>172</td>
</tr>
<tr>
<td>Modifying an admin users account</td>
<td>172</td>
</tr>
<tr>
<td>Deleting an admin users account</td>
<td>173</td>
</tr>
<tr>
<td>Changing local users’ passwords</td>
<td>173</td>
</tr>
<tr>
<td><strong>What grid tasks are</strong></td>
<td>175</td>
</tr>
<tr>
<td>Running grid tasks</td>
<td>175</td>
</tr>
<tr>
<td>Frequently used grid tasks</td>
<td>175</td>
</tr>
<tr>
<td>Monitoring grid tasks</td>
<td>176</td>
</tr>
<tr>
<td>Charting a grid task</td>
<td>178</td>
</tr>
<tr>
<td>Running a grid task</td>
<td>179</td>
</tr>
<tr>
<td>Pausing an active grid task</td>
<td>180</td>
</tr>
<tr>
<td>Resuming a paused grid task</td>
<td>180</td>
</tr>
<tr>
<td>Cancelling a grid task</td>
<td>181</td>
</tr>
<tr>
<td>Aborting a grid task</td>
<td>181</td>
</tr>
<tr>
<td>Removing grid tasks from the Historical table</td>
<td>182</td>
</tr>
<tr>
<td>Troubleshooting grid tasks</td>
<td>182</td>
</tr>
<tr>
<td>Grid task fails to complete and moves to Historical table</td>
<td>183</td>
</tr>
<tr>
<td>Troubleshooting grid task retries</td>
<td>183</td>
</tr>
</tbody>
</table>
Understanding the StorageGRID Webscale system

The Administrator Guide contains system administration information and procedures required to manage and monitor the StorageGRID Webscale system on a day-to-day basis. This guide also includes information on how to configure the StorageGRID Webscale system to meet a deployment’s unique operational requirements.

This guide is not intended as an introduction to the StorageGRID Webscale system and its functional areas. For a general introduction to the StorageGRID Webscale system, see the Grid Primer.

This guide is intended for technical personnel trained to configure and support the StorageGRID Webscale system.

This guide assumes a general understanding of the StorageGRID Webscale system. A fairly high level of computer literacy is assumed, including knowledge of Linux®/UNIX® command shells, networking, and server hardware setup and configuration.

Related information

StorageGRID Webscale 10.3 Grid Primer

What the StorageGRID Webscale system is

The StorageGRID Webscale system is a distributed object storage system that stores, protects, and preserves fixed-content data over long periods of time. By employing a grid architecture that distributes copies of object data throughout the system, a highly reliable system is created where data is continuously available. If one part of the system goes down, another immediately takes over, resulting in objects always being available for retrieval.

To implement this architecture, the StorageGRID Webscale system employs a system of network-connected servers hosting grid nodes. These grid nodes host a collection of one or more services, each providing a set of capabilities to the StorageGRID Webscale system.

To manage objects ingested into the system, the StorageGRID Webscale system employs metadata-based information lifecycle management (ILM) rules. These ILM rules determine what happens to an object’s data once it is ingested — where it is stored, how it is protected from loss, and for how long it is stored.

The StorageGRID Webscale system operates over wide area network (WAN) links, providing the system with the capability of off-site loss protection. Copies are made and distributed throughout the system so that objects are continuously available. In systems with multiple sites, this distribution of
copies means that if a site is lost, data is not lost, and clients are able to seamlessly retrieve from other sites. For a general introduction to the StorageGRID Webscale system, see the Grid Primer.

Related information

*StorageGRID Webscale 10.3 Grid Primer*

**Working with the StorageGRID Webscale system**

Most day-to-day activities are performed through a supported web browser. The StorageGRID Webscale system's browser-based interface provides access to the various levels of system functionality.

When you first sign in to the StorageGRID Webscale system, the Dashboard lets you monitor system activities at a glance. The Dashboard includes information about health and alerts, usage metrics, and operational trends and graphs.

**Grid Topology tree**

The Grid Topology tree provides access to StorageGRID Webscale system elements: sites, grid nodes, services, and components.
To access the Grid Topology tree, select **Grid** from the menu bar above the Dashboard.

**Grid nodes**

The basic building block of a StorageGRID Webscale system is the grid node. A grid node consists of one or more services hosted by a virtual machine. For a detailed description of grid nodes, see the *Grid Primer*.

**Services**

A service is a software module, which provides a set of capabilities to a grid node. The same service can be installed and used on more than one grid node. Changes made to settings for one service do not affect the settings of the same service type for a different grid node. Services are listed under each grid node. For a detail description of services, see the *Grid Primer*.

**Components**

A sub-group of each service that performs a particular function for that service.

**Attributes**

Attributes report values and statuses for all of the functions of the StorageGRID Webscale system. Attributes and the values they report form the basis for monitoring the StorageGRID Webscale system.
Signing in to the StorageGRID Webscale system

You access the StorageGRID Webscale system by signing in through a supported web browser using the web address or host name defined by your system administrator.

Before you begin

- You must have an authorized user name and password.
- Cookies must be enabled in your web browser.
- You must have the IP address or domain name of the StorageGRID Webscale system. If signing in for the first time, note the IP address of the Admin Node as listed in the Configuration.txt file.
- You must have access to a supported web browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

When you sign in to the StorageGRID Webscale system, you are connecting to a data center site's Admin Node. In a multi-site StorageGRID Webscale deployment, each site may include an Admin Node. You can connect to any Admin Node and each Admin Node displays a similar view of the StorageGRID Webscale system; however, alarm acknowledgments made through one Admin Node are not copied to other Admin Nodes. Therefore, the Grid Topology tree might not look the same for each Admin Node.

The StorageGRID Webscale system uses a self-signed certificate based on the system’s IP address. The expected URL is this IP address and not a domain name. In cases where a domain name is used...
to connect to the StorageGRID Webscale system's Admin Node, your browser might not be able to match the self-signed certificate to the identity of the grid node. For information about importing this certificate into a browser, see your browser’s documentation.

**Steps**

1. Launch a supported web browser.

2. In the browser’s address bar, enter the IP address or domain name of the StorageGRID Webscale system's Admin Node.

3. If you are prompted with a security alert, do one of the following:
   - Proceed with this session. The alert will appear again the next time you access this URL.
   - View and install the certificate using the browser’s installation wizard. The alert will not appear the next time you access this URL.

   The StorageGRID Webscale system's Sign In page appears.

4. Enter your case-sensitive username and password, and click **Sign In**.

   The StorageGRID Webscale system's front page, which includes the Dashboard, appears.

**Web browser requirements**

You need to access the StorageGRID Webscale system using a supported web browser.

<table>
<thead>
<tr>
<th>Web browser</th>
<th>Minimum supported version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>43</td>
</tr>
<tr>
<td>Microsoft Internet Explorer</td>
<td>11</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>38.0.5</td>
</tr>
</tbody>
</table>

You should set the browser window to a recommended width.

<table>
<thead>
<tr>
<th>Browser width</th>
<th>Pixels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum</td>
<td>1024</td>
</tr>
<tr>
<td>Optimum</td>
<td>1280 or larger</td>
</tr>
</tbody>
</table>
Signing out of the StorageGRID Webscale system

When you have completed working with the StorageGRID Webscale system, to keep the system secure, you must sign out.

**Step**

1. Click Sign Out located at the top-right corner of the page.
   
   The signing out message appears.
   
   **Note:** Failure to sign out can give unauthorized users access to your StorageGRID Webscale system. Simply closing your browser is not sufficient to sign out of the system.

Changing your password

If you are a local StorageGRID Webscale user, you can modify your own password.

**Before you begin**

You must have signed in to the Grid Management Interface using a supported browser.

**About this task**

Federated users cannot change their passwords directly in StorageGRID Webscale; they must change passwords in the external identity source, for example, LDAP.

**Steps**

1. From the StorageGRID Webscale header, select your login name > Change password.

2. To change your password:
   
   a. Enter your current password.
   
   b. Type a new password.
      
      Your password must contain between 8 and 32 characters and is case-sensitive.
   
   c. Re-enter the new password.

3. Click Save.

Changing the browser session timeout period

You can specify the timeout period for the StorageGRID Webscale system's browser-based interface. If a user is inactive for the specified timeout period, the StorageGRID Webscale system times out and the Sign In page is displayed.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.

- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

The GUI Inactivity Timeout defaults to 900 seconds (15 minutes).

**Note:** To maintain the security of the system, a separate, non-configurable timer for each user's authentication token will expire 16 hours after the user signs in. When a user's authentication
expires, that user is automatically signed out, even if the value for the GUI Inactivity Timeout has not been reached. To renew the token, the user must sign back in.

**Steps**

1. Select **Configuration > Display Options**.

2. For GUI Inactivity Timeout, enter a timeout period of 60 seconds or more. Set this field to 0 if you do not want to use this functionality. Users are signed out 16 hours after they sign in, when their authentication tokens expire.

3. Click **Apply Changes**.

   The new setting does not affect currently signed in users. Users must sign in again or refresh their browsers for the new timeout setting to take effect.

4. Sign out of the StorageGRID Webscale system.

5. Sign in again.

**Viewing StorageGRID Webscale license information**

You can view the license information for your StorageGRID Webscale system, such as the maximum storage capacity of your grid, whenever necessary.

**Step**

1. Select **Maintenance > License**.

   The license information is displayed including the grid serial number, license serial number, licensed storage capacity of the grid, and the contents of the license text file. This information is read-only. For licenses issued prior to version 10.3, the licensed storage capacity is not included in the license file, and a “See License Agreement” message is displayed instead of a value.

**Updating StorageGRID Webscale license information**

You must update the license information for your StorageGRID Webscale system any time the terms of your license change. For example, if you purchase additional storage capacity for your grid.

**Before you begin**

- You must have a new license file to apply to your StorageGRID Webscale system.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- You must have the provisioning passphrase.

**Steps**

1. Select **Maintenance > License**.

2. Enter the provisioning passphrase for your StorageGRID Webscale system in the **Provisioning Passphrase** text box.

3. Click **Browse**.

4. In the **Open** dialog box, locate and select the new license file (.txt), and click **Open**.

   The new license file is validated and displayed.

5. Click **Save**.
Understanding the StorageGRID Webscale Management API

StorageGRID Webscale provides a REST API for performing system and tenant management tasks. The StorageGRID Webscale Management API is accessed through the NMS service over HTTPS and requires the same authorization as the management GUI.

StorageGRID Webscale Management API Documentation

You can access the StorageGRID Webscale Management API documentation in two places depending on the APIs you want more information on:

• For system level APIs, sign in to the StorageGRID Webscale system and select API docs in the web application header.

• For tenant user APIs, log in to the Tenant UI and select Help > API Docs in the web application header.

StorageGRID Webscale uses Swagger for the REST API documentation. Swagger allows both developers and non-developers to interact with the API in a UI that illustrates how the API responds to parameters and options. This documentation assumes that you are familiar with standard Web technologies and the JSON (JavaScript Object Notation) data format.

  **Attention:** Operations performed via the Swagger documentation UI perform live operations on the grid.

API

Each of the REST API commands is composed of the API's URL, an HTTP action, a URL parameter, and an expected API response.

In the Swagger output, you see API details similar to the following:
The StorageGRID Webscale Management API is separated into the following sections:

- **accounts**: Operations to perform management of storage tenant accounts.
  The Management API allows the user to list the current storage tenant accounts, create new accounts or delete empty accounts. An account is created with a descriptive name and a set of capabilities including which protocol is supported. Individual accounts, referenced by their ID, may be modified after creation but the supported protocol may not be changed. Storage usage, comprised of the number of objects and the number of bytes of object data, may be retrieved for a given account and the buckets or containers in that account.

- **alarms**: Operations to list current alarms, and return information about the health of the grid.

- **auth**: Operations to perform user session authentication.
  The Management API supports the Bearer Token Authentication Scheme. To login, the client provides username and password in the JSON body of the authentication request (i.e., `POST /api/v1/authorize`) and a security token is returned if successfully authenticated. The returned token must be provided with subsequent API requests, with ‘Bearer’ for Authorization followed by the token. For system APIs, the username and password provided is that of the Root account for the StorageGRID Webscale system.

- **config**: Operations on current session information.

- **dns-servers**: Operations on external DNS servers.

- **expansion**: Operations on expansion (procedure-level).

- **expansion-nodes**: Operations on expansion (node-level).
• **expansion-sites**: Operations on expansion (site-level).
• **grid-networks**: Operations on the Grid Network List.
• **groups**: Operations to perform management of LDAP federated groups for a given account.
  The Management API allows the user to list the currently configured LDAP groups associated with a given account, and associate new groups with the account. Group names and user membership are validated against the configured LDAP server. For S3 tenant accounts, the group can be configured with permissions to enable access to the tenant UI/API for authenticated members of this group to create S3 access keys. The group may also be configured with an S3 policy to control access to buckets within this account, for access keys belonging to this group.
• **identity-source**: Operations to interact with an external LDAP server.
  The Management API allows the user to configure, or manually start synchronization between the LDAP server and the StorageGRID Webscale system.
• **ilm**: Operations on Information Lifecycle Management (ILM).
• **license**: Operations to retrieve or update the StorageGRID Webscale license.
• **ntp-servers**: Operations to perform management of external Network Time Protocol (NTP) servers.
  The Management API allows the user to list or update NTP server information.
• **recovery**: Operation to list the grid nodes available for recovery.
• **s3**: Operations to perform management of S3 root access keys for a given account.
  The Management API allows the user to create new root access keys, delete existing access keys, or list the existing access keys. Access keys may be created with an optional expiry time. Root access keys have full access to buckets in the account.
• **server certificates**: Operations to view and update Management Interface server certificates
• **users**: Operations to view and manage StorageGRID Webscale users.

**Top level resources**
The StorageGRID Webscale Management API provides the following top level resources.

• **/grid**: Access is restricted to NMS user accounts with Grid Management or Maintenance permissions. Grid Management permissions are required for APIs which perform modifications. Grid Maintenance permissions enable read-only access. Sub-resources available include **identity-source** for LDAP configuration, and tenant accounts for storage tenant account management including **group** and **s3-access-key** root access keys.

• **/org**: Access is restricted to LDAP federated users belonging to a group enabled for the given tenant account. Sub-resources available include **s3-access-keys** for the current authenticated user.

• **/private**: Access is restricted to internal access to the StorageGRID Webscale system. This resource path is not publicly documented.

**Versioning**
The current REST API version is shown in the URL. For example, below is version 1 of the API.
https://hostname_or_ip_address/api/v1/grid/accounts/001122334455/usage

**Note:**
• For a minor release (for example, 1.x), the API will be backwards compatible. That is, functions will be added; however, these updates will not affect existing contracts.
• For a major release (for example, 2.x), the API may not be backwards compatible; you may have to rework the client code.
Managing storage tenant accounts

StorageGRID Webscale supports the creation of tenant accounts to provide access to storage for S3 and Swift clients.

Access credentials are created within the context of the tenant account to provide S3 or Swift clients access to the buckets or containers and objects within the account. A tenant account is created with support for either S3 or Swift protocol access, but not both. LDAP federation can also be used to enable users belonging to configured LDAP groups to acquire access credentials for the tenant account. Configuration of tenant accounts is supported both through the StorageGRID Webscale system and through the REST API. Storage usage tracking is provided at the tenant account level, including the storage used by each bucket or container owned by that account.

To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Related concepts
- Understanding the StorageGRID Webscale Management API on page 15
- Controlling system access with administration user accounts and groups on page 168

Managing S3 tenant accounts

You can create S3 tenant accounts to provide access to buckets and objects from authorized S3 client applications.

StorageGRID Webscale supports S3 v2 and v4 authentication, where the client’s request is authenticated by the AccessID provided, and the request header signature is validated with the secret key associated with that AccessID. Root S3 access keys may be created, providing full access to the account’s buckets and objects unless explicitly disabled by a bucket policy. Cross-account access is not permitted unless explicitly enabled by a bucket policy. Using LDAP identity federation, users belonging to configured LDAP groups can create user-level S3 access keys with access permissions defined by the configured group policy for the LDAP group.

Creating tenant accounts for S3

You can create an S3 tenant account for each group that requires access to the StorageGRID Webscale system using the S3 REST API. A tenant account can be created for an organization, division, department, or any other internal or external group you want to use to define access to storage in your StorageGRID Webscale system.

Before you begin
- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps
1. Select Tenants.
   The Tenant Accounts page appears.
2. Click Create.

3. Configure the tenant account in the Add Tenant Account dialog box:
   a. Select S3 as the protocol.
   b. In the Name text box, enter the name to be displayed.
   c. Click Save.

   **Note:** The Save Keys dialog box is displayed listing the Access Key ID and Secret Access Key for the tenant account. Do not close this dialog box until you have copied or downloaded this information.

4. In the Save Keys dialog box, note the Secret Access Key, or click Download to save a spreadsheet file (.csv) with the Access Key ID and Secret Access Key. The Secret Access Key is not displayed anywhere else in the user interface, and only the last four characters of the Access Key ID are displayed.

5. Click Finish.

   The tenant account is created with a unique access key identifier. You can click on the Login link to sign in to the tenant account, or copy the link and send the URL to the users of the tenant account.

**Editing tenant accounts for S3**

You can edit the configuration settings associated with the tenant account, including the name and the LDAP group, if this information changes.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select Tenants.
The Tenant Accounts page appears.

2. Select the tenant account entry you want to edit.
3. Click **Edit Account**.
4. In the **Edit Tenant Account** dialog box, update the tenant details and click **Save**.

**Editing group policies for S3 tenant accounts**

You can manage permissions to access S3 tenant accounts by importing the group information from an external LDAP server and configuring policies for those groups.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Tenants**.
2. Select the tenant account entry you want to edit.
3. Click **Edit Group Policies**.
4. If you want to associate permissions with specific LDAP groups, you need to import each individual group you want to assign permissions to:
   a. Click **Import LDAP Group**.
   b. In the **Import LDAP Group** dialog box, enter the unique name of the LDAP group to import and click **Import**.
      
      For Active Directory, the unique name is associated with the “sAMAccountName” attribute. For OpenLDAP, the unique name is associated with the “uid” attribute.
   c. If you want to allow users that belong to the group to create and delete the S3 access keys associated with their tenant account, select the **Manage Your Own S3 Credentials** checkbox.
   d. If you want to create, update, or delete the S3 group policy, enter the group policy in the **S3 Policy** text box.
      
      The group policy must be entered using a valid JSON formatted string. The string is validated as it is entered, and you can only save valid group policy strings. See the information on S3 access control policies for the options and correct formatting for group policies.
For example, the following group policy grants the associated group permissions to perform all operations on all resources belonging to the tenant account:

```
{
    "Statement": [
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "urn:sgws:s3::*"
        }
    ]
}
```

e. Click **Save**.

5. If you want to update the group policies for an existing group, select the group, click **Edit Policies** and make any necessary changes, and then click **Save**.

6. If you want to remove a group's permissions from the StorageGRID Webscale system, select the group and click **Remove**, and then click **OK** in the confirmation dialog box.

7. Click **Close**.

Due to caching, changes to access policies may take up to 15 minutes to take effect across all grid nodes.

**Related concepts**

*Group and bucket access policies* on page 22

**Group and bucket access policies**

The StorageGRID Webscale system implements a subset of the S3 API policy language that you can use to control access to buckets and objects within those buckets.

**Overview**

StorageGRID Webscale bucket and group policies contain statements. Statements contain the following elements, which you need to define:

- **Resources**
  You can allow or deny permissions to buckets and objects using the uniform resource name (URN) to identify the resource.

- **Principals**
  You can allow groups and accounts to access specific resources and perform specific actions. If no S3 signature is included in the request, anonymous access is allowed by specifying the wildcard character (*). Access to resources is granted to anonymous users through the permissions. By default, anonymous users have no access to resources. You only need to specify the principal in a bucket policy. For group policies, the group to which the policy is attached is the implicit principal.

- **Permissions**
  When a group requests a resource they are either granted or denied access to the resource. Access is denied unless you specifically assign permissions, but you can also explicitly deny access to a resource, so that a group cannot access it even if a different policy grants access. Permissions have two components:
    - **Action**
      You need to identify operations you allow (or deny) on buckets or objects using the supported action keywords. You can use the wildcard character (*) to specify all operations, or a subset of operations (i.e. "s3:*Object").
Effect
You need to specify whether the specified operations are allowed or denied.

The following example policy shows a complete bucket policy that allows the admin and finance groups `s3:ListBucket` and `s3:GetObject` permissions for the `mybucket` bucket:

```json
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "SGWS": [
          "urn:sgws:identity::27233906934684427525:federated-group/admin",
          "urn:sgws:identity::27233906934684427525:federated-group/finance"
        ],
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": ["urn:sgws:s3:::mybucket", "urn:sgws:s3:::mybucket/*"]
    }
  ]
}
```

The bucket policy has a size limit of 20,480 bytes, and the group policy has a size limit of 5,120 bytes.

Group policies are cached for 15 minutes, and bucket policies are cached for 8 seconds. Therefore, due to caching, changes to group and bucket policies may take up to 15 minutes to take effect across all grid nodes. If you want bucket policy changes to take effect immediately, you can set the bucket consistency level to “all” using the PUT bucket consistency request or set the “Consistency-Control” header to “all” for the PUT bucket policy request.

Specify resources in a policy

You use the common uniform resource name (URN) format to identify any S3 resources or identity resources in the StorageGRID Webscale system:

- `urn:sgws:s3:::bucket_name`
- `urn:sgws:s3:::bucket_name/key_name`
- `urn:sgws:identity::27233906934684427525:root`
- `urn:sgws:identity::27233906934684427525:user/Bob`

- The StorageGRID Webscale REST API implementation of identity resources differs from Amazon's implementation:
  - For principals, the service component is “identity” instead of “iam”.
  - For principals, the `group-uuid` resource type is an additional StorageGRID Webscale specific resource type.
    - You need to specify the resource type and the UUID, instead of using a UUID alone.
    - For example:
      ```text
      urn:sgws:identity::27233906934684427525:group-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
      ```
  - For resources, the region component must be empty.
  - For resources, service component remains “s3”. 
For example:

```
"Resource": "urn:sgws:s3:::mybucket/"
```

- The principal value can specify a group name that does not yet exist when the bucket policy is created.
- The resource value can specify a bucket that does not yet exist when the group policy is created.
- The version value is not used; if you specify one, it is ignored and the following apply:
  - Policy variables are not supported.
  - Conditions are not supported.
- International characters, which can be specified in the object key, should be encoded using JSON UTF-8 or use JSON \u escape sequences. Percent-encoding, as outlined in RFC 2141 URN Syntax, is not supported. The request body for the PUT Bucket policy operation must be encoded as JSON UTF-8, and UTF-8 is always set as the content type.

**Specify a principal in a policy**

Account-based identities must be specified in one of the following formats:

- "SGWS": "account_ID"
- "SGWS": "account_URN"

You can specify an account using an ID. This example uses the ID 27233906934684427525, which includes the account root and all users in the account):

```
"Principal": { "SGWS": "27233906934684427525" }
```

You can specify just the account root:

```
"Principal": { "SGWS": "urn:sgws:identity::27233906934684427525:root" }
```

You can specify a specific federated user ("Bob"):

```
"Principal": { "SGWS": "urn:sgws:identity::27233906934684427525:federated-user/Bob" }
```

You can specify a specific federated group ("Managers"):

```
"Principal": { "SGWS": "urn:sgws:identity::27233906934684427525:federated-group/Managers" }
```

You can specify an anonymous principal:

```
"Principal": "*"
```

The Canonical User ID is not supported.

**Specifying permissions in a policy**

There are a set of permissions that you can specify in a policy. Each of these keywords maps to specific S3 Rest API operations.
Permissions applicable to buckets:

<table>
<thead>
<tr>
<th>Permissions</th>
<th>S3 Rest API operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>s3:CreateBucket</td>
<td>PUT Bucket</td>
</tr>
<tr>
<td>s3:DeleteBucket</td>
<td>DELETE Bucket</td>
</tr>
<tr>
<td>s3:DeleteBucketPolicy</td>
<td>DELETE Bucket policy</td>
</tr>
<tr>
<td>s3:GetBucketAcl</td>
<td>GET Bucket ACL</td>
</tr>
<tr>
<td>s3:GetBucketConsistency</td>
<td>GET Bucket Consistency</td>
</tr>
<tr>
<td>s3:GetBucketLastAccessTime</td>
<td>GET Bucket Last Access Time</td>
</tr>
<tr>
<td>s3:GetBucketPolicy</td>
<td>GET Bucket policy</td>
</tr>
<tr>
<td>s3:GetBucketVersioning</td>
<td>GET Bucket versioning</td>
</tr>
<tr>
<td>s3:ListAllMyBuckets</td>
<td>GET Service, GET Storage Usage</td>
</tr>
<tr>
<td>s3:ListBucket</td>
<td>GET Bucket (List Objects)</td>
</tr>
<tr>
<td>s3:ListBucketMultipartUploads</td>
<td>List Multipart Uploads</td>
</tr>
<tr>
<td>s3:ListBucketVersions</td>
<td>GET Bucket versions</td>
</tr>
<tr>
<td>s3:PutBucketConsistency</td>
<td>PUT Bucket Consistency</td>
</tr>
<tr>
<td>s3:PutBucketLastAccessTime</td>
<td>PUT Bucket Last Access Time</td>
</tr>
<tr>
<td>s3:PutBucketPolicy</td>
<td>PUT Bucket policy</td>
</tr>
<tr>
<td>s3:PutBucketVersioning</td>
<td>PUT Bucket versioning</td>
</tr>
</tbody>
</table>

Permissions applicable to objects:

<table>
<thead>
<tr>
<th>Permissions</th>
<th>S3 Rest API operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>s3:AbortMultipartUpload</td>
<td>Abort Multipart Upload</td>
</tr>
<tr>
<td>s3:DeleteObject</td>
<td>DELETE Object</td>
</tr>
<tr>
<td>s3:DeleteObjectVersion</td>
<td>DELETE Object (a specific version of the object)</td>
</tr>
<tr>
<td>s3:GetObject</td>
<td>GET Object</td>
</tr>
<tr>
<td>s3:GetObjectAcl</td>
<td>GET Object ACL</td>
</tr>
<tr>
<td>s3:GetObjectVersion</td>
<td>GET Object, HEAD Object</td>
</tr>
<tr>
<td>s3:ListMultipartUploadParts</td>
<td>List Parts</td>
</tr>
<tr>
<td>s3:PutObject</td>
<td>PUT Object</td>
</tr>
</tbody>
</table>

**Policies requiring special handling**

Sometimes a policy can grant permissions that are dangerous for security, or dangerous for continued operations. For example, locking out the root user of the account. The StorageGRID Webscale S3 API implementation is less restrictive during policy validation than Amazon, but equally strict during policy evaluation.
<table>
<thead>
<tr>
<th>Policy description</th>
<th>Policy type</th>
<th>Amazon behavior</th>
<th>StorageGRID behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny self any permissions to the root account</td>
<td>Bucket</td>
<td>Valid and enforced, but root user account retains permission for all S3 bucket policy operations</td>
<td>Same</td>
</tr>
<tr>
<td>Deny self any permissions to user/group</td>
<td>Group</td>
<td>Valid and enforced</td>
<td>Same</td>
</tr>
<tr>
<td>Allow a foreign account group any permission</td>
<td>Bucket</td>
<td>Invalid principal</td>
<td>Valid, but permissions for all S3 bucket policy operations return a 405 Method Not Allowed error when allowed by a policy</td>
</tr>
<tr>
<td>Allow a foreign account root or user any permission</td>
<td>Bucket</td>
<td>Valid, but permissions for all S3 bucket policy operations return a 405 Method Not Allowed error when allowed by a policy</td>
<td>Same</td>
</tr>
<tr>
<td>Allow everyone permissions to all actions</td>
<td>Bucket</td>
<td>Valid, but permissions for all S3 bucket policy operations return a 405 Method Not Allowed error for the foreign account root and users</td>
<td>Same</td>
</tr>
<tr>
<td>Deny everyone permissions to all actions</td>
<td>Bucket</td>
<td>Valid and enforced, but root user account retains permission for all S3 bucket policy operations</td>
<td>Same</td>
</tr>
<tr>
<td>Principal is a non-existent user or group</td>
<td>Bucket</td>
<td>Invalid principal</td>
<td>Valid</td>
</tr>
<tr>
<td>Resource is a non-existent S3 bucket</td>
<td>Group</td>
<td>Valid</td>
<td>Same</td>
</tr>
<tr>
<td>Principal is a local group</td>
<td>Bucket</td>
<td>Invalid principal</td>
<td>Valid</td>
</tr>
</tbody>
</table>

**Editing S3 root keys for S3 tenant accounts**

You can create or remove the S3 root keys used by a tenant account to connect to the StorageGRID Webscale system using client applications developed to use S3 web services.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
About this task

The S3 account information is used in the authentication process. When you later configure an S3 client, you need the Access Key ID and Secret Access Key information.

Steps

1. Select Tenants.

2. Select the tenant account entry you want to edit.

3. Click Edit S3 Root Keys.

4. If you want to create a new key:
   a. Click Create.
   b. Use the calendar control to select the expiration date and then set the time, or leave the default value of Never, and click Save.

      Note: The Save Keys dialog box is displayed listing the Access Key ID and Secret Access Key for the account. Do not close this dialog box until you have copied or downloaded this information.

   c. In the Save Keys dialog box, note the Secret Access Key, or click Download to save a spreadsheet file (.csv) with the Access Key ID and Secret Access Key. The Secret Access Key is not displayed anywhere else in the user interface, and only the last four characters of the Access Key ID are displayed.

   d. Click Finish.

5. If you want to remove an existing key:
   a. Select the entry to remove.
   b. Click Remove.
   c. Click OK in the confirmation dialog box.

Due to caching, access keys may remain valid for up to 15 minutes after you remove them.

Managing Swift tenant accounts

You can create Swift tenant accounts to provide access to Swift containers and objects from authorized Swift client applications.

Creating tenant accounts for Swift

You can create a Swift tenant account for each group that requires access to the StorageGRID Webscale system using the Swift REST API. A tenant account can be created for an organization, division, department, or any other internal or external group you want to use to define access to storage in your StorageGRID Webscale system. If you configured LDAP for this account, all groups and users in the LDAP domain can access Swift via this account.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
About this task

The Swift tenant account information is used in the authentication process. Configuring a Swift client requires one of the following sets of user credentials:

- If Identity Federation is enabled for the tenant account (for Active Directory or LDAP configurations), you should provide the username and password of the federated user from the AD or LDAP server. Alternatively, LDAP users can be referred to with their domain name, for example, X-Auth-User: Tenant_Account_ID:Username@Domain_Name

- For local accounts when LDAP is not configured, you should use the "swiftadmin" as the user name and the password provided during tenant account creation.

Steps

1. Select Tenants.
2. Click Create.
3. Configure the tenant account in the Add Tenant Account dialog box:
   a. Select Swift as the protocol.
   b. In the Name text box enter the name to display in the StorageGRID Webscale system.
   c. If you want to use the local Swift Administrator account, instead of or in addition to LDAP authentication, enter the password to use in the Password and Confirm Password text boxes. The password must be between 8 and 32 characters. You must enter a strong password to ensure the security of your StorageGRID Webscale system.
   d. Click Save.

Editing tenant accounts for Swift

You can edit the configuration settings associated with the tenant account, including the name and the password for the Swift Administrator account, if this information changes.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Tenants.
2. Select the tenant account entry you want to edit.
3. Click Edit Account.
4. In the Edit Tenant Account dialog box, you can update the tenant details:
   a. To rename the tenant account, enter the new name in the Name text box.
   b. To change the password for the local Swift Administrator account, enter the new password in the New Password and Confirm Password text boxes. The password must be between 8 and 32 characters. You must enter a strong password to ensure the security of your StorageGRID Webscale system.
   c. Click Save.
Editing group policies for Swift tenant accounts

You can manage permissions to access Swift tenant accounts by importing the group information from an external LDAP server and configuring policies for those groups. You can also define which groups have Administrator permissions for the Swift REST API.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Tenants.
2. Select the Swift tenant account entry for which you want to edit the group policy.
3. Click Edit Group Policies.
4. If you want to associate permissions with specific LDAP groups, you need to import each individual group you want to assign permissions to:
   a. Click Import LDAP Group.
   b. In the Import LDAP Group dialog box, enter the unique name of the LDAP group to import and click Import.
      For Active Directory, the unique name is associated with the “sAMAccountName” attribute.
      For OpenLDAP, the unique name is associated with the “uid” attribute.
   c. If you want to grant Administrator permissions to members of the LDAP group, select the Administrator checkbox.
   d. Click Save.
5. If you want to update the group policies for an existing group, select the group, click Edit Policies and make any necessary changes, and then click Save.
6. If you want to remove a group's permissions from the StorageGRID Webscale system, select the group and click Remove, and then click OK in the confirmation dialog box.
7. Click Close.

Deleting tenant accounts

You can delete a tenant account if you want to permanently remove the tenant's access to the system.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
• You must have removed all buckets and objects associated with the tenant account before you can delete it.
Steps
1. Select Tenants.
2. Select the tenant account entry you want to delete.
3. Click Remove.
4. Click OK in the confirmation dialog box.

Configuring LDAP for identity federation

You can configure LDAP if you want to use an external LDAP server to authenticate tenant accounts.

Before you begin
• You must have signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps
1. Select Configuration > Identity Federation.
2. Select Enable LDAP.

LDAP server configuration information appears.
3. Select the type of LDAP server to configure from the Service Type drop-down list.
The options are Active Directory, OpenLDAP, or Other. If you select Other, you need to enter additional information in the LDAP Attributes section:

- **Unique User Name**: The LDAP attribute that uniquely identifies each LDAP user relative to the User Base DN. This will be the name the user provides when authenticating (uid/sAMAccountName)
- **User UUID**: The LDAP attribute that uniquely identifies each LDAP user, permanently (entryUUID/objectGUID)
- **Group Unique Name**: The LDAP attribute that uniquely identifies each LDAP group (uid/sAMAccountName)
- **Group UUID**: The LDAP attribute that uniquely identifies each LDAP group, permanently (entryUUID/objectGUID)

4. Enter the required LDAP server and network connection information:

- **Hostname**: The server hostname or IP address of the identity source.
- **Port**: The port to use to connect to the identity source.
- **Username**: The username to use to access the identity source.

  The credentials for the specified user account must be sufficient to list group and users, and access the following attributes: cn, sAMAccountName/uid, objectGUID/entryUUID, memberOf.

- **Password**: The password to use to access the identity source.
- **Group Base DN**: The fully qualified Distinguished Name (DN) of an LDAP subtree you want to search for tenant groups.
The Unique User Name values must be unique within the Group Base DN they belong to.

- **User Base DN**: The fully qualified Distinguished Name (DN) of an LDAP subtree you want to search for tenant users.

- **Transport Layer Security**: Specifies if TLS is used to secure communications with the identity server. Select the appropriate security setting from the drop-down list:
  - **Use operating system CA certificate**: Use the default CA certificate installed on the operating system to secure connections.
  - **Use custom CA certificate**: Cut and paste the contents of the custom security certificate to use in the text area.
  - **Do not use**: The network traffic between the StorageGRID Webscale system and the LDAP server will not be secured.

5. Optional. Click **Test Connection** to validate your connection settings for the identity server.

6. Click **Save**.

**OpenLDAP server configuration guidelines**

If you are configuring OpenLDAP server for use with StorageGRID Webscale Identity Federation, you need to configure specific settings on the OpenLDAP server.

**Memberof overlay**

The memberof overlay should be enabled. For more information, see the “Reverse Group Membership Maintenance” section in the *OpenLDAP Software Administrator’s Guide*.  

**Indexing**

You must configure the following OpenLDAP attributes with the specified index keywords:

```
olcDbIndex: objectClass eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: cn eq,pres,sub
olcDbIndex: entryUUID eq
```

For more information on the `olcDBIndex` directive used for indexing attributes, see the *OpenLDAP Software Administrator’s Guide*.  
[http://www.openldap.org/doc/admin24/slapdconf2.html](http://www.openldap.org/doc/admin24/slapdconf2.html)

**Disabling LDAP for identity federation**

You can temporarily or permanently disable LDAP authentication for tenant accounts. Any settings you have configured are retained while LDAP is disabled, but there is no communication between the StorageGRID Webscale system and the LDAP server.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
About this task
Before you disable LDAP, you should be aware of the following:

• Federated users will be unable to log in.
• Federated users who are currently logged in will retain access to the StorageGRID Webscale system until their session expires, but they will be unable to log in after their session expires.
• Synchronization between the StorageGRID Webscale system and the LDAP server will not occur, and alarms will not be raised for accounts that have not been synchronized.

Steps
1. Select Configuration > Identity Federation.
2. Deselect the Enable LDAP checkbox.
3. Click Save.

Manually forcing synchronization with the LDAP server
The StorageGRID Webscale system periodically synchronizes federated groups and users from the LDAP server. You can manually force synchronization to start if you want changes to be reflected as soon as possible to enable or restrict user permissions to the system.

Before you begin
• You must have signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
• You must have configured an LDAP server.

Steps
1. Select Configuration > Identity Federation.
2. Click Synchronize.
   A confirmation message is displayed indicating that synchronization started successfully.

Managing federated user S3 credentials
Federated users can manage their S3 credentials for storage tenant accounts, which allows them to control client access to objects stored in the StorageGRID Webscale system.

