Monitoring and Managing the IBM Elastic Storage Server Using the GUI

Markus Rohwedder
Alexander Wolf-Reber
Stefan Roth
Liju Jose
# Contents

**Notices** ....................................................................................................................... v
**Trademarks** ..................................................................................................................... vi

**Preface** ............................................................................................................................. vii
**Authors** ............................................................................................................................. vii
**Comments welcome** .......................................................................................................... viii
**Stay connected to IBM Redbooks** .................................................................................... viii

**Chapter 1. Overview** .......................................................................................................... 1
1.1 Single-cluster support ....................................................................................................... 2
1.2 Role-based access control with GUI users ........................................................................ 2
1.3 Integration hub for configuration, health, and performance data ....................................... 2
1.4 Support matrix .................................................................................................................. 3
  1.4.1 Operating system levels .............................................................................................. 3
  1.4.2 IBM Spectrum Scale software requirements ............................................................. 3

**Chapter 2. Installation and configuration of the ESS GUI** .................................................. 5
2.1 Enabling performance monitoring tools in ESS GUI ........................................................ 6
2.2 Setting up the component database .................................................................................. 7
2.3 Securing the ESS GUI ....................................................................................................... 7
  2.3.1 Firewall recommendations and supported ports ......................................................... 7
  2.3.2 Creating an HTTPS certificate .................................................................................. 8
  2.3.3 Root privilege considerations for the ESS GUI ......................................................... 9
2.4 Configuring GUI to use sudo wrapper .............................................................................. 10
2.5 Node classes used for the management GUI ..................................................................... 10
2.6 Modifying GUI property file ........................................................................................... 11
2.7 Setting GUI preferences ................................................................................................... 11

**Chapter 3. Understanding the GUI options** ........................................................................ 13
3.1 Login ................................................................................................................................ 14
3.2 Navigation .......................................................................................................................... 15
3.3 Header area ......................................................................................................................... 16
3.4 Assistance for understanding the features associated with a GUI page .............................. 17

**Chapter 4. Monitoring options available in the GUI** .......................................................... 19
4.1 Monitoring hardware details ............................................................................................. 20
  4.1.1 Servers ....................................................................................................................... 20
  4.1.2 Disk enclosures .......................................................................................................... 20
  4.1.3 Edit rack components ............................................................................................... 21
  4.1.4 Replace broken disks ............................................................................................... 21
4.2 Monitoring performance ..................................................................................................... 21
  4.2.1 Display options in the Statistics page of the GUI ....................................................... 23
  4.2.2 Using dashboard to view performance charts ............................................................. 27
  4.2.3 Monitoring waiters .................................................................................................... 28
4.3 Monitoring capacity .......................................................................................................... 28
  4.3.1 Monitoring → Capacity window ................................................................................ 28
  4.3.2 Using information from the Monitoring → Statistics window .................................... 29
  4.3.3 Capacity information for file systems, pools, NSDs, and filesets ............................... 29
4.4 Monitoring system health .................................................................................................. 29
Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided “AS IS”, without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.
Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

| Enterprise Storage Server® | IBM Spectrum™ | Storwize® |
| GPFS™ | IBM Spectrum Scale™ | WebSphere® |
| IBM® | Redbooks® | |
| IBM Elastic Storage™ | Redbooks (logo) ™ | |

The following terms are trademarks of other companies:

Intel, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other company, product, or service names may be trademarks or service marks of others.
Preface

The Elastic Storage Server (ESS) GUI provides an easy way to configure and monitor various features that are available with the ESS system. The ESS GUI is a web application that runs on web browsers such as Chrome, Firefox, and Edge. It uses Java Script and Ajax technologies to enable smooth and desktop-like interfacing. Therefore, no client-side installation is required to use the GUI.

This document provides detailed information about the ESS GUI features. This edition applies to ESS version 5.2.

For detailed information about the ESS system, see IBM Knowledge Center.

Authors

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization, Tucson Center.

Markus Rohwedder is an IT Architect at IBM® Research and Development in Kelsterbach, Germany. He joined IBM in 1999 after acquiring a PhD in Physics. At IBM, Markus has focused on data-centric projects such as design and administration of a large, continuously available 24/7 data warehouse for production support and implementation of a searchable tape archive for structured data or benchmarking clustered databases. Since 2008, he has worked on creating graphical user interfaces for storage systems such as Information Archive, IBM Storwize® V7000 Unified, and IBM Spectrum™ Scale.

Alexander Wolf-Reber is an IT Architect in IBM Research and Development Kelsterbach, Germany. His current role is technical lead for the GUI and ReST-API components of IBM Spectrum Scale™. He joined IBM in 1999 and worked on various storage products like SAN Volume Controller, IBM Enterprise Storage Server®, and tape libraries. Since 2007, his focus is on clustered file systems. During his career, he also contributed to standardization bodies like the Storage Networking Association and the Java Community Process. He holds a PhD degree in Physics from the Johann Wolfgang Goethe University in Frankfurt, Germany.

Stefan Roth is a Software Engineer in IBM Research and Development in Kelsterbach, Germany. He works with the IBM Spectrum Scale development team on the graphical user interface. He joined IBM in 1996 and in the first years he developed software for IBM disk drives and semiconductor factories. Since 2008, he has worked on graphical user interfaces for various IBM storage products such as Scale Out Network Attached Storage, V7000 Unified, IBM Spectrum Scale, and Elastic Storage Server. He holds a technical college degree in Electrical Engineering from University of Applied Sciences, Darmstadt.

Liju Jose is an Information Developer with the IBM ISDL ID team. He is responsible for writing and editing the customer-facing documentation for various storage products such as IBM Spectrum Scale, IBM Elastic Storage™ Server, and IBM Storwize V7000 Unified. He has been with IBM for the last five years and holds a Bachelors degree in Physics and a Masters degree in Electronics Science from the Mahatma Gandhi University.
Thanks to the following people for their contributions to this project:

Larry Coyne
Ernest Keenan
International Technical Support Organization, Tucson Center

Sandeep Ramesh
Dietmar Fischer
Andreas Koeninger
Przemyslaw Podfigurny
Alifiya A Lohawalla
Dharmendra Rai
IBM Systems

Now you can become a published author, too!

Here’s an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks® publications in one of the following ways:

- Use the online Contact us review Redbooks form found at:
  ibm.com/redbooks
- Send your comments in an email to:
  redbooks@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:
  http://www.facebook.com/IBMRedbooks
Follow us on Twitter:
http://twitter.com/ibmredbooks

Look for us on LinkedIn:
http://www.linkedin.com/groups?home=&gid=2130806

Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

Stay current on recent Redbooks publications with RSS Feeds:
http://www.redbooks.ibm.com/rss.html
Overview

The Elastic Storage Server (ESS) GUI provides an easy way to configure and monitor various features that are available with the ESS system. The ESS GUI is a web application that runs on web browsers such as Chrome, Firefox, and Edge. It uses Java Script and Ajax technologies to enable smooth and desktop-like interfacing. Therefore, no client-side installation is required to use the GUI. Figure 1-1 shows the ESS GUI architecture.

The use cases for GUI are listed in the following sections of this chapter:

- Single-cluster support
- Role-based access control with GUI users
- Integration hub for configuration, health, and performance data
- Support matrix
1.1 Single-cluster support

The ESS GUI supports managing and monitoring a single cluster. The GUI must be installed on a cluster node and it does not need any specific license. This node can also be a client node. Nevertheless, the GUI must be able to contact all nodes in the cluster.

Due to performance reasons, the GUI and the collector must be installed on a separate Management Server (EMS). It is not recommended to install the GUI and the collector on a server that belongs to a storage server, which is also known as building block.

1.2 Role-based access control with GUI users

The GUI offers a role-based access model, which is not present in the core IBM GPFS™. Different roles are available to limit access to certain functions, from a read-only monitor role to a security administrator with full access on all GUI functions. GUI users are separate from the operating system users. The GUI comes with a built-in user database that allows you to register and manage users. It is also possible to configure the GUI to use an external authentication system such as LDAP or AD to authenticate the GUI users.

1.3 Integration hub for configuration, health, and performance data

You can perform the following important tasks through the ESS GUI:

- Monitor status of all servers, enclosures, and drives in an enclosure
- Monitor the performance of the system based on various aspects
- Monitor system health
- Create and manage file systems
- Create and manage filesets
- Create, manage, and schedule snapshots
- Create rules and policies for information lifecycle management
- Monitor active file management
- Monitor storage pools
- Monitor NSDs
- Monitor Vdisks and Pdisks
- Manage SMB service and SMB shares
- Manage NFS service and NFS exports
- Display and modify NFSv4ACL for files and directories
- Create users and define roles for the GUI users
- Define default, user, group, and fileset quotas
- Monitor the capacity details at various levels such as file system, pools, filesets, users, and user groups
- Configure event notifications through emails and SNMP
Collect diagnostic data to find the root cause and troubleshoot an issue reported in the system

- Monitor system health events
- Perform directed maintenance procedures to fix issues and optimize the system
- Monitor Transparent Cloud Tiering service
- Manage object storage, and create object users and roles

1.4 Support matrix

The GUI is supported on the following operating systems and IBM Spectrum Scale release levels.

1.4.1 Operating system levels

OS levels for GUI nodes are restricted. The following OS levels are supported:

- RHEL 7.1, 7.2, and 7.3 on x86, Power LE and BE, and IBM Z
  
  Clones such as CentOS and Scientific OS are also supported.

- SUSE Linux Enterprise Server 12 on x86 and Power LE, and IBM Z

The GUI nodes in the ESS cluster can be on any of the supported operating systems or hardware platforms. That is, an intermix of GUI nodes on various OS and hardware platforms are supported in a cluster.

1.4.2 IBM Spectrum Scale software requirements

The following list provides the IBM Spectrum Scale software requirements for GUI:

- The GUI is supported on the cluster that runs on IBM Spectrum Scale 4.2.0.0 or later. Issue the mmlsconfig command to see the value that is set for the minReleaseLevel attribute. The cluster needs to have a minimum release level of 4.2.0.

- All packages that are installed on the GUI node must be of the same release. For example, do not mix the 4.2.3 GUI rpm with a 4.2.2 base rpm. However, GUI PTFs and fixes can usually be applied without installing the corresponding PTF or fix of the base package. This is helpful if you want to resolve a GUI issue without changing anything on the base layer.

- The minimum release level of the cluster must be on the latest release level to display the latest features.

- GUI memory is set to 512 MiB.

- Collector memory requirements vary with number of elements that are being monitored.
Installation and configuration of the ESS GUI

ESS installs the necessary GUI RPMs during the installation process. For more information about the ESS installation process, see Install the ESS system at IBM Knowledge Center.

This chapter includes the following sections:
- Enabling performance monitoring tools in ESS GUI
- Setting up the component database
- Securing the ESS GUI
- Configuring GUI to use sudo wrapper
- Node classes used for the management GUI
- Modifying GUI property file
- Setting GUI preferences
2.1 Enabling performance monitoring tools in ESS GUI

Perform the following steps to enable performance monitoring tools in the GUI:

1. Generate performance collector in the External Management Server (EMS). The EMS must be part of the ESS cluster and node name must be the node name used in the cluster (for example: esm1-hs). Issue the following command:
   ```
   mmperfmon config generate --collectors ems1-hs
   ```

2. To set up the nodes in the `ems nodelclass` and `gss_ppc64 nodelclass` for performance monitoring, issue the following command:
   ```
   mmchnode --perfmon -N ems,gss_ppc64
   ```

   **Note:** This example is applicable if the cluster only consists of the EMS server and the ESS building blocks. To configure the sensors on the cluster nodes to send the monitored data to the collector, run the `mmchnode --perfmon` command and describe all the nodes that must be monitored in the `-N` attribute.

3. Capacity and fileset quota monitoring are not enabled in the GUI by default.
   a. To enable disk and fileset capacity data collection, issue the following command:
      ```
      mmperfmon config update GPFSDiskCap.restrict=<EMS nodename>
      GPFSDiskCap.period=<period in sec>
      ```
      ```
      mmperfmon config update GPFSFilesetQuota.restrict=<EMS nodename>
      GPFSFilesetQuota.period=<period in sec>
      ```
      The EMS specified in this example must be the name that is shown in the `mmlscluster` output.
   b. Verify whether the period is set correctly in the `/opt/IBM/zimon/ZIMonSensors.cfg` file. If it is not set correctly, verify whether the EMS is correctly provided. If the period is set to 86400 seconds (one day) and the task only runs in the `ems-hs` node (showing `ems1-hs.gpfs.net`) node, the system displays the output shown in Example 2-1.

   **Example 2-1**  Output when period is set to 86400 seconds
   ```
   { 
     name = "GPFSDiskCap"
     period = 86400
     restrict = "ems1-hs.gpfs.net"
   } 
   { 
     name = "GPFSFilesetQuota"
     period = 3600
     restrict = "ems1-hs.gpfs.net"
   }
   ```

   **Note:** To enable the fileset quota sensor, the file system quota checking must be enabled. You can check quota enablement and enable quota in the GUI page `Files → Quota` for each file system, or you can use the `mmchfs -Q` and `mmcheckquota` commands to do it.
4. Start sensors in the management server node and the I/O server nodes:

   ```bash
   systemctl start pmsensors
   xdsh gss_ppc64 "systemctl start pmsensors"
   ```

5. To ensure that the sensors are started when the server is restarted, issue the following command:

   ```bash
   systemctl enable pmsensors
   xdsh gss_ppc64 "systemctl enable pmsensors"
   ```

6. Start the performance collector in the management server node:

   ```bash
   systemctl start pmcollector
   ```

7. To ensure that the collector starts when the server is restarted, issue the following command:

   ```bash
   systemctl enable pmcollector
   ```

8. Enable and start gpfgui:

   ```bash
   systemctl enable gpfgui
   systemctl start gpfgui
   ```

9. To access the GUI, open your web browser and navigate to https://<host name>:443.

   The GUI then initializes, which might take a few minutes. After the initialization, the system setup wizard appears to complete the rest of the setup.

### 2.2 Setting up the component database

You can use the ESS GUI system setup wizard to set up the component database, which is the preferred method. Alternatively, you can set it up by using ESS commands. The ESS GUI system setup wizard is automatically started when logging in to GUI for the first time after the installation. Run the ESS GUI system setup and enter the rack locations of servers and enclosures, the IP or host name of the xCAT server, and other configuration information.

### 2.3 Securing the ESS GUI

You can secure the access to the GUI by using firewalls and HTTPS certificates.

#### 2.3.1 Firewall recommendations and supported ports

Configuring a firewall to allow access only from certain ports helps to secure EMS node that hosts the GUI. Different ports are used for securing installation GUI and management GUI.

Table 2-1 lists the ports that need to be used to secure GUI.

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Functions</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Management GUI</td>
<td>HTTP</td>
</tr>
<tr>
<td>443</td>
<td>Management GUI</td>
<td>HTTPS</td>
</tr>
<tr>
<td>47080</td>
<td>Management GUI</td>
<td>HTTP</td>
</tr>
<tr>
<td>47443</td>
<td>Management GUI</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>
Monitoring and Managing the IBM ESS Using the GUI

All nodes of the ESS cluster must be able to communicate with the GUI nodes through ports 80 and 443. If multiple GUI nodes are available in a cluster, the communication among those GUI nodes is carried out through port 443.

The port 80 is only open to receive events if an older version than 4.2.3 of GPFS is used. It cannot be used to access the GUI. Ports 443 is internally forwarded to 47443, and port 80 to 47080. This forwarding is done automatically by an iptables rule. The iptables rules are added when the gpfs gui service is started, and removed when it is stopped. Therefore, to access the GUI, not only ports 443 and 80 but also ports 47443 and 47080 must be opened.

Port 4444 is accessible only from the localhost.

### 2.3.2 Creating an HTTPS certificate

By default, the GUI uses a self-signed certificate for secure browsing. The certificate is stored in a Java keystore file (key.jks) that is created automatically by the installation process by using the security utility of IBM WebSphere® Liberty:

```
/opt/ibm/wlp/bin/securityUtility createSSLCertificate --server=gpfsgui
--password=Passw0rd --validity=36500
```

The created keystore file key.jks is saved in the following directory:

```
/opt/ibm/wlp/usr/servers/gpfsgui/resources/security
```

To use the self-signed certificate, the SSL communication and the keystore file must be defined in the `server.xml` file of the GPFS GUI profile of WebSphere Liberty. It is performed automatically by the installation process.

The marked lines shown in Example 2-2 are inserted into

```
/example 2-2 Lines added to /opt/ibm/wlp/usr/servers/gpfsgui/server.xml
```

```
<featureManager> ...
<feature>ssl-1.0</feature>
</featureManager>
<keyStore id="defaultKeyStore" password="{xor}Dz4sLChvLTs=" />
```

These lines enable the SSL communication and specify the keystore file with the default ID and the password. Note that you do not need to specify the name and location because the keystore has the default name (key.jks) and is stored in the default location.
If the keystore definition is correct, the certificate can be seen while accessing the GUI in the browser through HTTPS as shown in Figure 2-1.

![Certificate visible in the GUI](image)

**Figure 2-1  Certificate visible in the GUI**

### Replacing the HTTPS certificate

To replace the initial GUI certificate, modify the `server.xml` file and insert the path and password to the new Java keystore file in which the certificate is stored. Example 2-3 shows a sample.

**Example 2-3  Modifying the server.xml file**

```xml
<keyStore id="defaultKeyStore" password="<PasswordToNewKeystore>
  location="<PathWithNameToNewKeystore>" />
```

The GUI uses only the default SSL configuration. The ID must be `defaultKeyStore`, if no other SSL configuration is defined.

The password can be written in plain text or encoded in XOR or AES.

By default, IBM WebSphere Liberty searches for the keystore file in the `opt/ibm/wlp/usr/servers/gpfsgui/resources/security` directory.

After setting the new keystore definition, restart the GUI:

- RHEL7 or SLES12: `systemctl restart gpfsgui`
- RHEL6: `service gpfs gui restart`

### 2.3.3 Root privilege considerations for the ESS GUI

ESS 5.1 or later no longer runs the GUI WebSphere Java process as root, but as a user named `scalemgmt`. This change provides improved security because web applications running as root are vulnerable to security threats. The `scalemgmt` user is set up as a system account with no login privileges.

The GUI user still requires root privileges to perform the following tasks at the backend:

- Issue CLI commands.
- Bind to the privilege ports 80 (HTTP) and 443 (HTTPS). The `iptables` rule used in the system internally forwards port 80 to 47080 and port 443 to 47443.

The system automatically creates the `scalemgmt` user. It does not require any configuration to be performed by the user.
Enabling the scalemgmt user to monitor and manage the system through GUI

As the root privileges are not available to the GUI user, the system enables the scalemgmt user to run the CLI commands. The GUI uses sudo wrappers to run the CLI commands. The GUI installation adds the file /etc/sudoers.d/scalemgmt_sudoers that allows the scalemgmt user to run commands that match the wildcard “/usr/lpp/mmfs/bin/mm.”

2.4 Configuring GUI to use sudo wrapper

The GUI can be configured to run on a cluster where sudo wrappers are used. On such a cluster, the GUI process uses the sudo mechanism to run the CLI commands under the user name for which sudo wrappers were configured.

Make the following configuration changes to use the ESS GUI on a cluster where sudo wrappers are used:

1. Change GPFS_ADMIN=root to the user name that you configured as the sudo user in the gpfsgui.properties file that is at /usr/lpp/mmfs/gui/conf. For example, GPFS_ADMIN=gpfsguiadmin.

2. Issue the systemctl restart gpfsgui command to restart the GUI.

Passwordless SSH needs to be set up between the root user on the node where the GUI is running on all the remote nodes in the cluster. The SSH calls are equivalent to ssh gpfsguiadmin@destination-node. Therefore, it is not necessary to set up passwordless SSH between gpfsguiadmin users on any two nodes.

It is mandatory that the root user of the node where the GUI is running can perform passwordless SSH to any other node using the gpfsguiadmin user login. Therefore, unidirectional access from the GUI node to the remote nodes as gpfsguiadmin user is enough.

**Note:** If sudo wrappers are enabled on the cluster but GUI is not configured for it, the system raises an event.

2.5 Node classes used for the management GUI

The GUI automatically creates the following node classes during the installation:

- GUI_SERVERS: Contains all nodes with a server license and all the GUI nodes
- GUI_MGMT_SERVERS: Contains all GUI nodes
- GUI_RG_SERVERS: Contains all ESS building block nodes

Each node on which the GUI services are started is added to these node classes.

**Note:** These node classes must not be modified manually because the GUI regularly checks and possibly updates the node class members.
2.6 Modifying GUI property file

The GUI stores some settings that can be adjusted in the properties file at:
/usr/lpp/mmfs/gui/conf/gpfsgui.properties

The properties file is not maintained over upgrades, so modifications to this file need to be reapplied when the GUI is upgraded. Typically there is no need to update this file.