Before you begin
• You must have signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task
You can create and remove S3 access keys as required.
Steps

1. Select Tenants.

2. Click the Login link next to the S3 tenant account you want to access.
   A new StorageGRID Webscale window appears.

3. Enter the Username and Password for the tenant account and click Sign In.

4. If you want to create a new key:
   a. Click Create.
   b. Use the calendar control to select the expiration date and then set the time, or leave the default value of Never, and click Save.
      
      Note: The Save Keys dialog box is displayed listing the Access Key ID and Secret Access Key for the federated user. Do not close this dialog box until you have copied or downloaded this information. The Secret Access Key is not displayed anywhere else in the user interface, and only the last four characters of the Access Key ID are displayed.
   
   c. In the Save Keys dialog box, note the Secret Access Key, or click Download to save a spreadsheet file (.csv) with the Access Key ID and Secret Access Key.
   d. Click Finish.

5. If you want to remove an existing key:
   a. Select the entry to remove.
   b. Click Remove.
   c. Click OK in the confirmation dialog box.
Monitoring the StorageGRID Webscale system

The StorageGRID Webscale system provides you with the capabilities to monitor the daily activities of the system including its health. Alarms and notifications help you evaluate and quickly resolve trouble spots that sometimes occur during the normal operation of a StorageGRID Webscale system.

The StorageGRID Webscale system also includes support for NetApp’s AutoSupport feature.

The StorageGRID Webscale system also includes an auditing feature that retains a record of all system activities through audit logs. Audit logs are managed by the Audit Management System (AMS) service, which is found on the Admin Node. The AMS service logs all audited system events to a text file on the Admin Node. For more information about auditing, see the Audit Message Reference Guide.

Related concepts
- Configuring audit client access on page 155
- What AutoSupport is on page 60

Related information
- StorageGRID Webscale 10.3 Audit Message Reference

About alarms and email notifications

An email notification is a message automatically sent by the StorageGRID Webscale system to configured recipients, which notifies recipients of a newly triggered alarm or service state change. You can configure email notifications and set mailing lists to receive these email notifications for any particular alarm severity or state change.

If an email address (or list) belongs to multiple mailing lists, only one email notification is sent when a notification triggering event occurs. For example, one group of administrators within your organization can be configured to receive notifications for all alarms regardless of severity. Another group might only require notifications for alarms with a severity of Critical. You can belong to both lists. If a Critical alarm is triggered, you receive one notification, not two. For a general overview of alarms, see the Grid Primer.

Related information
- StorageGRID Webscale 10.3 Grid Primer

Alarm notification types

The StorageGRID Webscale systems sends out two types of alarm notifications: severity level and service state.

Severity level notifications

Severity level notifications are sent at the alarm level and are associated with attributes. A mailing list receives all notifications related to alarm for the selected severity: Notice, Minor, Major, and Critical. A notification is sent when an event triggers an alarm for the selected alarm level. A notification is also sent when the alarm leaves the alarm level — either by being resolved or by entering a different alarm severity level.

Service state notifications

Service State notifications are sent at the services level and are associated with services; for example, the LDR service or CMS service. A mailing list receives all notifications related to changes in the
selected state: Unknown, or Administratively Down. A notification is sent when a service enters the selected Service State and when it leaves the selected Service State.

**Notification status and queues**

You can view the current status of the NMS service’s ability to send notifications to the mail server and the size of its notifications queue through the Interface Engine page.

Notifications are processed through the e-mail notifications queue and are sent to the mail server one after another in the order they are triggered. If there is a problem (for example, a network connection error) and the mail server is unavailable when the attempt is made to send the notification, a best effort attempt to resend the notification to the mail server continues for a period of 60 seconds. If the notification is not sent to the mail server after 60 seconds, the notification is dropped from the notifications queue and an attempt to send the next notification in the queue is made. Because notifications can be dropped from the notifications queue without being sent, it is possible that an alarm can be triggered without a notification being sent. In the event that a notification is dropped from the queue without being sent, the MINS (E-mail Notification Status) Minor alarm is triggered.

For a StorageGRID Webscale system configured with multiple Admin Nodes (and thus multiple NMS services), if the “standby” sender detects a Server Connection Error with the preferred sender, it will begin sending notifications to the mail server. The standby sender will continue to send notifications until it detects that the preferred sender is no longer in an error state and is again successfully sending notifications to the mail server. Notifications in the preferred sender’s queue are not copied to the standby sender. Note that in a situation where the preferred sender and the standby sender are islanded from each other, duplicate messages can be sent.

**Related tasks**

*Selecting a preferred sender* on page 43

**Configuring notifications**

By default, notifications are not sent. You must configure the StorageGRID Webscale to send notifications when alarms are raised.

**Steps**

1. **Configuring email server settings** on page 36
   
The EMail Server page allows you to configure SMTP mail server settings that enable the sending of alarm notifications and AutoSupport messages. The StorageGRID Webscale system only sends email; it cannot receive email.
2. Creating email templates on page 38
   Create an email template to customize the header, footer, and subject line of a notification. You can use email templates to send unique notifications that contain the same body text to different mailing lists.

3. Creating mailing lists on page 39
   You can create mailing lists for notifications. A mailing list enables you to send one e-mail message to multiple e-mail addresses. These mailing lists are used to send notifications when an alarm is triggered or when a service state changes. You must create a mailing list before you can send notifications. To send a notification to a single recipient, create a mailing list with one e-mail address.

4. Configuring global email notifications on page 40
   In order to receive global email notifications, recipients must be a member of a mailing list and that list must be added to the Notifications page. Notifications are configured to send email to recipients only when an alarm with a specified severity level is triggered or when a service state changes. Thus, recipients only receive the notifications they need to receive.

5. Sending a test email on page 41
   To confirm that you have configured the email server connection correctly, you can send a test e-mail. When you send a test e-mail, a message is sent from all Admin Nodes. This includes a test email from the standby sender (if one is configured).

Configuring email server settings

The EMail Server page allows you to configure SMTP mail server settings that enable the sending of alarm notifications and AutoSupport messages. The StorageGRID Webscale system only sends email; it cannot receive email.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

Only the SMTP protocol is supported for the sending e-mail.

Steps

1. Select Configuration > Email Setup.

2. From the Email menu, select Server.
3. Add the following SMTP mail server settings:

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

4. Under **From Address**, enter a valid email address that the SMTP server will recognize as the sending email address. This is the official e-mail address from which the alarm notification or AutoSupport message is sent.

5. Optionally, send a test email, confirming that your SMTP mail server settings are correct:

   Test emails are sent from all NMS services. This includes the standby sender (if the system includes a second Admin Node). Thus, multiple test emails can be sent.

   a. In the **Test E-mail > To** box, add an email addresses to which you can send a confirmation message.

      E-mail addresses can be any single address, multiple e-mail addresses comma delineated, or a mailing list as configured on the Email Lists page.

   b. Select **Send Test E-mail**.

   c. Click **Apply Changes**.

      The system sends a test email to the configured address.

6. Click **Apply Changes**.

   SMTP mail server settings are saved. If configured and selected, a test e-mail is sent.

**Related tasks**

*Creating mailing lists* on page 39
You can create mailing lists for notifications. A mailing list enables you to send one e-mail message to multiple e-mail addresses. These mailing lists are used to send notifications when an alarm is triggered or when a service state changes. You must create a mailing list before you can send notifications. To send a notification to a single recipient, create a mailing list with one e-mail address.

Creating email templates

Create an email template to customize the header, footer, and subject line of a notification. You can use email templates to send unique notifications that contain the same body text to different mailing lists.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

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

Steps

1. Select Configuration > Email Setup.
2. From the Email menu, select Templates.
3. Click Edit (or Insert if this is not the first template).
4. In the new row add the following:

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
</tr>
<tr>
<td>Subject Prefix</td>
</tr>
</tbody>
</table>
### Creating mailing lists

You can create mailing lists for notifications. A mailing list enables you to send one e-mail message to multiple e-mail addresses. These mailing lists are used to send notifications when an alarm is triggered or when a service state changes. You must create a mailing list before you can send notifications. To send a notification to a single recipient, create a mailing list with one e-mail address.

### Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

### Steps

1. Select **Configuration > Email Setup**.
2. From the Email menu, select **Lists**.
3. Click **Edit** (or **Insert** if this is not the first mailing list).
4. In the new row, add the following:

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
</table>
| **Group Name** | Unique name used to identify the mailing list. Mailing list names cannot be duplicated.  
**Note:** If you change the name of a mailing list, the change is not propagated to the other locations that use the mailing list name. You must manually update all configured notifications to use the new mailing list name. |
5. Click **Apply Changes**.
   
   A new mailing list is created.

### Related tasks

*Creating email templates* on page 38

Create an email template to customize the header, footer, and subject line of a notification. You can use email templates to send unique notifications that contain the same body text to different mailing lists.

### Configuring global email notifications

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

### Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- You must have configured an email list.

### Steps

1. Select **Configuration > Notifications**.
2. Click **Edit** (or **Insert** if this is not the first notification).
3. Under **E-mail List**, add a mailing list.
4. Select one or more alarm severity levels and service states:

<table>
<thead>
<tr>
<th>Notification Type</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>Severity Level</td>
<td>An unusual condition exists that does not affect normal operation.</td>
</tr>
<tr>
<td>Minor</td>
<td>Severity Level</td>
<td>An abnormal condition exists that could affect operation in the future.</td>
</tr>
<tr>
<td>Major</td>
<td>Severity Level</td>
<td>An abnormal condition exists that is currently affecting operation.</td>
</tr>
<tr>
<td>Critical</td>
<td>Severity Level</td>
<td>An abnormal condition exists that has stopped normal operation.</td>
</tr>
<tr>
<td>Unknown</td>
<td>Service State</td>
<td>An unknown condition exists that has stopped normal service operation.</td>
</tr>
</tbody>
</table>
### Notification Type
- **Administratively Down**

### Category
- **Service State**

### Description
A condition whereby a service has been purposefully stopped.

5. Click **Apply Changes**.

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

#### Related tasks

*Creating mailing lists* on page 39

You can create mailing lists for notifications. A mailing list enables you to send one e-mail message to multiple e-mail addresses. These mailing lists are used to send notifications when an alarm is triggered or when a service state changes. You must create a mailing list before you can send notifications. To send a notification to a single recipient, create a mailing list with one e-mail address.

### Sending a test email

To confirm that you have configured the email server connection correctly, you can send a test e-mail. When you send a test e-mail, a message is sent from all Admin Nodes. This includes a test email from the standby sender (if one is configured).

#### Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- You must have configured your email server.

#### About this task

When a test e-mail is sent, the NMS service does not confirm success or failure. You must check the test recipient's inbox. Make sure, when sending a test e-mail, that it will be sent to an address you can access. Test emails are sent to the mail server immediately and are not sent through the notifications queue. Note that a connection problem between the NMS service and the mail server triggers the MINS (NMS Notification Status) Minor alarm.

#### Steps

1. Select **Configuration > Email Setup**.
2. In the Test E-mail section:
   a. Under To, add email addresses you want to send a confirmation message to. Email addresses are comma delineated.
   b. Select **Send Test E-mail**.
3. Click **Apply Changes**.

   A test e-mail is immediately sent. In a system with multiple Admin Nodes, each Admin Node sends an email.

   Receipt of this test email confirms that your SMTP mail server settings are correct and that the NMS service is successfully connecting to the mail server.
Suppressing email notifications for a mailing list

You can suppress notifications for a mailing list system-wide when you do not want a mailing list to receive notifications, for example while performing maintenance procedures.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Alarms**.
2. Select **Configuration > Notifications**.
3. Click **Edit** next to the mailing list for which you want to suppress notifications.
4. Under **Suppress**, select the check box next to the mailing list you want to suppress, or select **Suppress** at the top of the column to suppress all mailing lists.
5. Click **Apply Changes**.

Notifications are suppressed for the selected mailing lists.

Suppressing email notifications system wide

You can block the StorageGRID Webscale system's ability to send notifications when an alarm is triggered.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Configuration > Display Options**.
2. From the Display Options menu, select **Options**.
3. Select **Notification Suppress All**.
4. Click **Apply Changes**.

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

**Selecting a preferred sender**

Each site in a StorageGRID Webscale deployment may include an Admin Node. If a deployment includes multiple Admin Nodes, one Admin Node is configured as the preferred sender of notifications and AutoSupport messages. Any Admin Node can be selected as the preferred sender and can be changed at any time.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

The Display Options page lists the Admin Node that is currently sending notifications. In most cases, this Admin Node is the same as the Preferred Sender; however, if an Admin Node is islanded from the rest of the system, it is unable to use the Preferred Sender and automatically updates to become the Current Sender. In the case of islanded Admin Nodes, multiple Admin Nodes will attempt to send notifications and AutoSupport message and thus it is possible that multiple copies of notifications will be received.
Steps
1. Select Configuration > Display Options.
2. From the Display Options menu, select Options.
3. Select Preferred Sender > Admin Node.
4. Click Apply Changes.
   The Admin Node is set as the preferred sender of notifications.

Alarms management
Customizing alarms lets you customize your StorageGRID Webscale system based on your unique monitoring requirements. You can configure customized alarms either globally (Global Custom alarms) or for individual services (Custom alarms). You can create custom alarms with alarm levels that override default alarms and you can create alarms for attributes that do not have a default alarm.

Alarm customization is restricted to accounts with Maintenance permissions.

Warning: Alarm settings are enabled during the installation process. You should not make changes to alarm settings for the sake of convenience. Changing alarm settings can conceal underlying problems that should be resolved. If you find that an alarm persists, discuss the situation with technical support before making changes.

For a basic introduction to alarm monitoring, see the Grid Primer. For a list of alarm codes, see the Troubleshooting Guide.

Related concepts
Controlling system access with administration user accounts and groups on page 168

Related information
StorageGRID Webscale 10.3 Troubleshooting Guide
StorageGRID Webscale 10.3 Grid Primer

Alarm class types
Alarms are separated into three mutually exclusive alarm classes.

- Default: Standard alarm configurations set at installation
• Global Custom: Configured after installation to override default settings, custom alarms are set at a global level so that they apply to all services of a given type anywhere in the StorageGRID Webscale system

• Custom: Configured after installation to override default settings, custom alarms are set on individual services or components.

Default alarms

Default alarms are configured on a global basis and cannot be modified; however, they can be disabled or overridden by Custom alarms and Global Custom alarms.

Default alarms can be disabled both globally and at the services level. If a Default alarm is disabled globally, at the services level on the Configuration page, the Enabled check box appears with an adjacent asterisk. The asterisk indicates that the Default alarm has been disabled through the Alarms > Custom page even though the Enabled check box is selected.

Default alarms for a particular service or component can be viewed on the Grid > service or component > Configuration > Alarms page.

Related tasks

Disabling default alarms for services on page 55
Disabling a default alarm system wide on page 56

Viewing all default alarms

You can view all default alarms that are standard alarm configurations set as part of the installation.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Configuration > Global Alarms.

2. For Filtered by select Attribute Code or Attribute Name.

3. For equals, enter the wildcard symbol: * .

4. Under Default Alarms, click the adjacent arrow.

   All default alarms are listed.
Global Custom Alarms

Global Custom alarms monitor the status of conditions system-wide. By creating a Global Custom alarms, you can override a Default alarms system-wide. You can also create a new Global Custom alarms that will monitor status system-wide. This can be useful for monitoring any customized conditions of your StorageGRID Webscale system.

You can create global custom alarms, and disable global custom alarms system wide or for individual services.

Related tasks
- Creating custom global alarms on page 52
- Disabling global custom alarms for services on page 57
- Disabling global custom alarms system wide on page 58

Custom alarms

Custom alarms can be created to override a default alarm or global custom alarm at the service or component level. You can also create new custom alarms based on the service’s unique requirements.

The configuration of custom alarms is performed on each service's Configuration > Alarms page in the Grid Topology tree.
Alarm triggering logic

Each alarm class is organized into a hierarchy of five severity levels from Normal to Critical. An alarm is triggered when a threshold value is reached that evaluates to true against a combination of alarm class and alarm severity level. Note that a severity level of Normal does not trigger an alarm.

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

Attribute values are evaluated against the list of enabled alarms defined for that attribute in the Alarms table on the Alarms page for a specific service or component (for example, LDR > Storage > Alarms > Main). The list of alarms is checked in the following order to find the first alarm class with a defined and enabled alarm for the attribute:

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

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

Alarm triggering examples

Example 1

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

<table>
<thead>
<tr>
<th>Threshold Values</th>
<th>Global Custom alarm (enabled)</th>
<th>Default alarm (enabled)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>&gt;= 1500</td>
<td>&gt;= 1000</td>
</tr>
<tr>
<td>Minor</td>
<td>&gt;= 15,000</td>
<td>&gt;= 1000</td>
</tr>
<tr>
<td>Major</td>
<td>&gt;= 150,000</td>
<td>&gt;= 250,000</td>
</tr>
</tbody>
</table>

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

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

After the above scenario, if the Global Custom alarm is disabled, nothing changes. The attribute value must be evaluated again before a new alarm level is triggered.
With the Global Custom alarm disabled, when the attribute value is evaluated again, the attribute value is evaluated against the threshold values for the Default alarm. The alarm level triggers a Notice level alarm and an e-mail notification is sent to the designated personnel.

Note, however, that if there are custom alarms for an attribute, these alarms are still evaluated as custom alarms have a higher priority than Global Custom alarms.

**Example 2**

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

<table>
<thead>
<tr>
<th>Threshold Values</th>
<th>Custom alarm (enabled)</th>
<th>Global Custom alarm (enabled)</th>
<th>Default alarm (enabled)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>&gt;= 500</td>
<td>&gt;= 1500</td>
<td>&gt;=1000</td>
</tr>
<tr>
<td>Minor</td>
<td>&gt;= 750</td>
<td>&gt;= 15,000</td>
<td>&gt;=10,000</td>
</tr>
<tr>
<td>Major</td>
<td>&gt;=1,000</td>
<td>&gt;= 150,000</td>
<td>&gt;= 250,000</td>
</tr>
</tbody>
</table>

If the attribute is evaluated when its value is 1000, a Major alarm is triggered and an e-mail notification is sent to the designated personnel. The Custom alarm takes precedence over both the Global Custom alarm and Default alarm. A value of 1000 reaches the threshold value of the Major severity level for the Custom alarm. As a result, the attribute value triggers a Major level alarm.

Within the same scenario, if the Custom alarm is then disabled and the attribute value evaluated again at 1000, the alarm level is changed to Normal. The attribute value is evaluated against the threshold values of the Global Custom alarm, the next alarm class that is defined and enabled. A value of 1000 does not reach any threshold level for this alarm class. As a result, the attribute value is evaluated to be Normal and no notification is sent. The Notice level alarm from the previous evaluation is cleared.

**Example 3**

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

<table>
<thead>
<tr>
<th>Threshold Values</th>
<th>Custom alarm (enabled)</th>
<th>Global Custom alarm (enabled)</th>
<th>Default alarm (enabled)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>&gt;= 500</td>
<td>&gt;= 1500</td>
<td>&gt;=1000</td>
</tr>
<tr>
<td>Minor</td>
<td>&gt;= 750</td>
<td>&gt;= 15,000</td>
<td>&gt;=10,000</td>
</tr>
<tr>
<td>Major</td>
<td>&gt;=1,000</td>
<td>&gt;= 150,000</td>
<td>&gt;= 250,000</td>
</tr>
</tbody>
</table>

If the attribute is evaluated when its value is 10,000, a Notice alarm is triggered and an e-mail notification is sent to the designated personnel.

The Custom alarm is defined, but disabled; therefore, the attribute value is evaluated against the next alarm class. The Global Custom alarm is defined, enabled, and it takes precedence over the Default alarm. The attribute value is evaluated against the threshold values set for the Global Custom alarm class. A value of 10,000 reaches the Notice severity level for this alarm class. As a result, the attribute value triggers a Notice level alarm.

If the Global Custom alarm is then disabled and the attribute value evaluated again at 10,000, a Minor level alarm is triggered. The attribute value is evaluated against the threshold values for the Default alarm class, the only alarm class in that is both defined and enabled.
A value of 10,000 reaches the threshold value for a Minor level alarm. As a result, the Notice level alarm from the previous evaluation is cleared and the alarm level changes to Minor. An e-mail notification is sent to the designated personnel.

**Alarms of same severity**

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

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

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

**Alarm class overrides**

To override a class of alarms, disable all alarms within that class. If all alarms within a class for an attribute are disabled, the NMS service interprets the class as having no alarms configured for the attribute and evaluates the next lower class for enabled alarms.

For example, if an alarm is triggered at the Global Custom alarm class level, it means that there are no enabled alarms at the Custom alarms class level for that attribute.

For example, to override a Default alarm, add a Global Custom alarm or Custom alarm for that attribute. This override is achieved because the NMS service does not evaluate lower priority alarm
classes once an alarm setting is detected within a class. If this override is performed after an alarm has already been triggered, the override will not take effect until the alarm is triggered again.

Severity changes

If an alarm’s severity changes, the severity is propagated up the network hierarchy as needed. If there is a notification configured, a notification is sent. The notification is sent only at the time the alarm enters or leaves the new severity level.

Notifications

A notification reports the occurrence of an alarm or the change of state for a service. It is an e-mail communication to designated personnel that the system requires attention.

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

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

New services

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

Creating custom service or component alarms

Customizing alarm settings enables you to create a customized methodology for monitoring the StorageGRID Webscale system. You can create alarms on individual services or components in addition to creating global alarms.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

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

Steps

1. Select Grid.
2. Select a service or component in the Grid Topology tree.
3. Click Configuration > Alarms.
4. Add a new row to the Custom alarms table:
   - Click **Edit** *(if this is the first entry)* or **Insert** to add a new alarm.
   - Copy an alarm from the Default alarms or Global Custom alarms tables. Click **Copy** next to the alarm you want to modify.

5. Make any necessary changes to the custom alarm settings:

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

6. Click **Apply Changes**.

### Creating custom global alarms

You can configure custom global alarms when you require a unique alarm that is the same for every service of the same type. Customizing alarm settings enables you to create a customized methodology for monitoring the StorageGRID Webscale system.

**Before you begin**
- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

Global alarms override default alarms. It is recommended that you do not change default alarm values unless absolutely necessary. By changing default alarms, you run the risk of concealing problems that might otherwise trigger an alarm.
Steps

1. Select **Configuration > Global Alarms**.

2. Add a new row to the Global Custom Alarms table:
   - Click Edit (if this is the first entry) or Insert to add a new alarm.
   - Copy Default alarms to the table.

   **Note:** Selecting **Disabled Defaults** displays a list of all currently disabled default global alarms.

   ◦ Search for the Default alarm. Under Filter by, select either **Attribute Code** or **Attribute Name**, type a search string, and then click **Submit**.
   
   You can use the wildcards * (for multiple characters) and ? (for single characters) in the search string.

3. In the list of results, click **Copy** next to the alarm you want to modify. The default alarm is copied to the Global Custom alarms table.

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

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

5. **Click Apply Changes.**

### Disabling alarms

Alarms are enabled by default, but you can disable alarms that are not required.

Disabling an alarm for an attribute that currently has an alarm triggered does not clear the current alarm. The alarm will be disabled the next time the attribute crosses the alarm threshold, or you can clear the triggered alarm.
Warning: There are consequences to disabling alarms and extreme care should be taken. Disabling an alarm can result in no alarm being triggered. Because alarms are evaluated by alarm class and then severity level within the class, disabling an alarm at a higher class does not necessarily result in a lower class alarm being evaluated. All alarms for a specific attribute must be disabled before a lower alarm class will be evaluated.

Related tasks

*Clearing triggered alarms* on page 59

Alarms and tables

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

For example, in the following figure, there are two critical Entries Available (VMFI) alarms. You can disable the VMFI alarm so that the Critical level VMFI alarm is not triggered (both currently Critical alarms would appear in the table as green); however, you cannot disable a single alarm in a table row so that one VMFI alarm displays as a Critical level alarm while the other remains green.

### Volumes

<table>
<thead>
<tr>
<th>Mount Point</th>
<th>Device</th>
<th>Status</th>
<th>Size</th>
<th>Space Available</th>
<th>Total Entries</th>
<th>Entries Available</th>
<th>Write Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>sda1</td>
<td>Online</td>
<td>19.6 GB</td>
<td>7.46 GB</td>
<td>656,360</td>
<td>559,263</td>
<td>Enabled</td>
</tr>
<tr>
<td>/var/local</td>
<td>sda2</td>
<td>Online</td>
<td>63.4 GB</td>
<td>59.4 GB</td>
<td>3,922,160</td>
<td>3,921,942</td>
<td>Unknown</td>
</tr>
<tr>
<td>/var/local/rangedb/0</td>
<td>sdb</td>
<td>Online</td>
<td>53.4 GB</td>
<td>53.4 GB</td>
<td>52,428,800</td>
<td>52,427,856</td>
<td>Enabled</td>
</tr>
<tr>
<td>/var/local/rangedb/1</td>
<td>sdc</td>
<td>Online</td>
<td>53.4 GB</td>
<td>53.4 GB</td>
<td>52,428,800</td>
<td>52,427,848</td>
<td>Enabled</td>
</tr>
<tr>
<td>/var/local/rangedb/2</td>
<td>sdd</td>
<td>Online</td>
<td>53.4 GB</td>
<td>53.4 GB</td>
<td>52,428,800</td>
<td>52,427,856</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Disabling default alarms for services

To temporarily stop alarms for a specific service, you can disable default alarms for that service.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Grid.
2. Select a service or component in the Grid Topology tree.
3. Click Configuration > Alarms.
4. In the Default Alarms table, click Edit next to the alarm you want to disable.

5. Clear the Enabled check box for the alarm.

6. Click Apply Changes.

   The Default alarm is disabled for the service or component.

   Note: alarms cannot be disabled for individual rows in a table.

Disabling a default alarm system wide

You can temporarily disable a default alarm system wide.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Click deployment > Configuration > Alarms.

2. Search for the default alarm to disable:
   a. In the Default Alarms section, select Filtered by > Attribute Code or Attribute Name.
b. Type a search string, and then click the Submit arrow.

You can use the wildcards * and ? in the search string. Asterisks (*) represent multiple characters and question marks (?) represent a single character.

**Note:** Selecting Disabled Defaults displays a list of all currently disabled Default Global alarms.

3. In the Default Alarms table, click **Edit** next to the alarm you want to disable.

4. Clear the Enabled check box.

5. Click **Apply Changes**.

   The default alarm is disabled system wide.

**Disabling global custom alarms for services**

You cannot disable a global alarm for a service unless you create another enabled global alarm for the attribute. This is because if all alarm within a class for an attribute are disabled, the NMS service interprets the class as having no alarms configured for the attribute and evaluates the next lower class for enabled alarm.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

Instead of creating a global custom alarm and disabling it for selected services, reconfigure the alarms such that you create individual local custom alarms for the services that require the alarm. If you want to ensure that all these custom alarms have the same configuration, you can create a global custom alarm, disable it, and then enable it for selected services as a custom alarm.
If you want to create a global custom alarm and disable it for selected services, you must create a local custom alarm for that service that will never be triggered. Doing this overrides all global custom alarms for that service.

**Note:** Alarms cannot be disabled for individual rows in a table.

**Steps**
1. Create a local custom alarm for a service that will never be triggered.
2. Select Grid.
3. Select the service or component in the Grid Topology tree.
4. Click **Configuration > Alarms**.
5. In the Global Custom alarm table, click **Copy** next to the alarm you want to disable.
   The alarm is copied to the Custom Alarms table.
6. Clear **Enabled** for the alarm.
7. Click **Apply Changes**.

**Related tasks**
*Creating custom service or component alarms* on page 50

### Disabling global custom alarms system wide

**Before you begin**
- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

**Note:** Alarms cannot be disabled for individual rows in a table.

**Steps**
1. Select **Configuration > Global Alarms**.
2. In the Global Custom Alarms table, click **Edit** next to the alarm you want to disable.
3. Clear **Enabled**.

4. Click **Apply Changes**.

   The Global Custom alarm is disabled system wide.

### Clearing triggered alarms

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

**Before you begin**

You must have the Root password as listed in the `Passwords.txt` file.

**Steps**

1. Disable the alarm.
   
   For details, see disabling default alarms.

2. At the Admin Node, access a command shell and log in as root using the password listed in the `Passwords.txt` file.

3. Restart the NMS service:
   
   `/etc/init.d/nms restart`

4. Log out of the Admin Node:
   
   `exit`

   The alarm is cleared.

**Related concepts**

*Disabling alarms* on page 54
What AutoSupport is

AutoSupport enables technical support to proactively monitor the health of your StorageGRID Webscale system. In addition to the automatic weekly message, an AutoSupport message can be sent at any time by manually triggering AutoSupport’s “call home” mechanism.

The AutoSupport’s “call home” mechanism sends a message to technical support that includes the following information:

- StorageGRID Webscale software version
- Operating system version
- System-level and location-level attribute information
- All alarms raised in the last seven days
- Current status of all grid tasks, including historical data
- Events information as listed on the SSM > Events > Overview page
- Admin Node database usage
- Number of lost or missing objects
- Grid configuration settings
- NMS entities
- Active ILM policy
- Provisioned grid specification file.

By analyzing this information, technical support can help you determine the health and status of your StorageGRID Webscale system and troubleshoot any problems that might occur. This also includes monitoring the storage needs of the system, such as the need to expand.

For more information about AutoSupport, go to NetApp Support.

Triggering AutoSupport messages

You can manually trigger an AutoSupport message at any time.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
Steps

1. Select **Configuration > AutoSupport**.

2. From the AutoSupport menu, select **User-triggered**.

3. Click **Send**.

   The StorageGRID Webscale system attempts to send an AutoSupport message to technical support. If the attempt is successful, the Last Attempt attribute updates to Successful. If there is a problem, the Last Attempt attribute updates to Failed. The StorageGRID Webscale system does not try again.

   If a failure occurs, check that the StorageGRID Webscale system’s e-mail server is correctly configured and that your e-mail server is running.

Related tasks

*Configuring email server settings* on page 36

The EMail Server page allows you to configure SMTP mail server settings that enable the sending of alarm notifications and AutoSupport messages. The StorageGRID Webscale system only sends email; it cannot receive email.

### Disabling weekly AutoSupport messages

By default, the StorageGRID Webscale system is configured to send an AutoSupport message to NetApp Support once a week.

#### Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.

- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

#### About this task

To determine when the weekly AutoSupport message is sent, see the Next Scheduled Time attribute on the AutoSupport > Weekly page. You can disable the automatic sending of an AutoSupport message at any time.

#### Steps

1. Select **Configuration > AutoSupport**.

2. From the AutoSupport menu, select **Weekly**.

3. Clear the **Enabled** check box.
4. Click **Apply Changes**.

**Troubleshooting AutoSupport**

If the attempt to send the regularly scheduled AutoSupport message fails, the Most Recent Result attribute updates to Retrying.

The StorageGRID Webscale system attempts to resend the AutoSupport message 15 times every four minutes for one hour. If after one hour a message is not sent, the Most Recent Result attribute updates to Failed. The StorageGRID Webscale system will try again at the next scheduled time. If a failure occurs, check that the StorageGRID Webscale system’s e-mail server is correctly configured and that your e-mail server is running.

In the event that the NMS service is unavailable and thus an AutoSupport message cannot be sent, when the NMS service is once again available, if an AutoSupport message has not been sent in the past seven days, an AutoSupport message is immediately sent; otherwise, AutoSupport maintains its regular schedule.

**Note:** To send an AutoSupport message, the StorageGRID Webscale system’s e-mail server must be correctly configured.

**Related tasks**

*Configuring email server settings* on page 36

The EMail Server page allows you to configure SMTP mail server settings that enable the sending of alarm notifications and AutoSupport messages. The StorageGRID Webscale system only sends email; it cannot receive email.

**Monitoring servers and grid nodes**

Various services hosted by the StorageGRID Webscale system's grid nodes provide you with mechanisms to monitor the system.

**What is the SSM service**

The Server Status Monitor (SSM) service is present on all grid nodes and monitors the grid node’s status, services, and resources.

The SSM service monitors the condition of the server and related hardware, polls the server and hardware drivers for information, and displays the processed data. Information monitored includes:

- CPU information (type, mode, speed)
- Memory information (available, used)
- Performance (system load, load average, uptime, restarts)
- Volumes (status, available space)
- Network (addresses, interfaces, resources)
- Services
- NTP synchronization
Services

The Services component tracks the services and support modules running on a grid node. It reports the service’s current version, status, the number of threads (CPU tasks) running, the current CPU load, and the amount of RAM being used.

The services are listed as well as the support modules (such as time synchronization). Also listed is the operating system and the StorageGRID Webscale software version installed on the grid node.

The status of a service is either Running or Not Running. A service is listed with a status of Not Running when its state is Administratively Down.

Related concepts

*Alarm notification types* on page 34

Resetting event counters

The Events component relays logged events. You can treat this data as a general indicator of problems with the system.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Grid.
2. Select a grid node in the Grid Topology tree.
3. Select SSM > Events.
4. Click Configuration > Main.
5. Select the Reset check boxes for the specific counters to be reset.
6. Click Apply Changes.
Resources

The SSM service uses the standard set of resources attributes that report on the service health and all computational, disk device, and network resources. In addition, the Resources attributes report on memory, storage hardware, network resources, network interfaces, network addresses, and receive and transmit information. The Resources component of the SSM service provides the ability to reset network error counters.

If the Storage Node is a StorageGRID Webscale appliance, appliance information appears in the Resources section. For details, see the StorageGRID Webscale Appliance Installation and Setup Guide.

Timing

The SSM service uses the set of timing attributes that report on the state of the grid node’s time and the time recorded by neighboring grid nodes. In addition, the SSM Timing attributes report on NTP Synchronization.

Monitoring StorageGRID Webscale Appliance Storage Nodes

You can view status information for every installed and operational StorageGRID Webscale Appliance Storage Nodes. This includes appliance hardware information, connectivity issues, alarm notifications, services, and disk device information.

Viewing information about an appliance Storage Node

You can view information about a StorageGRID Webscale appliance Storage Node at any time. For example, you might want to view the E-Series array name and review appliance-specific information to ensure correct configuration and status.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

Each StorageGRID Webscale appliance is represented as one Storage Node.

The StorageGRID Webscale appliance Storage Node lists information about service health and all computational, disk device, and network resources. You can also see memory, storage hardware, network resources, network interfaces, network addresses, and receipt and transmittal information.

Steps

1. Select Grid.

2. In the Grid Topology Tree, select an appliance Storage Node.

3. Select SSM > Resources.
4. In the **Memory** section, note the information in the Installed Memory field.
   
   The Installed Memory for the appliance version shows 25.3 GB of RAM.

5. In the **Processors** section, note the information in the Processor Number column.
   
   The appliance shows twelve E5-1428L v2 cores (six physical cores with 2:1 hyperthreading enabled).

6. In the **Disk Devices** section, note the device names.
   
   These LUN names match the LUN names you see if you connectSANtricity Storage Manager to the E2700 controller. To help you interpret disk read and write statistics related to volume mount points, the names in the Disk Devices section match the device names in the Volumes section on this page.

7. In the **Storage Hardware** section, note the information in these fields.
   
   This section appears only if the Storage Node is an appliance. If not, all the attributes and alarms associated with storage hardware do not display.
<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Controller Name</td>
<td>Name of the E2700 controller, as shown in SANtricity Storage Manager.</td>
</tr>
<tr>
<td>Storage Controller Management IP</td>
<td>Management IP address of the E2700 controller You can use this IP to connect SANtricity to the E2700 controller in this StorageGRID Webscale appliance to troubleshoot storage issues.</td>
</tr>
<tr>
<td>Storage Controller Model</td>
<td>The physical type of Storage Node controller: for example, 2u12 or 4u60.</td>
</tr>
<tr>
<td>Storage Controller WWN</td>
<td>The worldwide identifier of the E2700 controller, as shown in SANtricity Storage Manager.</td>
</tr>
<tr>
<td>Storage Appliance Chassis Serial Number</td>
<td>Serial number associated with the appliance.</td>
</tr>
<tr>
<td>Software Platform</td>
<td>The software platform used to generate the storage hardware status and alarms.</td>
</tr>
<tr>
<td>Overall Power Supply Status</td>
<td>The status of power to a StorageGRID Webscale appliance enclosure.</td>
</tr>
<tr>
<td>Power Supply A and B Status</td>
<td>The status of power supply A or B in the StorageGRID Webscale appliance.</td>
</tr>
<tr>
<td>CPU Temperature</td>
<td>The temperature of E5600SG controller CPU.</td>
</tr>
<tr>
<td>Module Temperature</td>
<td>The temperature of the E5600SG controller.</td>
</tr>
<tr>
<td>Multipath State</td>
<td>The current multipath I/O state of the physical paths, for example, Simplex or Nominal. If one of the SAS connections on the appliance is not operational, then &quot;Simplex&quot; appears and performance and fault tolerance are impacted. If both paths are not operational, the appliance also stops working. For details about resolving performance or fault tolerance issues, refer to the E-Series documents.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Storage Controller Status | The overall status of the E2700 controller. If the Storage Node is a StorageGRID Webscale appliance and it needs attention, then both the StorageGRID Webscale and SANtricity systems indicate that the storage controller needs attention. If the status is “needs attention,” first check the E2700 controller using SANtricity. Then, ensure that no other alarms exist that apply to the E5600SG controller.

8. In the **Storage Hardware** section, note that each of status fields have associated alarms:

<table>
<thead>
<tr>
<th>Field</th>
<th>Alarm code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Power Supply Status</td>
<td>OPST</td>
</tr>
<tr>
<td>Power Supply A &amp; B Status</td>
<td>PSAS or PSBS</td>
</tr>
<tr>
<td>CPU Temperature</td>
<td>CPUT</td>
</tr>
<tr>
<td>Module (Board) Temperature</td>
<td>BRDT</td>
</tr>
<tr>
<td>Storage Controller Status</td>
<td>SOSS</td>
</tr>
</tbody>
</table>

For details about alarms in StorageGRID Webscale, see the *Troubleshooting Guide*.

9. In the **Network Resources**, **Network Interfaces**, and **Network Addresses** sections, note the information in these fields.

The interface names encode the port numbers: for example, a hic2 and hic4 could be 10 GB ports. These two ports might exist in an active/standby bond, rather than operating independently, and they would appear with the same IP address. To distinguish the active port, note the bytes and packets received in the Receive table. In the screenshot, hic1 and hic3, and hic2 and hic4, are bonded to enable two 10 GB ports.
You can view events related to a StorageGRID Webscale appliance Storage Node at any time. You might want to monitor events related to the E5600SG controller, the E2700 controller, the multipath state of the appliance connections, and the enclosure to ensure operational status. Some events trigger alarms.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

The StorageGRID Webscale appliance reports on events that impact the service health and all computational, disk devices, hardware, and network resources. For the appliance, you can gauge the hardware status of both the E5600SG controller and the E2700 controller by viewing storage hardware events.

For details about events and alarms, refer to alarms and troubleshooting information.
Steps

1. Select Grid.
2. Select an appliance Storage Node in the Grid Topology tree.
3. Select SSM > Events.
4. In the System Events section, note the count for Storage Hardware Events.
5. If a hardware event is noted here, identify the cause by completing the following steps:
   a. Select SSM > Resources.
   b. Look for abnormal conditions in the Storage Hardware section.
Managing objects through information lifecycle management

You manage objects through the configuration of information lifecycle management (ILM), which determines how the StorageGRID Webscale system creates and distributes copies of object data and then manages these copies over time.

Every object ingested into the StorageGRID Webscale is filtered against the system's active ILM policy and the ILM rules that it contains. When the filtering process finds an ILM rule that matches the object, filtering stops and object data is processed and distributed according to the matching ILM rule's placement instructions.

Designing and implementing an ILM policy that manages objects in the manner that you intend requires careful planning and an understanding of ILM. You must define the logic for how objects are to be filtered, copied, and distributed throughout the system, taking into account the topology of the StorageGRID Webscale system, object protection requirements, and available storage types.

What an information lifecycle management policy is

An ILM policy is a set of prioritized ILM rules. It determines how the StorageGRID Webscale system manages object data over time.

The StorageGRID Webscale system's active ILM policy filters all ingested objects, copying object data to storage based on the matching ILM rule's placement instructions. To create an ILM policy, you must create ILM rules and then add them to the ILM policy. Once configured, your ILM policy does not start filtering objects until you activate it.

This diagram illustrates an ILM policy, which dictates that at ingest ILM rules store one copy at data center site one (DC1) on disk (Storage Nodes), one copy at data center site two (DC2) on disk (Storage Nodes), and one copy at DC2 (Archive Node). At the end of one year, ILM rules delete the copy on disk at DC2.

Related concepts

Order of ILM rules within an ILM policy on page 87
What an information lifecycle management rule is

An information lifecycle management (ILM) rule determines how the StorageGRID Webscale system stores object data over time. You configure ILM rules and then add them to an ILM policy.

ILM rules determine:
- Where an object’s data is stored (storage pools)
- The type of storage used to store object data (disk or archival media)
- The number and type of copies made (replicated and erasure coded)
- Which objects are stored
- How the object’s data is managed over time, where it is stored and how it is protected from loss (placement instructions)

How object storage locations are determined

You determine where the StorageGRID Webscale system stores object data by configuring storage pools.

A storage pool is a logical grouping of Storage Nodes (LDR services) or Archive Nodes (ARC services) and is used in ILM rules to determine where object data is stored. A storage pool has two attributes: storage grade and site. Storage grade refers to the type of storage; for example, Flash. Site is the location to which object data is stored.

Related concepts

What an Erasure Coding profile is on page 71

How object data is protected from loss

ILM rules provide you with two mechanisms to protect object data from loss: replication and erasure coding.

Replication

Protecting object data from loss through replication means that exact copies of object data are made and stored to multiple Storage Nodes or Archive Nodes. ILM rules dictate the number of copies made, where those copies are made, and for how long they are retained by the system. If a copy is lost as a result of a Storage Node loss, the object is still available if a copy of it exists elsewhere in the StorageGRID Webscale system.

Erasure coding

Protecting object data from loss through erasure coding means that an erasure coding scheme is applied to object data. The erasure coding scheme breaks object data into data and parity fragments, which are distributed across multiple Storage Nodes. If fragments are lost, object data can still be recovered through the information encoded in the remaining fragments.

What an Erasure Coding profile is

You create an Erasure Coding profile by associating a storage pool with an erasure coding scheme. You then select this storage pool and its associated Erasure Coding profile when configuring an ILM rule’s content placement instructions. If an object matches an ILM rule that includes this
configuration, ILM functionality creates an erasure coded copy and distributes its fragments among the selected storage pool’s Storage Nodes.

Erasure coding protects object data from loss by breaking it into data and parity fragments. If fragments are lost, object data can still be recovered through the information encoded in the remaining fragments. A data fragment is a portion of the object’s data, while a parity fragment contains the information required to reconstruct object data if data fragments are lost. The number of data and parity fragments that object data is broken into depends on the selected erasure coding scheme.

An erasure code's parameters define its scheme. An erasure code's parameters are the number of data and parity fragments generated for each erasure coded object. This determines the maximum number of fragments that can be lost before an object is lost. For example, a 6+3 erasure coding scheme encodes an object's data into six data fragments and three parity fragments. The system distributes these nine fragments across nine Storage Nodes and a maximum of three fragments can be lost.

The following is an example of a 6+3 erasure coding scheme, detailing the number of fragments that object data is broken into and the maximum number of fragments that can be lost without impacting retrievals.

Any three fragments (data or parity) can be lost and object data is still recoverable. This is the erasure coding scheme’s fault tolerance.

However, if the erasure coding scheme’s fault tolerance is breached (four in the case of a 6+3 erasure coding scheme), the object is considered lost.
Object data protected from loss through erasure coding consumes less disk space than if it is protected through replication. For example, a 10 MB object that is replicated once consumes 20 MB of disk space, while an object that is erasure coded with a 6+3 scheme only consumes 15 MB of disk space. However, a StorageGRID Webscale deployment that creates erasure coded copies may initially require more Storage Nodes than a deployment that will create replicated copies and may also require more sites. For example, if using an erasure coding scheme of 6+3, to protect erasure coded object data from a site loss, a StorageGRID Webscale deployment must include a minimum of three sites. At the same time, to protect replicated object data from a site loss, a StorageGRID Webscale deployment requires a minimum of two sites.

Depending on the configuration of storage pools, it may take longer to retrieve an erasure coded copy than a replicated copy. A large object that is erasure coded and distributed across sites will take longer to retrieve than an object that is replicated and available locally (the same site to which the client connects). Due to the overhead of managing the number of fragments associated with an erasure coded copy, do not use Erasure Coding profiles for objects smaller than one megabyte.

Related concepts

*How object storage locations are determined* on page 71

Related tasks

*Configuring storage pools* on page 78

*Configuring Erasure Coding profiles* on page 81

Related information

*StorageGRID Webscale 10.3 Grid Primer*

**How ILM rules filter objects**

All objects ingested into the StorageGRID Webscale system have their metadata filtered against the active ILM policy and its ILM rules. When a metadata match is made, the content placement instructions for that rule distribute object data throughout the system.

**Filtering logic**

Within the active ILM policy, an object is evaluated against the first ILM rule and then against subsequent ILM rules until a metadata match is made. If a match is not found after evaluating all ILM rules, the default ILM rule is applied. This figure describes the filtering logic used to determine when an ILM rule applies to an object.
Advanced filtering

With advanced filtering, you can specify metadata against which objects are filtered. If metadata is not used to filter objects, the ILM rule applies to all objects ingested.

The table shows the metadata available for each API. Note that the API itself is also metadata. When you specify an API in an ILM rule, the rule applies only to objects ingested through that API. If you do not specify an API, the ILM rule applies to all objects ingested.

<table>
<thead>
<tr>
<th>Metadata</th>
<th>API</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingest Time</td>
<td>S3: Yes</td>
</tr>
<tr>
<td></td>
<td>Swift: Yes</td>
</tr>
<tr>
<td>Key</td>
<td>S3: Yes</td>
</tr>
<tr>
<td></td>
<td>Swift: Yes</td>
</tr>
<tr>
<td>Last Access Time</td>
<td>S3: Yes</td>
</tr>
<tr>
<td></td>
<td>Swift: Yes</td>
</tr>
<tr>
<td>Object Size</td>
<td>S3: Yes</td>
</tr>
<tr>
<td></td>
<td>Swift: Yes</td>
</tr>
<tr>
<td>Security Partition</td>
<td>S3: No</td>
</tr>
<tr>
<td></td>
<td>Swift: Yes</td>
</tr>
<tr>
<td>User Metadata</td>
<td>S3: Yes</td>
</tr>
<tr>
<td></td>
<td>Swift: Yes</td>
</tr>
</tbody>
</table>

When you use advanced filtering, you can specify multiple metadata fields and values. For example, if you wanted the rule to match objects between 10 MB and 100 MB in size, you would specify two metadata values.
Advanced filtering allows you have to have precise control over which objects are matched. In the following example, the rule applies to objects that have a Brand A or Brand B as the value of the Camera Type user metadata. However, the rule only applies to Brand B objects if they are smaller than 10 MB.

What dual commit is

At ingest and before an object is evaluated against the active ILM policy, Dual Commit functionality synchronously creates two copies of object data and distributes these copies to two Storage Nodes. The purpose of Dual Commit is to protect objects from accidental loss in the event that a storage location is lost before an object is evaluated against the active ILM policy.

Objects are simultaneously queued for ILM evaluation. When ILM rules are evaluated, additional copies may be made in different locations and initial “Dual Commit” copies deleted.

If the request to create initial copies fails (for example, because of a network issue that prevents the second initial copy from being made) the StorageGRID Webscale system does not retry and ingest fails.
Dual Commit is enabled by default. If ILM rules are configured to only store one instance of replicated object data, disable Dual Commit to avoid unnecessarily creating and then deleting copies generated by the dual commit operation.

For configuration information, see the appropriate StorageGRID Webscale API guide.

Related information

- StorageGRID Webscale 10.3 Simple Storage Service Implementation Guide
- StorageGRID Webscale 10.3 Swift Implementation Guide
- StorageGRID Webscale 10.3 Cloud Data Management Interface Implementation Guide

Configuring information lifecycle management rules and policy

When you configure your StorageGRID Webscale system's information lifecycle management rules and policy, there is a standard set of steps and related procedures that you work through in order to correctly configure your ILM.

Steps

1. Creating and assigning storage grades on page 76
2. Configuring storage pools on page 78
3. Configuring Erasure Coding profiles on page 81
4. Specifying time values for time based metadata on page 83
5. Creating an ILM rule on page 83
6. Configuring and activating an ILM policy on page 87
7. Working with ILM rules and ILM policies on page 93

Creating and assigning storage grades

You can optionally create a unique storage grade and then associate this storage grade with a Storage Node. This allows for the easy identification of the Storage Node when configuring storage pools. If storage grade is not a concern (for example, your StorageGRID Webscale system includes only one type of disk storage), skip this procedure and instead use the system-generated storage grade “All Disks” when configuring a storage pool.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

A storage grade is the type of storage used by a Storage Node to store object data. Because a StorageGRID Webscale deployment can incorporate multiple spinning and archival media storage technologies, a label can be created for a storage grade and then attached to a Storage Node. This allows for the easy identification of the storage technology used by a Storage Node, which can then be used to select the correct Storage Node when configuring storage pools and determining where object data resides.

A storage grade refers to the storage media type; for example, flash. Creating a unique label for the storage grade and then assigning the storage grade to an LDR service helps you when configuring
storage pools. This assignment lets you easily determine the storage type you are assigning to a storage pool.

When creating storage grades, follow these guidelines:

- Do not create more storage grades than necessary. For example, do not create one storage grade for each Storage Node. Instead, assign each storage grade to two or more nodes. Storage grades assigned to only one node can cause ILM backlogs if that node becomes unavailable.

Note: You cannot configure storage grades for Archive Nodes.

Steps
1. Select ILM > Storage Grades.
2. Create a storage grade:
   a. For each storage grade you need to define, click Insert to add a row and enter a label for the storage grade.
      The Default storage grade cannot be modified. It is reserved for new LDR services added during a StorageGRID Webscale system expansion.
   b. To edit an existing storage grade, click Edit and modify the label as required.
      Note: You cannot delete storage grades.
   c. Click Apply Changes.
      These storage grades are now available for assignment to LDR services.
3. Assign a storage grade to an LDR service:
a. For each Storage Node's LDR service, click **Edit** and select a storage grade from the list.

![Storage Grades](image)

**Warning**: Assign a storage grade to a given Storage Node only once. A Storage Node recovered from failure maintains the previously assigned storage grade. Do not change this assignment once the ILM policy is activated. If the assignment is changed, data is stored based on the new storage grade.

b. Click **Apply Changes**.

### Configuring storage pools

You configure storage pools to determine where object data is stored. You then select these storage pools when configuring Erasure Coding profiles and ILM rules. You can also change a storage pool that is already in use by an ILM rule.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

When creating storage pools, follow these guidelines:

- Keep storage pool configurations as simple as possible. Do not create more storage pools than necessary. For example, do not create one storage pool for each LDR service.
• Create storage pools with as many nodes as possible. Storage pools are recommended to contain two or more nodes. Storage pools with only one node can cause ILM backlogs if that node becomes unavailable.

• Consider how the ILM rule will be configured for the type of copies made: replicated or erasure coded. Available erasure coding schemes are limited by the number of Storage Nodes a storage pool contains.

• For a storage pool that will be associated with an erasure code, it is recommended that you distribute Storage Nodes across sites as evenly as possible. For example, to support a scheme of 4+2, configure a storage pool that includes three Storage Nodes at three sites.

• Confirm that the storage pools you create have sufficient storage capacity.

• Consider whether or not copies will be archived. Archived copies require a storage pool that only includes Archive Nodes. You cannot create a storage pool that includes both Storage Nodes and Archive Nodes. A storage pool includes either disk or archive media, but not both. If an Archive Node’s Target Type is Cloud Tiering - Simple Storage Service (S3), this Archive Node must be in its own storage pool.

A storage pool must include enough storage to satisfy content placement instructions. A replicated copy duplicates complete instances of object data to storage devices within the storage pool. One copy equals one Storage Node or Archive Node. An erasure coded copy distributes fragments to the various Storage Nodes within the storage pool. Storage pools are associated with erasure coding schemes through Erasure Coding profiles. Available erasure coding schemes are limited by the number of Storage Nodes a storage pool contains. There is a one-to-one relationship between the number of Storage Nodes in a storage pool and the erasure coding scheme that can be used.

**Note:** A storage pool cannot include both Storage Nodes and Archive Nodes.

When configuring storage pools with Archive Nodes, StorageGRID Webscale best practices are that you always maintain redundancy of object data to protect it from loss. Maintain at least one replicated or erasure-coded copy on Storage Nodes when keeping one copy in the Archive Node.

### Steps

1. Select **ILM > Storage Pools**.

2. Create a storage pool:

   a. Click **Insert** at the end of the row for the last storage pool.
b. When creating a pool name, create a representative name for the storage pool. This makes for easy identification when configuring Erasure Coding profiles and ILM rules.

c. Select Storage Grade > storage_grade to set the type of storage to which object data will be copied if an ILM rule uses this storage pool. The values All Disks and Archive Nodes are system-generated.

d. Select Site > site_name to set the location to which object data will be copied if an ILM rule uses this storage pool. The value All Sites is system-generated. When you select a Site, the number of grid nodes and storage capacity information (Installed, Used, and Available) are automatically updated. Make sure that storage pools have sufficient storage and Storage Nodes to support planned ILM rules and the types of copies that will be made.

e. To add another storage grade/site combination to the storage pool, click Insert next to Site. You cannot create storage pools that include LDR and ARC services in the same storage pool. A storage pool includes either disks or archive media, but not both.

f. To remove a storage grade/site combination, click Delete next to Site.

3. To delete a storage pool, click Delete next to the storage pool name. You cannot delete a storage pool that is used in a saved ILM rule.

4. Click Apply Changes.

   **Note:** Changes made to a storage pool that is currently in use by an ILM policy do not take effect until the ILM policy is reactivated.

**Related tasks**

*Creating and assigning storage grades* on page 76

*Activating the ILM policy* on page 90
Viewing current storage pools

You can view the current configuration of storage pools at any time.

Before you begin

You must have signed in to the Grid Management Interface using a supported browser.

Steps

1. Select ILM > Storage Pools.

For each storage pool, you can view the number of Storage Nodes or Archive Nodes as well as the amount of storage installed, used, and available.

Note: For Archive Nodes, storage installed and available is not shown.

If you have just run expansion grid tasks for Storage Nodes, the total number of LDR services is displayed correctly. However, information related to available storage capacity, storage grade, and site will not be accurate until the new grid nodes are started (services enabled).

2. Click Expand All to display the storage grade and site defined for each storage pool. Click Close All to hide details.

Configuring Erasure Coding profiles

Before you can create an ILM rule that erasure codes object data, you must first create an Erasure Coding profile.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

• You must have configured storage pools.
About this task

To create an Erasure Coding profile, associate a storage pool with an erasure coding scheme. This determines the number of fragments created and where the system distributes these fragments.

Note: Once created, an Erasure Coding profile cannot be changed or deleted.

Steps

1. Select ILM > Erasure Coding.

2. If this is not the first profile, click Insert to add a new profile.

   Note: You must update the default Erasure Coding profile listed on the page before adding a new profile.

3. Enter a representative name for the Erasure Coding profile.

   Note: Create a name that makes for easy identification when configuring ILM rules.

4. Select a storage pool.

   When selecting a storage pool, remember that the number of Storage Nodes associated with a storage pool determine which erasure coding schemes are made available for that profile.

5. Select an available erasure coding scheme.

   Note: Available erasure coding schemes are limited by the number of Storage Nodes available in the selected storage pool.

   When selecting an erasure coding scheme, the profile automatically updates Storage Overhead, Storage Node Redundancy, and Site Redundancy values.

6. To add another profile, click Insert.

   Once created, an Erasure Coding profile cannot be changed or deleted.

7. Click Apply Changes.
Specifying time values for time based metadata

When you configure an ILM rule's advanced filtering, you can select Ingest Time or Last Access Time metadata.

About this task

Ingest Time and Last Access Time are specified in microseconds since Unix Epoch.

Steps

1. Determine the UTC date and time to filter against. You may need to convert from your local time zone to UTC.

2. Convert the UTC date and time to microseconds since Unix Epoch. For example, use `date` from a Linux command prompt:

   Example

   ```
   # date -d '2015-03-14 00:00:00 UTC' +%s000000
   14262912000000
   ```

3. If Last Access Time is used, enable last access time updates on each S3 bucket or Swift container, as required. See the appropriate StorageGRID Webscale API guide.

Related information

- StorageGRID Webscale 10.3 Simple Storage Service Implementation Guide
- StorageGRID Webscale 10.3 Cloud Data Management Interface Implementation Guide

Creating an ILM rule

To manage the placement of object data over time, you must create ILM rules, which is achieved through the Create New ILM Rules wizard.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- You have configured storage pools.
- To use last access time metadata, Last Access Time must be enabled by bucket for S3, by container for Swift, or by client for CDMI.
- If you are creating erasure coded copies, you must have configured Erasure Coding profiles.
About this task

Objects are first evaluated against the ILM rule’s filtering criteria and then, if there is a match, object data is copied and placed based on the matching ILM rule’s placement instructions. Object metadata is not managed by ILM rules. Metadata is kept in the distributed key value store, which makes three copies of an object’s metadata in each data center.

Placement instructions determine where, when, and how object data is stored. If more than one placement instruction is configured, when a set time expires, the content placement instructions for the next time period are applied to objects at the next ILM evaluation time.

**Warning:** Although it is possible to create an ILM rule that creates one replicated copy only, it is not recommended. If the only replicated copy is lost or corrupted, data will be irrevocably lost.

Steps

1. Select ILM > Rules.

2. Click Create.

The Create ILM Rule wizard opens. The screen shots in this section show an example rule named “Finance Records.”
3. Complete the pages of the Create ILM Rule wizard.
   
a. Optionally, click Advanced filtering and configure metadata against which the ILM rule filters object data.
   
   If you do not configure advanced filtering for your ILM rule, the ILM rule matches all objects ingested within the currently configured scope (tenants, buckets, and object type), if any.
   
b. Click Save.
   
c. Click Next.
   
d. In Step 2 of the wizard, create placement instructions.
For Reference Time, select a time from which the ILM calculates the start time for a placement instruction.

Under Placements, set the storage location, length of time, and type of copy made for matching object data. When you select a storage location (storage pool) for erasure coded object data, the selected storage pool also indicates the erasure coding profile used (in parentheses).

For replicated copies, in addition to the preferred storage pool, you can specify a temporary storage pool. This location is used temporarily if the preferred storage pool is unavailable.

**Warning:** Using a temporary storage pool is strongly recommended. Failure to specify a temporary storage pool puts object data at risk if the preferred pool is unavailable.

e. Click **Refresh** to update the Retention Diagram

Use the retention diagram to confirm your placement instructions. Each line represents a copy of object data and when the copy is placed in the selected storage pool. Each storage location type is depicted by the following icons:

- ![Erasure coded](image)
- ![Replicated](image)
Related concepts

- How ILM rules filter objects on page 73
- Configuring and activating an ILM policy on page 87

Related tasks

- Configuring storage pools on page 78

Configuring and activating an ILM policy

After you have created ILM rules, you add them to an ILM policy and then activate the ILM policy. Before you create an ILM policy, determine the following:

- The number and type of copies required (replicated or erasure coded), and their placement over time.
- The metadata used in the applications that connect to the StorageGRID Webscale system. Objects are filtered against metadata.
- The StorageGRID Webscale system’s topology and storage configurations.

Keep the ILM policy as simple as possible. This avoids potentially dangerous situations where object data is not protected as intended as changes are made to the StorageGRID Webscale system over time.

**Warning:** An ILM policy that has been incorrectly configured can result in unrecoverable data loss. Carefully review the ILM policy and its ILM rules before activating it. Always confirm that the ILM policy will work as intended.

Related tasks

- Activating the ILM policy on page 90

Order of ILM rules within an ILM policy

The order in which you place ILM rules within an ILM policy determines how ILM rules are applied. The object is first evaluated against the top priority ILM rule and then subsequent ILM rules until a match is made. To match an ILM rule’s filter, an object must match all of the filter’s criteria. If an object does not have the metadata tag specified in the criteria, the object does not match the filter.

One ILM rule must be set as the default ILM rule. If none of the other ILM rules match the object, the placement instructions specified in the default rule are applied. When the StorageGRID Webscale system is first installed, the stock ILM rule “Make 2 Copies” is the default ILM rule.

Configuring the ILM policy

After creating your ILM rules and determining the order that these rules will be placed within the ILM policy, configure the ILM policy. When activated, this policy determines how object data is managed.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

• You must have created ILM rules.

Steps
1. Select ILM > Policies.
2. Select ILM Policies > Configure.
   The proposed ILM policy appears below the list of available ILM rules.

   ![Configure ILM Policies](image)

   - By default, the proposed ILM policy is the same as the active ILM policy when the proposed ILM policy first appears. The currently active ILM policy appears below the proposed ILM policy.
   - Select the Add to Policy check box next to an ILM rule in the Saved Rules table.
     The selected ILM rule appears in the Proposed Policy section.
   - Optionally, change the name of the proposed ILM policy.
   - Optionally, clear the Add to Policy check box next to an ILM rule in the Saved Rules table.
     The selected ILM rule disappears from the Proposed Policy section.
   - Note: You can also click Delete next to the ILM rule in the Proposed Policy section.
   - Drag ILM rules up or down within the Rules to reorder priorities.
     Warning: The order of ILM rules within an ILM policy is extremely important. Objects are filtered against ILM rules as they are listed in the table: from top to bottom.
   - Select Default next to an ILM rule.
     Every ILM policy must contain a default ILM rule.
8. Click **Save**.

9. Review filtering criteria and placement instructions carefully to ensure that the proposed ILM policy is correct and then do one of the following:
   
   - **Click Activate.**
     The system activates the ILM policy and now filters all objects against this ILM policy.
   
   - **Click Revert to Active Policy.**
     All changes are discarded.
     
     **Note:** It is not possible to revert to the active ILM policy unless another proposed ILM policy exists.

**Result**

Each ILM policy is automatically assigned a version number in the form major.minor (for example, 2.5). A change to the ILM policy triggers a major revision. A change to an ILM rule that is part of the ILM policy triggers a minor revision.

**Related concepts**

- *How ILM rules filter objects* on page 73

**Related tasks**

- *Activating the ILM policy* on page 90

**Updating an ILM policy**

**Warning:** Errors in an ILM policy can cause unrecoverable data loss. Carefully review the policy before activating it to make sure it will work as intended.

Typical reasons for updating an ILM policy include:

- An error exists in the current ILM policy.
- Changes are made to a storage pool.
- An Archive Node is added to the StorageGRID Webscale system.
- New client application connections are added.
- New storage retention requirements (for example, a change in regulatory requirements) are defined.

If you change the ILM policy, objects that have completed ILM evaluation are not re-evaluated against the updated ILM policy and object data stays “as is”. Any object that has been ingested, but not yet evaluated, is managed according to the new ILM policy.

After you activate an updated ILM policy, the StorageGRID Webscale system immediately starts applying that ILM policy to all newly ingested objects. To verify the ILM policy, you might want to activate and verify it with test objects at a time when normal ingest does not occur.

If the updated ILM policy includes an ILM rule to move object data to a new storage pool after a set period of time, it might not be practical to wait to verify this future placement. You might want to activate and verify an ILM policy with a temporary or test ILM rule that uses shorter time periods, but is otherwise identical to the current ILM policy, before activating the final version of your ILM policy for regular operations.
Activating the ILM policy

After you have added ILM rules to your proposed ILM policy, activate it. Once activated the ILM rules in your ILM policy begin filtering objects.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- You must have saved the proposed ILM policy.

About this task

**Warning:** Errors in an ILM policy can cause unrecoverable data loss. Carefully review the policy before activating it and confirm that it will work as intended.

Steps

1. Select **ILM > Policies**.
2. Select **ILM Policies > Configure**.
3. Carefully review the proposed ILM policy to make sure it is correct.
4. Click **Activate**.
5. Click **OK** to confirm you want to change the ILM policy.

The system activates the ILM policy and it now appears in the **ILM Policy > Active** and **ILM Policy > Historical** pages. The **CMS > Content > Overview > Main** page also lists the active ILM page.

The StorageGRID Webscale system manages all newly ingested objects according to the new ILM policy.
6. If required, apply the new ILM policy to previously evaluated objects. Click **Re-evaluate Content**.

If you choose to apply the new ILM policy to previously evaluated objects, the ILM Re-evaluation (User Triggered) grid task runs in the background and forces all CMS services to re-evaluate all objects. Copies are created and deleted as necessary according to the new ILM rules.

**Related tasks**

- [Verifying an ILM policy](#) on page 91
- [Evaluating previously ingested objects against a new ILM policy](#) on page 95

### Verifying an ILM policy

After you have activated a new ILM policy, you should ingest test objects into the StorageGRID Webscale system and confirm that copies are being made as intended and placed in the correct locations. Perform an “object lookup” for the ingested object. To confirm the location of an object’s data through an object lookup, you need the object’s identifier.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- You must have an object identifier, one of:
  - **CBID**: An object’s CBID can be obtained from latest audit log, which is located on the Admin Node at `/var/local/audit/export`.
  - **S3 bucket and key**: When an object is ingested through the S3 interface, the client application uses a bucket and key combination to store and identify the object. For details, see the *Simple Storage Service Implementation Guide*.
  - **CDMI data object ID**: When an object is ingested through the CDMI interface, the StorageGRID Webscale system returns a CDMI data object ID to the client application. For details, see the *Cloud Data Management Interface Implementation Guide*.
  - **Swift container and object**: When an object is ingested through the Swift interface, the client application uses a container and object combination to store and identify the object. For details, see the *Swift Implementation Guide*.

**About this task**

If the Audit option is enabled, you can also monitor the audit log for the “ORLM Object Rules Met” message. The ORLM audit message can provide you with more information about the status of the ILM evaluation process, but it cannot give you information about the correctness of the object data’s placement or the completeness of the ILM policy. You must evaluate this yourself. For more information, see the *Audit Message Reference*.

**Steps**

1. Ingest an object.
   Before ingesting the object, confirm that you have the object's identifier.

2. "Lookup" the ingested object and confirm that it is stored correctly:
   a. Select **Grid**.
b. Select **primary Admin Node** > CMN > Object Lookup.

c. Click **Configuration** > **Main**.

d. Click **Configuration** > **Main**.

e. Enter the object’s identifier (CBID, S3 bucket/key, Swift container/object, or CDMI data object ID).

f. Click **Apply Changes**

The CMN > Object Lookup > Overview page displays the current location of the object and any metadata associated with the object.
g. Confirm that the object is stored in the correct location and that it is the correct type of copy.

Related concepts

Configuring audit client access on page 155

Related information

StorageGRID Webscale 10.3 Audit Message Reference
StorageGRID Webscale 10.3 Cloud Data Management Interface Implementation Guide
StorageGRID Webscale 10.3 Simple Storage Service Implementation Guide
StorageGRID Webscale 10.3 Swift Implementation Guide

Working with ILM rules and ILM policies

Once you have created ILM rules and an ILM policy, you can continue to work with them, modifying their configuration as your storage requirements change.

Deleting an ILM rule

To keep the list of current ILM rules manageable, delete any ILM rules that you are not likely to use. You cannot delete the stock ILM rule (“Make 2 Copies”), ILM rules listed in the active policy, or ILM rules currently listed in the proposed policy.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select ILM > Rules.

2. Select the ILM rule you want to delete and click Remove.

3. Click OK to confirm that you want to delete the ILM rule.

   The ILM rule is deleted.

Related concepts

Configuring and activating an ILM policy on page 87

Editing an ILM rule

After creating an ILM rule, and before adding it to the active ILM policy, you can edit it. You cannot edit the stock ILM rule (“Make 2 Copies”), ILM rules listed in the active policy, ILM rules currently listed in the proposed policy, or ILM rules created before StorageGRID Webscale 10.3.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
Steps
1. Select ILM > Rules.

2. Select the ILM rule you want to edit and click Edit.
   The ILM rule wizard opens.

3. Edit the ILM rule and click Save.
   The ILM rule is updated.

Viewing historical ILM policies
You can view historical ILM rules at any time. These are ILM rules that have been at some point in time included in an active ILM policy.

Before you begin
• You must have signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task
Historical ILM policies include ILM policies that are no longer active. Historical ILM policies cannot be deleted.

Steps
1. Select ILM > Policies.

2. Select ILM Policies > Historical.

3. To view the ILM rules and storage pools associated with an ILM policy, click Expand.
   All policies are displayed with start and end dates.

4. Within an ILM rule, click Expand to display more information about its configuration.

Viewing the ILM policy activity queue
You can view the number of objects that are in queue to be evaluated against the ILM policy at any time. You might want to monitor the ILM processing queue to determine system performance. A large queue might indicate that the system is not able to keep up with the ingest rate, the load from the client is too great, or that some abnormal condition exists.

Before you begin
• You must have signed in to the Grid Management Interface using a supported browser.
To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. **Select Dashboard.**

2. Monitor the Information Lifecycle Management (ILM) section paying attention to the number of objects queued beyond 24 hours.

**Evaluating previously ingested objects against a new ILM policy**

After you change the ILM policy, all new objects ingested into the StorageGRID Webscale system are evaluated against the new ILM policy and object data is copied and stored according to ILM policy’s ILM rules. However, previously evaluated objects are not re-evaluated and object data remains “as is”. To re-evaluate previously evaluated objects against the new ILM policy, you must trigger an ILM Re-evaluation (User Triggered).

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

Evaluating previously ingested objects against the new ILM policy is not always required. If the change to the ILM policy only applies to content written after the policy has been activated, a re-evaluation is not required. For example, if you add a new site to the StorageGRID Webscale system and update the ILM policy to add ILM rules for objects ingested at that new site, there might be no need to re-evaluate objects already in the StorageGRID Webscale system and protected from loss.

**Note:** Because an ILM re-evaluation places additional load on the StorageGRID Webscale system, confirm that it is a necessary action.

**Steps**

1. Check whether an ILM re-evaluation has already been triggered:

   a. **Select Grid.**
b. Select primary Admin Node > CMN > Grid Tasks.

c. If you see the grid task ILM Re-evaluation (User Triggered) in the table of Active tasks, you must cancel the active ILM evaluation before triggering a new one.
   • Under Actions, select Pause, then click Apply Changes.
   • When Status updates to Paused, under Actions, select Abort, and then click Apply Changes.
     The ILM Re-evaluation (User Trigger) grid task moves to the Historical table with a status of Aborted.
     If you start a new ILM Re-evaluation (User Triggered) grid task while an earlier one is still in progress, the second ILM Re-evaluation (User Triggered) grid task fails.

2. Review the active policy to ensure that it is correct:
   a. Select ILM > Policies.
   
   b. Select ILM Policies > Configure.

3. Click Re-evaluate Content.

4. Click OK to confirm that you want to apply the new ILM policy to existing content.
   The StorageGRID Webscale system re-evaluates all stored objects against the active ILM policy and creates or deletes objects as required.

5. Monitor the re-evaluation’s progress:
   a. Select Grid.
   
   b. Select primary Admin Node > CMN > Grid Tasks.
   
   c. Monitor the progress of the ILM Evaluation (User Triggered) grid task.
     Charting the % Complete provides you with an estimate on when the ILM re-evaluation will complete.

Example ILM rules and policy

You can use the following examples as starting points to define ILM rules and policies that meet your object protection and retention requirements.

Warning: The following ILM rules and policy are only examples. There are many ways to configure ILM rules. Carefully analyze your ILM rules before adding them to an ILM policy to confirm that they will work as intended to protect content from loss.
Example ILM rule 1: Copy object data to two data centers

This example ILM rule copies object data to storage pools in two data centers.

<table>
<thead>
<tr>
<th>Rule definition</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Pools</td>
<td>Two storage pools, each at different data centers, named Storage Pool DC1 and Storage Pool DC2.</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Two Copies Two Data Centers</td>
</tr>
<tr>
<td>Reference Time</td>
<td>Ingest Time</td>
</tr>
</tbody>
</table>
| Content Placement | • On Day 0, keep a replicated copy in Storage Pool DC1 forever; temp copies in Storage Pool DC2  
                   • On Day 0, keep a replicated copy in Storage Pool DC2 forever; temp copies in Storage Pool DC1 |

Create ILM Rule

Configure placement instructions to determine where the system stores matching object data, for how long, and the type of copy made (replicated or erasure coded).

Two Copies Two Data Centers

Reference Time: Ingest Time

Placements

From day 0 store forever

Create 1 copies as replicated in Storage Pool DC1 or temporarily in Storage Pool DC2

Create 1 copies as replicated in Storage Pool DC2 or temporarily in Storage Pool DC1

Retention Diagram

Trigger: Day 0

Storage Pool DC1

Storage Pool DC2

Duration: Forever
Example ILM rule 2: Erasure Coding profile with bucket matching

This example ILM rule uses an Erasure Coding profile and an S3 bucket to determine where and how long the object is stored.

<table>
<thead>
<tr>
<th>Rule definition</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erasure Coding Profile</td>
<td>• One storage pool across three data centers</td>
</tr>
<tr>
<td></td>
<td>• Use 4+2 Erasure Coding scheme</td>
</tr>
<tr>
<td>Rule Name</td>
<td>EC for S3 Bucket FinanceRecords</td>
</tr>
<tr>
<td>Reference Time</td>
<td>Ingest Time</td>
</tr>
<tr>
<td>Content Placement</td>
<td>For objects in the S3 Bucket FinanceRecords, create one Erasure Coded copy in the pool specified by the Erasure Coding profile. Keep this copy forever.</td>
</tr>
</tbody>
</table>

Example ILM rule 3: Store object to DC1 and Archive

This example ILM rule creates two copies. One copy is stored in Data Center 1 for one year, and the second copy is stored in an Archive Node forever.

<table>
<thead>
<tr>
<th>Rule definition</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Pools</td>
<td>A disk storage pool and an archive storage pool.</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Archive</td>
</tr>
<tr>
<td>Reference Time</td>
<td>Ingest Time</td>
</tr>
<tr>
<td>Rule definition</td>
<td>Example value</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------</td>
</tr>
</tbody>
</table>
| Content Placement | • On Day 0, keep a replicated copy in Storage Pool DC1 for 365 days; temp copies in Storage Pool DC2  
• On Day 0, keep a replicated copy in Storage Pool Archive forever; temp copies in All Storage Nodes |

**Example ILM policy**

The StorageGRID Webscale system allows you to design sophisticated and complex ILM policies; however, in practice, most ILM policies are simple.