The following list provides the important settings that can be done in the properties file:

- **KEEP_LOG_INTERVAL=168**
  - Number of hours that the logs must be kept before they are discarded:
    - JDBC_DB_URL=jdbc:postgresql://localhost:5432/postgres

- **MAX_ALLOWED_TIME_DIFF=60**
  - The maximum time difference in seconds that is allowed between the GUI node and any other cluster node before an event is triggered. It is important to synchronize the time across the cluster to ensure functioning of various features that are configured in the system. You can use NTP or some other similar function to synchronize time across the cluster:
    - ZIMonAddress=localhost, ZIMonPort=9084
  - The host name and port where the performance collector service is running. The only supported configuration is hosting the collector on the node where the GUI is running:
    - GPFS_ADMIN=root

On clusters where sudo wrappers are enabled, the GUI needs to know the user name of the sudo user that was enabled for the remote login to other nodes in the cluster. Change this setting if sudo wrappers are enabled on the cluster.

2.7 Setting GUI preferences

In contrast to the GUI properties file, the GUI preferences are shared between two GUIs through CCR and persist even after uninstalling or upgrading the GUI.

The GUI preferences are stored in the following JSON files at the /var/lib/mmfs/gui directory:

- **notification.json** (in CCR_gui.notification)
  - Notification-related objects such as the email server configuration.

- **settings.json** (in CCR_gui.settings)
  - For general setting objects, like custom attributes, acl templates, policies, and thresholds.

- **user.repo.json** (in CCR_gui.user.repo)
  - For all user, group, and password-related objects.

- **snapshots.json** (in CCR_gui.snapshots)
  - For snapshot-related objects.

- **dashboards.json** (in CCR_gui.dashboards)
  - Dashboard-related data.
Understanding the GUI options

This chapter provides an overview of the basic options available in the GUI. It includes the following sections:

- Login
- Navigation
- Header area
- Assistance for understanding the features associated with a GUI page
3.1 Login

The users who are created by using the Access → GUI Users page can log in to the GUI (Figure 3-1). The default user name and password to access the GUI are admin and admin001.
3.2 Navigation

You can navigate to the various GUI pages through the navigation menu on the left side of the GUI page (Figure 3-2). Each GUI page has a unique URL that you can use to directly access the page, bookmark pages, and start the GUI in-context.

Figure 3-2  Navigation pane of the GUI

Note: The Object and Protocols menus are displayed only when these features are enabled in the cluster.
3.3 Header area

The header area provides the following details:

- List of events of type “tips”. The tips events give recommendations to the user to avoid certain issues in the future (Figure 3-3).

![Figure 3-3 Tips menu](image)

- Health status of various services. Only the events that are in the Warning or Critical status are displayed. Figure 3-4 shows the Health status menu.

![Figure 3-4 Health Status menu](image)

- Link to the context-sensitive help page. This help file provides detailed explanation of the features that are associated with the page. The context-sensitive help files are available in the Help menu, which is placed in the upper right corner of the GUI page (Figure 3-5).

![Figure 3-5 Help menu](image)
The link to the IBM Spectrum Scale Knowledge Center is also available in the Help menu, which is placed in the upper right corner of the GUI page.

Currently logged in user name and options to log out and modify password are available in the User menu (Figure 3-6).

Figure 3-6   Log in menu

3.4 Assistance for understanding the features associated with a GUI page

The following three levels of assistance are available for the GUI users:

1. Hover help: When you hover the mouse over the tiny question mark next to the field label, the system displays a brief description of the feature that is associated with that field. Hover help is available only for the important and complex fields.

2. Context-sensitive help: Provides a detailed explanation of the features that are associated with the page. The context-sensitive help files are available in the Help menu, which is in the upper right corner of the GUI page.

3. IBM Knowledge Center: This is the third level of information where the users can find entire details of the product. The link to the IBM Spectrum Scale Knowledge Center is also available in the Help menu, which is in the upper right corner of the GUI page.
Chapter 4. Monitoring options available in the GUI

This chapter provides the various monitoring options that are available with the GUI. It includes the following sections:

- Monitoring hardware details
- Monitoring performance
- Monitoring capacity
- Monitoring system health
- Monitoring nodes
- Monitoring Transparent Cloud Tiering
- Monitoring active file management
- Monitoring file systems
- Monitoring filesets
- Monitoring pools
- Monitoring NSDs
4.1 Monitoring hardware details

From the Monitoring → Hardware and Monitoring → Hardware Details windows in the GUI, you can view the status of all servers, enclosures, and drives in an enclosure.

Figure 4-1 shows the Hardware window in the GUI.

![Hardware window in ESS GUI](image)

Click a server or enclosure to view the details of that particular hardware component. You can also run a procedure to replace one or more broken drives within an enclosure.

You can also view the free and used native RAID raw capacity. The raw capacity includes the capacity that is required for RAID modes, so the actual usable data capacity is less than what is displayed in the GUI.

4.1.1 Servers

The servers provide the GPFS file system cluster nodes to store the data. The server (or node) acts as an IBM Spectrum Scale RAID storage controller. The disks that are provided through the disk enclosures are attached to the servers through serial-attached SCSI (SAS).

All servers host the command-line interface, but the GUI is installed only on the servers that are either called as external management server (EMS) or just management servers. Besides GUI, the management server also hosts the performance monitoring collectors and xCAT. You can configure only one xCAT in the EMS.

An Elastic Storage Server (ESS) system consists of one or more building blocks. Each building block consists of two servers and one or more disk enclosures.

4.1.2 Disk enclosures

The disk enclosures contain disks that are used to store the GPFS file systems. The disk enclosures are JBODs whose disks are attached to both the servers through a SAS.
Use the Filter option in the Monitoring → Hardware Details window to filter the servers and enclosures based on keywords. You can also filter the unhealthy devices by selecting the Display unhealthy devices option.

### 4.1.3 Edit rack components

The Edit Rack Components option available in the Actions menu of the Monitoring → Hardware window helps to discover new servers and enclosures, and edit rack locations for all servers and enclosures.

### 4.1.4 Replace broken disks

If there are broken disks with the status Replaceable, you can use the corresponding directed maintenance procedure to replace the broken disks. To replace broken links, select Replace Broken Disks from the Actions menu in the Monitoring → Hardware window. You can also run this fix procedure from the Monitoring → Events and Storage → Physical window.

### 4.2 Monitoring performance

You can use the ESS GUI to monitor the status and historical trends of key indicators. You can then use this data to help make decisions more quickly and efficiently.

Table 4-1 lists the performance monitoring options that are available in the ESS GUI.

<table>
<thead>
<tr>
<th>GUI window</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring → Statistics</td>
<td>Displays performance of system resources and file and object storage in various performance charts. You can select the required charts and monitor the performance based on the filter criteria. It is possible to pan and zoom charts to see detailed metrics and past intervals.</td>
</tr>
<tr>
<td>Monitoring → Dashboards</td>
<td>Provides an easy to read and real-time user interface that shows a graphical representation of the status and historical trends of key performance indicators. This feature helps the users to make decisions quickly and easily.</td>
</tr>
<tr>
<td>Monitoring → Nodes</td>
<td>Provides an easy way to monitor the performance, health status, and configuration aspects of all available nodes in the ESS cluster.</td>
</tr>
<tr>
<td>Files → File Systems</td>
<td>Provides a detailed view of the performance and health aspects of individual file systems.</td>
</tr>
<tr>
<td>Storage → NSDs</td>
<td>Provides a detailed view of the performance and health aspects of individual Network Shared Disks (NSDs).</td>
</tr>
<tr>
<td>Storage → Pools</td>
<td>Provides a detailed view of the performance and health aspects of storage pools.</td>
</tr>
</tbody>
</table>
The performance and capacity data are collected with the help of the following two components (Figure 4-2):

- **Sensor**: The sensors are placed on all the nodes and they share the data with the collector. The sensors run on any node that is required to collect metrics.

- **Collector**: Collects data from the sensors. The metric collector must run on at least one node to gather metrics from all the nodes that are running the associated sensors. The metrics are stored in a database on the collector node. The collector ensures aggregation of data after data gets older. The collector can run on any node in the system. You can configure multiple collectors in the system. To configure performance monitoring through GUI, it is mandatory to configure a collector on each GUI node. Figure 4-2 illustrates the performance monitoring configuration for GUI.

The `mmperfmon` command can be used to configure the performance data collection through CLI. The GUI displays a subset of the available metrics that are available in the performance monitoring tool.

When there are multiple collectors and GUI nodes in the cluster for high-availability configuration, you can configure the performance monitoring in two ways:

- Each sensor sends its data to one or two collectors but all the collectors are in synchronization. This mode is called federated mode.

- The collectors are not synchronized. In this case, each sensor needs to send its data to every collector as shown in Figure 4-2. It is not recommended to use this mode to avoid performance issues.
You can configure the system to monitor the performance of the following functional areas in the system:

- Network
- System resources
- Native RAID
- NSD server
- IBM Spectrum Scale client
- NFS
- SMB
- Object
- CTDB
- Transparent Cloud Tiering
- AFM
- Waiters

**Note:** The functional areas such as NFS, SMB, Object, CTDB, and Transparent Cloud Tiering are available only if the feature is enabled in the system.

### 4.2.1 Display options in the Statistics page of the GUI

The **Monitoring → Statistics** page is used for selecting the attributes based on which the performance of the system are monitored and comparing the performance based on the selected metrics. You can also use this page to monitor capacity. The customized charts that are marked as favorite charts become available for selection when you add widgets in the dashboard. You can display either one or two charts at a time in the Statistics page.
The predefined performance charts and metrics help in investigating every node or any particular node that is collecting the metrics. Figure 4-3 shows various configuration options that are available in the Statistics window of the management GUI (Figure 4-3).

Predefined charts are available for selection from predefined chart list. You can add additional charts to the predefined list by using the Favorites button.

**Display options in performance charts**

The charting section displays the performance details based on various aspects. The GUI provides a rich set of controls to view performance charts. You can use these controls to perform the following actions on the charts that are displayed in the page:

- Zoom in the chart by using the mouse wheel or resizing the timeline control. The y-axis can be automatically adjusted during zooming.
- Click and drag the chart or the timeline control at the bottom. The y-axis can be automatically adjusted during panning.
- Compare charts side by side. You can synchronize y-axis and bind x-axis. To modify the x- and y-axes of the chart, click the configuration symbol next to the Statistics title and select the options that you want.
- Link the timelines of the two charts together by using the display options that are available.
- The Dashboard page helps to access all charts, which are either predefined or custom-created favorites.
Selecting performance and capacity metrics

To monitor the performance and capacity of the system, use the predefined charts or select the appropriate metrics and create a chart (Figure 4-4).

Figure 4-4  List of predefined charts in the Statistics window
Create customized performance charts
Complete the following steps to create performance charts:

1. Click **Edit** in the menu to view the modification options, as shown in Figure 4-5.

![Figure 4-5 Options to create a performance chart on the Statistics page](image)

The performance metrics are grouped under the combination of resource types and aggregation levels. The resource types determine the area from which the data is taken to create the performance analysis. The aggregation level determines the level at which the data is aggregated. The aggregation levels that are available for selection vary based on the resource type. Sensors are configured against each resource type.

2. Select the required resource type in the **Resource type** field.
3. Select the aggregation level in the **Aggregation level** field.
4. Select the resource that you want to monitor.
5. Select the time frame for the performance data display.
6. Select the required metrics to be displayed on the performance chart.
7. Click **Apply** to apply the changes or **Close** to cancel the process.
4.2.2 Using dashboard to view performance charts

The **Monitoring → Dashboard** window provides an easy to read, single page, and real-time user interface that provides a quick overview of the system performance.

The dashboard consists of several dashboard widgets and the associated favorite charts that can be displayed within a chosen layout. Currently, the following important widget types are available in the dashboard:

- Statistics
- File system capacity by fileset
- System health events
- System overview
- Filesets with the largest growth rate in last week
- Timeline

Figure 4-6 highlights the configuration options that are available in the edit mode of the dashboard.

![Dashboard page in the edit mode](image)

**Layout options**

The highly customizable dashboard layout options help adding and removing widgets and change its display options. Select **Layout Options** from the menu that is available in the upper right corner of the Dashboard GUI page to change the layout options. While selecting the layout options, you can either select the basic layouts that are available for selection or create layout by selecting an empty layout as the starting point.

Some predefined dashboard layouts are delivered with the product, but the user can create new dashboards. After new dashboards are created, they are available to any other GUI user. You can also modify and save a dashboard so that it can be used by other users. Select the **Create Dashboard** and **Delete Dashboard** options from the menu that is available in the upper right corner of the Dashboard page to create and delete dashboards. If several GUIs are running by using CCR, saved dashboards are available on all nodes.
When you open the ESS GUI after the installation or upgrade, you can see the default dashboards that are included with the product. You can further modify or delete the default dashboards to suit your requirements.

**Widget options**

Several dashboard widgets can be added in a selected dashboard layout. Select the **Edit Widgets** option from the menu that is available on the upper right corner of the Dashboard GUI page to edit or remove widgets in the dashboard. You can also modify the size of the widget in the edit mode. Use the **Add Widget** option that is available in the edit mode to add widgets in the dashboard.

The widgets with type **Performance** list the charts that are marked as favorite charts in the Statistics page of the GUI. Favorite charts along with the predefined charts are available for selection when you add widgets in the dashboard.

To create favorite charts, click the **Star** icon that is placed next to the chart title on the **Monitoring → Statistics** page.

### 4.2.3 Monitoring waiters

The metrics related to waiters are collected on the cluster level. Different wait time thresholds such as 0.1s, 0.2s, 0.5s, 1s, 30s, and 60s can be selected. You can create charts to monitor the waiters by selecting **Waiters** as the resource type in the **Monitoring → Statistics** page.

### 4.3 Monitoring capacity

You can monitor the capacity of file system, pools, filesets, users, and user groups.

The historical capacity data collection for file systems, pools, and filesets depend on the correctly configured data collection sensors for fileset quota and disk capacity. The capacity data collection is configured by default. You can also use the `mmperfmon` command to enable data collection for capacity data.

The following topics describe the capacity monitoring options that are available in the GUI.

#### 4.3.1 Monitoring → Capacity window

The **Monitoring → Capacity** window provides predefined capacity reports for file systems, pools, filesets, users, and groups. Although capacity information of file systems, pools, and filesets is available in the respective areas of the GUI, the **Monitoring → Capacity** window is the only place where information about used capacity per user or group is available.

For filesets, users, and user groups, you can see the total capacity and whether quotas are set for these objects. For each fileset, you can see a used capacity trend over a 30-day time period as a sparkline. It also displays the percentage of soft limit and hard limit usage. When the hard limit is exceeded, no more files belong to the respective user, user group, or fileset can be written. However, exceeding the hard limit allows a certain grace period before disallowing more file writes.
Soft and hard limits for disk capacity are measured in units of kilobytes (KiB), megabytes (MiB), or gigabytes (GiB). This information is automatically collected once an hour by performance monitoring collector. Use Files → Quotas to change the quota limits. The file system implements quotas to control and monitor file system usage by users and groups across the system.

If some filesets are not listed in the filesets section, the system displays a note at the bottom of the page that shows the reason for this issue. The issue is either because the quota is disabled for some filesets or the list of filesets is outdated.

You can also view capacity values of file systems and filesets on the corresponding panes.

### 4.3.2 Using information from the Monitoring → Statistics window

The Monitoring → Statistics page allows you to create customized capacity reports for file systems, pools, and filesets. You can store these reports as favorites and add them to the dashboard as well.

### 4.3.3 Capacity information for file systems, pools, NSDs, and filesets

The dedicated GUI windows combine information about configuration, health, performance, and capacity in one place. The following GUI windows provide the corresponding capacity views:

- Files → File Systems
- Files → Filesets
- Storage → Pools
- Storage → NSDs

### 4.4 Monitoring system health

Table 4-2 lists the system health monitoring options that are available in the ESS GUI.

<table>
<thead>
<tr>
<th>GUI window</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring → Hardware</td>
<td>Displays the status of all servers, enclosures, and drives in an enclosure. Click a server or enclosure to view the details of that particular hardware component.</td>
</tr>
<tr>
<td>Monitoring → Hardware Details</td>
<td>Displays status and details of the servers and enclosures that are a part of the system. Click any system component to view its details. This view also provides a text search and filtering for unhealthy hardware.</td>
</tr>
<tr>
<td>Monitoring → Events</td>
<td>Lists the events that are reported in the system. You can monitor and troubleshoot errors on your system on the Events page.</td>
</tr>
<tr>
<td>Monitoring → Tips</td>
<td>Lists the events of type “tips”. The tip events give recommendations to the user about certain events that might occur in the future.</td>
</tr>
<tr>
<td>Home</td>
<td>Provides the overall system health of the ESS system.</td>
</tr>
</tbody>
</table>

Table 4-2 System health monitoring options available in ESS GUI
<table>
<thead>
<tr>
<th>GUI window</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring → Nodes</td>
<td>Displays the health status of nodes and lists the events reported at the node level.</td>
</tr>
<tr>
<td>Files → File Systems</td>
<td>Displays the health status of file systems and lists the events reported at the file system level.</td>
</tr>
<tr>
<td>Files → Filesets</td>
<td>Displays the health status of filesets and lists the events reported at the fileset level.</td>
</tr>
<tr>
<td>Files → Transparent Cloud Tiering</td>
<td>Lists the events reported for the Transparent Cloud Tiering service. The GUI displays this page only if the Transparent Cloud Tiering feature is enabled in the system.</td>
</tr>
<tr>
<td>Files → Active File Management</td>
<td>Displays health status and lists events reported for AFM cache relationship, AFM disaster recovery (AFMDR) relationship, and gateway nodes.</td>
</tr>
<tr>
<td>Storage → Pools</td>
<td>Displays health status and lists events reported for storage pools.</td>
</tr>
<tr>
<td>Storage → NSDs</td>
<td>Displays health status of NSDs and lists the events reported at the NSD level.</td>
</tr>
<tr>
<td>Health indicator that is available in the upper right corner of the GUI</td>
<td>Displays the number of events with warning and critical status specific to each component.</td>
</tr>
<tr>
<td>System overview widget in the Monitoring → Dashboard window</td>
<td>Displays the number of events reported against each component.</td>
</tr>
<tr>
<td>System health events widget in the Monitoring → Dashboard window</td>
<td>Provides an overview of the warning and error events that are reported in the system.</td>
</tr>
<tr>
<td>Timeline widget in the Monitoring → Dashboard window</td>
<td>Displays the events that are reported in a selected time frame on the selected performance chart.</td>
</tr>
<tr>
<td>Storage → Physical</td>
<td>Displays the health information and properties of physical disks (pdisks) and the corresponding declustered arrays.</td>
</tr>
<tr>
<td>Storage → Volumes</td>
<td>Displays the health information and properties of logical volumes (vdisks) and the corresponding declustered arrays.</td>
</tr>
</tbody>
</table>
4.5 Monitoring nodes

The **Monitoring → Nodes** window options to monitor the performance, health status, and configuration aspects of the respective components (Figure 4-7).

The properties of a node display the status of various CES services such as Object, NFS, and SMB as well as the authentication status of these services if they are enabled. It also displays other details such as network status, information about attached NSDs and file systems, and so on.

4.5.1 Nodes tables

The following three different specific nodes tables that provide a pre-filtered view on nodes with specific information:

- **All nodes**
  Shows all nodes in the cluster and provides information about node roles, services, node health, and basic performance information about system and IBM Spectrum Scale client level.

- **NSD server nodes**
  Shows all nodes that are NSD servers with specific performance information related to NSDs. If there are no NSD servers in the cluster, this table is not displayed.

- **Protocol nodes**
  Shows all protocol nodes. Specific performance and health information related to protocol services are displayed in this table. If there are no protocol nodes in the cluster, this table is not displayed.

The three different tables can be customized individually by adding or removing columns by using the **Customize Columns** action.
You can use the Set Attributes option that is available in the Actions menu to set the node attributes such as site, room, and rack on any of the views. You can set attributes of multiple nodes at a time. The attributes can be used to filter nodes in the nodes view.

The health status information of each service and component can have the following values:

- **Healthy**: The component is working as expected.
- **Disabled**: The component is not enabled.
- **Suspended**: When a CES is in the suspended state, most components also report suspended.
- **Starting**: The component (or monitor) has been recently started. This state is a transient state that is updated after the startup is complete.
- **Unknown**: Something is preventing the monitoring from determining the state of the component.
- **Stopped**: The component was intentionally stopped. This situation might happen briefly if a service is being restarted due to a configuration change. It might also happen if a user issues the `mmces service stop protocol` command for a node.
- **Degraded**: A problem occurred with the component but not a complete failure. This state does not cause the CES addresses to be reassigned.
- **Failed**: The monitoring detected a significant problem with the component that means it is unable to function correctly. This state causes the CES addresses of the node to be reassigned.
- **Dependency failed**: This state implies that a component has a dependency that is in a failed state. For example, NFS or SMB service show `Dependency failed` if authentication is failed.

### 4.5.2 Performance monitoring of nodes

The Nodes page provides the following options to analyze the performance of nodes:

- A quick view that gives the number of nodes in the system, and the overall performance of nodes based on CPU and memory usages. You can access this view by clicking the Expand button next to the title of the page. You can close this view if not required.