A typical ILM policy for a multi-site topology might include ILM rules such as the follows:

- At ingest, use 4+2 Erasure Coding to store all objects belonging to the S3 Bucket FinanceReports across three data centers.
- If an object does not match the first ILM rule, use the default ILM rule to store a copy of that object in two data centers, DC1 and DC2.
## Configure ILM Policies

**Saved Rules**

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Add to Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive v1.0</td>
<td></td>
</tr>
<tr>
<td>EC for S3 Bucket FinanceRecords v1.0</td>
<td></td>
</tr>
<tr>
<td>Make 2 Copies v1.0</td>
<td></td>
</tr>
<tr>
<td>Rule 2 v1.0</td>
<td></td>
</tr>
<tr>
<td>Two Copies Two Data Centers v1.0</td>
<td></td>
</tr>
</tbody>
</table>

**Proposed Policy**

**Policy:** Object Storage Policy

<table>
<thead>
<tr>
<th>Rules (Evaluated Top Down)</th>
<th>Default</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC for S3 Bucket FinanceRecords v1.0</td>
<td></td>
<td><img src="icon" alt="icon" /> <img src="icon" alt="icon" /> <img src="icon" alt="icon" /></td>
</tr>
<tr>
<td>Two Copies Two Data Centers v1.0</td>
<td></td>
<td><img src="icon" alt="icon" /> <img src="icon" alt="icon" /> <img src="icon" alt="icon" /></td>
</tr>
</tbody>
</table>

**Storage Pools**

<table>
<thead>
<tr>
<th>1. All Storage Nodes</th>
</tr>
</thead>
</table>
Managing disk storage

Storage Nodes provide disk storage capacity and services.

What a Storage Node is

A Storage Node includes the services and processes required to store, move, verify, and retrieve object data and metadata on disk.

What the LDR service is

Hosted by a Storage Node, the Local Distribution Router (LDR) service handles content transport for the StorageGRID Webscale system. Content transport encompasses many tasks including data storage, routing, and request handling. The LDR service does the majority of the StorageGRID Webscale system's hard work by handling data transfer loads and data traffic functions.

The LDR service handles the following tasks:

- Object data storage
- Object data transfers from another LDR service (Storage Node)
- Data storage management
- Protocol interfaces (S3, Swift, and CDMI)

For general information about the LDR service's role in the management of objects, see the StorageGRID Webscale 10.3 Grid Primer.

What the DDS service is

Hosted by a Storage Node, the Distributed Data Store (DDS) service interfaces with the distributed key value store and manages metadata stored in the StorageGRID Webscale system. Included in this management is the distribution of metadata copies to multiple instances of the distributed key value store so that metadata is always protected against loss.

The DDS service also manages the mapping of S3 and Swift objects to the unique “content handles” (UUIDs) that the StorageGRID Webscale system assigns to each ingested object.
Object counts

The DDS service lists the total number of objects ingested into the StorageGRID Webscale system as well as the total number of objects ingested through each of the system’s supported interfaces (S3, Swift, and CDMI).

Because object metadata synchronization occurs over time, object count attributes (see DDS > Data Store > Overview > Main) can differ between DDS services. Eventually, all distributed key value stores will synchronize and counts should become the same.

Queries

You can identify the average time that it takes to run a query against the distributed key value data store through the specific DDS service, the total number of successful queries, and the total number of queries that failed because of a timeout issue.

You might want to review query information to monitor the health of the key data store, Cassandra, which impacts the system’s ingest and retrieval performance. For example, if the latency for an average query is slow and the number of failed queries due to time out is high, that might indicate that the data store is encountering a higher load or performing another operation.

You can also view the total number of queries that failed because of consistency failures. Consistency level failures result from an insufficient number of available distributed key value stores at the time a query is performed through the specific DDS service.

Consistency guarantees and controls

StorageGRID Webscale guarantees read-after-write consistency for newly created objects. Any GET operation following a successfully completed PUT operation will be able to read the newly written data. Overwrites of existing objects, metadata updates, and deletes remain eventually consistent.
Metadata protection

Object metadata is information related to or a description of an object; for example, object modification time, or storage location. Metadata is stored in a distributed key value store maintained by the StorageGRID Webscale system’s DDS services.

To ensure redundancy and thus protection against loss, the StorageGRID Webscale system stores copies of the object metadata in different distributed key value stores throughout the StorageGRID Webscale system including between sites. This replication is non-configurable and performed automatically by the DDS service.

CMS service

The Content Management System (CMS) service manages objects to ensure that the StorageGRID Webscale system’s information lifecycle management (ILM) policy is satisfied.

The CMS service carries out the operations of the active ILM policy’s ILM rules, determining how object data is protected over time. For general information about the role of the CMS service when content is ingested and copied, see the Grid Primer.

Related tasks

Configuring information lifecycle management rules and policy on page 76

Related information

StorageGRID Webscale 10.3 Grid Primer

ADC service

The Administrative Domain Controller (ADC) service authenticates grid nodes and their connections with each other. The ADC service is hosted on each of the first three Storage Nodes at a site.

The ADC service maintains topology information including the location and availability of services. When a grid node requires information from another grid node or an action to be performed by another grid node, it contacts an ADC service to find the best grid node to process its request. In addition, the ADC service retains a copy of the StorageGRID Webscale deployment’s configuration bundles, allowing any grid node to retrieve current configuration information.

To facilitate distributed and islanded operations, each ADC service synchronizes certificates, configuration bundles, and information about services and topology with the other ADC services in the StorageGRID Webscale system.

In general, all grid nodes maintain a connection to at least one ADC service. This ensures that grid nodes are always accessing the latest information. When grid nodes connect, they cache other grid nodes’ certificates, enabling systems to continue functioning with known grid nodes even when an ADC service is unavailable. New grid nodes can only establish connections by using an ADC service.

The connection of each grid node lets the ADC service gather topology information. This grid node information includes the CPU load, available disk space (if it has storage), supported services, and the grid node’s site ID. Other services ask the ADC service for topology information through topology queries. The ADC service responds to each query with the latest information received from the StorageGRID Webscale system.
What the nodetool repair operation is

Periodically, the StorageGRID Webscale system runs the nodetool repair operation on Storage Nodes checking for and repairing metadata replication inconsistencies that may occur over time.

Nodetool repair is run every 12 to 14 days at random times on different Storage Nodes, so that it does not run on every Storage Node at the same time. The nodetool repair operation is a seamless activity that occurs in the background of normal system operations.

Managing Storage Nodes

Object stores

The underlying data storage of an LDR service is divided into a fixed number of object stores (also known as storage volumes or rangedbs), each a separate mount point.

Object stores are identified by a hexadecimal number from 0000 to 000F, which is known as the volume ID. Replicated copies and erasure coded fragments are stored to all available object stores within a Storage Node, while object metadata is stored only to volume 0000.

To ensure even space usage for replicated copies, object data for a given object is stored to one object store based on available storage space. When one or more object stores fill to capacity, the remaining object stores continue to store objects until there is no more room on the Storage Node.

Monitoring Storage Node capacity

To monitor the amount of usable space available on a Storage Node go to Storage > Overview > Main and note the current value for the attribute Total Usable Space (STAS).
Total Usable Space (STAS) is calculated by adding together the available space of all object stores for a Storage Node. A Storage Node does not become read-only until all object stores are filled to configured watermark settings.

Total Usable Space = Useable Space 0 + Useable Space 1 + Useable Space 2 + Useable Space 3

Related concepts

*Watermarks* on page 106
Watermarks

You use watermark settings to globally manage a Storage Node’s usable storage space. Watermarks settings trigger alarms that assist you in monitoring available storage and determine when adding Storage Nodes is required.

A Storage Node becomes read-only when all of a Storage Node’s object stores reach the Storage Volume Hard Read-Only Watermark. If available space falls below this configured watermark amount, a Notice alarm is triggered for the Storage Status (SSTS) attribute. This allows you to manage storage proactively and add capacity only when necessary.

The StorageGRID Webscale system’s current watermark values can be obtained at any time. Go to Configuration > Storage Options > Overview.

### Object Segmentation

<table>
<thead>
<tr>
<th>Description</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segmentation</td>
<td>Enabled</td>
</tr>
<tr>
<td>Maximum Segment Size</td>
<td>1 GB</td>
</tr>
</tbody>
</table>

### Storage Watermarks

<table>
<thead>
<tr>
<th>Description</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Volume Soft Read-Only Watermark</td>
<td>10 GB</td>
</tr>
<tr>
<td>Storage Volume Hard Read-Only Watermark</td>
<td>5 GB</td>
</tr>
<tr>
<td>Metadata Reserved Free Space</td>
<td>2,000 GB</td>
</tr>
</tbody>
</table>

### Ports

<table>
<thead>
<tr>
<th>Description</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLB HTTP Port</td>
<td>8880</td>
</tr>
<tr>
<td>CLB S3 Port</td>
<td>8823</td>
</tr>
<tr>
<td>CLB Swift Port</td>
<td>8883</td>
</tr>
<tr>
<td>LDR HTTP Port</td>
<td>18086</td>
</tr>
<tr>
<td>LDR S3 Port</td>
<td>18002</td>
</tr>
<tr>
<td>LDR Swift Port</td>
<td>18083</td>
</tr>
</tbody>
</table>

### Watermark related attributes
<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Default Setting</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Volume Soft Read-Only Watermark</td>
<td>10 GB</td>
<td>VHWM</td>
<td>Indicates when a Storage Node transitions to soft read-only mode. Soft read-only mode means that the Storage Node advertises read-only services to the rest of the StorageGRID Webscale system, but fulfills all pending write requests. The Storage Volume Soft Read-Only Watermark value is calculated against the Total Space value for the Storage Node, but measured against the Total Usable Space value for the Storage Node. When the value of Total Usable Space falls below the value of Storage Volume Soft Read-Only Watermark, the Storage Node transitions to soft read-only mode: • The Storage State – Current (SSCR) changes to Read-Only. If Storage State – Desired is set to Online, Storage Status (SSTS) changes to Insufficient Free Space and a Notice alarm is triggered. • An alarm for Total Usable Space (Percent) (SAVP) can be triggered, depending on the relationship between the watermark setting (in bytes) and the alarm settings (in percent). The Storage Node is writable again if Total Usable Space (STAS) becomes greater than Storage Volume Soft Read-Only Watermark.</td>
</tr>
<tr>
<td>Storage Volume Hard Read-Only Watermark</td>
<td>5 GB</td>
<td>VROM</td>
<td>Indicates when a Storage Node transitions to hard read-only mode. Hard read-only mode means that the Storage Node is read-only and no longer accepts write requests. The Storage Volume Hard Read-Only Watermark value is calculated against the Total Space value for the Storage Node, but measured against the Total Usable Space value for the Storage Node. When the value of Total Usable Space falls below the value of Storage Volume Hard Read-Only Watermark, the Storage Node transitions to hard read-only mode. The Storage Volume Hard Read-Only Watermark value must be less than value for The Storage Volume Soft Read-Only Watermark.</td>
</tr>
<tr>
<td>Metadata Reserved Space Watermark</td>
<td>2 TB</td>
<td>CAWM</td>
<td>The amount of free space reserved on object store volume 0 for metadata storage. If the storage capacity of volume 0 is less than 500 GB, only 10% of the storage volume’s capacity is reserved for metadata.</td>
</tr>
<tr>
<td>Service/Component</td>
<td>Attribute Name</td>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| LDR               | HTTP/CDMI State | HSTE | Set the LDR service to one of:  
- Offline: No operations are allowed, and any client application that attempts to open an HTTP session to the LDR service receives an error message. Active sessions are gracefully closed.  
- Online: Operation continues normally |
| Auto-Start HTTP   |                | HTAS | Enable the HTTP component when the LDR service is restarted. If not selected, the HTTP interface remains Offline until explicitly enabled.  
If Auto-Start HTTP is selected, the state of the system on restart depends on the state of the LDR > Storage component. If the LDR > Storage component is Read-only on restart, the HTTP interface is also Read-only. If the LDR > Storage component is Online, then HTTP is also Online. Otherwise, the HTTP interface remains in the Offline state. |
| LDR > Storage     | Storage State – Desired | SSDS | A user-configurable setting for the desired state of the storage component. The LDR service reads this value and attempts to match the status indicated by this attribute. The value is persistent across restarts.  
For example, you can use this setting to force storage to become read-only even when there is ample available storage space. This can be useful for troubleshooting.  
The attribute can take one of the following values:  
- Offline: When the desired state is Offline, the LDR service takes the LDR > Storage component offline.  
- Read-only: When the desired state is Read-only, the LDR service moves the storage state to read-only and stops accepting new content. Note that content might continue to be saved to the Storage Node for a short time until open sessions are closed.  
- Online: Leave the value at Online during normal system operations. The Storage State – Current of the storage component will be dynamically set by the service based on the condition of the LDR service, such as the amount of available object storage space. If space is low, the component becomes Read-only. |
<p>| Health Check Timeout |             | SHCT | The time limit in seconds within which a health check test must complete in order for a storage volume to be considered healthy. Only change this value when directed to do so by Support. |</p>
<table>
<thead>
<tr>
<th>Service/Component</th>
<th>Attribute Name</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LDR &gt; Verification</strong></td>
<td>Reset Missing Objects Count</td>
<td>VCMI</td>
<td>Resets the count of Missing Objects Detected (OMIS). Use only after foreground verification completes. Missing replicated object data is restored automatically by the StorageGRID Webscale system.</td>
</tr>
<tr>
<td>Verify</td>
<td>FVOV</td>
<td></td>
<td>Select object stores on which to perform foreground verification.</td>
</tr>
<tr>
<td>Verification Priority</td>
<td>VPRI</td>
<td></td>
<td>Set the priority rate at which background verification takes place. See <em>Configuring the background verification rate</em> on page 119.</td>
</tr>
<tr>
<td>Reset Corrupt Objects Count</td>
<td>VCCR</td>
<td></td>
<td>Reset the counter for corrupt replicated object data found during background verification. This option can be used to clear the Corrupt Objects Detected (OCOR) alarm condition. For more information, see the <em>StorageGRID Webscale 10.3 Troubleshooting Guide</em>.</td>
</tr>
<tr>
<td><strong>LDR &gt; Erasure Coding</strong></td>
<td>Reset Writes Failure Count</td>
<td>RSWF</td>
<td>Reset to zero the counter for write failures of erasure coded object data to the Storage Node.</td>
</tr>
<tr>
<td>Reset Reads Failure Count</td>
<td>RSRF</td>
<td></td>
<td>Reset to zero the counter for read failures of erasure coded object data from the Storage Node.</td>
</tr>
<tr>
<td>Reset Deletes Failure Count</td>
<td>RSDF</td>
<td></td>
<td>Reset to zero the counter for delete failures of erasure coded object data from the Storage Node.</td>
</tr>
<tr>
<td>Reset Missing Copies Detected Count</td>
<td>RSCC</td>
<td></td>
<td>Reset to zero the counter for the number of missing copies of erasure coded object data on the Storage Node.</td>
</tr>
<tr>
<td>Reset Corrupt Fragments Detected Count</td>
<td>RSCD</td>
<td></td>
<td>Reset to zero the counter for corrupt fragments of erasure coded object data on the Storage Node.</td>
</tr>
<tr>
<td>Service/Component</td>
<td>Attribute Name</td>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LDR &gt; Replication</td>
<td>Reset Inbound Replication Failure Count</td>
<td>RICR</td>
<td>Reset to zero the counter for inbound replication failures. This can be used to clear the RIRF (Inbound Replication – Failed) alarm.</td>
</tr>
<tr>
<td></td>
<td>Reset Outbound Replication Failure Count</td>
<td>ROCR</td>
<td>Reset to zero the counter for outbound replication failures. This can be used to clear the RORF (Outbound Replications – Failed) alarm.</td>
</tr>
<tr>
<td></td>
<td>Disable Inbound Replication</td>
<td>DSIR</td>
<td>Select to disable inbound replication as part of a maintenance or testing procedure. Leave unchecked during normal operation. When inbound replication is disabled, objects can be retrieved from the Storage Node for copying to other locations in the StorageGRID Webscale system, but objects cannot be copied to this Storage Node from other locations: the LDR service is read-only.</td>
</tr>
<tr>
<td></td>
<td>Disable Outbound Replication</td>
<td>DSOR</td>
<td>Select to disable outbound replication (including content requests for HTTP retrievals) as part of a maintenance or testing procedure. Leave unchecked during normal operation. When outbound replication is disabled, objects can be copied to this Storage Node, but objects cannot be retrieved from the Storage Node to be copied to other locations in the StorageGRID Webscale system. The LDR service is write-only.</td>
</tr>
<tr>
<td>LDR &gt; CDMI</td>
<td>Reset CDMI Counts</td>
<td>CACR</td>
<td>Reset to zero the counter for all CDMI transactions.</td>
</tr>
<tr>
<td>LDR &gt; HTTP</td>
<td>Reset HTTP Counts</td>
<td>LHAC</td>
<td>Reset to zero the counter for all HTTP transactions.</td>
</tr>
</tbody>
</table>

Related information

*StorageGRID Webscale 10.3 Troubleshooting Guide*

**Managing full Storage Nodes**

As Storage Nodes reach capacity, you must expand the StorageGRID Webscale system through the addition of new storage. There are two options available when considering how to increase storage capacity: adding Storage Nodes and adding storage volumes.

**Adding Storage Nodes**

You can increase storage capacity by adding Storage Nodes. Careful consideration of currently active ILM rules and capacity requirement must be taken when adding storage. For more information about how to add storage volumes and Storage Nodes, see the *Expansion Guide*.

**Adding storage volumes**

Each Storage Node supports a maximum of 16 storage volumes. If a Storage Node includes less than 16 storage volumes, you can increase its capacity by adding storage volume up to the maximum of 16.
Monitoring storage

Monitoring storage includes looking at total storage capacity, consumed storage, and usable storage. You might want to monitor storage capacity to determine your usable storage for the entire StorageGRID Webscale system or for select data center sites.

Monitoring storage capacity system-wide

At the deployment level, you can monitor installed storage capacity, used storage capacity, and usable storage capacity.

Before you begin

You must have signed in to the Grid Management Interface using a supported browser.

Step

1. Select Dashboard.

   Note the values for the StorageGRID Webscale system’s storage capacity.

Monitoring storage capacity per Storage Node

You can track the amount of usable space available on a Storage Node through the Total Usable Space (STAS) attribute, which is calculated by adding together the available space of all object stores for a Storage Node.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.

About this task

A Storage Node does not become read-only until all object stores are filled to configured watermark settings.

Steps

1. Select Grid.
2. Select Storage Node > LDR > Storage.

3. Note the current value for the attribute Total Usable Space (STAS).

![Image of Storage Grid Management Interface](image)

**Overview:**
- **Storage State - Desired:** Online
- **Storage State - Current:** Online
- **Storage Status:** No Errors

**Utilization**
- **Total Space:** 160 GB
- **Total Usable Space:** 155 GB
- **Total Data:** 5.34 GB
- **Total Data (Percent):** 3.33%

**Replication**
- **Block Reads:** 3,392
- **Block Writes:** 3,561
- **Objects Retrieved:** 1,197
- **Objects Committed:** 675
- **Objects Deleted:** 673
- **Delete Service State:** Enabled

**Object Stores**

<table>
<thead>
<tr>
<th>ID</th>
<th>Total</th>
<th>Available</th>
<th>Stored Data</th>
<th>Stored (%)</th>
<th>Cached Data</th>
<th>Cached (%)</th>
<th>Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>53.4 GB</td>
<td>48 GB</td>
<td>5.34 GB</td>
<td>10.002%</td>
<td>32.3 MB</td>
<td>0.00%</td>
<td>No Errors</td>
</tr>
<tr>
<td>0001</td>
<td>53.4 GB</td>
<td>53.4 GB</td>
<td>727 KB</td>
<td>0.001%</td>
<td>34 MB</td>
<td>0.064%</td>
<td>No Errors</td>
</tr>
<tr>
<td>0002</td>
<td>53.4 GB</td>
<td>53.4 GB</td>
<td>582 KB</td>
<td>10.002%</td>
<td>83.5 MB</td>
<td>0.151%</td>
<td>No Errors</td>
</tr>
</tbody>
</table>

**Related concepts**
- *Watermarks* on page 106

**Configure settings for stored objects**

**Configuring stored object encryption**

Stored object encryption enables the encryption of stored object data so that if an object store is compromised data cannot be retrieved in a readable form. By default, objects are not encrypted.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

Objects can also be encrypted using the AES-128 or AES-256 encryption algorithm. Stored object encryption enables the encryption of all object data ingested through S3, Swift, or CDMI. If disabled, currently encrypted objects remain encrypted. For S3 objects, the Stored Object Encryption setting can be overridden by the `x-amz-server-side-encryption` header. If you use the `x-amz-server-side-encryption` header, you must specify the AES-256 encryption algorithm in the request.
Note: If you change this setting, it may take a short period of time for the new setting to be applied. The configured value is cached for performance and scaling. If you want to ensure that the new setting is applied immediately, you need to restart the StorageGRID Webscale system.

Steps
1. Select Configuration > Grid Options.
2. From the Grid Options menu, select Configuration.
3. Change Stored Object Encryption to Disabled, AES-256, or AES-128.
4. Click Apply Changes.

Configuring stored object hashing

The Stored Object Hashing option specifies the hashing algorithm used by the LDR service to hash data when new content is stored. These hashes are verified during retrieval and verification to protect the integrity of data.

Before you begin
• You must have signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task
By default, object data is hashed using the SHA-1 algorithm. Object data can also be hashed using the SHA-256 algorithm.

Steps
1. Select Configuration > Grid Options.
2. From the Grid Options menu, select Configuration.
3. Change Stored Object Hashing to SHA-256 or SHA-1.
4. Click Apply Changes.

**Configuring stored object compression**

Stored Object Compression uses lossless compression of object data to reduce the size of objects and thus consume less storage.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

Applications saving an object to the StorageGRID Webscale system can compress the object before saving it; however, if a client application compresses an object before saving it to the StorageGRID Webscale system, enabling Stored Object Compression does not further reduce an object’s size.

Stored Object Compression is disabled by default.

**Note:** If you change this setting, it may take a short period of time for the new setting to be applied. The configured value is cached for performance and scaling. If you want to ensure that the new setting is applied immediately, you need to restart the StorageGRID Webscale system.

**Steps**

1. Select **Configuration > Grid Options**.

2. From the Grid Options menu, select **Configuration**.

3. Change Stored Object Compression to **Enabled**.
4. Click Apply Changes.

**Deletion protection settings**

You can choose to prevent object deletion for specific objects as they are evaluated against ILM rules or for all objects system wide.

**System wide client delete protection**

Enabling Disable Client Delete through the Grid Configuration page (Configuration > Grid Options > Configuration) overrides the delete and last access time permissions defined for CDMI profiles through HTTP Management - Permissions page (Configuration > CDMI > Permissions). Disable Client Delete is a system wide setting.

The following actions occur depending on the API client:

- For S3 clients, all delete bucket and delete object requests are denied.
- For Swift clients, all delete container and delete object requests are denied.
- For a CDMI client, all delete, metadata update, and last access time updates are denied.
Mounted storage devices

At installation, each storage device is assigned a file system UUID and is mounted to a rangedb directory on the Storage Node using that file system UUID. The file system UUID and the rangedb directory are captured in the /etc/fstab file.

The device name, rangedb directory, and the size of the mounted volume are displayed at Storage Node > SSM > Resources > Overview > Main.

In the following example, device /dev/sdb has a volume size of 830 GB, is mounted to /var/local/rangedb/0, using the device name /dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba in the /etc/fstab file.

What security partitions are

Security partitions is a system-wide setting that restricts CDMI client access to objects. A security partition prevents CDMI client applications from retrieving objects ingested through another CDMI client application. CDMI client applications are only permitted read-write access to a specific security partition, but can be configured with read-only access to other security partitions.

Note: Security partitions are ignored for objects ingested through the S3 and Swift interfaces.
Objects ingested before security partitions are enabled are not assigned a security partition and can be retrieved, queried, and deleted by any client application. If security partitions are enabled, objects ingested by a client application that is not assigned a security partition can be retrieved, queried, and deleted by any other client application—client applications are not automatically assigned a security partition.

**Related information**

*StorageGRID Webscale 10.3 Cloud Data Management Interface Implementation Guide*

**What object segmentation is**

Object segmentation is the process of splitting up an object into a collection of smaller fixed-size objects in order to optimize storage and resources usage for large objects. S3 multi-part upload also creates segmented objects, with an object representing each part.

When an object is ingested into the StorageGRID Webscale system, the LDR service splits the object into segments, and creates a segment container that lists the header information of all segments as content. For CDMI clients, the OID of the segment container is returned as the ingest result.

If your StorageGRID Webscale system includes an Archive Node whose Target Type is Cloud Tiering – Simple Storage Service and the targeted archival storage system is Amazon Web Services (AWS), the Maximum Segment Size must be less than or equal to 4.5 GiB (4,831,838,208 bytes). This upper limit ensures that the AWS PUT limitation of five GBs is not exceeded. Requests to AWS that exceed this value fail.
On retrieval of a segment container, the LDR service assembles the original object from its segments and returns the object to the client.

The container and segments are not necessarily stored on the same Storage Node. Container and segments can be stored on any Storage Node.

Each segment is treated by the StorageGRID Webscale system independently and contributes to the count of attributes such as Managed Objects and Stored Objects. For example, if an object stored to the StorageGRID Webscale system is split into two segments, the value of Managed Objects increases by three after the ingest is complete, as follows:

\[
\text{segment container} + \text{segment 1} + \text{segment 2} = \text{three stored objects}
\]

You can improve performance when handling large objects by ensuring that:

- Each Gateway and Storage Node has sufficient network bandwidth for the throughput required. For example, configure separate Grid and Client networks on 10Gbps Ethernet interfaces.
- Enough Gateway and Storage Nodes are deployed for the throughput required.
- Each Storage Node has sufficient disk IO performance for the throughput required.

### Verifying object integrity

The StorageGRID Webscale system verifies the integrity of object data on Storage Nodes, checking for both corrupt and missing objects.

There are two verification processes: background verification and foreground verification. Background verification runs automatically and continuously checks for corrupt object data. Foreground verification is manually triggered to detect missing objects.

#### Related concepts

- [What background verification is](#) on page 118
- [What foreground verification is](#) on page 120

#### Related information

- *[StorageGRID Webscale 10.3 Troubleshooting Guide](#)*

### What background verification is

The background verification process automatically and continuously checks Storage Nodes to determine if there are corrupt copies of replicated object data or corrupt fragments of erasure coded object data. If problems are found, the StorageGRID Webscale system automatically attempts to replace the missing or corrupt object data from copies stored elsewhere in the system. Background verification does not run on Archive Nodes.

If the background verification process detects that a copy of replicated object data is corrupt, that corrupt copy is removed from its location and quarantined elsewhere on the Storage Node. The Storage Node’s LDR service then sends a request to the DDS service to create a new uncorrupted copy. The DDS service fulfills this request by running an existing copy through an ILM evaluation, which will determine that the current ILM policy is no longer being met for this object because the corrupt object no longer exists at the expected location. A new copy is generated and placed to satisfy the system’s active ILM policy. This new copy may not be placed in the same location that the corrupt copy was stored. Corrupt object data is quarantined rather than deleted from the system, so that it can still be accessed. For more information on accessing quarantined object data, contact Support.
If the background verification process detects that a fragment of erasure coded object data is corrupt, that missing erasure coded fragment is rebuilt in place on the same Storage Node from the remaining fragments for that copy of erasure coded object data.

If background verification cannot replace the corrupted object because it cannot locate another copy, a LOST (Lost Object) alarm is triggered. Note that for erasure coded copies, if an object cannot be retrieved from the expected location an ECOR (Missing Copies Detected) alarm is triggered on the Storage Node from which the retrieval was attempted and an attempt is made to retrieve another copy. Only when no other copies are found, the LOST (Lost Objects) alarm is also triggered.

Background verification cannot be stopped; however, the rate at which it runs can be changed.

**Configuring the background verification rate**

For each Storage Node, you can change the rate that background verification checks replicated object data.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

You can change the rate at which background verification takes place by adjusting the Verification Priority value:

- **Adaptive**: Default setting. The task is designed to verify at a maximum of four MB/s or 10 objects/s (whichever is exceeded first).
- **High**: Storage verification proceeds quickly, at a rate that can slow ordinary system activities. Use the High verification priority only when you suspect that a hardware or software fault might have corrupted replicated object data. After the High priority background verification completes, the Verification Priority value automatically resets to Adaptive.

**Steps**

1. Select **Grid**.
2. Select **Storage Node > LDR > Verification**.
3. Click **Configuration > Main**.
4. Go to **LDR > Verification > Configuration > Main**.
5. Under Background Verification, select **Verification Priority > High** or **Verification Priority > Adaptive**.
Note: Setting the Verification Priority to High triggers a Notice level alarm for VPRI (Verification Priority).

6. Click **Apply Changes**.

7. Monitor the results of background verification. Go to **LDR > Verification > Overview > Main** and monitor the attribute Corrupt Objects Detected.

   If background verification finds corrupt replicated object data, the attribute Corrupt Objects Detected is incremented. The LDR service recovers by quarantining the corrupt object data and sending a message to the DDS service to create a new copy of the object data. The new copy can be made anywhere in the StorageGRID Webscale system that satisfies the active ILM policy.

8. If corrupt object data is found, contact Support to clear the quarantined copies from the StorageGRID Webscale system and determine the root cause of the corruption.

**What foreground verification is**

The foreground verification process allows you to manually verify the existence of replicated object data on a Storage Node. Foreground verification does not check for missing fragments of erasure coded object data.

If a copy of replicated object data is found to be missing, the StorageGRID Webscale system automatically attempts to replace the missing object data from copies stored elsewhere in the system. The Storage Node's LDR service sends a request to the DDS service to create a new copy. The DDS service fulfills this request by running an existing copy through an ILM evaluation, which will determine that the current ILM policy is no longer being met for this object because the missing object no longer exists at the expected location. A new copy is generated and placed to satisfy the system's active ILM policy. This new copy may not be placed in the same location that the missing copy was stored.

**Running foreground verification**

Foreground verification enables you to verify the existence of replicated object data on a Storage Node. This foreground verification process can help you to determine if there are integrity issues
with a storage device. Missing objects might indicate an issue with the underlying storage, which the LDR service uses.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- Ensure that the following grid tasks are not running:
  - Grid Expansion: Add Server (GEXP), when adding a Storage Node
  - Storage Node Decommissioning (LDCM) on the same Storage Node

  If these grid tasks are running, wait for them to complete or release their lock, or abort them as appropriate.
- Storage must be online.

**About this task**

Foreground verification only checks for missing replicated object data and does not check for missing fragments of erasure coded object data.

You can configure foreground verification to check all of a Storage Node's object stores or only specific object stores. If foreground verification determines that a copy of replicated object data is missing, the count for the Missing Objects Detected (OMIS) attribute (see Grid > site > Storage Node > LDR > Verification > Overview > Main) goes up by one. A replacement copy is automatically created by the system and stored to a location that satisfies the active ILM policy. The replacement copy is not necessarily stored on the Storage Node from which it originally went missing. If a replacement copy cannot be made, the LOST (Lost Object) alarm might be triggered.

Foreground verification generates an LDR Foreground Verification grid task that, depending on the number of objects stored on a Storage Node, can take days or weeks to complete. It is possible to select multiple Storage Nodes at the same time; however, these grid tasks are not run simultaneously, but rather queued and run one after the other until completion. When foreground verification is in progress on a Storage Node, you cannot start another foreground verification task on that same Storage Node even though the option to verify additional volumes might appear to be available for the Storage Node.

If a Storage Node other than the one where foreground verification is being run goes offline, the grid task continues to run until the % Complete attribute reaches 99.99 percent. The % Complete attribute then falls back to 50 percent and waits for the Storage Node to return to online status. When the Storage Node's state returns to online, the LDR Foreground Verification grid task continues until it completes.

**Steps**

1. Select Grid.
2. Select Storage Node > LDR > Verification.
3. Click Configuration > Main.
4. Under Foreground Verification, select ID for the storage volume or volumes to verify.
5. Click **Apply Changes**.

Wait until the page auto-refreshes and reloads before you leave the page. Once refreshed, object stores become unavailable for selection on that Storage Node.

An LDR Foreground Verification grid task is generated and runs until it completes or is aborted. To view its progress, go to **Grid > site > Admin Node > CMN > Grid Task > Overview > Main**. If object data is found to be missing, the missing object data is automatically replicated.

6. Monitor missing objects:

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

   b. From the Grid Options menu, click **Overview**.

   c. Under **Verification Results** note the value of **Missing Objects Detected**.

      If the count for the attribute **Missing Objects Detected** is large (if there are a hundreds of missing objects), there is likely an issue with the Storage Node's storage. In this case, cancel foreground verification by aborting the Foreground Verification grid task, resolve the storage issue, and then rerun foreground verification for the Storage Node.

      If foreground does not detect a significant number of replicated objects are missing, then the storage is operating normally.

**After you finish**

If foreground verification finds no (or few) missing objects, and you still have concerns about data integrity, it is recommended that you verify the integrity of the stored objects on the LDR by increasing the priority of the background verification process.
How load balancing works

To balance ingest and retrieval workloads, optionally deploy the StorageGRID Webscale system with API Gateway Nodes, or integrate a third-party load balancer.

API Gateway Node

The API Gateway Node provides load balancing functionality to the StorageGRID Webscale system and distributes the workload when multiple client applications perform ingest and retrieval operations.

The Connection Load Balancer (CLB) service directs incoming requests to the optimal LDR service, based on availability and system load. When the optimal LDR service is chosen, the CLB service establishes an outgoing connection and forwards the traffic to the chosen grid node.

HTTP connections from the StorageGRID Webscale system to a client application use the CLB service to act as a proxy unless the client application is configured to connect through an LDR service. The CLB services operates as a connection pipeline between the client application and an LDR service.
Managing archival storage

Optionally, each of your StorageGRID Webscale system's data center sites can be deployed with an Archive Node, which allows you to connect to a targeted external archival storage system.

What an Archive Node is

The Archive Node provides an interface through which you can target an external archival storage system for the long term storage of object data. The Archive Node also monitors this connection and the transfer of object data between the StorageGRID Webscale system and the targeted external archival storage system.

Object data that cannot be deleted, but is not regularly accessed, can at any time be moved off of a Storage Node's spinning disks and onto external archival storage such as the cloud or tape. This archiving of object data is accomplished through the configuration of a data center site's Archive Node and then the configuration of ILM rules where this Archive Node is selected as the "target" for content placement instructions. The Archive Node does not manage archived object data itself; this is achieved by the external archive device.

Note: Object metadata is not archived, but remains on Storage Nodes.

What the ARC service is

The Archive Node's Archive (ARC) service provides the management interface with which you configure connections to external archival storage such as the cloud through the S3 API or tape through TSM middleware.

It is the ARC service that interacts with an external archival storage system, sending object data for nearline storage and performing retrievals when a client application requests an archived object. When a client application requests an archived object, a Storage Node requests the object data from the ARC service. The ARC service makes a request to the external archival storage system, which retrieves the requested object data and sends it to the ARC service. The ARC service verifies the object data and forwards it to the Storage Node, which in turn returns the object to the requesting client application.

Requests for object data archived to tape through TSM middleware are managed for efficiency of retrievals. Requests can be ordered so that objects stored in sequential order on tape are requested in...
that same sequential order. Requests are then queued for submission to the storage device. Depending upon the archival device, multiple requests for objects on different volumes can be processed simultaneously.

**Related information**

*StorageGRID Webscale 10.3 Grid Primer*

**About supported archive targets**

When you configure the Archive Node to connect with an external archive, you must select the target type.

The StorageGRID Webscale system supports the archiving of object data to the cloud through an S3 interface or to tape through TSM middleware.

**Archiving to the cloud through the S3 API**

You can configure an Archive Node to target any external archival storage system that is capable of interfacing with the StorageGRID Webscale system through the S3 API.

The Archive Node's ARC service can be configured to connect directly to Amazon Web Services (AWS) or to any other system that can interface to the StorageGRID Webscale system through the S3 API; for example, another instance of the StorageGRID Webscale system.

**Archiving to tape through TSM middleware**

You can configure an Archive Node to target a Tivoli Storage Manager (TSM) server which provides a logical interface for storing and retrieving object data to random or sequential access storage devices, including tape libraries.

The Archive Node's ARC service acts as a client to the TSM server, using Tivoli Storage Manager as middleware for communicating with the archival storage system.

**Tivoli Storage Manager Management Classes**

Management classes defined by the TSM middleware outline how the TSM's backup and archive operations function, and can be used to specify rules for content that are applied by the TSM server. Such rules operate independently of the StorageGRID Webscale system’s ILM policy, and must be consistent with the StorageGRID Webscale system’s requirement that objects are stored permanently and are always available for retrieval by the Archive Node. After object data is sent to a TSM server by the Archive Node, the TSM lifecycle and retention rules are applied while the object data is stored to tape managed by the TSM server.

The TSM management class is used by the TSM server to apply rules for data location or retention after objects are sent to the TSM server by the Archive Node. For example, objects identified as database backups (temporary content that can be overwritten with newer data) could be treated differently than application data (fixed content that must be retained indefinitely).

**Managing connections to archival storage**

You can configure an Archive Node to connect to an external archival storage system through either the S3 API or TSM middleware.

Once the type of archival target is configured for an Archive Node, the target type cannot be changed.
Configuring connection settings for S3 API

There are a number of settings you must configure, before the Archive Node can communicate with an external archival storage system that connects to the StorageGRID Webscale system through the S3 API.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- You need to create a bucket on the target archival storage system:
  - The bucket must be dedicated to a single Archive Node. It cannot be used by other Archive Nodes or other applications.
  - The bucket must have the appropriate region selected for your location.
  - The bucket should be configured with versioning suspended.
- Object Segmentation must be enabled and the Maximum Segment Size must be less than or equal to 4.5 GiB (4,831,838,208 bytes). S3 API requests that exceed this value will fail if Simple Storage Service (S3) is used as the external archival storage system.

About this task

Until these settings are configured, the ARC service remains in a Major alarm state as it is unable to communicate with the external archival storage system.

Steps

1. Select Grid.
2. Select Archive Node > ARC > Target.
3. Click Configuration > Main.
4. Select **Cloud Tiering - Simple Storage Service (S3)** from the **Target Type** drop-down list.

   **Note:** Configuration settings are unavailable until you select a Target Type.

5. Configure the cloud tiering (S3) account through which the Archive Node will connect to the target external S3 capable archival storage system.

   Most of the fields on this page are self-explanatory. The following describes fields for which you might need guidance.

   - **Region:** Only available if Use AWS is selected. The region you select must match the bucket’s region.

   - **Endpoint and Use AWS:** For Amazon Web Services (AWS), select Use AWS. Endpoint is then automatically populated with an endpoint URL based on the Bucket Name and Region attributes. For example, `https://bucket.region.amazonaws.com`

     For a non-AWS target, enter the URL of the system hosting the bucket, including the port number. For example, `https://system.com:1080`

   - **Endpoint Authentication:** Enabled by default. Clear to disable endpoint SSL certificate and hostname verification for the targeted external archival storage system. Only clear the checkbox if the network to the external archival storage system is trusted. If another instance of a StorageGRID Webscale system is the target archival storage device and the system is configured with publicly signed certificates, you do not need to clear the checkbox.

   - **Storage Class:** Select Standard, the default value, for regular storage, or Reduced Redundancy, which provides lower cost storage with less reliability for objects that can be easily recreated. If the targeted archival storage system is another instance of the StorageGRID Webscale system, Storage Class controls the target system's dual-commit behavior.

6. Click **Apply Changes**.

   The specified configuration settings are validated and applied to your StorageGRID Webscale system. Once configured, the target cannot be changed.
Modifying connection settings for S3 API

After the Archive Node is configured to connect to an external archival storage system through the S3 API, you can modify some settings should the connection change.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

If you change the Cloud Tiering (S3) account, you must ensure that the user access credentials have read/write access to the bucket, including all objects that were previously ingested by the Archive Node to the bucket.

**Steps**

1. Select **Grid**.
2. Select **Archive Node > ARC > Target**.
3. Click **Configuration > Main**.

4. Modify account information, as necessary.
   
   If you change the storage class, new object data is stored with the new storage class. Existing object continue to be stored under the storage class set when ingested.
   
   **Note:** Bucket Name, Region, and Endpoint, use AWS values and cannot be changed.
5. Click **Apply Changes**.
Modifying the Cloud Tiering Service state

You can control the Archive Node's ability read and write to the targeted external archival storage system that connects through the S3 API by changing the state of the Cloud Tiering Service.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
- The Archive Node must be configured.

About this task

You can effectively take the Archive Node offline by changing the Cloud Tiering Service State to Read-Write Disabled.

Steps

1. Select Grid.
2. Select Archive Node > ARC.
3. Click Configuration > Main.
4. Select a Cloud Tiering Service State.
5. Click Apply Changes.

Configuring connections to Tivoli Storage Manager middleware

Before the Archive Node can communicate with Tivoli Storage Manager (TSM) middleware, you must configure a number of settings.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

Until these settings are configured, the ARC service remains in a Major alarm state as it is unable to communicate with the Tivoli Storage Manager.
**Steps**

1. Select Grid.

2. Select Archive Node > ARC > Target.

3. Click Configuration > Main.

4. Select Tivoli Storage Manager (TSM) from the Target Type drop-down list.

5. By default, the Tivoli Storage Manager State is set to Online, which means that the Archive Node is able to retrieve object data from the TSM middleware server. Select Offline to prevent retrievals from the TSM middleware server.

6. Complete the following information:
   - Server IP or Hostname: Specify the IP address or Fully Qualified Domain Name (FQDN) of the TSM middleware server used by the ARC service. The default IP address is 127.0.0.1.
   - Server Port: Specify the port number on the TSM middleware server that the ARC service will connect to. The default is 1500.
   - Node Name: Specify the name of the Archive Node. You must enter the name (arc-user) that you registered on the TSM middleware server.
   - User Name: Specify the user name the ARC service uses to log in to the TSM server. Enter the default user name (arc-user) or the administrative user you specified for the Archive Node.
   - Password: Specify the password used by the ARC service to log in to the TSM server. Re-enter the password when you are prompted to confirm it.
   - Management Class: Specify the default management class to use if a management class is not specified when the object is being save to the StorageGRID Webscale system, or the specified management class is not defined on the TSM middleware server.

   If the specified management class does not exist on the TSM server, the object cannot be saved to the TSM archive. The object remains in the queue on the StorageGRID Webscale
system and the CMS > Content > Overview > Objects with ILM Evaluation Pending count is incremented.

- **Number of Sessions**: Specify the number of tape drives on the TSM middleware server that are dedicated to the Archive Node. The Archive Node concurrently creates a maximum of one session per mount point plus a small number of additional sessions (less than five). You need to change this value to be the same as the value set for MAXNUMMP (maximum number of mount points) when the Archive Node was registered or updated. (In the register command, the default value of MAXNUMMP used is 1, if no value is set.) You must also change the value of MAXSESSIONS for the TSM server to a number that is at least as large as the Number of Sessions set for the ARC service. The default value of MAXSESSIONS on the TSM server is 25.

- **Maximum Retrieve Sessions**: Specify the maximum number of sessions that the ARC service can open to the TSM middleware server for retrieve operations. In most cases, the appropriate value is Number of Sessions minus Maximum Store Sessions. If you need to share one tape drive for storage and retrieval, specify a value equal to the Number of Sessions.

- **Maximum Store Sessions**: Specify the maximum number of concurrent sessions that the ARC service can open to the TSM middleware server for archive operations. This value should be set to one except when the targeted archival storage system is full and only retrievals can be performed. Set this value to zero to use all sessions for retrievals.

7. Click **Apply Changes**.

**Managing Archive Nodes**

**Optimizing Archive Node's TSM middleware sessions**

Typically, the number of concurrent sessions that the Archive Node has open to the TSM middleware server is set to the number of tape drives the TSM server has dedicated to the Archive Node. One tape drive is allocated for storage while the rest are allocated for retrieval.

However, in situations where a Storage Node is being rebuilt from Archive Node copies or the Archive Node is operating in Read-only mode, you can optimize TSM server performance by setting the maximum number of retrieve sessions to be the same as number of concurrent sessions. The result is that all drives can be used concurrently for retrieval, and, at most, one of these drives can also be used for storage if applicable.

**Optimizing Archive Node for TSM middleware sessions**

You can optimize the performance of an Archive Node that connects to an external archival storage system through the S3 API by configuring the Archive Node's sessions.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Grid**.
2. Select **Archive Node > ARC > Target**.
3. Click **Configuration > Main**.
4. Change **Maximum Retrieve Sessions** to be the same as **Number of Sessions**.

![Configuration: ARC (DC1-ARC1-98-165) - Target](image)

5. Click **Apply Changes**.

**Managing an Archive Node when TSM server reaches capacity**

The TSM server has no way to notify the Archive Node when either the TSM database or the archival media storage managed by the TSM server is nearing capacity. The Archive Node continues to accept object data for transfer to the TSM server after the TSM server stops accepting new content. This content cannot be written to media managed by the TSM server. An alarm is triggered if this happens. This situation can be avoided through proactive monitoring of the TSM server.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

To prevent the ARC service from sending further content to the TSM server, you can take the Archive Node offline by taking its **ARC > Store** component offline. This procedure can also be useful in preventing alarms when the TSM server is unavailable for maintenance.

**Steps**

1. Select **Grid**.
2. Select **Archive Node > ARC > Store**.
3. Click **Configuration > Main**.
4. Change Archive Store State to **Offline**.

5. Select **Archive Store Disabled on Startup**.

6. Click **Apply Changes**.

**Setting Archive Node to read-only if TSM middleware reaches capacity**

If the targeted TSM middleware server reaches capacity, the Archive Node can be optimized to only perform retrievals.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Grid**.

2. Select **Archive Node > ARC > Target**.

3. Click **Configuration > Main**.

4. Change Maximum Retrieve Sessions to be the same as the number of concurrent sessions listed in Number of Sessions.

5. Change Maximum Store Sessions to 0.

   **Note:** Changing Maximum Store Sessions to 0 is not necessary if the Archive Node is Read-only. Store sessions will not be created.

6. Click **Apply Changes**.

**Configuring Archive Node replication**

You can configure the replication settings for an Archive Node and disable inbound and outbound replication, or reset the failure counts being tracked for the associated alarms.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.
Steps

1. Select Grid.
2. Select Archive Node > ARC > Replication.
3. Click Configuration > Main.

4. Modify the following settings, as necessary:

   - Reset Inbound Replication Failure Count: Select to reset the counter for inbound replication failures. This can be used to clear the RIRF (Inbound Replications – Failed) alarm.
   - Reset Outbound Replication Failure Count: Select to reset the counter for outbound replication failures. This can be used to clear the RORF (Outbound Replications – Failed) alarm.
   - Disable Inbound Replication: Select to disable inbound replication as part of a maintenance or testing procedure. Leave cleared during normal operation. When inbound replication is disabled, object data can be retrieved from the ARC service for replication to other locations in the StorageGRID Webscale system, but objects cannot be replicated to this ARC service from other system locations. The ARC service is read-only.
   - Disable Outbound Replication: Select the checkbox to disable outbound replication (including content requests for HTTP retrievals) as part of a maintenance or testing procedure. Leave unchecked during normal operation. When outbound replication is disabled, object data can be copied to this ARC service to satisfy ILM rules, but object data cannot be retrieved from the ARC service to be copied to other locations in the StorageGRID Webscale system. The ARC service is write-only.

5. Click Apply Changes.

Configuring retrieve settings

You can configure the retrieve settings for an Archive Node to set the state to Online or Offline, or reset the failure counts being tracked for the associated alarms.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Grid**.

2. Select **Archive Node > ARC > Retrieve**.

3. Click **Configuration > Main**.

4. Modify the following settings, as necessary:

   - **Archive Retrieve State**: Set the component state to either:
     - **Online**: The grid node is available to retrieve object data from the archival media device.
     - **Offline**: The grid node is not available to retrieve object data.

   - **Reset Request Failure Count**: Select the checkbox to reset the counter for request failures. This can be used to clear the ARRF (Request Failures) alarm.

   - **Reset Verification Failure Count**: Select the checkbox to reset the counter for verification failures on retrieved object data. This can be used to clear the ARRV (Verification Failures) alarm.

5. Click **Apply Changes**.

**Configuring the archive store**

You can configure store settings for an Archive Node.

**About this task**

Store settings differ based on the configured target type for the Archive Node.

**Related tasks**

*Managing an Archive Node when TSM server reaches capacity* on page 132
Configuring the archive store for TSM middleware connection

If your Archive Node connects to a TSM middleware server, you can configure an Archive Node’s archive store state to Online or Offline. You can also disable the archive store when the Archive Node first starts up, or reset the failure count being tracked for the associated alarm.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select **Grid**.

2. Select **Archive Node > ARC > Store**.

3. Click **Configuration > Main**.

4. Modify the following settings, as necessary:

   • **Archive Store State**: Set the component state to either:
     - **Online**: The Archive Node is available to process object data for storage to the archival storage system.
     - **Offline**: The Archive Node is not available to process object data for storage to the archival storage system.

   • **Archive Store Disabled on Startup**: When selected, the Archive Store component remains in the Read-only state when restarted. Used to persistently disable storage to the targeted the archival storage system. Useful when the targeted the archival storage system is unable to accept content.

   • **Reset Store Failure Count**: Reset the counter for store failures. This can be used to clear the ARVF (Stores Failure) alarm.

5. Click **Apply Changes**.
Configuring store settings for S3 API connection

If your Archive Node connects to an archival storage system through the S3 API, you can reset the Store Failures count, which can be used to clear the ARVF (Store Failures) alarm.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Grid.

2. Select Archive Node > ARC > Store.

3. Click Configuration > Main.

4. Select Reset Store Failure Count.

5. Click Apply Changes.

   The Store Failures attribute resets to zero.

Set custom alarms for the Archive Node

You should establish custom alarms for the ARQL and ARRL attributes that are used to monitor the speed and efficiency of object data retrieval from the archival storage system by the Archive Node.

• ARQL: Average Queue Length. The average time, in microseconds, that object data is queued for retrieval from the archival storage system.

• ARRL: Average Request Latency. The average time, in microseconds, needed by the Archive Node to retrieve object data from the archival storage system.

The acceptable values for these attributes depend on how the archival storage system is configured and used. (Go to ARC > Retrieve > Overview > Main.) The values set for request timeouts and the number of sessions made available for retrieve requests are particularly influential.

After integration is complete, monitor the Archive Node's object data retrievals to establish values for normal retrieval times and queue lengths. Then, create custom alarms for ARQL and ARRL that will trigger if an abnormal operating condition arises.

Related tasks

Creating custom service or component alarms on page 50
What an Admin Node is

The Admin Node provides services for the web interface, system configuration, and audit logs. Each site in a StorageGRID Webscale deployment may include one Admin Node.

What the AMS service is

The Audit Management System (AMS) service tracks system activity and events.

What the CMN service is

The Configuration Management Node (CMN) service manages system-wide configurations of connectivity and protocol features needed by all services. In addition, the CMN service is used to run and monitor grid tasks. One Admin Node per StorageGRID Webscale hosts the CMN service and is known as the primary Admin Node. No other Admin Node hosts the CMN service. There is only one per StorageGRID Webscale deployment.

What the NMS service is

The Network Management System (NMS) service powers the monitoring, reporting, and configuration options that are displayed through the StorageGRID Webscale system's browser-based interface.

Related concepts

- Monitoring grid tasks on page 176

Related tasks

- Verifying an ILM policy on page 91
Admin Node redundancy

A StorageGRID Webscale system can include multiple Admin Nodes. This provides you with the redundancy of multiple IP addresses from which you can sign in to StorageGRID Webscale system and perform various monitoring and configuration procedures.

Having multiple Admin Nodes provides you with the capability to continuously monitor and configure your StorageGRID Webscale system in the event that an Admin Node fails. If an Admin Node becomes unavailable, web clients can reconnect to any other available Admin Node and continue to view and configure the system. Meanwhile, attribute processing continues, alarms are still triggered, and related notifications sent. However, multiple Admin Nodes does not provide failover protection except for notifications and AutoSupport messages. Alarm acknowledgments made from one Admin Node are not copied to other Admin Nodes.

Related concepts

Alarm acknowledgments on page 139

Alarm acknowledgments

Alarm acknowledgments made from one Admin Node are not copied to any other Admin Node. Because acknowledgments are not copied to other Admin Nodes, it is possible that the Grid Topology tree will not look the same for each Admin Node.

This difference can be useful when connecting web clients. Web clients can have different views of the StorageGRID Webscale system based on the administrator needs.
Note that notifications are sent from the Admin Node where the acknowledgment occurs.

**E-mail notifications and AutoSupport messages**

In a multi-site StorageGRID Webscale system, one Admin Node is configured as the preferred sender of notifications and AutoSupport messages. This preferred sender can be any Admin Node. All other Admin Nodes become “standby” senders.

Under normal system operations, only the preferred sender sends notifications and AutoSupport messages. The standby sender monitors the preferred sender and if it detects a problem, the standby sender switches to online status and assumes the task of sending notifications and AutoSupport messages.

**The preferred vs. standby sender**

There are two scenarios in which both the preferred sender and the standby sender can send notifications and AutoSupport messages:

- It is possible that while the StorageGRID Webscale system is running in this “switch-over” scenario, where the standby sender assumes the task of sending notifications and AutoSupport messages, the preferred sender will maintain the ability to send notifications and AutoSupport messages. If this occurs, duplicate notifications and AutoSupport messages are sent: one from the preferred sender and one from the standby sender. When the Admin Node configured as the standby sender no longer detects errors on the preferred sender, it switches to “standby” status and stops sending notifications and AutoSupport messages. Notifications and AutoSupport messages are once again sent only by the preferred sender.

- If the standby sender cannot detect the preferred sender, the standby sender switches to online and sends notifications and AutoSupport messages. In this scenario, the preferred sender and standby senders are “islanded” from each other. Each sender (Admin Node) can be operating and monitoring the system normally, but because the standby sender cannot detect the other Admin Node of the preferred sender, both the preferred sender and the standby sender send notifications and AutoSupport messages.

When sending a test e-mail, all NMS services send a test e-mail.

**Related concepts**

*About alarms and email notifications* on page 34

*What AutoSupport is* on page 60

**Related tasks**

*Selecting a preferred sender* on page 43

*Sending a test email* on page 41
To confirm that you have configured the email server connection correctly, you can send a test e-mail. When you send a test e-mail, a message is sent from all Admin Nodes. This includes a test email from the standby sender (if one is configured).

## Changing the name of an Admin Node

You can change the name of an Admin Node as it appears on the various browser-based interface pages. Creating a unique name for each Admin Node can be useful in differentiating Admin Nodes. This is particularly useful in identifying a preferred sender of e-mail notifications and AutoSupport messages.

### Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

### About this task

When you change the name of an Admin Node using the following procedure, the name is only changed as it appears in the browser-based interface. The name of an Admin Node is not changed in the Grid Topology tree.

**Note:** When the name of an Admin Node is changed using the following procedure, changes are lost whenever the provision command is run. For example, during expansion.

### Steps

1. Select **Configuration > Display Options**.
2. From the Display Options menu, select **NMS Names**.
3. In the NMS Names table, click **Edit** next to the name you want to change.
4. Under **Name**, type a new name for the Admin Node.
5. Click **Apply Changes**.

### Related concepts

- **NMS entities** on page 142
Related tasks

*Selecting a preferred sender* on page 43

**NMS entities**

NMS entities refer to elements of the Grid Topology tree that appear above the component level (the names of the StorageGRID Webscale deployment, locations, grid nodes, and services).

NMS entity settings determine:

- The name that appears in the Grid Topology tree and elsewhere in the NMS MSI

Names are allocated to each entity through Object IDs (OIDs) that are unique to each entity while being hierarchically organized. Each row in the NMS Entities table allocates a name to an entity OID. The combination of OID hierarchy and position in the table determines the sequence of appearance in the Grid Topology tree.

**Note:** Do not change these setting unless advised by technical support.

**Table 1: NMS entities**

<table>
<thead>
<tr>
<th>Scope</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>Identifies entity&lt;br&gt;Object IDs (OIDs) are unique to each entity while being hierarchically organized. The combination of OID hierarchy and position in the table determines the sequence of appearance in the Grid Topology tree.</td>
</tr>
<tr>
<td>Device Model ID</td>
<td>Four-letter code identifying the type of the entity&lt;br&gt;BGRP is used to identify entities that include groups of services, and BXXX is used to identify individual services (where XXX is the ADC, AMS, and so on.)&lt;br&gt;The Device Model ID of an entity determines which entities and components appear below it in the hierarchy.</td>
</tr>
<tr>
<td>Device Model Version</td>
<td>Version of the device model&lt;br&gt;Entities can have more than one possible configuration, depending upon the requirements of the StorageGRID Webscale deployment. The entity’s configuration is selected by entering the appropriate version of its device model. Versioning is updated at regular intervals by the CMN service.</td>
</tr>
<tr>
<td>Name</td>
<td>Describes item in browser-based interface&lt;br&gt;A label describing an item in the user interface.</td>
</tr>
<tr>
<td>Language</td>
<td>The language of the text of the Name&lt;br&gt;Matched with the language of the user’s account, and used to determine which value for Name appears.</td>
</tr>
</tbody>
</table>

To export these settings for future reference, use the Export button 📋.
Changing an NMS entity name

When changing the name of an NMS entity, changes are lost whenever the provision command is run (for example, during expansion).

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Configuration > Display Options.
2. From the Display Options menu, select Entities.
3. Click Edit next to the item you want to rename and type a new name.
   
   **Note:** Do not change any other setting unless advised by Support.

4. Click Apply Changes.

Because changes are lost whenever you run the provision command, you should export and save these changes for future reference. To export these settings for future reference, click Export.
Managing networking

Because the topology of your StorageGRID Webscale system is that of a group of interconnected servers, over time as your system changes and grows you may be required to perform various updates to the system's networking.

You can change the configuration of the grid, client, or admin networks, or you can add new client and admin networks. You can also update external NTP source IP addresses and DNS IP addresses at any time.

**Note:** To use the grid network editor to modify or add a network for a grid node, see the Maintenance Guide for VMware Deployments or the Maintenance Guide for OpenStack Deployments. For more information about network topology, see the Grid Primer.

Grid network

Required. The grid network is the communication link between grid nodes. All hosts on the grid network must be able to talk to all other hosts. This network is used for all internal StorageGRID Webscale system communications.

Client network

Optional. The Client network can communicate with any subnet reachable through the local gateway.

Admin network

Optional. The Admin network allows for restricted access to the StorageGRID Webscale system for maintenance and administration.

Guidelines

- A StorageGRID Webscale grid node requires a dedicated network interface, IP address, subnet mask, and gateway for each network it is assigned to.
- A grid node is not permitted to have more than one interface on a network.
- A single gateway, per network, per grid node is supported, and it has to be on the same subnet as the node. You can implement more complex routing in the gateway, if required.
- The network interfaces are mapped simply: eth0: Grid; eth1: Admin; eth2: Client
- For SGA, eth0: hic 2 and hic 4, eth1: the left hand 1GbE port; eth2: hic 1 and hic3
- The default route is generated automatically, per node. If eth2 is enabled, then 0.0.0.0/0 uses the Client network on eth2. If eth2 is not enabled, then 0.0.0.0/0 uses the Grid network on eth0.
- The client network does not become operational until the grid node has joined the grid
- The Admin network can be configured during VM deployment to allow access to the installation UI before the grid is fully installed.

Related information

StorageGRID Webscale 10.3 Maintenance Guide for VMware Deployments
StorageGRID Webscale 10.3 Maintenance Guide for OpenStack Deployments
StorageGRID Webscale 10.3 Grid Primer
Viewing IP addresses

You can view the IP address for each grid node that makes up your StorageGRID Webscale system. You can then use this IP address to log into the grid node at the command line and perform various maintenance procedures.

Before you begin

You must have signed in to the Grid Management Interface using a supported browser.

About this task

For information on changing IP addresses, see the Maintenance Guide for VMware Deployments or the Maintenance Guide for OpenStack Deployments.

Steps

1. Select Grid.
2. Select SSM > Resources.
3. From the Grid Options menu, click Overview.
   IP addresses are listed in the Network Addresses table.

Example

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>192.168.0.10</td>
</tr>
<tr>
<td>eth0</td>
<td>fe80::5679:fffe606:6127</td>
</tr>
</tbody>
</table>

For VM-based deployments, the IP address assigned to eth0 is always the grid node’s grid network IP address. For StorageGRID Webscale appliance-based deployments, the IP address assigned to hic2 and hic4 is always the grid node’s grid network IP address.

The Network Addresses table always displays link-local IPv6 addresses beginning with fe80::, which are automatically assigned by Linux.

Related information

StorageGRID Webscale 10.3 Maintenance Guide for VMware Deployments
StorageGRID Webscale 10.3 Maintenance Guide for OpenStack Deployments

Modifying the DNS configuration for a single grid node

Rather than configure Domain Name Service (DNS) globally for the entire deployment, you can configure DNS differently for each Admin Node or Archive Node. When DNS is enabled, you can use Fully Qualified Domain Name (FQDN) hostnames rather than IP addresses. This affects email notifications, AutoSupport, and server connectivity.

Steps

1. At the Admin Node or Archive Node, access a command shell and log in as root using the password listed in the Passwords.txt file.
2. Run the DNS setup script: `setup_resolv.rb`.
   The script responds with the list of supported commands.

   Tool to modify external name servers
   available commands:
   add search <domain>
   add a specified domain to search list
   e.g. > add search netapp.com
   remove search <domain>
   remove a specified domain from list
   e.g. > remove search netapp.com
   add nameserver <ip>
   add a specified IP address to the name server list
   e.g. > add nameserver 192.0.2.65
   remove nameserver <ip>
   remove a specified IP address from list
   e.g. > remove nameserver 192.0.2.65
   remove nameserver all
   remove all nameservers from list
   save
   write configuration to disk and quit
   abort
   quit without saving changes
   help
   display this help message

   Current list of name servers:
   192.0.2.64
   Name servers inherited from global DNS configuration:
   192.0.2.126
   192.0.2.127
   Current list of search entries:
   netapp.com

   Enter command [add search <domain>|remove search <domain>|add nameserver <ip>]
   [remove nameserver <ip>|remove nameserver all|save|abort|help]

3. Add the IP address of a server that provides domain name service for your network: `add nameserver IP_address`

4. Repeat the command to add name servers.

5. Follow instructions as prompted for other commands.

6. Save your changes and exit the application: `save`

7. Close the command shell on the server: `exit`

8. Repeat from step 1 for each grid node.

**Configure SNMP monitoring**

A Simple Network Management Protocol (SNMP) agent is installed with each grid node during the installation process. SNMP is used to monitor system status. StorageGRID Webscale’s SNMP agent sends StorageGRID Webscale system status through object identifier (OID) data values to a third party monitoring server.

The StorageGRID Webscale system provides a custom management information base (MIB) file that can be installed on the monitor server to translate OID data into a readable form displayed by the monitor.

The StorageGRID Webscale system supports version v2c of the SNMP protocol (SNMPv2c).
For information about how to install and configure a third-party monitor and have it receive SNMP status from the StorageGRID Webscale system, refer to documentation specific to the SNMP monitor employed.

Management Information Base file

A Management Information Base (MIB) file is needed by the monitor to translate SNMP data from the StorageGRID Webscale system into readable text.

Copy the StorageGRID Webscale MIB file (BYCAST-STORAGWRID-MIB.mib) to the monitor server.

The StorageGRID Webscale MIB file is available on the StorageGRID Webscale Software CD at: /mibs/BYCAST-STORAGEGRID-MIB.mib

Detailed registry

The following OID is displayed on third-party monitor servers. This OID reports the overall system status of the StorageGRID Webscale system.

<table>
<thead>
<tr>
<th>Element</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>1.3.6.1.4.1.28669.1.0.1.1.1</td>
</tr>
<tr>
<td>Hierarchy</td>
<td>iso.org.dod.internet.mgmt.private.enterprises.bycast.version1.common.nmsmi.system.status</td>
</tr>
<tr>
<td>Values</td>
<td>One of the following values is displayed: 1 = unknown 11 = adminDown 21 = normal 31 = notice 41 = minor 51 = major 61 = critical</td>
</tr>
<tr>
<td>The MIB contains this enumeration mapping. If the monitor uses SNMP GET, the textual value will appear instead of the numerical value.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Element</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>1.3.6.1.4.1.28669.1.0.1.1.2</td>
</tr>
<tr>
<td>Hierarchy</td>
<td>iso.org.dod.internet.mgmt.private.enterprises.bycast.version1.common.nmsmi.system.label</td>
</tr>
<tr>
<td>Values</td>
<td>Text string of the system label.</td>
</tr>
</tbody>
</table>

Link costs

Link costs refers to the relative costs of communicating between data center sites. Link costs are used to determine which grid nodes should provide a requested service.

For example, link cost information is used to determine which LDR services are used to retrieve objects. All else being equal, the service with the lowest link cost is preferred.
In the example shown below, if a client application at data center site two (DC2) retrieves an object that is stored both at data center site one (DC1) and at data center site three, the LDR service at DC1 is responsible for sending the object because the link cost from DC1 to DC2 is 0, which is lower than the link cost from the DC3 site to the DC2 site (25).

![Diagram of data center sites with link costs](image)

**Table 4: Example link costs**

<table>
<thead>
<tr>
<th>Link</th>
<th>Link cost</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Between physical data center sites</td>
<td>25 (default)</td>
<td>Usually a high-speed WAN link exists between sites.</td>
</tr>
<tr>
<td>Between logical data center sites</td>
<td>0</td>
<td>Logical data centers at the same physical site connected by a LAN.</td>
</tr>
</tbody>
</table>

**Updating link costs**

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Configuration > Link Cost**.
2. Select a site under **Link Source** and enter a cost value between 0 and 100 under **Link Destination**.

   You cannot change the link cost if the source is the same as the destination.

   To cancel changes, click **Revert**.

3. Click **Apply Changes**.

### Changing network transfer encryption

The StorageGRID Webscale system uses Transport Layer Security (TLS) to protect internal control traffic between grid nodes. The Network Transfer Encryption option sets the algorithm used by TLS to encrypt control traffic between grid nodes. This setting does not affect data encryption.

#### Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

#### About this task

By default, network transfer encryption uses the AES256-SHA algorithm. Control traffic can also be encrypted using the AES128-SHA algorithm.

#### Steps

1. Select **Configuration > Grid Options**.

2. From the Grid Options menu, select **Configuration**.
3. Change Network Transfer Encryption to **AES256-SHA** or **AES128-SHA**.

![Configure Grid Options](image)

4. Click **Apply Changes**.

**Configuring passwordless SSH access**

The primary Admin Node acts as an SSH access point for other grid nodes. This means that after you log in to the command shell of the primary Admin Node, you can access any other grid node through SSH without entering the grid node’s password.

**About this task**

You are only prompted to enter the SSH Access Password. Optionally, you can enable passwordless access to grid nodes by starting ssh-agent. In this case, you are only prompted for the SSH Access Password once.

To connect to a grid node through SSH, you can:

- From any grid node, use the remote server password.
- From the primary Admin Node, use the SSH private key password (SSH Access Password listed in the **Passwords.txt** file).
- From the primary Admin Node, without entering any password except the SSH Access Password once.

To enable passwordless SSH access to remote grid nodes, you need:

- The password for the SSH private key (SSH Access Password in the **Passwords.txt** file). By default the SSH access point is installed with a password.
- The SSH private key to be on the primary Admin Node. By default, the private key is located on the primary Admin Node. However, it might have been removed to prevent the Admin Node from acting as an SSH access point.
- The private key added to the SSH agent. This must be done each time you log in to the primary Admin Node at the command line.
Steps

1. At the primary Admin Node, access a command shell and log in as root using the password listed in the Passwords.txt file.

2. Add the SSH private key to the ssh agent to allow the primary Admin Node passwordless access to the StorageGRID Webscale system’s other grid nodes. Enter: `ssh-add`

   You need to add the ssh private key to the ssh agent each time you log in at the command line.

3. When prompted, enter the SSH Access Password listed in the Passwords.txt file or the one created in “Adding or changing the SSH private key password” on page 186.

   You can now access any grid node from the primary Admin Node through ssh without entering additional passwords.

4. When you no longer require passwordless access to other servers, remove the private key from the ssh agent. Enter: `ssh-add -D`

5. Log out of the primary Admin Node. Enter: `exit`

Configuring certificates

You can customize the certificates used by the StorageGRID Webscale system.

The StorageGRID Webscale system uses security certificates for two distinct purposes:

- Management Interface Server Certificates: Used to secure access to the Management Interface, which end-users access through their web browser, or the Management API.
- Storage API Server Certificates: Used to secure access to the Storage Nodes and API Gateway Nodes, which API client applications use to upload and download object data.

You can use the default certificates created during installation, or you can replace either, or both, of these default types of certificates with your own custom certificates.

Configuring custom server certificates for the grid management interface

You can replace the default grid management interface server certificates with custom certificates that allows users to access the grid management interface without encountering security warnings.

About this task

You need to complete configuration on the server, and depending on the root Certificate Authority (CA) you are using, users may also need to install a client certificate in the web browser they will use to access the grid management interface.

Steps

1. Select Configuration > Server Certificates.

2. In the Management Interface Server Certificate section, click Install Custom Certificate.

3. Upload the required server certificate files:

   - **Server Certificate**: The custom server certificate file (.crt).
   - **Server Certificate Private Key**: The custom server certificate private key file (.key).
   - **CA Bundle**: A single file containing the certificates from each intermediate issuing Certificate Authority (CA). The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.
4. Click Save.
   The custom server certificates are used for all subsequent new client connections.

5. Refresh the page to ensure the web browser is updated.

**Restoring the default server certificates for the grid management interface**

You can revert to using the default server certificates for the grid management interface.

**Steps**

1. Select Configuration > Server Certificates.

2. In the Manage Interface Server Certificate section, click Use Default Certificates.

3. Click OK in the confirmation dialog box.
   When you restore the default Management Interface server certificates, the custom server certificate files you configured are deleted and cannot be recovered from the system. The default server certificates are used for all subsequent new client connections.

4. Refresh the page to ensure the web browser is updated.

**Configuring custom server certificates for storage API endpoints**

You can replace the default object storage API service endpoint server certificates with a single custom server certificate that is specific to your organization.

**About this task**

API service endpoints on Storage Nodes are secured and identified by X.509 server certificates. By default, every Storage Node is issued a certificate signed by the grid CA. These CA signed certificates can be replaced by a single common custom server certificate and corresponding private key.

You need to complete configuration on the server, and depending on the root Certificate Authority (CA) you are using, users may also need to install a client certificate in the API client they will use to access the system.

**Steps**

1. Select Configuration > Server Certificates.

2. In the Object Storage API Service Endpoints Server Certificate section, click Install Custom Certificate.

3. Upload the required server certificate files:
   - **Server Certificate**: The custom server certificate file (.crt).
   - **Server Certificate Private Key**: The custom server certificate private key file (.key).
   - **CA Bundle**: A single file containing the certificates from each intermediate issuing Certificate Authority (CA). The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.

4. Click Save.
   The custom server certificates are used for all subsequent new API client connections.

5. Refresh the page to ensure the web browser is updated.
Restoring the default server certificates for storage API endpoints

You can revert to using the default server certificates for the storage API endpoints.

Steps

1. Select Configuration > Server Certificates.

2. In the Object Storage API Service Endpoints Server Certificate section, click Use Default Certificates.

3. Click OK in the confirmation dialog box.

   When you restore the default object storage API service endpoints server certificates, the custom server certificate files you configured are deleted and cannot be recovered from the system. The default server certificates are used for all subsequent new API client connections.

4. Refresh the page to ensure the web browser is updated.

Copying the StorageGRID Webscale system’s CA certificate

You can copy the StorageGRID Webscale system’s certificate authority (CA) certificate from the StorageGRID Webscale system for client applications that require server verification. If a custom server certificate has been configured, then client applications should verify the server using the root CA certificate that issues the custom server certificate, rather than copy the CA certificate from the StorageGRID Webscale system.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Configuration > Grid Options.

2. From the Grid Options menu, click Overview.

3. Under API Server Certificates, expand CA Certificate.

4. Select the CA certificate.

   Include the “-----BEGIN CERTIFICATE-----” and the “-----END CERTIFICATE-----” in your selection.
5. Right-click the selected certificate, and then select **Copy**.

6. Refresh the page to ensure the web browser is updated.
Configuring audit client access

The Admin Node, through the Audit Management System (AMS) service, logs all audited system events to a log file available through the audit share, which is added to each Admin Node at installation. For easy access to audit logs, you can configure client access to audit shares for both CIFS and NFS.

The StorageGRID Webscale system uses positive acknowledgment to prevent loss of audit messages before they are written to the log file or audit feed. A message remains queued at a service until the AMS service or an intermediate audit relay service has acknowledged control of it.

For information about audit messages, see the Audit Message Reference.

Related concepts

What an Admin Node is on page 138

Related information

StorageGRID Webscale 10.3 Audit Message Reference

Configuring audit clients for CIFS

The procedure used to configure an audit client depends on the authentication method: Windows Workgroup or Windows Active Directory (AD). When added, the audit share is automatically enabled as a read-only share.

Configuring audit clients for Workgroup

Perform this procedure for each Admin Node in a StorageGRID Webscale deployment from which you want to retrieve audit messages.

Before you begin

• You must have the Passwords.txt file with the root account passwords (available in the SAID package).
• You must have the Configuration.txt file (available in the SAID package).

Steps

1. At the Admin Node, access a command shell and log in as root using the password listed in the Passwords.txt file.
2. Confirm that all services have a state of Running or Verified: storagegrid-status
   If all services are not Running or Verified, resolve issues before continuing.
3. Return to the command line, press Ctrl+C.
4. Start the CIFS configuration utility: config_cifs.rb

<table>
<thead>
<tr>
<th>Shares</th>
<th>Authentication</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>add-audit-share</td>
<td>set-authentication</td>
<td>validate-config</td>
</tr>
<tr>
<td>enable-disable-share</td>
<td>set-netbios-name</td>
<td>help</td>
</tr>
<tr>
<td>add-user-to-share</td>
<td>join-domain</td>
<td>exit</td>
</tr>
</tbody>
</table>
5. Set the authentication for the Windows Workgroup:

   If authentication has already been set, an advisory message appears. If authentication has already been set, go to step 6.

   a. Enter: `set-authentication`

   b. When prompted for Windows Workgroup or Active Directory installation, enter: `workgroup`

   c. When prompted, enter a name of the Workgroup:

      `workgroup_name`

   d. When prompted, create a meaningful NetBIOS name:

      `workgroup_name`

      or

      Press Enter to use the Admin Node’s hostname as the NetBIOS name.