Many graphs in the overview show the three nodes that have the highest average performance metric over a past period. These graphs are refreshed regularly. The refresh intervals of the top three entities depend on the displayed time frame as follows:

- Every minute for the 5-minute time frame
- Every 15 minutes for the 1-hour time frame
- Every six hours for the 24 hour time frame
- Every two days for the 7 days time frame
- Every seven days for the 30 days time frame
- Every four months for the 365 days time frame

- A Nodes table that displays many different performance metrics. To find nodes with extreme values, you can sort the values displayed in the nodes table by different performance metrics. Click the performance metric in the table header to sort the data based on that metric.

You can select the time range that determines the averaging of the values that are displayed in the table and the time range of the charts in the overview from the time range selector, which is placed in the upper right corner.
The metrics in the table do not update automatically. You can use the Refresh button above the table to refresh the table content with more recent data.

- A detailed view of the performance and health aspects of individual nodes is available on the Nodes page. Select the node for which you need to view the performance details and select View Details. The system displays various performance charts on the right pane.

The detailed performance view helps to drill-down to various performance aspects. The following list provides the performance details that can be obtained from each tab of the performance view:

- The Overview tab provides performance chart for the following data:
  - Client IOPS
  - Client data rate
  - Server data rate
  - Server IOPS
  - Network
  - CPU
  - Load
  - Memory

- The Events tab can be used to monitor the events that are reported in the node. Similar to the Events page, you can also perform operations like marking events as read and running fix procedure from the Events tab. Only the current issues are displayed in this view. The Monitoring → Events page displays the entire set of events that are reported in the system.

- The File Systems tab provides performance details of the file systems that are mounted on the node. The file system's read or write throughput, average read or write transactions size, and file system read or write latency are also available.

  You can also mount or unmount individual file systems or multiple file systems on the selected node. For more details, see 5.2, “Mounting a file system through GUI” on page 48 and 5.3, “Unmounting a file system through GUI” on page 49.

- The NSDs tab provides the status of the disks that are attached to the node. The NSD tab is displayed only when the node is configured as an NSD server.

- The SMB and NFS tabs provide the performance details of the SMB and NFS services that are hosted on the node. These tabs appear in the chart only when the node is configured as a protocol node.

- The Network tab displays the network performance details.

- The AFM tab displays the details of the AFM and AFM DR relationships for which the node is configured as a gateway node.

- The Properties tab provides an overview of the node-related attributes. You can also use the Prevent file system mounts option to allow or prevent file systems from mounting the node.
4.6 Monitoring Transparent Cloud Tiering

Transparent Cloud Tiering is a separately installable feature of ESS that provides a native cloud storage tier. It allows data center administrators to free up on-premises storage capacity by moving cooler data to the cloud storage. This process helps to reduce capital and operational expenditures.

The Transparent Cloud Tiering feature uses the existing Information Lifecycle Management (ILM) policy query language semantics. The system administrators can define policies to tier data to a cloud storage.

On an ESS cluster with multiple storage tiers configured, this external cloud storage can be used as the cooler storage tier to store infrequently accessed data from a cool storage pool. For performance reasons, avoid moving any active or hot data to this external storage pool because it drives excessive data traffic that results in delays and application timeouts.

The following are the core functions of the Transparent Cloud Tiering service (Figure 4-8):

- **Migrate**: Migrates the specified files or filesets to the cloud storage tier.
- **Recall**: Recalls the specified files or filesets from the cloud storage tier.
- **Remove**: Deletes the cloud storage tier.

The **Files → Transparent Cloud Tiering** window provides performance and health details of the Transparent Cloud Tiering service through various charts available under these tabs:

- **Overview**: Displays the aggregated data of all file systems and nodes that are associated with a particular cloud provider.
- **Events**: Displays events that are associated with the Transparent Cloud Tiering service.
- **Nodes**: Lists the node on which the cloud services are installed. The cloud services such as Transparent Cloud Tiering, Cloud Data Sharing, or both can be activated on this node.
- **File Systems**: Displays the details of the file systems that are mapped with the Transparent Cloud Tiering service.
You can select either a line chart or a bar chart to display the details. The line chart shows an average rate, whereas the bar chart shows aggregated data. For example, the aggregate view can be used by administrators to see how much data was transferred in one day.

### 4.7 Monitoring active file management

The **Files → Active File Management** window provides an easy way to monitor the performance, health status, and configuration aspects of the AFM and AFM DR relationships in the ESS cluster. It also provides details of the gateway nodes that are part of the AFM or AFM DR relationships.

The GUI combines the following sources on the cache or primary side:

- AFM sensors from the performance monitoring tool
- Health status and events from the mmhealth component
- AFM configuration information

Figure 4-9 illustrates the AFM GUI architecture.
Figure 4-10 shows the Active File Management window in the GUI.

The following options are available to monitor AFM and AFM DR relationships and gateway nodes:

- A quick view that gives the details of top relationships between cache and home sites in an AFM or AFM DR relationship. It also provides performance of gateway nodes by used memory and number of queued messages. The graphs that are displayed in the quick view are refreshed regularly. The refresh intervals depend on the selected time frame. The following list shows the refresh intervals corresponding to each time frame:
  - Every minute for the 5-minute time frame
  - Every 15 minutes for the 1-hour time frame
  - Every 6 hours for the 24 hours time frame
  - Every two days for the 7 day time frame
  - Every seven days for the 30 day time frame
  - Every four months for the 365 day time frame

- Different performance metrics and configuration details in the tabular format. The following tables are available:
  - Cache
    Provides the information about configuration, health, and performance of the AFM feature that is configured for data caching and replication.
  - Disaster Recovery
    Provides information about configuration, health, and performance of AFM DR configuration in the cluster.
  - Gateway Nodes
    Provides details of the nodes that are designated as the gateway node in the AFM or AFM DR configuration.
To find an AFM or AFM DR relationship or a gateway node with extreme values, you can sort the values that are displayed on the table by different attributes. Click the performance metric in the table header to sort the data based on that metric.

You can select the time range that determines the averaging of the values that are displayed in the table and the time range of the charts in the overview from the time range selector, which is in the upper right corner. The metrics in the table do not update automatically. The Refresh button above the table allows you to refresh the table with more recent data.

- A detailed view of the performance and health aspects of the individual AFM or AFM DR relationship or gateway node. To see the detailed view, either double-click the row that lists the relationship or gateway node of which you need to view the details or select the item from the table and click View Details. The following details are available for each item:

  - Cache
    - Overview: Provides number of available cache inodes and displays charts that show the amount of data that is transferred, data backlog, and memory used for the queue.
    - Events: Provides details of the system health events reported for the AFM component.
    - Snapshots: Provides details of the snapshots that are available for the AFM fileset. The snapshots are taken for back-up purposes. The snapshot taken in the AFM cache relationship is called peer snapshot. It functions in the same way as the GPFS snapshots. When a snapshot is taken on the cache site, it also propagates the request to take a snapshot of the home.
    - Gateway Nodes: Provides details of the nodes that are configured as gateway node in the AFM configuration.

  - Disaster Recovery
    - Overview: Provides the number of available primary inodes and displays charts that show the amount of data that is transferred, data backlog, and memory used for the queue.
    - Events: Provides details of the system health events reported for the AFM component.
    - Snapshots: Provides details of the snapshots that are available for the AFM fileset. The snapshots taken in the AFM DR are called recovery point objective (RPO) snapshots. These are peer snapshots that are taken at the same time on both the primary and the secondary sites.
    - Gateway Nodes: Provides details of the nodes that are configured as gateway node in the AFM configuration.

### 4.7.1 Gateway nodes

The details of gateway nodes are available under the following tabs. The same details are also available on the Monitoring → Nodes page.

- The Overview tab provides performance chart for the following:
  - Client IOPS
  - Client data rate
  - Server data rate
  - Server IOPS
– Network
– CPU
– Load
– Memory

The Events tab provides details of the events that are reported in the node. Similar to the Events page, you can also perform the operations like marking events as read and running fix procedure from this events view. Only current issues are shown in this view. The Monitoring → Events page displays the entire set of events that are reported in the system.

The File Systems tab provides performance details of the file systems mounted on the node. The file systems’ read or write throughput, average read or write transactions size, and file system read or write latency are also available.

Use the Mount File System or Unmount File System option to mount or unmount individual file systems or multiple file systems on the selected node. The nodes on which the file system need to be mounted or unmounted can be selected individually from the list of nodes or based on node classes.

The NSDs tab provides status of the disks that are attached to the node. The NSD tab appears only if the node is configured as an NSD server.

The SMB and NFS tabs provide the performance details of the SMB and NFS services that are hosted on the node. These tabs appear in the chart only if the node is configured as a protocol node.

The AFM tab provides details of the configuration and status of the AFM and AFM DR relationships for which the node is configured as the gateway node.

The Network tab displays the network performance details.

The Properties tab displays the basic attributes of the node. You can use the Prevent file system mounts option to specify whether you can prevent file systems from mounting on the node.
4.8 Monitoring file systems

The Files → File Systems window provides options to monitor the performance, health status, and configuration aspects of all available file systems in the ESS cluster (Figure 4-11).

![File Systems window]

The following options are available to analyze file system performance:

- A quick view that gives the number of protocol nodes, NSD servers, and NSDs that are part of the available file systems that are mounted on the GUI server. It also provides overall capacity and total throughput details of these file systems. You can access this view by clicking the Expand button next to the title of the page. You can close this view if it is not required.

  The graphs displayed in the quick view are refreshed regularly. The refresh intervals depend on the displayed time frame as follows:
  - Every minute for the 5-minute time frame
  - Every 15 minutes for the 1-hour time frame
  - Every six hours for the 24 hour time frame
  - Every two days for the 7 day time frame
  - Every seven days for the 30 day time frame
  - Every four months for the 365 days time frame

- A file systems table that displays many different performance metrics. To find file systems with extreme values, you can sort the values displayed in the file systems table by using the different performance metrics. Click the performance metric in the table header to sort the data based on that metric.

  You can select the time range that determines the averaging of the values that are displayed in the table and the time range of the charts in the overview from the time range selector, which is in the upper right corner. The metrics in the table do not update automatically. You can use the Refresh button above the table to refresh the table with more recent data.
A detailed view of the performance and health aspects of individual file systems. To see the detailed view, either double-click the file system for which you need to view the details or select the file system and click **View Details**.