      The script restarts the Samba server and changes are applied. This should take less than one minute. After setting authentication, add an audit client.

   e. When prompted, press Enter.

      The CIFS configuration utility is displayed.

6. Add an audit client:

   a. Enter: `add-audit-share`

      **Note:** The share is automatically added as read-only.

   b. When prompted, add a user or group: `user`

   c. When prompted, enter the audit user name: `audit_user_name`

   d. When prompted, enter a password for the audit user: `password`

   e. When prompted, re-enter the same password to confirm it: `password`

   f. When prompted, press Enter.

      The CIFS configuration utility is displayed.

      **Note:** There is no need to enter a directory. The audit directory name is predefined.

7. If more than one user or group is permitted to access the audit share, add the additional users:

   a. Enter: `add-user-to-share`

      A numbered list of enabled shares is displayed.

   b. When prompted, enter the number of the audit-export share: `share_number`

   c. When prompted, add a user or group:

      `user`

      or

      `group`

   d. When prompted, enter the name of the audit user or group: `audit_user` or `audit_group`
e. When prompted, press Enter.
   The CIFS configuration utility is displayed.

f. Repeat step 9 for each additional user or group that has access to the audit share.

8. Optionally, verify your configuration: validate-config

   The services are checked and displayed. You can safely ignore the following messages:

   Can't find include file /etc/samba/includes/cifs-interfaces.inc
   Can't find include file /etc/samba/includes/cifs-filesystem.inc
   Can't find include file /etc/samba/includes/cifs-custom-config.inc
   Can't find include file /etc/samba/includes/cifs-shares.inc
   rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)

   **Note:** The setting ‘security=ads’ should NOT be combined with the ‘password server’ parameter (by default Samba will discover the correct DC to contact automatically).

a. When prompted, press Enter.
   The audit client configuration is displayed.

b. When prompted, press Enter.
   The CIFS configuration utility is displayed.

9. Close the CIFS configuration utility: exit

10. If the StorageGRID Webscale deployment is a single site, go to step 11.

    or

    Optionally, if the StorageGRID Webscale deployment includes Admin Nodes at other sites, enable these audit share as required:

a. Remotely log in to a site’s Admin Node: ssh Admin_Node_IP_address
   IP addresses are listed in the Configuration.txt file. If prompted for a password, find the required password in the Passwords.txt file.

b. Repeat steps 4 through 9 to configure the audit share for each additional Admin Node.

c. Close the remote secure shell login to the remote Admin Node: exit

11. Log out of the command shell: exit

### Configuring audit clients for Active Directory

**Before you begin**

- You must have the Passwords.txt file with the root account passwords (available in the SAID package).
- You must have the CIFS Active Directory username and password.
- You must have the Configuration.txt file (available in the SAID package).

**About this task**

Perform this procedure for each Admin Node in a StorageGRID Webscale deployment from which you want to retrieve audit messages.
Steps

1. At the Admin Node, access a command shell and log in as root using the password listed in the `Passwords.txt` file.

2. Confirm that all services have a state of Running or Verified: `storagegrid-status`
   
   If all services are not Running or Verified, resolve issues before continuing.

3. Return to the command line, press `Ctrl+C`.

4. Start the CIFS configuration utility: `config_cifs.rb`

   ┌───────────┬───────────────┬──────┐
   │ Shares    │ Authentication│ Config │
   │ add-audit-share │ set-authentication │ validate-config │
   │ enable-disable-share │ set-netbios-name │ help │
   │ add-user-to-share │ join-domain │ exit │
   │ remove-user-from-share │ add-password-server │ │
   │ modify-group │ add-wins-server │ │
   │                      │ remove-wins-server │ │
   └───────────┴───────────────┴──────┘

5. Set the authentication for Active Directory: `set-authentication`

   In most deployments, you must set the authentication before adding the audit client. If authentication has already been set, an advisory message appears. If authentication has already been set, go to step 6.

   a. When prompted for Workgroup or Active Directory installation: `ad`

   b. When prompted, enter the name of the AD domain (short domain name).

   c. When prompted, enter the domain controller’s IP address or DNS hostname.

   d. When prompted, enter the full domain realm name.
      Use uppercase letters.

   e. When prompted to enable winbind support: `y`
      Winbind is used to resolve user and group information from AD servers.

   f. When prompted, enter the NetBIOS name.

   g. When prompted, press `Enter`.
      The CIFS configuration utility is displayed.

6. Join the domain:

   a. If not already started, start the CIFS configuration utility: `config_cifs.rb`

   b. Join the domain: `join-domain`

   c. You are prompted to test if the Admin Node is currently a valid member of the domain. If this Admin Node has not previously joined the domain, enter: `no`

   d. When prompted, provide the Administrator’s username: `administrator_username`
      where `administrator_username` is the CIFS Active Directory username, not the StorageGRID Webscale username.

   e. When prompted, provide the Administrator’s password: `administrator_password`
were `administrator_password` is the CIFS Active Directory username, not the StorageGRID Webscale password.

f. When prompted, press **Enter**.
   The CIFS configuration utility is displayed.

7. Verify that you have correctly joined the domain:
   a. Join the domain: `join-domain`
   b. When prompted to test if the server is currently a valid member of the domain, enter: **y**
      If you receive the message “Join is OK,” you have successfully joined the domain. If you do not get this response, try setting authentication and joining the domain again.
   c. When prompted, press **Enter**.
      The CIFS configuration utility is displayed.

8. Add an audit client: `add-audit-share`
   a. When prompted to add a user or group, enter: **user**
   b. When prompted to enter the audit user name, enter the audit user name.
   c. When prompted, press **Enter**.
      The CIFS configuration utility is displayed.

9. If more than one user or group is permitted to access the audit share, add additional users: `add-user-to-share`
   A numbered list of enabled shares is displayed.
   a. Enter the number of the audit-export share.
   b. When prompted to add a user or group, enter: **group**
      You are prompted for the audit group name.
   c. When prompted for the audit group name, enter the name of the audit user group.
   d. When prompted, press **Enter**.
      The CIFS configuration utility is displayed.
   e. Repeat step 9 for each additional user or group that has access to the audit share.

10. Optionally, verify your configuration: `validate-config`
    The services are checked and displayed. You can safely ignore the following messages:
    • Can’t find include file `/etc/samba/includes/cifs-interfaces.inc`
    • Can’t find include file `/etc/samba/includes/cifs-filesystem.inc`
    • Can’t find include file `/etc/samba/includes/cifs-interfaces.inc`
    • Can’t find include file `/etc/samba/includes/cifs-custom-config.inc`
    • Can’t find include file `/etc/samba/includes/cifs-shares.inc`
    • `rlimit_max`: increasing `rlimit_max` (1024) to minimum Windows limit (16384)
    • WARNING: The setting ‘security=ads’ should NOT be combined with the ‘password server’ parameter. (by default Samba will discover the correct DC to contact automatically).
   a. When prompted, press **Enter** to display the audit client configuration.
b. When prompted, press **Enter**.
The CIFS configuration utility is displayed.

11. Close the CIFS configuration utility: **exit**

12. If the StorageGRID Webscale deployment is a single site, go to step 13.

or

Optionally, if the StorageGRID Webscale deployment includes Admin Nodes at other sites, enable these audit shares as required:

a. Remotely log in to a site’s Admin Node: `ssh Admin_Node_IP_address`
   IP addresses are listed in the `Configuration.txt` file. If prompted for a password, passwords are listed in the `Passwords.txt` file.

b. Repeat steps 4 through 11 to configure the audit shares for each Admin Node.

c. Close the remote secure shell login to the Admin Node: **exit**

13. Log out of the command shell: **exit**

### Adding a user or group to a CIFS audit share

**Before you begin**

- You must have the `Passwords.txt` file with the root account passwords (available in the SAID package).
- You must have the `Configuration.txt` file (available in the SAID package).

**About this task**
The following procedure is for an audit share integrated with AD authentication.

**Steps**

1. At the Admin Node, access a command shell and log in as root using the password listed in the `Passwords.txt` file.

2. Confirm that all services have a state of Running or Verified. Enter: `storagegrid-status`
   If all services are not Running or Verified, resolve issues before continuing.

3. Return to the command line, press **Ctrl+C**.

4. Start the CIFS configuration utility: **config_cifs.rb**

<table>
<thead>
<tr>
<th>Shares</th>
<th>Authentication</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>add-audit-share</td>
<td>set-authentication</td>
<td>validate-config</td>
</tr>
<tr>
<td>enable-disable-share</td>
<td>set-netbios-name</td>
<td>help</td>
</tr>
<tr>
<td>add-user-to-share</td>
<td>join-domain</td>
<td>exit</td>
</tr>
<tr>
<td>remove-user-from-share</td>
<td>add-password-server</td>
<td></td>
</tr>
<tr>
<td>modify-group</td>
<td>remove-password-server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>add-wins-server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>remove-wins-server</td>
<td></td>
</tr>
</tbody>
</table>

5. Start adding a user or group: **add-user-to-share**
   A numbered list of audit shares that have been configured is displayed.
6. When prompted, enter the number for the audit share (audit-export): \texttt{audit\_share\_number}
   You are asked if you would like to give a user or a group access to this audit share.

7. When prompted, add a user or group: \texttt{user} or \texttt{group}

8. When prompted for the user or group name for this AD audit share, enter the name.
   The user or group is added as read-only for the audit share both in the server’s operating system
   and in the CIFS service. The Samba configuration is reloaded to enable the user or group to
   access the audit client share.

9. When prompted, press \texttt{Enter}.
   The CIFS configuration utility is displayed.

10. Repeat steps 5 to 8 for each user or group that has access to the audit share.

11. Optionally, verify your configuration: \texttt{validate\_config}
    The services are checked and displayed. You can safely ignore the following messages:
    • Can't find include file \texttt{/etc/samba/includes/cifs-interfaces.inc}
    • Can't find include file \texttt{/etc/samba/includes/cifs-filesystem.inc}
    • Can't find include file \texttt{/etc/samba/includes/cifs-custom-config.inc}
    • Can't find include file \texttt{/etc/samba/includes/cifs-shares.inc}
    a. When prompted, press \texttt{Enter} to display the audit client configuration.
    b. When prompted, press \texttt{Enter}.

12. Close the CIFS configuration utility: \texttt{exit}

13. If the StorageGRID Webscale deployment is a single site, go to step 14.
    — or —
    Optionally, if the StorageGRID Webscale deployment includes Admin Nodes at other sites,
    enable these audit shares as required:
    a. Remotely log in to a site’s Admin Node: \texttt{ssh Admin\_Node\_IP\_address}
       IP addresses are listed in the Configuration.txt file. If prompted for a password,
       passwords are listed in the Passwords.txt file.
    b. Repeat steps 4 through 12 to configure the audit shares for each Admin Node.
    c. Close the remote secure shell login to the remote Admin Node: \texttt{exit}

14. Log out of the command shell: \texttt{exit}

\textbf{Removing a user or group from a CIFS audit share}

You cannot remove the last user or group permitted to access the audit share.

\textbf{Before you begin}

- You must have the Passwords.txt file with the root account passwords (available in the SAID
  package).
- You must have the Configuration.txt file (available in the SAID package).
Steps

1. At the Admin Node, access a command shell and log in as root using the password listed in the `Passwords.txt` file.

2. Start the CIFS configuration utility: `config_cifs.rb`

3. Start removing a user or group: `remove-user-from-share`
   
   A numbered list of available audit shares for the Admin Node is displayed. The audit share is labeled audit-export.

4. Enter the number of the audit share: `audit_share_number`

5. When prompted to remove a user or a group:

   - `user`
   - `group`

   A numbered list of users or groups for the audit share is displayed.

6. Enter the number corresponding to the user or group you want to remove: `number`

   The audit share is updated, and the user or group is no longer permitted access to the audit share. For example:

   ```
   Enabled shares
   1. audit-export
   Select the share to change: 1
   Remove user or group? [User/group]: User
   Valid users for this share
   1. audituser
   2. newaudituser
   Select the user to remove: 1
   Removed user "audituser" from share "audit-export".
   Press return to continue.
   ```

7. Close the CIFS configuration utility: `exit`

8. If the StorageGRID Webscale deployment includes Admin Nodes at other sites, disable the audit share at each site as required.

9. Log out of each command shell when configuration is complete: `exit`

Changing a CIFS audit share user or group name

Steps

1. Add a new user or group with the updated name to the audit share.
2. Delete the old user or group name.

Related tasks
- Adding a user or group to a CIFS audit share on page 160
- Removing a user or group from a CIFS audit share on page 161

Verifying CIFS audit integration
The audit share is read-only. Log files are intended to be read by computer applications and verification does not include opening a file. It is considered sufficient verification that the audit log files appear in a Windows Explorer window. Following connection verification, close all windows.

Configuring the audit client for NFS
The audit share is automatically enabled as a read-only share.

Before you begin
- You must have the Passwords.txt file with the root account passwords (available in the SAID package).
- You must have the Configuration.txt file (available in the SAID package).

About this task
Perform this procedure for each Admin Node in a StorageGRID Webscale deployment from which you want to retrieve audit messages.

Steps
1. At the Admin Node, access a command shell and log in as root using the password listed in the Passwords.txt file.

2. Confirm that all services have a state of Running or Verified. Enter: storagegrid-status
   If any services are not listed as Running or Verified, resolve issues before continuing.

3. Return to the command line, press Ctrl+C.

4. Start the NFS configuration utility. Enter: config_nfs.rb

<table>
<thead>
<tr>
<th>Shares</th>
<th>Clients</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>add-audit-share</td>
<td>add-ip-to-share</td>
<td>validate-config</td>
</tr>
<tr>
<td>enable-disable-share</td>
<td>remove-ip-from-share</td>
<td>refresh-config</td>
</tr>
<tr>
<td></td>
<td></td>
<td>help</td>
</tr>
<tr>
<td></td>
<td></td>
<td>exit</td>
</tr>
</tbody>
</table>

5. Add the audit client: add-audit-share
   a. When prompted, enter the audit client’s IP address or IP address range for the audit share: client_IP_address
      IP address ranges must be expressed using a subnet mask in CIDR notation (that is, in a form such as 192.168.110.0/24).
   b. When prompted, press Enter.
6. If more than one audit client is permitted to access the audit share, add the IP address of the additional user: `add-ip-to-share`
   a. Enter the number of the audit share: `audit_share_number`
   b. When prompted, enter the audit client’s IP address or IP Address range for the audit share: `client_IP_address`
      IP address ranges must be expressed using a subnet mask in CIDR notation (that is, in a form such as 192.168.110.0/24).
   c. When prompted, press `Enter`.
      The NFS configuration utility is displayed.
   d. Repeat step 6 for each additional audit client that has access to the audit share.

7. Optionally, verify your configuration: `validate-config`
   The services are checked and displayed.
   a. When prompted, press `Enter`.
      The NFS configuration utility is displayed.

8. Close the NFS configuration utility: `exit`

9. If the StorageGRID Webscale deployment is a single site, go to step 10.
   — or —
   Optionally, if the StorageGRID Webscale deployment includes Admin Nodes at other sites, enables these audit shares as required:
   a. Remotely log in to a site’s Admin Node: `ssh Admin_Node_IP_address`
      IP addresses are listed in the `Configuration.txt` file. If prompted for a password, passwords are listed in the `Passwords.txt` file.
   b. Repeat steps 4 through 8 to configure the audit shares for each additional Admin Node.
   c. Close the remote secure shell login to the remote Admin Node. Enter: `exit`

10. Log out of the command shell: `exit`
    
    NFS audit clients are granted access to an audit share based on their IP address. Grant access to the audit share to a new NFS audit client by adding its IP address to the share, or remove an existing audit client by removing its IP address.

### Adding an NFS audit client to an audit share

NFS audit clients are granted access to an audit share based on their IP address. Grant access to the audit share to a new NFS audit client by adding its IP address to the audit share.

**Before you begin**

- You must have the `Passwords.txt` file with the root account passwords (available in the SAID package).
- You must have the `Configuration.txt` file (available in the SAID package).

**Steps**

1. At the Admin Node, access a command shell and log in as root using the password listed in the `Passwords.txt` file.
2. Start the NFS configuration utility: `config_nfs.rb`
3. Enter: **add-ip-to-share**

   A list of NFS audit shares enabled on the Admin Node is displayed. The audit share is listed as: `/var/local/audit/export`

4. Enter the number of the audit share: **audit_share_number**

5. When prompted, enter the audit client’s IP address or IP Address range for the audit share: **client_IP_address**

   IP address ranges must be expressed using a subnet mask in CIDR notation (form such as 192.168.110.0/24).

   The audit client is added to the audit share.

6. When prompted, press **Enter**.

   The NFS configuration utility is displayed.

7. Repeat from step 3 for each audit client that should be added to the audit share.

8. Optionally, verify your configuration: **validate-config**

   The services are checked and displayed.

   a. When prompted, press **Enter**.

      The NFS configuration utility is displayed.

9. Close the NFS configuration utility: **exit**

10. If the StorageGRID Webscale deployment is a single site, go to step 11.

    — or —

    Optionally, if the StorageGRID Webscale deployment includes Admin Nodes at other sites, enable these audit shares as required:

    a. Remotely log in to a site’s Admin Node: **ssh Admin_Node_IP_address**

       IP addresses are listed in the `Configuration.txt` file. If prompted for a password, find the required password in the `Passwords.txt` file.

    b. Repeat steps 2 through 9 to configure the audit shares for each Admin Node.

    c. Close the remote secure shell login to the remote Admin Node: **exit**

11. Log out of the command shell: **exit**
Verifying NFS audit integration

After you configure an audit share and add an NFS audit client, you can mount the audit client share and verify that the files are available from the audit share.

Steps

1. Verify connectivity (or variant for the client system) using the client-side IP address of the Admin Node hosting the AMS service. Enter: `ping IP_address`
   Verify that the server responds, indicating connectivity.

2. Mount the audit read-only share using a command appropriate to the client operating system. A sample Linux command is (enter on one line):
   ```bash
   mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export myAudit
   ```
   Use the IP address of the Admin Node hosting the AMS service and the predefined share name for the audit system. The mount point can be any name selected by the client (for example, `myAudit` in the previous command).

3. Verify that the files are available from the audit share. Enter: `ls myAudit /*`
   where `myAudit` is the mount point of the audit share. There should be at least one log file listed.

Removing an NFS audit client from the audit share

NFS audit clients are granted access to an audit share based on their IP address. You can remove an existing audit client by removing its IP address.

Before you begin

- You must have the `Passwords.txt` file with the root account passwords (available in the SAID package).
- You must have the `Configuration.txt` file (available in the SAID package).

About this task

You cannot remove the last IP address permitted to access the audit share.

Steps

1. From the service laptop, log in to the primary Admin Node as root using the password listed in the `Passwords.txt` file.

2. Start the NFS configuration utility: `config_nfs.rb`

<table>
<thead>
<tr>
<th>Shares</th>
<th>Clients</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>add-audit-share</td>
<td>add-ip-to-share</td>
<td>validate-config</td>
</tr>
<tr>
<td>enable-disable-share</td>
<td>remove-ip-from-share</td>
<td>refresh-config</td>
</tr>
<tr>
<td></td>
<td></td>
<td>help</td>
</tr>
<tr>
<td></td>
<td></td>
<td>exit</td>
</tr>
</tbody>
</table>

3. Remove the IP address from the audit share: `remove-ip-from-share`
   A numbered list of audit shares configured on the server is displayed. The audit share is listed as: `/var/local/audit/export`
4. Enter the number corresponding to the audit share: `audit_share_number`

A numbered list of IP addresses permitted to access the audit share is displayed.

5. Enter the number corresponding to the IP address you want to remove.

The audit share is updated, and access is no longer permitted from any audit client with this IP address.


The NFS configuration utility is displayed.

7. Close the NFS configuration utility: `exit`

8. If your StorageGRID Webscale deployment is a multiple data center site deployment with additional Admin Nodes at the other sites, disable these audit shares as required:

   a. Remotely log in to each site’s Admin Node:

      ```
      ssh Admin_Node_IP_address
      ```

      IP addresses are listed in the `Configuration.txt` file. If prompted for a password, find the required password in the `Passwords.txt` file.

   b. Repeat steps 2 through 7 to configure the audit shares for each additional Admin Node.

   c. Close the remote secure shell login to the remote Admin Node: `exit`

9. Log out of the command shell: `exit`

**Changing the IP address of an NFS audit client**

**Steps**

1. Add a new IP address to an existing NFS audit share.

2. Remove the original IP address.

**Related tasks**

- *Adding an NFS audit client to an audit share* on page 164
- *Removing an NFS audit client from the audit share* on page 166
Controlling system access with administration user accounts and groups

By managing administration user accounts and administration groups, you can control access to the StorageGRID Webscale system. Each administration group account is assigned permissions that control access to StorageGRID Webscale features and functionality. You then add administration users to one or more administration group accounts to control individual user access.

You can perform the following tasks related to users and groups:

- Create, edit, clone, and remove local and federated groups.
- Create, edit, clone, and remove local users.
- Edit local users’ passwords.

Additionally, local users can edit their own passwords.

Some accounts are managed by the identity source, for example, the LDAP server. For details, see information about user accounts, identity federation, and LDAP.

About administration user groups

Administration user groups govern user access to specific features of the StorageGRID Webscale system. You can add administration users to one or more administration groups. Creating groups with specific access permissions promotes efficient account maintenance.

Permissions

To log in, users must have been assigned at least one permission. All users who have the ability to log in can perform the following tasks:

- Monitor grid topology
- Monitor alarms
- Change their own password

You can assign the following permissions to a group:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Access</td>
<td>Provides access to all grid administration features.</td>
</tr>
<tr>
<td>Acknowledge Alarms</td>
<td>Provides access to acknowledge and respond to alarms. All users have the ability to monitor alarms. If you want a user to monitor grid topology and acknowledge alarms only, you should assign this permission.</td>
</tr>
<tr>
<td>Grid Topology Page Configuration</td>
<td>Provides access to the Configuration tabs in Grid Topology.</td>
</tr>
<tr>
<td>Permission</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Provides access to maintenance options, such as the following. If you do not have this permission, you do not see the following options in the menu:</td>
</tr>
<tr>
<td></td>
<td>• Software upgrade</td>
</tr>
<tr>
<td></td>
<td>• Grid expansion</td>
</tr>
<tr>
<td></td>
<td>• Grid decommission</td>
</tr>
<tr>
<td></td>
<td>• Recovery package creation</td>
</tr>
<tr>
<td></td>
<td>• Recovery</td>
</tr>
<tr>
<td></td>
<td>Provides access to these additional options. If you do not have this permission, you see the options in the menu and the pages; however, you cannot make changes in these pages:</td>
</tr>
<tr>
<td></td>
<td>• DNS Servers</td>
</tr>
<tr>
<td></td>
<td>• NTP Servers</td>
</tr>
<tr>
<td></td>
<td>• License update</td>
</tr>
<tr>
<td>Other Grid Configuration</td>
<td>Provides access to the all other grid configuration options, such as:</td>
</tr>
<tr>
<td></td>
<td>• Configuration &gt; System Settings &gt; Domain Names, Grid Options, Link Cost Groups, Storage Options, Display Options, CDMI</td>
</tr>
<tr>
<td></td>
<td>• Configuration &gt; Monitoring &gt; Global Alarms, Notifications, Email Setup, AutoSupport, Audit, Events</td>
</tr>
<tr>
<td></td>
<td>• Configuration &gt; Access Control &gt; Admin Users, Admin Groups, Identity Federation</td>
</tr>
<tr>
<td></td>
<td>Access to these items also requires Grid Topology Page Configuration permissions.</td>
</tr>
<tr>
<td>Tenant Accounts</td>
<td>Provides access to the Tenant Accounts page from the Tenants option so that you can add, edit, or remove tenant accounts and manage their group policies. If you do not have this permission, you do not see the Tenants option in the menu.</td>
</tr>
</tbody>
</table>

**About admin user accounts**

You can manage admin user accounts in the StorageGRID Webscale system and also add them to one or more admin groups that govern access to system features. The StorageGRID Webscale system includes one predefined local user, named “root”.

**Note:** If you upgraded from a previous version of StorageGRID Webscale you will also retain the built-in “Vendor” and “Admin” accounts. The best practice is to switch from using the “Vendor” account to the “root” account.

StorageGRID Webscale includes local and federated users:
• Local users: You can add admin user accounts that are local to StorageGRID Webscale system and add these users to StorageGRID Webscale local admin groups.

• Federated users: An external identity source, such as LDAP federation, can be used to enable users belonging to configured LDAP groups to acquire access credentials for tenant accounts. The LDAP server manages the LDAP groups to which users belong, so you cannot add federated users to StorageGRID Webscale federated groups. Also, you cannot edit federated user information; federated user information is automatically synchronized with the external identity source, such as the LDAP server.

Although you can add and delete users, you cannot delete the root user. After creating groups, you assign users to one or more groups.

Creating admin groups

You can create admin groups to manage the security permissions for a group of admin user accounts.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Configuration > Admin Groups.

2. Click Add.

3. Select either Local or Federated as the type of group.

4. For local groups, enter the group's name that will appear to users, for example, “Development US”.

5. Enter a unique name without spaces for the group, for example, “Dev_US”.

6. Select a set of permissions.

7. Click Save.

A new group is created and added to the list of group names available for user accounts. User accounts can now be associated with the new group.
Modifying an admin groups account

You can modify an admin groups account to update the display name or permissions associated with the group.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Configuration > Admin Groups.
2. Select the name of the group and click Edit.
3. For local groups, enter the group's name that will appear to users, for example, “Development US”.
   You cannot change the unique name, which is the internal group name.
4. Select a set of permissions.
5. Click Save.

Deleting an admin groups account

You can delete an admin group when you want to remove the group from the system, and remove all permissions associated with the group, which removes any admin user accounts from the group. Deleting an admin group account does not delete the admin user accounts.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

When you delete a group, users assigned to that group will lose all access privileges to the StorageGRID Webscale system, unless they are granted privileges by a different group.

Steps

1. Select Configuration > Admin Groups.
2. Select the name of the group.
3. Click Remove.
4. Click OK.
Creating an admin users account

You can create a new local user and assign the user to a defined admin group with permissions that govern access to system features. If an admin group with the necessary permission settings does not exist, you must first create an admin groups account.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

You can create only local users. Federated user details are automatically synchronized with the external identity source, for example, the LDAP server.

Steps

1. Select Configuration > Admin Users.
2. Click Create.
   The list of group names is generated from the Groups table.
3. Enter the user's display name, unique name, and password.
4. Assign the user to one or more groups that govern the access permissions.
5. Click Save.
   New settings are applied the next time you sign out and then sign back in to the StorageGRID Webscale system.

Related tasks

Creating admin groups on page 170

Modifying an admin users account

You can modify a local admin users account to update the full display name or group membership that governs access to system features. You can also temporarily prevent the user from accessing the system.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.
• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

You can edit only local users. Federated user details are automatically synchronized with the external identity source, for example, the LDAP server.
Steps

1. Select **Configuration > Admin Users**.
2. Select the user account you want to edit.
3. Click **Edit**.
4. Make changes to the name or group membership.
5. To prevent the user from accessing the system temporarily, check **Deny Access**.
6. Click **Save**.

   The new settings are applied the next time the user signs out and then signs back in to the StorageGRID Webscale system.

Deleting an admin users account

You can delete accounts for local users that no longer require access to the StorageGRID Webscale system.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Configuration > Admin Users**.
2. Select the user account you want to delete.
   
   **Note:** You cannot delete StorageGRID Webscale system’s built-in root user.
3. Click **Remove**.
4. Click **OK** to confirm the deletion.

Changing local users' passwords

While local users can change their own passwords using the **Change Password** option in the StorageGRID Webscale header, you can change passwords of all local users.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

You can change passwords only for local users; you cannot change passwords for federated users. They must change their passwords in the external identity source, for example, LDAP, that originally provided the information to StorageGRID Webscale.
Steps

1. Select Configuration > Admin Users.
2. From the Users page, select a user and click Change Password.
3. Enter and confirm the password and click Save.
What grid tasks are

Grid tasks are scripts that implement specific changes to the StorageGRID Webscale system.

Most grid tasks are automatically generated when the provisioning process is run as part of maintenance and expansion procedures. Some grid tasks must be manually started and monitored, but most are run automatically at the appropriate time. For example, decommissioning a Storage Node causes the StorageGRID Webscale system to automatically generate and run the Storage Node Decommissioning grid task. For some Storage Node recovery procedures, you must start and monitor the grid tasks manually.

Running grid tasks

When performing procedures that generate grid tasks that you must run manually, you must ensure that you run the grid tasks in the correct order.

Each grid task’s description includes a revision number. No grid task should be run before all grid tasks from previous revisions have completed or been aborted.

Along with running grid tasks in the correct order, plan the execution of grid tasks based on the fact that most grid tasks cannot be run concurrently. This restriction occurs because most grid tasks require exclusive access to the same system resources. There are, however, a number of grid tasks that can be run concurrently. Information about which grid tasks can be run concurrently is listed with each procedure.

- System performance
  System-wide tasks are prioritized lower than normal system operations (such as processing retrieval requests from client applications). However, because running system-wide tasks puts additional load on the StorageGRID Webscale system, they can impact overall system performance during peak load. Moreover, if several system-wide tasks are in progress, they compete for resources, delaying the completion of individual tasks.

  If either of these situations occur, go to the Grid > primary Admin Node > CMN > Grid Tasks > Overview > Main page to identify which grid tasks are in progress, and which are closest to completion. You can pause grid tasks to reduce the overall load on the StorageGRID Webscale system or to allow other grid tasks to complete sooner.

- Resource locking
  When a grid task is started, it might require temporary sole access to specific system resources to complete successfully. When this occurs, the grid task locks the resources that it requires, which might block other grid tasks from using the same resource. This might result in the temporary blocking of other grid tasks that are running concurrently. When the grid task finishes with the system resource, it unlocks it, allowing other grid tasks to access the system resource and run to completion.

Related concepts

Monitoring grid tasks on page 176

Frequently used grid tasks

There are several grid tasks that are most frequently generated that you will encounter as you work through maintenance or expansion procedures.

The following table lists the most frequently used grid tasks:
<table>
<thead>
<tr>
<th>Code</th>
<th>Grid task name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BDLI</td>
<td>Bundle Import</td>
<td>Used when a configuration bundle needs to be updated, usually as one step of a larger maintenance procedure.</td>
</tr>
<tr>
<td>CCLE</td>
<td>Clean Up Unused Cassandra Keys</td>
<td>Used during the expansion procedure when adding Storage Nodes.</td>
</tr>
<tr>
<td>GDCM</td>
<td>Gateway Node Decommissioning</td>
<td>Used during the decommissioning of an API Gateway Node.</td>
</tr>
<tr>
<td>GEXP</td>
<td>Grid Expansion: Initial — or — Grid Expansion: Add Server</td>
<td>Used during the expansion procedure when adding grid nodes.</td>
</tr>
<tr>
<td>ILME</td>
<td>ILM Evaluation (Volume Lost) — or — ILM Re-evaluation (User Triggered)</td>
<td>Used to reapply the ILM policy to content.</td>
</tr>
<tr>
<td>LDCM</td>
<td>Storage Node Decommissioning</td>
<td>Moves all content off the specified Storage Node to other Storage Nodes and then permanently removes the selected Storage Node from the StorageGRID Webscale system.</td>
</tr>
<tr>
<td>VFGV</td>
<td>LDR Foreground Verification</td>
<td>Verifies the existence of replicated object data on a Storage Node.</td>
</tr>
</tbody>
</table>

**Monitoring grid tasks**

You can monitor the progress of grid tasks to verify that a system configuration step is complete; for example, as part of a maintenance or expansion procedure.

You can view the status of grid tasks on the Grid > **primary Admin Node** > CMN > Grid Tasks > Overview > Main page.
Grid tasks go through three phases:

- **Pending**: The grid task has been submitted, but not started yet.
- **Active**: The grid task has been started.
  - It can be either actively running or temporarily paused. If a grid task's status changes to Error, it will continuously retry until it is able to complete successfully or is aborted.
  - A common reason for a grid task to enter an error state is if a grid node becomes unavailable (lost connection or crash) or another grid task is running. For grid tasks stuck with a Status of Error, when the issue is resolved, the grid task automatically starts running again.
- **Historical**: A grid task that has been submitted, but is no longer active.
  - This includes grid tasks that completed successfully, were canceled, aborted, or that have failed.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task ID</td>
<td>Unique identifier assigned when the task is created.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the grid task’s purpose.</td>
</tr>
<tr>
<td></td>
<td>A description can include a revision number, which is used to determine</td>
</tr>
<tr>
<td></td>
<td>the order in which grid tasks have been created and must be run. You</td>
</tr>
<tr>
<td></td>
<td>should always run the earliest generated grid task first.</td>
</tr>
<tr>
<td>Valid From</td>
<td>Date from which the grid task is valid and can be run.</td>
</tr>
<tr>
<td></td>
<td>The grid task fails if it is submitted before this date.</td>
</tr>
<tr>
<td>Valid To</td>
<td>Date until which the grid task is valid and can be run.</td>
</tr>
<tr>
<td></td>
<td>The grid task fails if it is submitted after this date.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Date and time when the grid task was started.</td>
</tr>
<tr>
<td>Duration</td>
<td>Amount of time since the grid task was started.</td>
</tr>
<tr>
<td>Stage</td>
<td>Description of the current stage of the active grid task.</td>
</tr>
<tr>
<td>% Complete</td>
<td>Progress indicator for the current stage of the active grid task.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Status</td>
<td>Current status of the active or historical grid task. For active grid tasks, one of:</td>
</tr>
<tr>
<td></td>
<td>• Starting</td>
</tr>
<tr>
<td></td>
<td>• Running</td>
</tr>
<tr>
<td></td>
<td>• Pausing</td>
</tr>
<tr>
<td></td>
<td>• Paused (either paused by the user or automatically paused by the grid task)</td>
</tr>
<tr>
<td></td>
<td>• Error: An error has been encountered. User action might be required. Grid task retries until successful or aborted.</td>
</tr>
<tr>
<td></td>
<td>• Aborting</td>
</tr>
<tr>
<td></td>
<td>• Abort Paused: Grid task failed to be aborted and is paused in error.</td>
</tr>
<tr>
<td></td>
<td>• Retrying</td>
</tr>
<tr>
<td></td>
<td>For historical grid tasks, one of:</td>
</tr>
<tr>
<td></td>
<td>• Successful</td>
</tr>
<tr>
<td></td>
<td>• Rollback Failed</td>
</tr>
<tr>
<td></td>
<td>• Expired</td>
</tr>
<tr>
<td></td>
<td>• Aborted</td>
</tr>
<tr>
<td></td>
<td>• Canceled</td>
</tr>
<tr>
<td></td>
<td>• Unauthorized</td>
</tr>
<tr>
<td></td>
<td>• Duplicate</td>
</tr>
<tr>
<td></td>
<td>• Invalid</td>
</tr>
<tr>
<td>Message</td>
<td>Information about the last stage of the active grid task.</td>
</tr>
<tr>
<td>Completion time</td>
<td>The date and time on which the grid task completed (or was canceled, expired, or was aborted).</td>
</tr>
</tbody>
</table>

**Charting a grid task**

You can chart the progress of an active grid task—particularly a grid task that takes a long time to complete—at primary Admin Node > CMN > Grid Tasks > Reports > Charts. This enables you to track a grid task’s progress and determine if the grid task is stalled.
Running a grid task

You must run grid tasks to update the StorageGRID Webscale system, as a step in some maintenance procedures.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

About this task

Under normal circumstances, grid tasks required for maintenance procedures appear automatically in the Pending table as part of the provisioning process.

If the Pending table includes grid tasks from multiple provisioning revisions, you must run grid tasks from the earliest revision (lowest revision number) first. If there is an active grid task currently listed with a status of Error, do not run any other grid tasks until either the problem is resolved and the grid task begins running again or the grid task is aborted.

Steps

1. Select Grid.

2. Select **primary Admin Node** > CMN > Grid Tasks.

3. Click **Configuration** > **Main**.

4. Under Actions, select **Start** for the grid task you want to run.

   **Note:** If there is an error after starting and the grid task updates to a status of Error, the grid task continuously retries until it completes successfully or is aborted.

5. Click **Apply Changes**.

   The grid task moves from the Pending table to the Active table. You must wait for the page to refresh before the change is visible. Do not submit the change again. The grid task continues to execute until it completes, is paused, or is aborted. When the grid task completes successfully, it moves to the Historical table with a Status of Successful. If the grid task fails, it might be for one of several reasons.

   **Note:** Configuration does not update automatically. To monitor the progress of a grid task, go to the Overview page and then, if necessary, back to the Configuration page to make changes.

Related concepts

*Troubleshooting grid tasks* on page 182
Pausing an active grid task

You can pause an active grid task before it finishes, to improve system performance. Pausing a grid task might be necessary if the StorageGRID Webscale system becomes particularly busy and you need to free resources used by the grid task operation.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Grid.
2. Select primary Admin Node > CMN > Grid Tasks.
3. Click Configuration > Main.
4. Under Actions, select Pause for the Active grid task you want to suspend temporarily.
5. Click Apply Changes.

The grid task remains on the Active table with its Status changed to Paused. This can be seen by returning to primary Admin Node > CMN > Grid Tasks > Overview > Main.

Resuming a paused grid task

You can resume a paused grid task when conditions permit.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Grid.
2. Select primary Admin Node > CMN > Grid Tasks.
3. Click Configuration > Main.
4. Under Actions, select Run for the Active grid task you want to resume.
5. Click Apply Changes.
Cancelling a grid task

You can cancel a grid task from the Pending table so that it is no longer available for execution.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**Steps**

1. Select **Grid**.
2. Select **primary Admin Node > CMN > Grid Tasks**.
3. Click **Configuration > Main**.
4. Under Actions, select **Cancel** for the Pending grid task that you want to cancel.
5. Click **Apply Changes**.

The grid task remains on the Active table, with its status changed to Active. You can confirm this by returning to **primary Admin Node > CMN > Grid Tasks > Overview > Main**.

Aborting a grid task

You can abort a grid task from the Active table so that it is no longer available for execution.

**Before you begin**

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

**About this task**

Not all grid tasks can be aborted. To determine whether a grid task can be aborted, follow the guidelines in the procedures where the grid task is discussed.

Aborting an active grid task causes it to leave affected entities in a reliable state. This might require you to roll back some actions or reset device states. The result is that the grid task can remain on the Active table with a status of Aborting for an extended period of time. When the programmed abort process is complete, the grid task moves to the Historical table.

**Steps**

1. Select **Grid**.
2. Select **primary Admin Node > CMN > Grid Tasks**.
3. Click **Configuration > Main**.
4. Under Actions, select **Pause** for the Active grid task you want to abort.
5. Click Apply Changes.
   When the page refreshes, the status of the grid task changes to Paused.

6. Under Actions, select Abort.

7. Click Apply Changes.
   The grid task remains on the Active table with its status changed to Active. You can confirm this
   by returning to primary Admin Node > CMN > Grid Tasks > Overview > Main.

After you finish
You can run an aborted grid task again by resubmitting it with a Task Signed Text Block.

Related tasks
- Submitting a Task Signed Text Block on page 184
  If the grid task you need to run is not in the Pending table (for example, it has been aborted),
  you can manually load the grid task by submitting the Task Signed Text Block.

Removing grid tasks from the Historical table
You can manually remove grid tasks listed in the Historical table.

Before you begin
- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about
  controlling system access with administration user accounts and groups.

Steps
1. Select Grid.

2. Select primary Admin Node > CMN > Grid Tasks.

3. Click Configuration > Main.

4. Select the Remove check box for the grid task.

5. Click Apply Changes.
   The grid task remains on the Active table with its status changed to Active. You can confirm this
   by returning to primary Admin Node > CMN > Grid Tasks > Overview > Main.

Troubleshooting grid tasks

Choices
- Grid task fails to complete and moves to Historical table on page 183
  In some cases, you might observe that a grid task moves to the Historical table without completing
  successfully.

- Troubleshooting grid task retries on page 183
  You might observe that a grid task does not complete successfully, but that the StorageGRID
  Webscale system retries running the grid task multiple times. You should identify and solve this
  issue to conserve system resources.
• **Grid task error management** on page 184
  If a grid task status changes to Error, the grid task retries until it is successful or aborted. Do not run any other grid tasks until the grid task with a status of Error completes successfully or is aborted.

• **Aborting grid tasks** on page 184
  If a grid task you are aborting enters an Internal Error state, you should attempt to abort the grid task again. If the grid task is still unable to complete the abort sequence, you should contact technical support.

• **Submitting a Task Signed Text Block** on page 184
  If the grid task you need to run is not in the Pending table (for example, it has been aborted), you can manually load the grid task by submitting the Task Signed Text Block.

**Grid task fails to complete and moves to Historical table**

In some cases, you might observe that a grid task moves to the Historical table without completing successfully.

If a grid task fails to finish successfully, it moves to the Historical table with one of the following statuses:

• Aborted: The grid task was aborted.
• Canceled: The grid task was canceled.
• Duplicate: The grid task has been previously loaded into the CMN service.
• Expired: The “task valid before” time has already passed.
• Invalid: The grid task was not valid.
• Rollback Failed: The grid task did not complete normally and failed to be aborted.
• Unauthorized: The grid task signature did not pass verification.

The most common reason for a grid task failure is that it has expired. If a grid task expires, it can never be run. A new grid task must be created and run. If there are multiple versions of the same grid task, you should always run the earliest generated (lowest revision number) grid task first.

Note that a grid task failure is not the same as a grid task error. The status of a grid task that encounters an error updates to Error and then Retrying as it attempts to finish. In this case, the grid task does not fail and move to the Historical table unless it is aborted.

**Troubleshooting grid task retries**

You might observe that a grid task does not complete successfully, but that the StorageGRID Webscale system retries running the grid task multiple times. You should identify and solve this issue to conserve system resources.

**Steps**

1. Pause and then restart the grid task.
2. Check the StorageGRID Webscale system for connectivity issues.
3. Restart the CMN service.
4. Abort the grid task, remove it from the Historical table, and then resubmit it.
5. Contact technical support.
Grid task error management

If a grid task status changes to Error, the grid task retries until it is successful or aborted. Do not run any other grid tasks until the grid task with a status of Error completes successfully or is aborted.

At the same time that the grid task enters the error state, a Grid Task Status alarm (SCAS) is triggered.

For information about the error, go to Grid > primary Admin Node > CMN > Grid Tasks > Overview > Main and look up the grid task message. This message displays information about the error (for example, `check failed on node 12130011`). After you have investigated and corrected the problem, if the grid task has not been aborted, it moves out of the error state and continues to a successful completion. If the grid task is aborted, it must be resubmitted.

Related tasks

*Submitting a Task Signed Text Block* on page 184

If the grid task you need to run is not in the Pending table (for example, it has been aborted), you can manually load the grid task by submitting the Task Signed Text Block.

Aborting grid tasks

If a grid task you are aborting enters an Internal Error state, you should attempt to abort the grid task again. If the grid task is still unable to complete the abort sequence, you should contact technical support.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Select Grid.
2. Select primary Admin Node > CMN > Grid Tasks.
3. Click Configuration > Main.
4. Under Actions, select Abort.

Submitting a Task Signed Text Block

If the grid task you need to run is not in the Pending table (for example, it has been aborted), you can manually load the grid task by submitting the Task Signed Text Block.

Before you begin

- You must have signed in to the Grid Management Interface using a supported browser.
- To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

Steps

1. Retrieve the grid task from the Grid_Tasks folder of the SAID package.
2. Copy the Task Signed Text Block file to the same computer that you will use to access the StorageGRID Webscale system.

3. Open the file that contains the grid task (Task Signed Text Block) using a text editor.

4. Copy the Task Signed Text Block to the clipboard:
   a. Select the text, including the opening and closing delimiters:

   ```plaintext
   -----BEGIN TASK-----
   AAAAAH1RTSUJDT05UAAANB1RCTEtjbmN0AAAM+1RCTEtDT05UAAAA
   EFRWVRVJSTMyAAAAAQAAABBUU0lEVUkzMoEecsEAAAAYVFNSQ0NTV
   ... 
   s5zJz1795J3x7TWeqBAInHDVEMKg95O95VJUW5kQj5SRjtoWLAYX
   -----END TASK-----
   ```

   If the Task Signed Text Block has a readable description above the opening delimiter, it can be included but is ignored by the StorageGRID Webscale system.

   b. Copy the selected text.

5. Select Grid.

6. Click Configuration > Main.

7. Under Submit New Task, paste the Task Signed Text Block.

8. Click Apply Changes.

   The StorageGRID Webscale system validates the Task Signed Text Block and either rejects the grid task or adds it to the table of pending grid tasks.
What data migration is

You can migrate large amounts of data to the StorageGRID Webscale system while simultaneously using the StorageGRID Webscale system for day to day operations.

The following section is a guide to understanding and planning such a data migration into the StorageGRID Webscale system. It is not a general guide to data migration, nor is it a detailed step by step procedure for executing such a migration. Instead, it provides you with the information required to plan and carry-out your data migration. Following the guidelines and instructions in this section ensures that data is migrated efficiently into the StorageGRID Webscale system without interfering with its day to day operations, and that once ingested, migrated data is handled appropriately by the StorageGRID Webscale system.

Confirm capacity of the StorageGRID Webscale system

Before migrating large amounts of data into the StorageGRID Webscale system, confirm that the StorageGRID Webscale system has the disk capacity to handle the anticipated volume.

If the StorageGRID Webscale system includes an Archive Node and a copy of migrated objects are saved to nearline storage (such as tape), ensure that the Archive Node’s storage has sufficient capacity for the anticipated volume of migrated data.

As part of the capacity assessment, assess the data profile of the objects that you plan to migrate and calculate the amount of disk capacity required. For information about monitoring the disk capacity of your StorageGRID Webscale system, see the Grid Primer.

Determine the ILM policy for migrated data

The StorageGRID Webscale system’s ILM policy determines how many copies are made, the locations to which copies are stored, and for how long these copies are retained. An ILM policy consists of a set of ILM rules that describe how to filter objects and manage object data over time.

Depending on how migrated data is used and your requirements for migrated data, you might want to define unique ILM rules for migrated data that are different from the ILM rules used for day to day operations. For example, if there are different regulatory requirements for day to day data management than there are for the data that is included in the migration, you might want a different number of copies of the migrated data on a different grade of storage.

You can configure rules that apply exclusively to migrated data if it is possible to uniquely distinguish between migrated data and object data saved from day to day operations.

If you can reliably distinguish between the types of data using one of the metadata criteria, you can use this criteria to define an ILM rule that applies only to migrated data.

Before beginning data migration, ensure that you understand the StorageGRID Webscale system’s ILM policy, how it will apply to migrated data, and that you have made and tested any changes to the ILM policy.

Warning: An ILM policy that has been incorrectly specified can cause unrecoverable data loss. Carefully review all changes you make to an ILM policy before activating it to make sure the policy will work as intended.

Related concepts

How ILM rules filter objects on page 73
Impact of migration on operations

A StorageGRID Webscale system is designed to provide efficient operation for object storage and retrieval, and to provide excellent protection against data loss through the seamless creation of redundant copies of object data and metadata.

However, data migration must be carefully managed according to the instructions in this chapter to avoid having an impact on day to day system operations, or, in extreme cases, placing data at risk of loss in case of a failure in the StorageGRID Webscale system.

Migration of large quantities of data places additional load on the system. When the StorageGRID Webscale system is heavily loaded, it responds more slowly to requests to store and retrieve objects. This can interfere with store and retrieve requests which are integral to day to day operations. Migration can also cause other operational issues. For example, when a Storage Node is nearing capacity, the heavy intermittent load due to batch ingest can cause the Storage Node to cycle between read-only and read-write, generating notifications.

If the heavy loading persists, queues can develop for various operations that the StorageGRID Webscale system must perform to ensure full redundancy of object data and metadata.

Data migration must be carefully managed according to the guidelines in this document to ensure safe and efficient operation of the StorageGRID Webscale system during migration. You must use either batch ingest or throttled continuous ingest, and continuously monitor the StorageGRID Webscale system during data migration to ensure that various attribute values are not exceeded. Controlling the rate of migration of data into the system is outside of the scope of StorageGRID Webscale software functionality.

Related tasks

- Performing a batch ingest on page 188
- Performing throttled continuous ingest on page 189

Scheduling data migration

Avoid migrating data during core operational hours. Limit data migration to evenings, weekends, and other times when system usage is low.

If possible, do not schedule data migration during periods of high activity. However, if it is not practical to completely avoid the high activity period, it is safe to proceed as long as you closely monitor the relevant attributes and take action if they exceed acceptable values.

Related concepts

- Monitoring data migration on page 187

Monitoring data migration

Data migration must be monitored and adjusted as necessary to ensure a good balance between reliable and responsive daily system operations and the best possible data migration rate.

This table lists information about the attributes that you must monitor during data migration, and the issues that they represent.
Table 5: Attributes to monitor during data migration

<table>
<thead>
<tr>
<th>Monitor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard - Information Lifecycle Management (ILM)</td>
<td>Monitor the number of objects listed to be evaluated in the next 24 hours and beyond 24 hours. If an IQSZ (Number of Objects) alarm is triggered, a dangerous queue of objects that have yet to be evaluated against the active ILM policy has formed. Objects in this queue are in danger of loss as they have yet to be copied and stored according to the ILM policy’s ILM rules. Control this object queue by throttle the ingest rate of objects.</td>
</tr>
<tr>
<td>Targeted archival system's storage capacity</td>
<td>If the ILM policy saves a copy of the migrated data to a targeted archival storage system (tape or the cloud), monitor the capacity of the targeted archival storage system to ensure that there is sufficient capacity for the migrated data.</td>
</tr>
<tr>
<td>Archive Node &gt; ARC &gt; Store &gt; Store Failures (ARVF)</td>
<td>If an alarm for this attribute is triggered, the targeted archival storage system might have reached capacity. Check the targeted archival storage system and resolve any issues that triggered an alarm.</td>
</tr>
</tbody>
</table>

Related tasks
- Performing a batch ingest on page 188
- Performing throttled continuous ingest on page 189

Performing a batch ingest

Batch ingest is when you periodically save a large batch of data to the StorageGRID Webscale system through a client application (S3, Swift, or CDMI). The StorageGRID Webscale system does not throttle data ingest or otherwise control how data arrives, but processes each batch at its maximum possible rate.

About this task
Because of the load batch ingests put on the StorageGRID Webscale system, perform this procedure outside of core operational hours and, if performing multiple batch ingests, wait until each batch ingest completes before starting the next. Because of the large queues of data that need to be processed before an operational request can be satisfied, performing a batch ingest during operational hours will interfere with the normal ingest and retrieval of data after each batch.

Warning: Do not perform a batch ingest simultaneously with day to day operations of the StorageGRID Webscale system. Perform this procedure outside of core operational hours.

Steps
1. Ingest multiple objects.
2. Monitor key attributes:
   - Configure custom notifications for migration alarms, so that you are alerted if any of the attributes exceed their acceptable levels.
   - Ensure attributes remain at acceptable values and alarm levels do not exceed the maximum levels.
   Attributes with a maximum acceptable alarm level of Minor have an acceptable attribute level chosen to provide an operational “window” for migration. For these attributes, if a Minor level
alarm is triggered, migration can continue as long as the attribute stays below the maximum value.

3. If an attribute value or alarm level exceeds minimum acceptable levels:
   • Suspend migration.
   • Wait until numerical attribute values decline to near zero (and other attributes return to an acceptable value), and all alarms are cleared.
   • Reduce the size of the next batch.

4. If attribute values remain in range and no alarms are triggered:
   • Wait until the StorageGRID Webscale system finishes ingesting a batch and returns to a “quiet” state. That is, numerical attribute values decrease to near zero, and all alarms are cleared.

5. Ingest the next batch of data.
   If necessary, adjust the size of the batch based on the StorageGRID Webscale system’s behavior when storing the previous batch.

6. After all migration data is transferred to the StorageGRID Webscale system, remember to:
   • Disable any custom notifications you created for the migration process in step 2.

Related tasks

Creating custom notifications for migration alarms on page 190

Performing throttled continuous ingest

If you have a way to throttle the rate at which data is saved to the StorageGRID Webscale system, you can migrate data through continuous ingest.

About this task

You can use continuous ingest, for example, if you:

• Have a data migration tool.
• Can configure the client application to throttle its copy rate.
• Have a method that permits you to limit the bandwidth consumed by migration data.

Throttling the rate that data is saved to the StorageGRID Webscale system is not a feature of StorageGRID Webscale software: to use throttled continuous ingest you must have an independent way to control the rate that data is sent to StorageGRID Webscale system.

Depending on the daily ingest load, it might also be possible to migrate data at a low rate during normal operational hours if it is possible to do so without exceeding the threshold levels that indicate that migration is consuming too many system resources.

Steps

1. Configure your data migration tool to save data continuously to the StorageGRID Webscale system at a low, controlled rate.
2. Monitor the value of the key attributes:
   • Configure custom notifications for migration alarms, so that you are alerted if any of the attributes exceed their acceptable levels.
• Ensure that attributes remain at acceptable values and alarm levels do not exceed the maximum levels.

Attributes with a maximum acceptable alarm level of Notice have an acceptable attribute value chosen to provide an operational “window” for migration. For these attributes, if a Notice level alarm is triggered migration can continue as long as the attribute stays below the maximum value.

• Ensure that attribute values remain relatively constant and do not gradually increase over time.

3. If the attribute values remain stable and well below the values, you can adjust the data migration rate up slightly.

Monitor the StorageGRID Webscale system closely to ensure that the new data migration rate is sustainable.

4. If the attribute values and alarm levels exceed minimal acceptable levels or numerical attribute values increase over time:

• Suspend data migration until the values and alarm levels return to acceptable levels.

• Lower the rate at which data is being saved to the StorageGRID Webscale system.

• Resume migration.

5. After all migration data is transferred to the StorageGRID Webscale system, remember to:

• Disable any custom notifications you created for the migration process in step 2.

Related tasks

Creating custom notifications for migration alarms on page 190

Creating custom notifications for migration alarms

You might want to configure the StorageGRID Webscale system to send a notification e-mail to the system administrator responsible for monitoring migration if the attribute values exceed their recommended maximum values.

Before you begin

• You must have signed in to the Grid Management Interface using a supported browser.

• To perform this task, you need specific access permissions. For details, see information about controlling system access with administration user accounts and groups.

• You must have configured email settings.

Steps

1. Create an e-mail list that includes all administrators responsible for monitoring the data migration.

   Optionally, you can create a template to customize the subject line, header, and footer of data migration notification e-mails.

2. Create a Global Custom alarm for each attribute you need to monitor during data migration:

   a. Select Configuration > Global Alarms.

   b. Under Default Alarms, search for the default alarms for the first attribute. Under Filter by, select Attribute Code, then type the four letter code for the attribute. For example, ARVF.
c. Click the submit icon.

d. In the results list, click the copy icon next to the alarm you want to modify. The alarm moves to the Global Custom Alarms table.

e. Under Global Custom Alarms, in the Mailing List column for the copied attribute, add the mailing list you created in step 3.

f. Repeat for each remaining attribute.

g. When finished creating Global Custom alarms, click Apply Changes.

After you finish

Administrators responsible for monitoring data migration now receive an e-mail notification if the values of key attributes exceed their maximum acceptable levels during migration.

Remember to disable these notifications after data migration is complete. Note that global custom alarms override default alarms. If there are any, enable custom alarms at the grid node level as global custom alarms cannot be triggered.

Related tasks

*Configuring email server settings* on page 36

The EMail Server page allows you to configure SMTP mail server settings that enable the sending of alarm notifications and AutoSupport messages. The StorageGRID Webscale system only sends email; it cannot receive email.

*Creating mailing lists* on page 39

You can create mailing lists for notifications. A mailing list enables you to send one e-mail message to multiple e-mail addresses. These mailing lists are used to send notifications when an alarm is triggered or when a service state changes. You must create a mailing list before you can send notifications. To send a notification to a single recipient, create a mailing list with one e-mail address.
What Server Manager is

The Server Manager application runs on every grid node, supervising the starting and stopping of services, and ensuring services gracefully join and leave the StorageGRID Webscale system. Server Manager also monitors every grid node’s services and automatically attempts to restart any that report faults.

During system start-up, Server Manager is automatically started by the operating system (OS), executing a sequential series of scripts to verify that support services are running, and starting them as needed. The start-up and shut-down sequences are reversed, ensuring that dependent services are in place as needed, and are not removed prematurely.

Server Manager provides the following capabilities:

- Stopping and starting of services to:
  - Restart services that have gone offline
  - Bring up the services after a reconfiguration
- Monitoring of services on an ongoing basis and restarting them as needed.
- Automatically starting of services if a server is power cycled or reset, and to recover from unintentional restarts.
- Detection of OS shutdown and gracefully closing of services.
- Restarting a grid node (bring down everything, including the OS, and rebooting the machine from the BIOS up).
- Shutting down a grid node to the point where it must be manually restarted. This enables you to safely power down a server for hardware maintenance.

Server Manager command shell procedures

You access Server Manager through the command line of any grid node.

Always remember to log out after you are finished with Server Manager, which is accomplished by closing the current command shell session. Enter: exit

Viewing Server Manager status and version

For each grid node, you can view the current status and version of Server Manager running on that grid node. You can also obtain the current status of all services running on that grid node.

Before you begin

You must have the Passwords.txt file.

Steps

1. At the grid node, access a command shell and log in as root using the password in the Passwords.txt file.
2. View the current status of Server Manager running on a grid node: /etc/init.d/servermanager status
The current status of Server Manager running on the grid node is reported (running or not). If Server Manager’s status is running, the time it has been running since last it was started is listed. For example,

servermanager running for 1d, 13h, 0m, 30s

This status is the equivalent of the status shown in the header of the local console display.

3. View the current version of Server Manager running on a grid node: /etc/init.d/servermanager version

The current version of Server Manager running on the grid node is reported. For example,

10.3.0-20160125.2055.fe1efd1

This information can be useful when updating the StorageGRID Webscale system.

4. Log out of the command shell: exit

**Viewing current status of all services**

You can view the current status of all services running on a grid node at any time.

**Before you begin**

You must have the `Passwords.txt` file.

**Steps**

1. At the grid node, access a command shell and log in as root using the password in the `Passwords.txt` file.

2. View a continuously updated report of status for all services running on the grid node: `storagegrid-status`

The current status of all service running on the grid node is reported (running or not). For example,

<table>
<thead>
<tr>
<th>Host Name</th>
<th>DC1-ADM1-104-80</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.0.2.64</td>
</tr>
<tr>
<td>Operating System Kernel</td>
<td>3.16.0</td>
</tr>
<tr>
<td>Operating System Environment</td>
<td>Debian 8.2</td>
</tr>
<tr>
<td>StorageGRID Webscale Release</td>
<td>10.3.0</td>
</tr>
<tr>
<td>Networking</td>
<td>Verified</td>
</tr>
<tr>
<td>Storage Subsystem</td>
<td>Verified</td>
</tr>
<tr>
<td>Database Engine</td>
<td>5.5.46</td>
</tr>
<tr>
<td>Time Synchronization</td>
<td>1:4.2.6.p5+dfsg Running</td>
</tr>
<tr>
<td>Network Monitoring</td>
<td>10.3.0 Running</td>
</tr>
<tr>
<td>ams</td>
<td>10.3.0</td>
</tr>
<tr>
<td>cmm</td>
<td>10.3.0</td>
</tr>
<tr>
<td>nms</td>
<td>10.3.0</td>
</tr>
<tr>
<td>ssm</td>
<td>10.3.0</td>
</tr>
<tr>
<td>mi</td>
<td>10.3.0</td>
</tr>
<tr>
<td>tomcat</td>
<td>5.5.35.5 Running</td>
</tr>
<tr>
<td>mgmt api</td>
<td>10.3.0 Running</td>
</tr>
<tr>
<td>attrDownPurge</td>
<td>10.3.0 Running</td>
</tr>
<tr>
<td>attrDownSamp1</td>
<td>10.3.0 Running</td>
</tr>
<tr>
<td>attrDownSamp2</td>
<td>10.3.0 Running</td>
</tr>
</tbody>
</table>

If the status of a service changes, the report is immediately updated to reflect the change in status.

3. Return to the command line, press Ctrl+C.
4. View a static report of status for all services running on the grid node: `/usr/local/servermanager/reader.rb`

The current status of all services running on the grid node is reported (running or not). For example,

<table>
<thead>
<tr>
<th>Host Name</th>
<th>DC1-ADM1-104-80</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.0.2.64</td>
</tr>
<tr>
<td>Operating System Kernel</td>
<td>3.16.0</td>
</tr>
<tr>
<td>Operating System Environment</td>
<td>Debian 8.2</td>
</tr>
<tr>
<td>StorageGRID Webscale Release</td>
<td>10.3.0</td>
</tr>
<tr>
<td>Networking</td>
<td>Verified</td>
</tr>
<tr>
<td>Storage Subsystem</td>
<td>Verified</td>
</tr>
<tr>
<td>Database Engine</td>
<td>5.5.46</td>
</tr>
<tr>
<td>Time Synchronization</td>
<td>1:4.2.6.p5+dfsg</td>
</tr>
<tr>
<td>Network Monitoring</td>
<td>10.3.0</td>
</tr>
<tr>
<td>ams</td>
<td>10.3.0</td>
</tr>
<tr>
<td>cmn</td>
<td>10.3.0</td>
</tr>
<tr>
<td>nms</td>
<td>10.3.0</td>
</tr>
<tr>
<td>ssm</td>
<td>10.3.0</td>
</tr>
<tr>
<td>mi</td>
<td>10.3.0</td>
</tr>
<tr>
<td>tomcat</td>
<td>5.5.35.5</td>
</tr>
<tr>
<td>mgmt api</td>
<td>10.3.0</td>
</tr>
<tr>
<td>attrDownPurge</td>
<td>10.3.0</td>
</tr>
<tr>
<td>attrDownSamp1</td>
<td>10.3.0</td>
</tr>
<tr>
<td>attrDownSamp2</td>
<td>10.3.0</td>
</tr>
</tbody>
</table>

If the status of a service changes, the report does not update to reflect the change in status.

5. Log out of the command shell: `exit`

Starting Server Manager and all services

There may be times when you might have to start Server Manager, which also starts all services on the grid node.

Before you begin

You must have the `Passwords.txt` file.

About this task

Starting Server Manager on a grid node where it is already running, results in a restart of Server Manager and all services on the grid node.

Steps

1. At the grid node, access a command shell and log in as root using the password in the `Passwords.txt` file.

2. Start Server Manager: `/etc/init.d/servermanager start`

3. Log out of the command shell: `exit`

Restarting Server Manager and all services

You might need to restart server manager and all services running on a grid node.

Before you begin

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

1. At the grid node, access a command shell and log in as root using the password in the
   `Passwords.txt` file.
2. Restart Server Manager and all services on the grid node: `/etc/init.d/servermanager
   restart`
   Server Manager and all services on the grid node are stopped and then restarted.
   **Note:** Using the `restart` command is the same as using the `stop` command followed by the
   `start` command.
3. Log out of the command shell: `exit`

**Stopping Server Manager and all services**

Server Manager is intended to run at all times, but there might be a time when you need to stop
Server Manager and all services running on a grid node.

**Before you begin**

You must have the `Passwords.txt` file.

**About this task**

The only scenario that requires you to stop Server Manager while keeping the operating system
running is when you need to integrate Server Manager to other services. If there is a requirement to
stop the Server Manager for servicing of the hardware or reconfiguration of the server, the entire
server should be halted.

Steps

1. At the grid node, access a command shell and log in as root using the password in the
   `Passwords.txt` file.
2. Stop Server manager and all services running on the grid node: `/etc/init.d/servermanager
   stop`
   Server Manager and all services running on the grid node are gracefully terminated.
3. Log out of the command shell: `exit`

**Viewing current status of a service**

You can view the current status of a services running on a grid node at any time.

**Before you begin**

You must have the `Passwords.txt` file.

Steps

1. At the grid node, access a command shell and log in as root using the password in the
   `Passwords.txt` file.
2. View the current status of a service running on a grid node: `/etc/init.d/service status`
   The current status of the requested service running on the grid node is reported (running or not).
   For example,
Stopping a service

Some maintenance procedures require you to stop a single service while keeping other services on the grid node running. Only stop individual services when directed to do so by a maintenance procedure.

Before you begin

You must have the `Passwords.txt` file.

About this task

When a service is “administratively stopped” in this way, Server Manager does not automatically restart the service. You must either restart the single service manually or restart Server Manager.

Steps

1. At the grid node, access a command shell and log in as root using the password in the `Passwords.txt` file.

2. Stop an individual service:
   
   `/etc/init.d/service stop`
   
   For example,
   
   `/etc/init.d/ldr stop`

   **Note:** If the service fails to stop after 30 minutes, perform a manual termination of the service.

3. Log out of the command shell: `exit`

Related tasks

*Forcing a service to terminate* on page 196

Forcing a service to terminate

Occasionally, a service will not stop after you have run the `stop` command (`/etc/init.d/service stop`). This failure to stop can be the result of an unusual software state or other unexpected condition within the system.

Before you begin

You must have the `Passwords.txt` file.

Steps

1. At the grid node, access a command shell and log in as root using the password in the `Passwords.txt` file.

2. Manually force a service to terminate: `sv -w time force-stop service`
   
   where `time` is the number of seconds to wait before executing the command. For example,
   
   `sv -w30 force-stop ldr`
The system waits 30 seconds before terminating the ldr service.

3. Log out of the command shell: `exit`

**Restarting a service**

Some maintenance procedures require you to stop a single service while keeping other services on the grid node running. After you have completed tasks that required you to stop a service, restart that service.

**Before you begin**

You must have the `Passwords.txt` file.

**Steps**

1. At the grid node, access a command shell and log in as root using the password in the `Passwords.txt` file.
2. Restart a manually stopped service: `/etc/init.d/service start`
   
   For example,
   
   `/etc/init.d/ldr start`

3. Restart a running service: `/etc/init.d/service restart`

4. Log out of the command shell: `exit`

**Rebooting a grid node**

When you reboot a grid node, all services are started automatically.

**Before you begin**

You must have the `Passwords.txt` file.

**Steps**

1. At the grid node, access a command shell and log in as root using the password in the `Passwords.txt` file.

2. Optionally, stop services: `/etc/init.d/servermanager stop`

   This is an optional, but recommended step.

3. Reboot the grid node: `reboot`

   If a `reboot` command is directly issued to the system, you might not be able log in to the system remotely to monitor the shutdown process. Services can take some time to shut down.

4. Log out of the command shell: `exit`

**Powering down servers**

Before you power down a server, stop services on all grid nodes hosted by that server.

**Steps**

1. At the grid node, access a command shell and log in as root using the password in the `Passwords.txt` file.
2. Stop services:
   /etc/init.d/servermanager stop

3. Repeat steps 1 and 2 for each grid node hosted on the server to be shut down.

4. Shutdown the server: shutdown -h now

5. Log out of the command shell: exit

**Using a DoNotStart file**

When performing various maintenance or configuration procedures, you might want to use an interlock DoNotStart file to prevent services from starting when Server Manager is started or restarted.

To prevent a service from starting, place a DoNotStart file in the directory of the service you want to prevent from starting. At start-up, Server Manager looks for the DoNotStart file. If the file is present, the service (and any services dependent upon it) is prevented from starting. When the DoNotStart file is removed, the previously stopped service will start on the next start or restart of Server Manager. Services are not automatically started when the DoNotStart file is removed.

The most efficient way to prevent all services from restarting is to prevent the NTP service from starting. All services are dependent on the NTP service and cannot run if the NTP service is not running.

**Adding a DoNotStart file for a service**

You can prevent an individual service from starting by adding a DoNotStart file to that service's directory on a grid node.

**Before you begin**

You must have the Passwords.txt file.

**Steps**

1. At the grid node, access a command shell and log in as root using the password in the Passwords.txt file.

2. Add a DoNotStart file:
   touch /etc/sv/service/DoNotStart
   
   where service is the name of the service to be prevented from starting. For example,
   
   touch /etc/sv/ldr/DoNotStart

   A DoNotStart file is created. No file content is needed.

   When Server Manager or the grid node is restarted, Server Manager restarts, but the service does not.

3. Log out of the command shell: exit

**Removing a DoNotStart file for a service**

When you remove a DoNotStart file that is preventing a service from starting, you must start that service.

**Before you begin**

You must have the Passwords.txt file.
Steps
1. At the grid node, access a command shell and log in as root using the password in the
   `Passwords.txt` file.
2. Remove the DoNotStart file from the service directory: `rm /etc/sv/service/DoNotStart`
   where `service` is the name of the service. For example,
   ```
   rm /etc/sv/ldr/DoNotStart
   ```
3. Start the service: `/etc/init.d/service start`
   where `service` is the name of the service.
4. Log out of the command shell: `exit`

Troubleshooting Server Manager
There are several tasks you can follow to help determine the source of Server Manager related
problems.

Accessing the Server Manager log file
If a problem arises when using Server Manager, check its log file.

Error messages related to Server Manager are captured in the Server Manager log file, which is
located at: `/var/local/log/servermanager.log`
Check this file for error messages regarding failures. Escalate the issue to technical support if
required. You might be asked to forward log files to technical support.

Service fails to start
While running normally, Server Manager is constantly monitoring services. If a service fails, Server
Manager attempts to restart it. If there are three failed attempts to start a service within five minutes,
the service goes down and Server Manager does not attempt another restart.

Before you begin
You must have the `Passwords.txt` file.

About this task
The following procedure can be used if Server Manager fails to start a service or appears to halt
execution for an extended period (more than ten minutes).

Steps
1. At the grid node, access a command shell and log in as root using the password in the
   `Passwords.txt` file.
2. Determine the status of a service: `/etc/init.d/service status`
   For example,
   ```
   /etc/init.d/ldr status
   ```
   Status information is displayed. For example,
nms running for 2h, 59m, 29s

A status of disabled indicates the presence of a DoNotStart file.

3. If status is disabled, check for the service directory for a DoNotStart file: /etc/sv/service/DoNotStart

4. If the DoNotStart file is present:
   a. Delete the file: rm /etc/sv/service/DoNotStart exit
   b. Start the service: /etc/init.d/service start

5. Log out of the command shell: exit

Service with an error state

If you detect that a service has entered an error state, attempt to restart the service.

Before you begin

You must have the Passwords.txt file.

About this task

Server Manager monitors services and restarts any that have stopped unexpectedly. If a service fails, Server Manager attempts to restart it. If there are three failed attempts to start a service within five minutes, the service goes down, fails to start, and enters an error state. Server Manager does not attempt another restart.

Steps

1. At the grid node, access a command shell and log in as root using the password in the Passwords.txt file.

2. Confirm error state of a service: /etc/init.d/service status

   For example,

   /etc/init.d/ldr status

   If the service is in an error state, the following message is returned:
   service in error state

   For example,

   ldr in error state

3. Attempt to remove the error state by restarting the service: /etc/init.d/service restart

   If the service fails to restart contact support.

4. Log out of the command shell: exit
Integrating Tivoli Storage Manager

This section includes best practices and set-up information for integrating an Archive Node with a Tivoli Storage Manager (TSM) server, including Archive Node operational details that impact the configuration of the TSM server.

Archive Node configuration and operation

Your StorageGRID Webscale system manages the Archive Node as a location where objects are stored indefinitely and are always accessible.

When an object is ingested, copies are made to all required locations, including Archive Nodes, based on the Information Lifecycle Management (ILM) rules defined for your StorageGRID Webscale system. The Archive Node acts as a client to a TSM server, and the TSM client libraries are installed on the Archive Node by the StorageGRID Webscale software installation process. Object data directed to the Archive Node for storage is saved directly to the TSM server as it is received. The Archive Node does not stage object data before saving it to the TSM server, nor does it perform object aggregation. However, the Archive Node can submit multiple copies to the TSM server in a single transaction when data rates warrant.

After the Archive Node saves object data to the TSM server, the object data is managed by the TSM server using its lifecycle/retention policies. These retention policies must be defined to be compatible with the operation of the Archive Node. That is, object data saved by the Archive Node must be stored indefinitely and must always be accessible by the Archive Node, unless it is deleted by the Archive Node.

There is no connection between the StorageGRID Webscale system’s ILM rules and the TSM server’s lifecycle/retention policies. Each operates independently of the other; however, as each object is ingested into the StorageGRID Webscale system, you can assign it a TSM management class. This management class is passed to the TSM server along with object data. Assigning different management classes to different object types permits you to configure the TSM server to place object data in different storage pools, or to apply different migration or retention policies as required. For example, objects identified as database backups (temporary content than can be overwritten with newer data) might be treated differently than application data (fixed content that must be retained indefinitely).

The Archive Node can be integrated with a new or an existing TSM server; it does not require a dedicated TSM server. TSM servers can be shared with other clients, provided that the TSM server is sized appropriately for the maximum expected load. TSM must be installed on a server or virtual machine separate from the Archive Node.

It is possible to configure more than one Archive Node to write to the same TSM server; however, this configuration is only recommended if the Archive Nodes write different sets of data to the TSM server. Configuring more than one Archive Node to write to the same TSM server is not recommended when each Archive Node writes copies of the same object data to the archive. In the latter scenario, both copies are subject to a single point of failure (the TSM server) for what are supposed to be independent, redundant copies of object data.

Archive Nodes do not make use of the Hierarchical Storage Management (HSM) component of TSM.

Configuration best practices

When you are sizing and configuring your TSM server there are best practices you should apply to optimize it to work with the Archive Node.

When sizing and configuring the TSM server, you should consider the following factors:
Because the Archive Node does not aggregate objects before saving them to the TSM server, the TSM database must be sized to hold references to all objects that will be written to the Archive Node.

Archive Node software cannot tolerate the latency involved in writing objects directly to tape or other removable media. Therefore, the TSM server must be configured with a disk storage pool for the initial storage of data saved by the Archive Node whenever removable media are used.

You must configure TSM retention policies to use event-based retention. The Archive Node does not support creation-based TSM retention policies. Use the following recommended settings of retmin=0 and retver=0 in the retention policy (which indicates that retention begins when the Archive Node triggers a retention event, and is retained for 0 days after that). However, these values for retmin and retver are optional.