The detailed performance view helps to drill-down to various performance aspects. The following list provides the performance details that can be obtained from each tab of the performance view:

- **Overview**: Provides an overview of the file system performance.
- **Events**: System health events reported for the file system.
- **NSDs**: Details of the NSDs that are part of the file system.
- **Pools**: Details of the pools that are part of the file system.
- **Nodes**: Details of the nodes on which the file system is mounted.
- **Filesets**: Details of the filesets that are part of the file system.
- **NFS**: Details of the NFS exports created in the file system.
- **SMB**: Details of the SMB shares created in the file system.
- **Object**: Details of the IBM Spectrum Scale object storage on the file system.
- **Properties**: Provides details of the file system attributes. You can also use the **Automatic mount** option to configure the automatic mount mode of the file system.

### 4.9 Monitoring filesets

The **Files → Filesets** window provides an easy way to monitor the performance, health status, and configuration aspects of all available filesets in the ESS cluster (Figure 4-12).

The following options are available to view the fileset details:

- A fileset table that displays the details of the filesets that are available in the system. You can sort the values displayed in the filesets table by different attributes. Click the column header in the table to sort the data based on that attribute.
A detailed view of the performance and health aspects of individual filesets. To see the detailed view, you can either double-click the fileset for which you need to view the details or select the fileset and click View Details.

The detailed view helps to drill-down to various performance, health, and configuration aspects. The following list provides the details that can be obtained from each tab of the performance view:

- Overview: Provides an overview of the fileset capacity, inodes, and quota limits.
- Events: System health events reported for the fileset.
- NFS: Details of the NFS exports created in the fileset.
- SMB: Details of the SMB shares created in the fileset.
- Object: Details of the object storage policy that is mapped to the fileset. When objects are uploaded to a container, they are stored in the fileset that is associated with the container’s storage policy.
- Properties: Provides details of the fileset attributes.

### 4.10 Monitoring pools

The Storage \(\rightarrow\) Pools window provides options to monitor the performance, health status, and configuration aspects of the all available pools in the ESS cluster. The GUI shows a table of all internal pools in a cluster (Figure 4-13).

![Pools window in the detailed view](image)

The systems pool contains metadata for the whole file system. Therefore, the GUI shows separate lines for the system pool depending on the usage type of the NSDs in the system pool. If the system pool of a file system is used only for storing metadata, the GUI shows one row of details.

If the system pool consists of NSDs that are of type `metadataOnly` and `dataOnly`, the GUI shows two rows with separate data. The detailed view for this pool also shows separate performance and capacity information in the overview and NSD sections.
The following options are available to analyze the pools' performance:

- A pools table that displays many different performance metrics. To find pools with extreme values, you can sort the values that are displayed in the pools table by different performance metrics. Click the performance metric in the table header to sort the data based on that metric.

  You can select the time range that determines the averaging of the values that are displayed in the table and the time range of the charts in the overview from the time range selector, which is in the upper right corner. The metrics in the table do not update automatically. The **Refresh** button above the table allows you to refresh the table with more recent data.

- A detailed view of the performance and health aspects of individual pools. To see the detailed view, either double-click the pool for which you need to view the details or select the pool and click **View Details**.

  The detailed performance view helps to drill-down to various performance aspects. The following list provides the performance details that can be obtained from each tab of the performance view:
  - **Overview**: Provides an overview of the pools performance.
  - **Events**: Provides details of the system health events reported for the file system.
  - **NSDs**: Details of the NSDs that are part of the file system.
  - **Properties**: Overview of the pool's properties.

### 4.11 Monitoring NSDs

The **Storage → NSDs** page provides an easy way to monitor the performance, health status, and configuration aspects of all Network Shared Disks (NSDs) that are available in the ESS cluster (Figure 4-14).

An NSD is a logical grouping of storage disks in a network on file storage systems. It provides a method for cluster-wide disk naming and high-speed access to data for applications running on nodes that do not have direct access to the disks. The NSDs in the cluster might be physically attached to all nodes or serve their data through an NSD server that provides a virtual connection.
You are allowed to specify up to eight NSD servers for each NSD. If one server fails, the next server on the list takes control from the failed node.

For an NSD, each NSD server must have physical access to the same NSD. However, different servers can serve I/O to different non-intersecting sets of clients. The existing subnet functions in IBM Spectrum Scale determine which NSD server must serve a particular IBM Spectrum Scale client.

The following options are available in the NSDs page to analyze the NSD performance, health status, and configuration details:

- An NSD table that displays the available NSDs and many different performance metrics. To find NSDs with extreme values, you can sort the values that are displayed in the table by different performance metrics. Click the performance metric in the table header to sort the data based on that metric.

  You can select the time range that determines the averaging of the values that are displayed in the table from the time range selector, which is placed in the upper right corner. The metrics in the table are refreshed based on the selected time frame. You can refresh it manually to view the latest data.

- A detailed view of the performance and health aspects of individual NSDs are also available in the NSDs page. Select the NSD for which you need to view the performance details and select View Details. The system displays details of the NSD on the right pane.

  The detailed view helps to drill-down to various performance and configuration aspects. The following list provides the details that can be obtained from each tab of the detailed view:
  - Overview: Overview of the NSD performance details.
  - Events: System health events reported for the NSD.
  - Nodes: Details of the nodes that serve the NSDs.
  - Properties: Provides an overview of the NSD-related attributes. This tab does not provide any performance details.

**Note:** NSD performance metrics are not collected if the client is running on the NSD server. Therefore, the GUI does not display all SAN environments or workload from local clients.
Chapter 5. Configuring and managing ESS using the GUI

This chapter lists various configuring and managing tasks that can be performed by using the GUI. It includes the following sections:

- Creating file systems
- Mounting a file system through GUI
- Unmounting a file system through GUI
- Creating filesets
- Creating and managing snapshots
- Configuring quota
- Information Lifecycle Management
- Managing storage
- Managing access control lists
- Managing object storage, SMB shares, and NFS exports
- Configuring role-based access for GUI users
5.1 Creating file systems

Use the Files → File Systems → Create File System option to create a file system. You need to select a file system architecture while creating a file system. Choosing a file system architecture provides predefined choices for file system creation (Figure 5-1).

![Create File System](image)

**Figure 5-1** Selecting Basic and Custom mode

You can choose from two different modes:

- In the Basic architecture mode, the file system is created with a single data pool. In this mode, the system automatically selects the default values of various attributes.
- The Custom architecture mode provides the entire set of choices that are available to create a file system. The file system can consist of up to eight pools. The user can choose in which declustered arrays the file system vdisks are created.

Table 5-1 lists the various features that are associated with each mode.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Basic</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>File system name</td>
<td>Can be specified.</td>
<td>One metadata pool is created with the name system that cannot be modified. You can create up to eight data pools but the number is limited to the number of declustered arrays. The names for data pools can be defined by the user.</td>
</tr>
<tr>
<td>Mount point</td>
<td>Can be specified. By default, it is /gpfs/&lt;file_system_name&gt;.</td>
<td></td>
</tr>
<tr>
<td>File system pools</td>
<td>The following pools are created:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Metadata pool with name system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data pool with name data. Pool names cannot be modified.</td>
<td></td>
</tr>
</tbody>
</table>
### Settings

<table>
<thead>
<tr>
<th>Metadata capacity</th>
<th>7% of data capacity.</th>
<th>1 - 20% of data capacity. The following default values are applicable: ▶ 7% if metadata replication is enabled. ▶ 3% if metadata replication is disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID codes</td>
<td>Instead of choosing a RAID level for metadata pool and data pool, you can select a disk fault tolerance level. It specifies the number of disks of data pool that can fail within a declustered array without causing data loss.</td>
<td>A different RAID code can be selected for every pool.</td>
</tr>
<tr>
<td>Block size</td>
<td>Data pool The default value is 4 MiB and it can be modified. Metadata pool The default size is 1 MiB and it cannot be modified.</td>
<td>Data pool The default value is 4 MiB and it can be modified. Metadata pool The default size is 1 MiB and it can be modified.</td>
</tr>
<tr>
<td>Supported block sizes</td>
<td>You cannot change the block size of the file system when it is set. You need to plan properly when specifying the block size. Block size defines the amount of data that can be written to each NSD in a file system before moving on to the next NSD.</td>
<td></td>
</tr>
<tr>
<td>Replication</td>
<td>Metadata pool and data pool are not replicated.</td>
<td>You can select one of the following options: ▶ Disable replication ▶ Replicate metadata pool only ▶ Replicate all pools</td>
</tr>
<tr>
<td>Maximum number of clients</td>
<td>Can be modified. The value can be 32 - 16384 and the default value is 32.</td>
<td></td>
</tr>
<tr>
<td>Maximum number of inodes of the root fileset</td>
<td>Cannot be specified.</td>
<td>Can be specified.</td>
</tr>
<tr>
<td>Size of inodes</td>
<td>Cannot be specified. The default value is used.</td>
<td>Can be specified.</td>
</tr>
<tr>
<td>Vdisk creation</td>
<td>Two vdisks are created on each declustered array: One for the metadata pool and one for the data pool.</td>
<td>The user can choose which declustered arrays provide storage to the pools. The system creates one vdisk for each declustered array to pool assignment. Every declustered array can provide storage to the metadata pool system. A declustered array can provide storage to only one data pool.</td>
</tr>
<tr>
<td>NSD creation</td>
<td>An NSD with the same name is created for every new vdisk.</td>
<td></td>
</tr>
<tr>
<td>Vdisk and NSD naming schema</td>
<td>The system follows the following naming methodology for new vdisks and NSDs: &lt;recovery group&gt;<em>&lt;file system name&gt;</em>&lt;pool name&gt;<em>&lt;sequence number&gt;</em>. The &lt;sequence number&gt; (0, 1, 2, 3, …) is set to avoid duplicate vdisk names.</td>
<td></td>
</tr>
</tbody>
</table>
### 5.2 Mounting a file system through GUI

You can use the ESS GUI to mount or unmount individual file systems or multiple file systems on the selected nodes. Use the Files → File Systems, Files → File Systems → View Details → Nodes, or Monitoring → Nodes → View Details → File Systems window in the GUI to mount or unmount a file system.