The disk pool must be configured to migrate data to the tape pool (that is, the tape pool must be the NXTSTGPOOL of the disk pool). The tape pool must not be configured as a copy pool of the disk pool with simultaneous write to both pools (that is, the tape pool cannot be a COPYSTGPOOL for the disk pool). To create offline copies of the tapes containing Archive Node data, configure the TSM server with a second tape pool that is a copy pool of the tape pool used for Archive Node data.

Completing the Archive Node setup

The Archive Node is not functional after you complete the installation process. Before the StorageGRID Webscale system can save objects to the TSM Archive Node, you must complete the installation and configuration of the TSM server and configure the Archive Node to communicate with the TSM server.

For more information about optimizing TSM retrieval and store sessions, see Managing archival storage on page 124.

Refer to the following IBM documentation, as necessary, as you prepare your TSM server for integration with the Archive Node in a StorageGRID Webscale system:

- IBM Tape Device Drivers Installation and User’s Guide
  http://www.ibm.com/support/docview.wss?rs=577&uid=ssg1S7002972
- IBM Tape Device Drivers Programming Reference
  http://www.ibm.com/support/docview.wss?rs=577&uid=ssg1S7003032

Installing a new TSM server

You can integrate the Archive Node with either a new or an existing TSM server. If you are installing a new TSM server, follow the instructions in your TSM documentation to complete the installation.

Note: An Archive Node cannot be co-hosted with a TSM server.

Configuring the TSM server

This section includes sample instructions for preparing a TSM server following TSM best practices. The following instructions guide you through the process of:

- Defining a disk storage pool, and a tape storage pool (if required) on the TSM server
- Defining a domain policy that uses the TSM management class for the data saved from the Archive Node, and registering a node to use this domain policy.

These instructions are provided for your guidance only; they are not intended to replace TSM documentation, or to provide complete and comprehensive instructions suitable for all configurations. Deployment specific instructions should be provided by a TSM administrator who is familiar both with your detailed requirements, and with the complete set of TSM Server documentation.
Defining TSM tape and disk storage pools

The Archive Node writes to a disk storage pool. To archive content to tape, you must configure the disk storage pool to move content to a tape storage pool.

About this task

For a TSM server, you must define a tape storage pool and a disk storage pool within Tivoli Storage Manager. After the disk pool is defined, create a disk volume and assign it to the disk pool. A tape pool is not required if your TSM server uses disk-only storage.

You must complete a number of steps on your TSM server before you can create a tape storage pool. (Create a tape library and at least one drive in the tape library. Define a path from the server to the library and from the server to the drives, and then define a device class for the drives.) The details of these steps can vary depending upon the hardware configuration and storage requirements of the site. For more information, see the TSM documentation.

The following set of instructions illustrates the process. You should be aware that the requirements for your site may be different depending on the requirements of your deployment. For configuration details and for instructions, see the TSM documentation.

**Note:** You must log onto the server with administrative privileges and use the dsmadmc tool to execute the following commands.

Steps

1. Create a tape library.

   ```bash
   define library tapelibrary libtype=scsi
   ```

   Where `tapelibrary` is an arbitrary name chosen for the tape library, and the value of `libtype` can vary depending upon the type of tape library.

2. Define a path from the server to the tape library.

   ```bash
   define path servername tapelibrary srctype=server desttype=library
device=lib-devicename
   ```

   - `servername` is the name of the TSM server
   - `lib-devicename` is the device name for the tape library

3. Define a drive for the library.

   ```bash
   define drive tapelibrary drivename
   ```

   `drivename` is the name you want to specify for the drive.

   You might want to configure an additional drive or drives, depending upon your hardware configuration. (For example, if the TSM server is connected to a Fibre Channel switch that has two inputs from a tape library, you might want to define a drive for each input.)

4. Define a path from the server to the drive you defined.

   ```bash
   define path servername drivename srctype=server desttype=drive
   library=tapelibrary device=drive-dname
   ```

   `drive-dname` is the device name for the drive, and `tapelibrary` is the name of the tape library.

   Repeat for each drive that you have defined for the tape library, using a separate drivename and drive-dname for each drive.

5. Define a device class for the drives.
define devclass DeviceClassName devtype=lto library=tapelibrary format=ultrium3

- DeviceClassName is the name of the device class
- lto describes the type of drive connected to the server
- tapelibrary is the tape library name you defined
- substitute the appropriate value for ultrium3 in the format= parameter to match your tape type

6. Add tape volumes to the inventory for the library.
   checkin libvolume tapelibrary
   tapelibrary is the tape library name you defined.

7. Create the primary tape storage pool.
   define stgpool BycastTapePool DeviceClassName description=description
collocate=filespace maxscratch=XX

   - BycastTapePool is the name of the Archive Node’s tape storage pool. You can select any
     name for the tape storage pool (as long as the name uses the syntax conventions expected by
     the TSM server).
   - DeviceClassName is the name of the device class name for the tape library.
   - description is a description of the storage pool that can be displayed on the TSM server
     using the ‘query stgpool’ command. For example: “Tape storage pool for the Archive Node”.
   - collocate=filespace specifies that the TSM server should write objects from the same
     filespace into a single tape.
   - XX is one of the following:
     - the number of empty tapes in the tape library (in the case that the Archive Node is the only
       application using the library)
     - the number of tapes allocated for use by the StorageGRID Webscale system (in instances
       where the tape library is shared)

8. On a TSM server, create a disk storage pool. At the TSM server’s administrative console, enter
   define stgpool BycastDiskPool disk description=description
maxsize=maximum_file_size nextstgpool=BycastTapePool
highmig=percent_high lowmig=percent_low

   - BycastDiskPool is the name of the Archive Node’s disk pool. You can select any name for
     the disk storage pool (as long as the name uses the syntax conventions expected by the TSM).
   - description is a description of the storage pool that can be displayed on the TSM server
     using the ‘query stgpool’ command. For example, “Disk storage pool for the Archive Node”.
   - maximum_file_size forces objects larger than this size to be written directly to tape, rather
     than being cached in the disk pool. It is recommended to set maximum_file_size to 10 GB.
   - nextstgpool=BycastTapePool refers the disk storage pool to the tape storage pool
     defined for the Archive Node.
   - percent_high sets the value at which the disk pool begins to migrate its contents to the tape
     pool. It is recommended to set percent_high to 0 so that data migration begins immediately
   - percent_low sets the value at which migration to the tape pool stops. It is recommended to
     set percent_low to 0 to clear out the disk pool.
9. On a TSM server, create a disk volume (or volumes) and assign it to the disk pool.

   define volume BycastDiskPool volume_name formatsize=size

   • BycastDiskPool is the disk pool name
   • volume_name is the full path to the location of the volume (for example /var/local/arc/stage6.dsm) on the TSM server where it writes the contents of the disk pool in preparation for transfer to tape
   • size is the size, in MB, of the disk volume

   For example, to create a single disk volume such that the contents of a disk pool fill a single tape, set the value of size to 200000 when the tape volume has a capacity of 200 GB.

   However, it might be desirable to create multiple disk volumes of a smaller size, as the TSM server can write to each volume in the disk pool. For example, if the tape size is 250 GB, create 25 disk volumes with a size of 10 GB (10000) each.

   The TSM server preallocates space in the directory for the disk volume. This can take some time to complete (more than three hours for a 200 GB disk volume).

Define a domain policy and register a node

You need to define a domain policy that uses the TSM management class for the data saved from the Archive Node, and then register a node to use this domain policy.

   Note: Archive Node processes can leak memory if the client password for the Archive Node in Tivoli Storage Manager (TSM) expires. Ensure that the TSM server is configured so the client username/password for the Archive Node never expires.

When registering a node on the TSM server for the use of the Archive Node (or updating an existing node), you must specify the number of mount points that the node can use for write operations by specifying the MAXNUMMP parameter to the REGISTER NODE command. The number of mount points is typically equivalent to the number of tape drive heads allocated to the Archive Node. The number specified for MAXNUMMP on the TSM server must be at least as large as the value set for the ARC > Target > Configuration > Main > Maximum Store Sessions for the Archive Node, which is set to a value of 0 or 1, as concurrent store sessions are not supported by the Archive Node.

The value of MAXSESSIONS set for the TSM server controls the maximum number of sessions that can be opened to the TSM server by all client applications. The value of MAXSESSIONS specified on the TSM must be at least as large as the value specified for ARC > Target > Configuration > Main > Number of Sessions in the NMS for the Archive Node. The Archive Node concurrently creates at most one session per mount point plus a small number (< 5) of additional sessions.

The TSM node assigned to the Archive Node uses a custom domain policy tsm-domain. The tsm-domain domain policy is a modified version of the “standard” domain policy, configured to write to tape and with the archive destination set to be the StorageGRID Webscale system’s storage pool (BycastDiskPool).

   Note: You must log in to the TSM server with administrative privileges and use the dsmadmc tool to create and activate the domain policy.

Creating and activating the domain policy

You must create a domain policy and then activate it to configure the TSM server to save data sent from the Archive Node.

Steps

1. Create a Domain Policy

   copy domain standard tsm-domain
2. If you are not using an existing management class, enter one of the following:
   
   ```
   define policyset tsm-domain standard
   define mgmtclass tsm-domain standard default
   ```
   
   `default` is the default management class for the deployment.

3. Create a copygroup to the appropriate storage pool. Enter (on one line):
   
   ```
   define copygroup tsm-domain standard default type=archive
   destination=BycastDiskPool retinit=event retmin=0 retver=0
   ```
   
   `default` is the default Management Class for the Archive Node. The values of retinit, retmin, and retver have been chosen to reflect the retention behavior currently used by the Archive Node.

   **Note:** Do not set retinit to retinit=create. Setting retinit=create blocks the Archive Node from deleting content since retention events are used to remove content from the TSM server.

4. Assign the management class to be the default.
   
   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Set the new policy set as active.
   
   ```
   activate policyset tsm-domain standard
   ```
   
   Ignore the “no backup copy group” warning that appears when you enter the activate command.

6. Register a node to use the new policy set on the TSM server. On the TSM server, enter (on one line):
   
   ```
   register node arc-user arc-password passexp=0 domain=tsm-domain
   MAXNUMMP=number-of-sessions
   ```
   
   `arc-user` and `arc-password` are same client node name and password as you define on the Archive Node, and the value of MAXNUMMP is set to the number of tape drives reserved for Archive Node store sessions.

   **Note:** By default, registering a node creates an administrative user ID with client owner authority, with the password defined for the node.
Glossary

ACL
Access control list. Specifies which users or groups of users are allowed to access an object and what operations are permitted, for example, read, write, and execute.

ADC service
Administrative Domain Controller. The ADC service maintains topology information, provides authentication services, and responds to queries from the LDR, CMN, and CLB services. The ADC service is present on each of the first three Storage Nodes installed at a site.

ADE
Asynchronous Distributed Environment. Proprietary development environment used as a framework for services within the StorageGRID Webscale system.

Admin Node
The Admin Node provides services for the web interface, system configuration, and audit logs. See also, primary Admin Node.

Amazon S3
Proprietary web service from Amazon for the storage and retrieval of data.

AMS service
Audit Management System. The AMS service monitors and logs all audited system events and transactions to a text log file. The AMS service is present on the Admin Node.

API Gateway Node
An API Gateway Node provides load balancing functionality to the StorageGRID Webscale system and is used to distribute the workload when multiple client applications are performing ingest and retrieval operations. API Gateway Nodes include a Connection Load Balancer (CLB) service.

ARC service
Archive. The ARC service provides the management interface with which you configure connections to external archival storage such as the cloud through an S3 interface or tape through TSM middleware. The ARC service is present on the Archive Node.

Archive Node
The Archive Node manages the archiving of object data to an external archival storage system.

atom
Atoms are the lowest level component of the container data structure, and generally encode a single piece of information.

audit message
Information about an event occurring in the StorageGRID Webscale system that is captured and logged to a file.

BASE64
A standardized data encoding algorithm that enables 8-bit data to be converted into a format that uses a smaller character set, enabling it to safely pass through legacy systems that can process only basic (low order) ASCII text excluding control characters. See RFC 2045 for more details.
bundle
A structured collection of configuration information used internally by various
components of the StorageGRID Webscale system. Bundles are structured in container
format.

Cassandra
An open-source database that is scalable and distributed, provides high availability, and
handles large amounts of data across multiple servers.

CBID
Content Block Identifier. A unique internal identifier of a piece of content within the
StorageGRID Webscale system.

CDMI
Cloud Data Management Interface. An industry-standard defined by SNIA that includes a
RESTful interface for object storage. For more information, see www.snia.org/cdmi.

CIDR
Classless Inter-Domain Routing. A notation used to compactly describe a subnet mask
used to define a range of IP addresses. In CIDR notation, the subnet mask is expressed as
an IP address in dotted decimal notation, followed by a slash and the number of bits in the
subnet. For example, 192.0.2.0/24.

CLB service
Connection Load Balancer. The CLB service provides a gateway into the StorageGRID
Webscale system for client applications connecting through HTTP. The CLB service is
part of the API Gateway Node.

Cloud Data Management Interface
See CDMI.

CMN service
Configuration Management Node. The CMN service manages system-wide configurations
and grid tasks. The CMN service is present on the primary Admin Node.

CMS service
Content Management System. The CMS service carries out the operations of the active
ILM policy’s ILM rules, determining how object data is protected over time. The CMS
service is present on the Storage Node.

command
In HTTP, an instruction in the request header such as GET, HEAD, DELETE, OPTIONS,
POST, or PUT. Also known as an HTTP method.

container
Created when an object is split into segments. A container object lists the header
information for all segments of the split object and is used by the LDR service to assemble
the segmented object when it is retrieved by a client application.

content block ID
See CBID.

content handle
See UUID.

CSTR
Null-terminated, variable-length string.

DC
Data Center site.
DDS service
Distributed Data Store. The DDS service interfaces with the distributed key-value store and manages object metadata. It distributes metadata copies to multiple instances of the distributed key-value store so that metadata is always protected against loss.

distributed key value store
Data storage and retrieval that unlike a traditional relational database manages data across grid nodes.

Enablement Layer
Used during installation to customize the Linux operating system installed on each grid node. Only the packages needed to support the services hosted on the grid node are retained, which minimizes the overall footprint occupied by the operating system and maximizes the security of each grid node.

Fibre Channel
A networking technology primarily used for storage.

GPT
Grid Provisioning Tool. A software tool included with StorageGRID Webscale software that permits you to provision a StorageGRID Webscale system for installation, maintenance, or expansion. GPT creates and maintains an encrypted repository of information about the system that is required to maintain the StorageGRID Webscale system and recover failed grid nodes.

Grid ID signed text block
A BASE64 encoded block of cryptographically signed data that contains the grid ID. See also, provisioning.

grid node
The basic software building block for the StorageGRID Webscale system, for example, Admin Node or Storage Node. Each grid node type consists of a set of services that perform a specialized set of tasks.

grid task
System-wide scripts used to trigger various actions that implement specific changes to the StorageGRID Webscale system. For example, most maintenance and expansion procedures involve running grid tasks. Grid tasks are typically long-term operations that span many entities within the StorageGRID Webscale system. See also, Task Signed Text Block.

ILM
Information Lifecycle Management. A process of managing content storage location and duration based on content value, cost of storage, performance access, regulatory compliance, and other factors. See also, Admin Node and storage pool.

LAN
Local Area Network. A network of interconnected computers that is restricted to a small area, such as a building or campus. A LAN can be considered a node to the Internet or other wide area network.

latency
Time duration for processing a transaction or transmitting a unit of data from end to end. When evaluating system performance, both throughput and latency need to be considered. See also, throughput.

LDR service
Local Distribution Router. The LDR service manages the storage and transfer of content within the StorageGRID Webscale system. The LDR service is present on the Storage Node.
LUN
See object store.

metadata
Information related to or describing an object stored in the StorageGRID Webscale system; for example, ingest time.

namespace
A set whose elements are unique names. There is no guarantee that a name in one namespace is not repeated in a different namespace.

nearline
A term describing data storage that is neither “online” (implying that it is instantly available, like spinning disk) nor “offline” (which can include offsite storage media). An example of a nearline data storage location is a tape that is loaded in a tape library, but is not mounted.

NFS
Network File System. A protocol (developed by SUN Microsystems) that enables access to network files as if they were on local disks.

NMS service
Network Management System. The NMS service provides a web-based interface for managing and monitoring the StorageGRID Webscale system. The NMS service is present on the Admin Node. See also, Admin Node.

node ID
An identification number assigned to a service within the StorageGRID Webscale system. Each service (such as an NMS service or ADC service) must have a unique node ID. The number is set during system configuration and tied to authentication certificates.

NTP
Network Time Protocol. A protocol used to synchronize distributed clocks over a variable latency network, such as the Internet.

object
An artificial construct used to describe a system that divides content into data and metadata.

object storage
An approach, where stored data is accessed by unique identifiers rather than by a user-defined hierarchy of directories and files. Each object has both data (for example, a picture) and metadata (for example, the date the picture was taken). Object storage operations act on entire objects as opposed to reading and writing bytes as is commonly done with files, and provided via APIs or HTTP instead of NAS (CIFS/NFS) or block protocols (iSCSI/ FC/FCOE).

object store
A configured file system on a disk volume. The configuration includes a specific directory structure and resources initialized at system installation.

object segmentation
A StorageGRID Webscale process that splits a large object into a collection of small objects (segments) and creates a segment container to track the collection. The segment container contains the UUID for the collection of small objects as well as the header information for each small object in the collection. All of the small objects in the collection are the same size. See also, segment container.

OID
Object Identifier. The unique identifier of an object.
primary Admin Node
Admin Node that hosts the CMN service. There is one per StorageGRID Webscale system. See also, Admin Node.

provisioning
The process of generating a new or updated SAID package and GPT repository. See also, SAID.

quorum
A simple majority: 50% + 1. Some system functionality requires a quorum of the total number of a particular service type.

SAID
Software Activation and Integration Data. Generated during provisioning, the SAID package contains site-specific files and software needed to install a StorageGRID Webscale system.

SATA
Serial Advanced Technology Attachment. A connection technology used to connect server and storage devices.

SCSI
Small Computer System Interface. A connection technology used to connect servers and peripheral devices, such as storage systems.

segment container
An object created by the StorageGRID Webscale system during the segmentation process. Object segmentation splits a large object into a collection of small objects (segments) and creates a segment container to track the collection. A segment container contains the UUID for the collection of segmented objects as well as the header information for each segment in the collection. When assembled, the collection of segments creates the original object. See also, object segmentation.

Server
Used when specifically referring to hardware. Might also refer to a virtual machine.

Service
A unit of the StorageGRID Webscale system, such as the ADC service, NMS service, or SSM service. Each service performs unique tasks critical to the normal operations of a StorageGRID Webscale system.

SQL
Structured Query Language. An industry-standard interface language for managing relational databases. An SQL database is one that supports the SQL interface.

ssh
Secure Shell. A UNIX shell program and supporting protocols used to log in to a remote computer and execute commands over an authenticated and encrypted channel.

SSM
Server Status Monitor. A component of the StorageGRID Webscale software that monitors hardware conditions and reports to the NMS service. Every grid node runs an instance of the SSM service.

SSL
Secure Socket Layer. The original cryptographic protocol used to enable secure communications over the Internet. See also, TLS.

Storage Node
The Storage Node provides storage capacity and services to store, move, verify, and retrieve objects stored on disks.
Storage pool
The element of an ILM rule that determines the location where an object is stored.

StorageGRID Webscale
A registered trademark of NetApp Inc. for their object storage grid architecture and software system.

Storage volume
See object store

Task Signed Text Block
A BASE64 encoded block of cryptographically signed data that provides the set of instructions that define a grid task.

TCP/IP

throughput
The amount of data that can be transmitted or the number of transactions that can be processed by a system or subsystem in a given period of time. See also, latency.

TLS
Transport Layer Security. A cryptographic protocol used to enable secure communications over the Internet. See RFC 2246 for more details.

transfer syntax
The parameters, such as the byte order and compression method, needed to exchange data between systems.

Tivoli Storage Manager
IBM storage middleware product that manages storage and retrieval of data from removable storage resources.

URI
Universal Resource Identifier. A generic set of all names or addresses used to refer to resources that can be served from a computer system. These addresses are represented as short text strings.

UTC
A language-independent international abbreviation, UTC is neither English nor French. It means both “Coordinated Universal Time” and “Temps Universel Coordonné.” UTC refers to the standard time common to every place in the world.

UUID
Universally Unique Identifier. Unique identifier for each piece of content in the StorageGRID Webscale system. UUIDs provide client applications with a content handle that permits them to access content in a way that does not interfere with the StorageGRID Webscale system’s management of that same content. A 128-bit number which is guaranteed to be unique. See RFC 4122 for more details.

Virtual machine (VM)
A software platform that enables the installation of an operating system and software, substituting for a physical server and permitting the sharing of physical server resources among several virtual servers.

XFS
A scalable, high-performance journaled file system originally developed by Silicon Graphics.
**WAN**

Wide area network. A network of interconnected computers that covers a large geographic area, such as a country.

**XML**

Extensible Markup Language. A text format for the extensible representation of structured information; classified by type and managed like a database. XML has the advantages of being verifiable, human readable, and easily interchangeable between different systems.
Trademark information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

• NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
• Telephone: +1 (408) 822-6000
• Fax: +1 (408) 822-4501
• Support telephone: +1 (888) 463-8277
Index

/etc/fstab file 116

A

aborting grid tasks
  procedure for 181
access control policies
  description of 22
  overview of 22
  supported 22
accounts, group
  deleting 171
accounts, user
  adding 172
  creating 172
  deleting 173
Active Directory
  adding users or groups to audit share 160
  audit clients 157
  changing audit client share user or group name 162
  configuring audit clients 157
  removing users from audit share 161
ADC
  link costs 147
ADC service 103
add-audit-share command, in config_cifs.rb 155, 157
add-ip-to-share command, in config_nfs.rb 164
add-user-to-share command 160
add-user-to-share command in config_cifs.rb 160
add-user-to-share command, in config_cifs.rb 155
adding
  Storage Nodes 110
  storage volumes 110
admin groups
  acknowledge alarm 168
  Grid Topology Page Configuration 168
  managing 168
  Other Grid Configuration 168
  permissions 168
Admin Node
  change name 141
  defined 138
  primary
    redundancy 139
  primary Admin Node
    passwordless access 150
admin users
  managing 168
administration guide 8
Administrative Domain Controller
  See ADC
AES-128 112
AES-256 112
alarm
  acknowledgments 139
  alarm triggering
    examples 47
alarms
  by code
    SAVP Total Usable Space (Percent) 106
    SSTS Storage Status 106
class overriders 49
clearing triggered alarms 59
configuring email notifications 36
creating custom alarms 50
creating custom global alarms 52
creating e-mail mailing lists 39
custom 46
custom notification migration 190
customizing alarms 44
default 45
disable default 55
disabling 54
disabling default alarms 56
disabling global custom alarms, grid wide 58
disabling global custom alarms, service level 57
email notifications 34
global custom 46
monitoring 47
new services 50
notifications 34, 35
of same severity 49
overriding higher priority alarm 49
severity changes 50
table, displayed in 55
triggering evaluation order 47
triggering logic 47
types 44
viewing default 45
All Storage Nodes storage pool 78
API Gateway Node
  decommissioning grid task 175
  description of 123
appliance
  viewing events 68
  viewing Storage Nodes 64
ARC
  archive read-only on startup 135, 136
  archive store state 135, 136
  configuration
    Target component 129
  optimizing for Tivoli Storage Manager 131
  optimizing performance, TSM sessions 131
  resetting store failure count 135–137
  retrieve component 134
  Tivoli Storage Manager
    unavailable 132
ARC service 124
archive
  read-only on startup 135, 136
  retrieve state 134
  store set 135–137
Archive Node
  configure replication settings 133
  configure target 125
  configuring cloud connections 126
  configuring S3 connections 126
optimizing for Tivoli Storage Manager middleware
setting custom alarms

target

Archive Nodes
capacity, full
configurations
   Archive Nodes
   configurations described
optimizing for Tivoli Storage Manager middleware
attributes
by code
   ROMK Hard Read-Only Watermark
   SSCR Storage Status - Current
   STAS Total Usable Space
   VHWM Storage Volume Soft Read-Only Watermark
   VROM Storage Volume Hard Read-Only Watermark
by name
   Hard Read-Only Watermark ROMK
   Storage Status - Current SSCR
   Storage Volume Soft Read-Only Watermark
   VHWM
   Total Usable Space STAS

audit client configuration
   CIFS, Active Directory
   CIFS, Windows Workgroup
   NFS

AutoSupport
described
   disabling
   preferred sender
   sending
   triggering

B
background verification
   adaptive
   configuring
   high verification priority
   LDR
   priority
   reset corrupt objects count
   verification priority

Baseline 2 Copy Rule policy
browser
   requirements
   bundle
      import grid task

C

capacity
   Archive Node
   of storage

cassandra
   CCLE grid task

Clean Up Unused Cassandra Keys grid task
nodetool repair

CBID
defined
   obtain

CDMI
   container objects
   profiles
   CDMI data object ID
   certificate authority (CA) certificates
   copying for StorageGRID Webscale system

CIFS
   audit file share configuration
   audit share

CIFS audit share
   adding groups
   adding users

CLB service
defined

client file shares
   CIFS
      audit directory, AD
      configuring audit clients

   CIFS audit share
      changing group name
      changing user name
      removing users

   NFS audit share
      adding clients
      changing client IP address

CMN service
defined

CMS
   metadata
   CMS service
   command shell
      accessing
      logging in
      logging out

comments
   how to send feedback about documentation
   compression
      lossless

content protection
   configuration settings
   delete permission in CDMI profile
   Disable Client Delete
   ILM rules
   permissions
   security partition
   content verification
   corrupt objects
   CPU status
   creating tenant accounts for S3
   custom alarms
      creating
      triggering logic
D

data migration
  attributes, monitoring
    ARVF 187
  batch ingest 188
  continuous ingest 189
  creating custom alarms 190
  grid capacity, check 186
  ILM policy 186
  impact on grid operations 187
  notifications 190
  schedule time of day 187
DC topology, sample ILM policy 99
DDS
  service 101
DDS service 101
default alarms
  disable 55
  triggering logic 47
deleting tenant accounts 29
Device Model ID 142
Device Model Version 142
Disable Client Delete 115
disable inbound replication 107
disable outbound replication 107
disabling LDAP 31
documentation
  how to receive automatic notification of changes to 216
  how to send feedback about 216
domain policy
  activating for TSM 205
  creating for TSM 205
DoNotStart file
  creating for individual service 198
  defined 198
  remove for service 198
dual commit 75

e

e-mail
  service state notifications 34
  severity level in notifications 34
e-mail notifications
  create mailing lists 39
  e-mail notifications 50
  events 35
  islanded Admin Nodes 43
  preferred sender 43
  queue 35
  status 35
  suppress grid wide 42
  suppress, grid-wide 42
  test e-mail 41
editing tenant accounts 20
e-mail
  notifications 34
email notifications
  configure global notification 40
  configuring email server 36
  create global notification 40
create templates 38
mail server settings 36
suppressing for mailing lists 42
template 38
email server
  configuring 36
email template 38
encryption
  disable 112
  network transfer 149
erasure codes, storage pool 71
erasure coding
  configure 81
error state 200
eth0 145
eth1 145
events
  alarms 34
  events, hardware
    viewing 68
examples
  alarm triggering 47

F

failed grid tasks
  types of status shown in Historical table 183
feedback
  how to send comments about documentation 216
file system
  UUID 116
force-stop 196
foreground verification
  missing replicated object data 120

G

GDCM grid task 175
global custom alarms
  disabling 57, 58
  triggering logic 47
grid capacity
  data migration 186
grid configuration
  network transfer encryption 149
tuning for object size 116
Grid Management tree 9
grid network IP addresses 144
grid node
  IP address 144
grid nodes
  monitor 62
  reboot 197
  viewing appliance 64
grid tasks
  aborting 181, 184
  active 176
API Gateway Node decommissioning 175
BDLI 175
bundle import 175
cancelling 181
CCLE 175
charting 178
description 175
expansion 175
GDCM 175
GEXP 175
Grid Expansion 175
grid performance 175
grid tasks
  VFGV 175
historical 176
ILM evaluation (Volume Lost) 175
ILM evaluation grid tasks 175
ILME 175
LDR foreground verification 120
LDR Foreground Verification 175
managing errors 184
monitoring 176
operations 175
pausing 180
pending 176
progress 176
reasons for failure 183
recovery 175
removing from the Historical table 182
resuming 180
running 179
status 176
Storage Node decommissioning 175
task signed text block 184
troubleshooting 182
troubleshooting retries 183
Grid Topology tree 9
grids
  access permissions 168
group accounts
deleting 171
group policies
  editing for S3 tenant accounts 21
  editing for Swift tenant accounts 29
  groups
    changing 171
    creating 170
    updating 171
  groups, in ILM policies 71

H

hardware
  viewing events 68
hashing, stored object 113
health check timeout
  LDR 107
historical ILM policies 94
Historical table
  status of failed grid tasks 183
HSTE
  HTTP/CDMI State 107
HTTP
  auto-start 107
HTTP DELETE
  operations 115
HTTP/CDMI State, set 107
HTTPS connections
copying CA certificates 153

I

identity federation
  configuring OpenLDAP for 31
  synchronization of LDAP server 32
ILM
  build policy 70
  content placement instructions 83
  content protection 115
  defined 71
dual commit 75
evaluation logic 70
filters 73, 83
groups 71
historical policies 94
ILM re-evaluation 95
Last Access Time 83
metadata 73
object identifier 91
Object not referenced by API 75
  policies
    activate 90
    apply, existing content 95
    build 70
    configure 87
    historical policies 94
    rules 75
    sample policies 99
    view historical 94
    viewing activity queue 94
  policy updates 89
  reference time
    ingest time 83
    Last Access Time 83
rules
  content placement instructions 83
  create 83
  delete 93
  edit 93
  examples 96–98
  Last Access Time 83
  Make 2 Copies rule 78
  modify 93
  ordering 87
storage 71, 76
storage grade
  assign to LDR 76
  configuring 71, 76
storage locations 71
storage pools
  built-in 78
  configure 78
  guidelines 78
  view existing 81
time values 83
ILM criteria evaluation 73
ILM policy
  viewing activity queue 94
ILM rules
  archival media 124
  default 87
default rule 87
examples 96–98
filtering logic 87
last access time 83
ordering 87
information
how to send feedback about improving documentation 216
IP address
grid network 144
supplementary network 144
view 145
J
join-domain command, in config_cifs.rb 157
L
last access time
ILM rules 83
Last Access Time 83
LDAP
configuring 30
disabling 31
LDAP server
forcing synchronization of 32
LDR
assign storage grade 76
background verification 107
configuration
Storage component 107
content balancing 104
corrupt objects 107
encryption 107
full 119
health check timeout 107
HTTP/CDMI State 107
monitor available space 104
object mapping 104
object stores 104
replication 107
reset missing copies count, erasure coding 107
reset read failures, erasure coding 107
reset write failures, erasure coding 107
service 101
storage grade 76
storage state-desired 107
verification 119
volume ID 104
LDR service 101
LDRBackground verification 119
license
updating 14
viewing details for 14
link costs
default values 147
update 148
lists, mailing
suppressing email notifications from 42
Local Distribution Router service
See LDR service
log files
servermanager.log 199
logging in
StorageGRID Webscale 11
logging out
StorageGRID Webscale 13
M
mailing lists
suppressing email notifications from 42
Make 2 Copies rule, ILM 70, 78
management API
overview 15
management class, Tivoli Storage Manager 125
metadata
in ILM rules 73
MIB
OID values 147
SNMP 147
modifying DNS configuration
for single grid node 145
monitoring
storage 111
system capacity
system-wide 111
Monitoring
storage capacity
per Storage Node 111
N
NAS Bridge
NFS protocol 9
SMB protocol 9
NetBIOS name
file share configuration 157
network connections
monitoring
viewing for appliance 64
network transfer encryption
disable 149
enable 149
NFS audit share
removing clients 166
verifying integration 166
NFS protocol
NAS Bridge 9
NFS share configuration
add a client to an audit share 164
changing client IP address 167
configure the audit client 163
remove a client from the audit share 166
NMS entities
changing name 143
device model ID 142
device model version 142
language 142
name 142
OID 142
settings 142
NMS management
timeout period 13
NMS service
  defined 138
node tool repair 104
notifications
  configuring 35
notifications, email
  suppressing for mailing lists 42

O
object count 102
object data
  corrupt 118
  missing 118, 120
  verify 120
  verify integrity 118
object lookup
  view 91
object metadata 103
Object not referenced by API 75
object segmentation 117
object store
  volume ID 104
object stores 104
OID
  defined 142
  values 147
OpenLDAP
  configuration guidelines for 31
optimizing performance, middleware sessions
  Tivoli Storage Manager 125
optimizing storage 117
ORLM 91

P
passwordless access, ssh 150
passwords
  changing 13
  changing others’ 173
permissions
  setting for groups 170
policies
  activate 87
  baseline 70
  configure 87
  migrated data 186
  verify 91
preferred sender, notifications 43
primary Admin Node
  passwordless access 150
product overview 8

R
RAM usage 63
reboot
  grid node 197
remove-ip-from-share command, in config_nfs.rb 166
remove-user-from-share command, in config_cifs.rb 161
removing tenant accounts 29
reset counters...
services, stop individual 196, 197
start services 194
start, manually 194
troubleshoot 199
troubleshooting
error state 200
version 192
Server Status Monitor
See SSM
servermanager.log 199
servers
power down 197
service
restart 197
status 193, 195
stop 196
services
creating alarms 50
disable global custom alarm 57
disabling default alarms 54, 55
stop 195
terminate 196
set-authentication command, in config_cifs.rb 155, 157
setting custom Archive Node 137
share configuration
add-audit-share command 155, 157
add-ip-to-share command 164
add-user-to-share command 155
audit share (CIFS) 155
audit share (NFS) 163
join-domain command 157
NetBIOS name 157
remove-ip-from-share command 166
remove-user-from-share command 161
set-authentication command 155, 157
signing in
StorageGRID Webscale 11
signing out
through web-browser 13
Simple Storage Service 125
SMB protocol
NAS Bridge 9
SMTP mail server settings 36
SNMP
agent 146
configure 146
system status 146
SNMP monitoring
configure 146
MIB 146
OID 146
SNMPv2c 146
SSCR Storage Status - Current 106
ssh
passwordless access 150
private key 150
SSM
components
events 63
resources 64
timing 64
configuration
Resources component 64
reset event counters 63
services 63
SSTS Storage Status alarm 106
STAS Total Usable Space
attribute 104
status
grid tasks 176
of failed grid tasks 183
storage
background verification 119
calculate capacity 104
ILM 71, 76
storage capacity
monitoring per Storage Node 111
monitoring system-wide 111
watermarks 106
storage grade
assign to LDR 76
configuring 76
creating a list 76
Storage Node
background verification 118
encryption 112
foreground verification 118, 120
LDR 104
object mapping 104
watermarks 106
Storage Node rebuild, optimizing Tivoli Storage Manager 131
Storage Nodes
viewing appliance 64
storage object compression
disable 114
storage pools
configure 78
ILM 71, 76
view existing 81
Storage Status - Current SSCR 106
Storage Status SSTS alarm 106
storage tenant account
managing federated user S3 credentials for 32
S3 access keys and 32
StorageGRID Webscale
copying CA certificates 153
logging in 11
logging out 13
StorageGRID Webscale system
defined 8
StorageGRID Webscale system
defined 8
storaged object compression 114
storaged object encryption
configure 112
storaged object hashing
configure 113
suggestions
how to send feedback about documentation 216
supplementary network IP addresses 144
Swift
editing tenant account group policies 29
editing tenant accounts 28
Swift clients
managing access overview 19
Swift REST API
creating tenant accounts 27
Swift tenant accounts
  managing 27
synchronization
  LDAP server and 32
system events 34
system status
  OID 146
  SNMP 146

T

template 38
tenant accounts
  authenticating with LDAP 30
  creating for S3 19
  creating for Swift 27
  deleting 29
  editing 20
  editing for Swift 28
  managing 19, 27
  managing overview 19
  removing 29
terminate services 196
test e-mail
  send 41
timeout period
  change 13
  view 13
Tivoli Storage Manager
  ARC 125
    configure 129
    domain policy for 205
    lifecycle and retention rules 125
    management class 125
    middleware 129
    register nodes for 205
Tivoli Storage Manager ARC
  optimizing Archive Node 131, 133
  optimizing performance 131
  unavailable 132
Total Usable Space (Percent) SAVP
  alarm 106
Total Usable Space STAS
  attribute 104
troubleshoot
  Server Manager 199
troubleshooting

grid task retries 183
grid tasks 182
log files 199
Server Manager
  service does not start 199
TSM tape storage pools
  defining 203
Twitter
  how to receive automatic notification of documentation changes 216

U

user accounts
  adding 172
  changing password 13
  creating 172
  deleting 173
  modifying 172
  permissions 13, 169
users
  changing their passwords 173
UUID
  obtain 91

V

verifying
  CIFS audit integration 163
version information 63
volume ID 104

W

watermarks
  view values 106
web browser
  signing out 13
Workgroup share configuration
  adding users or groups to audit share 160
  audit clients 155
  changing audit client share user or group name 162
  removing user from audit share 161