The GUI has the following options related to mounting the file system:
- Mount local file systems on nodes of the local ESS cluster.
- Mount remote file systems on local nodes.
- Select individual nodes, protocol nodes, or nodes by node class while selecting nodes on which the file system needs to be mounted.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Basic</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data pool capacity</td>
<td>Specified by user, the default size is the lowest free capacity of a declustered array.</td>
<td>Can be modified indirectly by choosing a percentage of data capacity. The metadata capacity can be chosen between 1% and 20% of data capacity.</td>
</tr>
<tr>
<td>Metadata pool capacity</td>
<td>7% of data capacity and it cannot be modified.</td>
<td>Can be modified indirectly by choosing a percentage of data capacity. The metadata capacity can be chosen between 1% and 20% of data capacity.</td>
</tr>
<tr>
<td>Vdisk size</td>
<td>When modifying data pool capacity, the size of vdisks that belong to the same pool are equally sized if possible. The default size of all vdisks of a pool is set to the smallest available free space of the assigned declustered arrays. While increasing the pool capacity, the vdisks of a pool can become unequally sized. If there is less than 1% of raw capacity of the declustered array that is left as free capacity, the data vdisk uses all free capacity.</td>
<td></td>
</tr>
</tbody>
</table>
| Considered declustered arrays | The following declustered arrays are not considered by the wizard to provide storage to the file system:  
  ▶ Declustered arrays that have less than 10 GiB free raw capacity.  
  ▶ Declustered arrays that contain the word "log" in their name.  
  ▶ Declustered arrays with name "nvr" or "ssd". |                                                                                  |
| Storage allocation        | All declustered arrays (except the ones that are mentioned as "considered declustered arrays") provide storage to all pools. | Can map declustered arrays to the pool. |
| Failure groups            | Besides using RAID codes, replication is an additional method to increase redundancy protection. Replication in IBM Spectrum Scale RAID ensures that there is a copy of each block that is written to two disks that do not share a common point of failure. A failure group is defined as a set of disks that share a common point of failure that might cause them all to become simultaneously unavailable.  
  The following settings are available:  
  ▶ Basic: Failure groups cannot be edited.  
  ▶ Custom: Failure groups can be edited. If the file system is created on only one building block, the failure groups can be edited per recovery group. If the file system is created on more than one building block, the failure groups can be edited per building block. |                                                                                  |
Prevent or allow file systems from mounting on individual nodes.

Perform the following steps to prevent file systems from mounting on a node:

a. Click Monitoring → Nodes.

b. Select the node on which you need to prevent or allow file system mounts.

c. Select Prevent Mounts from the Actions menu.

d. Select the required option and click Prevent Mount or Allow Mount based on the selection.

Configure the automatic mount option. The automatic mount option determines whether to automatically mount file system on nodes when the GPFS daemon starts or when the file system is accessed for the first time. You can also specify whether to exclude individual nodes while enabling the automatic mount option. To enable automatic mount, complete the following steps:

a. From the Files → File Systems window, select the file system for which you need to enable automatic mount.

b. Select the Configure Automatic Mount option from the Actions menu.

c. Select the required option from the list of automatic mount modes.

d. Click Configure.

**Note:** You can configure automatic mount option for a file system only after file system is unmounted from all nodes. That is, you need to stop I/O on this file system to configure this option. However, you can include or exclude the individual nodes for automatic mount without unmounting the file system from all nodes.

## 5.3 Unmounting a file system through GUI

You can use the ESS GUI to mount or unmount individual file systems or multiple file systems on the selected nodes. Use the Files → File Systems, Files → File Systems → View Details → Nodes, or Monitoring → Nodes → View Details → File Systems window in the GUI to mount or unmount a file system.

You can use the following unmount features that are supported in the GUI:

- Unmount the local file system from local nodes and remote nodes.

- Unmount the remote file system from the local nodes. When a local file system is unmounted from the remote nodes, the remote nodes can no longer be seen in the GUI. The Files → File Systems → View Details → Remote Nodes window lists the remote nodes that currently mount the selected file system. The selected file system can be a local or a remote file system but the GUI permits you to unmount only local file systems from the remote nodes.

- Select individual nodes, protocol nodes, or nodes by node class while selecting nodes from which the file system needs to be unmounted.

- Specify whether to force unmount. Selecting the Force unmount option while unmounting the file system unmounts the file system even if it is still busy performing the I/O operations. Forcing the unmount operation affects the outstanding operations and causes data integrity issues. The ESS system relies on the native unmount command to carry out the unmount operation.
The semantics of forced unmount are platform-specific. On certain platforms such as Linux, even when forced unmount is requested, the file system cannot be unmounted if it is still being referenced by the system kernel. To unmount a file system in such cases, identify and stop the processes that are referencing the file system. You can use system utilities like `ls/of` and `fuser` for this goal.

5.4 Creating filesets

Use the `Files → Filesets` window in the GUI (Figure 5-2) to create, manage, and monitor the filesets.

![Filesets window](image)

Use the `Files → Filesets → Create Fileset` option to create a fileset. You can create either an independent or dependent fileset. With an independent fileset, it is possible to specify the maximum number of inodes and the allocated number of inodes. You can also specify access control lists for the fileset.

5.5 Creating and managing snapshots

Use the `Files → Snapshots` window in the ESS GUI to manage snapshots through GUI.

Snapshots can be used in environments where multiple recovery points are necessary. A snapshot can be taken of file system or fileset data and the data then recovered from the snapshot if the production data becomes unavailable.

Note the following characteristics of snapshots:

- Snapshots are read-only. You can make changes only to the normal and active files and directories, not to the snapshot.
- When a snapshot of an independent fileset is taken, only nested dependent filesets are included in the snapshot.

5.5.1 Scheduling snapshot creation by using snapshot rules

You can either manually create the snapshots or create snapshot rules to automate the snapshot creation and retention.
To manually create a snapshot, complete the following steps:

1. Click **Create Snapshot** in the Snapshots window.
2. Enter the required details under the Manual tab of the Create Snapshot window.
3. Click **Create** after providing the details.

You can automate the snapshot creation and retention by creating a snapshot rule. That is, in a snapshot rule you can specify a frequency in which the snapshots must be created and the number of snapshots that must be retained for a period. The retention policy helps to avoid unwanted storage of snapshots that result in the waste of storage resources.

The retention policy has the following parameters:

- Frequency of snapshot creation.
- Number of most recent snapshots to be retained. The most recent snapshot is identified based on the frequency of snapshot creation.
- Number of days for which you need to keep the latest snapshot of each day.
- Number of weeks for which you need to keep the latest snapshot of each week.
- Number of months for which you need to keep the latest snapshot of each month.

**Example scenario for retention policy**

Table 5-2 provides an example of the values that are specified for these parameters.

<table>
<thead>
<tr>
<th>Snapshot deletion time</th>
<th>Frequency</th>
<th>Minute</th>
<th>Number of most recent snapshots</th>
<th>Keep latest snapshots for</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Hours</td>
</tr>
<tr>
<td>2:30 AM</td>
<td>Hourly</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Based on this retention rule, the snapshots listed in Table 5-3 are created and retained on March 20, 2016 at 06:10 AM.

**Table 5-3  Example of time stamp of snapshots that are retained based on the retention policy**

<table>
<thead>
<tr>
<th>Time stamp</th>
<th>Condition based on which snapshot is retained</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 31 (Thursday, 23:01 AM)</td>
<td>Keep the latest snapshot for last 3 months</td>
</tr>
<tr>
<td>January 31 (Sunday, 23:01 AM)</td>
<td>Keep the latest snapshot for last 3 months</td>
</tr>
<tr>
<td>February 29 (Monday, 23:01 AM)</td>
<td>Keep the latest snapshot for last 3 months</td>
</tr>
<tr>
<td>March 5 (Saturday, 23:01 AM)</td>
<td>Keep the latest snapshot for last 2 weeks</td>
</tr>
<tr>
<td>March 12 (Saturday, 23:01 AM)</td>
<td>Keep the latest snapshot for last 2 weeks</td>
</tr>
<tr>
<td>March 14 (Monday, 23:01 AM)</td>
<td>Keep the latest snapshot for last 6 days</td>
</tr>
<tr>
<td>March 15 (Tuesday, 23:01 AM)</td>
<td>Keep the latest snapshot for last 6 days</td>
</tr>
<tr>
<td>March 16 (Wednesday, 23:01 AM)</td>
<td>Keep the latest snapshot for last 6 days</td>
</tr>
<tr>
<td>March 17 (Thursday, 23:01 AM)</td>
<td>Keep the latest snapshot for last 6 days</td>
</tr>
<tr>
<td>March 18 (Friday, 23:01 AM)</td>
<td>Keep the latest snapshot for last 6 days</td>
</tr>
<tr>
<td>March 19 (Saturday, 23:01 AM)</td>
<td>Keep the latest snapshot for last 6 days</td>
</tr>
</tbody>
</table>
According to this rule, 13 snapshots are retained on March 20, 2016 at 06:10 AM.

To schedule snapshot creation and retention, complete the following steps:

1. Click **Files → Snapshots**.
2. Click **Create Snapshot**.
3. In the Create Snapshot window, type the path of the file system or independent fileset for which you need to create snapshots.
4. In the **Snapshot name** field, type the name of the snapshot.
5. Click **Snapshot Rules**.
6. Click **Create Rule** to schedule the snapshot creation and retention. The system displays the Create Snapshot Rule window.
7. In the **Name** field, type the name of the snapshot scheduling rule.
8. In the **Frequency** field, select the frequency in which you need to create snapshot. You must enter some more details based on the value that is selected in the **Frequency** field. For example, the selected value is **Multiple Times an Hour**, select the minutes of the hour in which you need to create snapshots.
9. In the **Retention** fields, specify the number of snapshots that must be retained in a time period.
10. In the **Prefix** field, specify a prefix to be added with the name of the snapshots that are created with this rule.
11. Click **OK** to save the changes.

If you do not specify a name for the snapshot, the default name is given. The default snapshot ID is generated at the creation time by using the format “@GMT-yyyy.MM.dd-HH.mm.ss”. If this option is given and the “@GMT-date-time” format is omitted, then this snapshot will not be identifiable by Windows VSS and the file restore is not possible by that method. Avoid white spaces, double and single quotation marks, the parentheses (), the star *, forward slash /, and backward slash \.

### 5.5.2 Deleting snapshots

To manually delete the snapshots, right-click the snapshot from the Snapshots page and select **Delete**. The snapshots that are automatically created based on the snapshot creation rule are deleted automatically based on the retention period that is specified in the rule. When the condition for deletion is met, the GUI immediately starts to delete the snapshot candidates.

**Note:** Snapshot capacity usage is not collected automatically because it can have a negative impact on the performance of the system. If you are trying to determine overall file system capacity, you must take the capacity that is used by snapshot into account and aggregate the overall capacity usage manually.
5.6 Configuring quota

Use the Files → Quotas window to control the allocation of files and data blocks in a file system. You can create default, user, group, and fileset quotas through the Quotas window.

You can create quotas and modify existing ones. A quota is the amount of disk space and the amount of metadata that is assigned as upper limits for a specified user, group of users, or fileset. Use the Actions menu to create or modify quotas. The management GUI allows you to only manage capacity-related quota. The inode-related quota management is only possible in the command-line interface.

You can specify a soft limit, a hard limit, or both.

When you set a soft limit quota, a warning is sent to the administrator when the file system is close to reaching its storage limit. A grace period starts when the soft quota limit is reached. Data is written until the grace period expires, or until the hard quota limit is reached. Grace time resets when the used capacity goes below the soft limit.

If you set a hard limit quota, you will not able to save data after the quota is reached. If the quota is exceeded, you must delete the files or raise the quota limit to store more data. The grace period can be modified per device by using the mmsetquota command.

Note the following about quotas:

- User or user group quotas for filesets are only supported if the Per Fileset option is enabled at the file system level. Use the command-line interface to set the option. See the man pages of mmcrfs and mmchfs commands for more detail.
- You need to unmount a file system to change the quota enablement method from per file system to per fileset or vice versa.

You can set the default user quotas at the file system level rather than defining user quotas explicitly for each user. Default quota limits can be set for users. You can specify the general quota collection scope such as per file system or per fileset to define whether the default quota needs to be defined at file system level or fileset level, and set the default user quota.

After this value is set, all child objects that are created under the file system or file set will be configured with the default soft and hard limits. You can assign a custom quota limit to individual child objects, but the default limits remain the same unless changed at the file system or fileset level.

5.7 Information Lifecycle Management

The ILM feature that is available in the ESS system facilitates automated tiered storage management. As part of the ILM, you need to create a set of policies and rules that automatically determine where to physically store your data regardless of its placement in the logical directory structure. Proper management of files ensures the efficient use and balance of premium and less expensive storage resources.

Use the Files → Information Lifecycle window in the ESS GUI to manage ILM rules and policies.
Policies and the rules are used to assign files to specific file system pools. A file system pool typically contains a set of volumes that provide a specific quality of service for a specific use. These uses can include storing frequently accessed files on a premium or a pool with high performance and the non-frequently accessed files on a less expensive pool.

A policy is a set of rules that describes the lifecycle of user data based on the file’s attributes. Each rule defines an operation or definition, such as placing new files into different pools or migrating files from one pool to another pool.

A policy rule is an SQL-like statement that tells the file system what to do with a file in a specific file system pool if the file meets specific criteria. A rule can apply to any file within a file system or only to files within a specific fileset or group of filesets.

The following are the main functions of ILM rules:

- Initial file placement
- File management activities such as migration of files from one storage pool to another pool, automatic file deletion, file compression, and file encryption
- File restore from external storage pool like tape

Figure 5-3 shows the Information Lifecycle window.

![Figure 5-3 Information Lifecycle window](image)

The active policy of a file system is available on the Files → Information Lifecycle → Active Policy window. Use the GUI to create additional policies for a file system that can be either applied manually by editing the existing active policy or create policy and apply it as the active policy for the file system.
5.7.1 Creating and applying policy

Select Policy Repository to create a policy and define rules for it. You can also modify the already created policies and apply a policy as the active policy for a file system. You must select Active Policy to see the active policy for a file system. You can also modify the active policy based on the requirement.

The following steps explain how to create and apply a policy:

1. Click Files → Information Lifecycle.
3. Click Create Policy and specify the required details.
   The policy is created. Now, you need to add rules in the policy that manages the files in the system.
4. Click Add Rule in the Policy Repository and define rules with the required rule types. You can create multiple rules in a policy. You can drag the rules in the rules list to change the order in which the rules are applied in a policy.
   The Add Rule option only supports to add placement, migration, file compression, or deletion rules, or to define an external pool. To add encryption, exclusion, or list rules, the policy text must be modified by using the text editor.
5. Optionally, you can use the text editor to edit policy text. Click the Policy Text option that is available in the upper right corner of the GUI page to start the text editor. To work with list rules or less used policy rule syntax constructs, the policy text must be modified through the text editor.
6. After editing the policy details, click Apply Changes.
7. If you want to apply a policy as the active policy for a file system, select the policy from the Policy Repository and then select the Apply as Active Policy option that is available in the Actions menu. You can also change the active policy of the file system.

5.7.2 Editing a policy by using text editor

To define or modify file placement, migration, file compression, deletion, or external pool rules, the GUI provides an easy to use graphical editing mode. For working with rules like encryption, exclusion, and list, you must manually edit the SQL policy text by using the text editor.

If there is only one rule in the policy and it is not supported in the graphical editing mode, the whole policy can only be displayed or modified through the policy text editor.

5.8 Managing storage

You can monitor and manage pools, NSDs, physical disks, and logical volumes of the IBM Spectrum Scale RAID system with the help of the GUI options that are listed in Table 5-4.

Table 5-4  Storage management options

<table>
<thead>
<tr>
<th>GUI option</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage → Pools</td>
<td>Provides an easy way to monitor the performance, health status, and configuration aspects of all of the pools that are available in the ESS cluster.</td>
</tr>
</tbody>
</table>
5.9 Managing access control lists

Use the Access → File System ACL page to create access control lists (ACLs) for the files or directories in a file system. Access to the files and directories is managed through ACLs. It ensures that only authorized users can access directories and files. The IBM Spectrum Scale ACLs are stored in the NFSV4 ACL format.

An ACL is a list of permissions that are associated with a directory or file. It defines which users are allowed to access a particular directory or file. An access control entry in the ACL defines the permissions for a user or a group of users. An ACL usually consists of multiple entries.

Each ACL has an owner that is associated with it, who owns the file or directory for which the ACL is defined. Owners usually have full access to the files or directories that they own. If the directory contains files or subdirectories, the owner, owning group, and ACL cannot be modified.

You can define ACL templates to help the users to set default access control permissions for files and directories. The use of ACL template helps to save time and ensures that the standard and desired values for each ACL entry are used. You can use any of the predefined ACL templates to set the access rights to files and directories.

Only users with DataAccess are allowed to modify ACLs of files and directories on the Access → File System ACLs window.

Users with Administrator, SecurityAdmin, and DataAccess roles are allowed to edit ACL templates.

Users with DataAccess role are allowed to modify the ACL of non-empty file system, filesets, and exports path by using the Edit Access Control option in the corresponding GUI pages.

Users with Administrator and SecurityAdmin role are only allowed to modify the ACLs of the file system root path, the fileset link path, and export paths if they are empty.
5.10 Managing object storage, SMB shares, and NFS exports

Table 5-5 lists the options that are available to configure, monitor, and manage the data exports through the NFS, SMB, and Object protocols.

<table>
<thead>
<tr>
<th>GUI page</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols → NFS Exports</td>
<td>Create and manage NFS exports and add NFS clients. Protocols pages are displayed in the GUI only when the protocol feature is enabled on the cluster.</td>
</tr>
<tr>
<td>Settings → NFS Service</td>
<td>Specify NFS server settings and start or stop NFS services.</td>
</tr>
<tr>
<td>Protocols → SMB Shares</td>
<td>Create and manage SMB shares. Protocols pages are displayed in the GUI only when the protocol feature is enabled on the cluster.</td>
</tr>
<tr>
<td>Settings → SMB Service</td>
<td>Specify SMB server settings and start or stop SMB services.</td>
</tr>
<tr>
<td>Object → Accounts</td>
<td>Create and manage accounts and containers in the object storage. Object pages are displayed in the GUI only when the object feature is enabled on the cluster.</td>
</tr>
<tr>
<td>Object → Users</td>
<td>Create object users.</td>
</tr>
<tr>
<td>Object → Roles</td>
<td>Define roles for the object users.</td>
</tr>
<tr>
<td>Settings → Object Administrator</td>
<td>Define object administrator who can manage accounts in the object storage.</td>
</tr>
<tr>
<td>Settings → Object Service</td>
<td>View and change the object service status.</td>
</tr>
</tbody>
</table>

5.11 Configuring role-based access for GUI users

GUI administrators of the ESS system can monitor, configure, and manage the ESS system and are distinguished from the data users.

You can manage GUI users either locally within the system or in an external authentication server such as Microsoft Active Directory (AD) or Lightweight Directory Access Protocol Server (LDAP). By default, the ESS system uses an internal authentication repository for GUI users. To use an external AD or LDAP server, disable the internal user repository that is used for the GUI user management and enable the LDAP/AD repository.

5.11.1 Managing GUI users locally in the ESS system

You can create users who can perform different administrative tasks on the system. Each user must be part of a user group or multiple groups that are defined on the system. When you create a user, you assign the user to one of the default user groups or to a custom user group. User groups are assigned with predefined roles that authorize the users within that group to a specific set of operations on the GUI.

Use the Access → GUI Users window to create users and add them to a user group.
Predefined roles are assigned to user groups to define the working scope within the GUI. If a user is assigned to more than one user group, the permissions are additive, not restrictive. The predefined role names cannot be changed.

The following are the default user groups:

- **Administrator**
  Manages all functions on the system except those dealing with managing users, user groups, and authentication.

- **SecurityAdmin**
  Manages all functions on the system, including managing users, user groups, and user authentication.

- **SystemAdmin**
  Manages clusters, nodes, alert logs, and authentication.

- **StorageAdmin**
  Manages disks, file systems, pools, filesets, and ILM policies.

- **SnapAdmin**
  Manages snapshots for file systems and filesets.

- **DataAccess**
  Controls access to data, such as managing access control lists.

- **Monitor**
  Monitors objects and system configuration, but cannot configure, modify, or manage the system or its resources.

- **ProtocolAdmin**
  Manages object storage and data export definitions of SMB and NFS protocols.

- **UserAdmin**
  Manages access for GUI users. Users who are part of this group have edit permissions only in the Access pages of the GUI.

The ESS system is delivered with a default GUI user named `admin`. This user is also stored in the local repository. You can log in to the system by using this user name to create additional GUI users and groups in local user repository.

Use the various controls that are available under the Password Policy tab of the GUI Users page to enforce strong passwords for the users. You can modify or expire password of the individual users or all the users that are created in the system. If the password is set as expired, the users will be prompted to change the password at the next login.

**Note:** Only users with the User Administrator role can modify the password policy of a user.

Use the various controls that are available under the Password Policy tab of the GUI Users page to enforce strong passwords for the users. You can modify or expire password of the individual users or all the users that are created in the system. If the password is set as expired, the users will be prompted to change the password at the next login.
User groups
Users who are part of Security Administrator and User Administrator user groups can create role-based user groups. Any user that is added to the group adopts the role that is assigned to that group.

Roles apply to users on the system and are based on the user group to which the user belongs. A user can be part of multiple user groups so that a single user can play multiple roles in the system. You can assign the following roles to your user groups:

- **Administrator**
  Users can access all functions on the GUI except those deals with managing users and user groups.

- **Security Administrator**
  Users can access all functions on the GUI, including managing users and user groups.

- **System Administrator**
  Users can manage clusters, nodes, and alert logs.

- **Storage Administrator**
  Users can manage disks, file systems, pools, and filesets.

- **Snapshot Administrator**
  Users can manage snapshots for file systems and filesets.

- **Monitor**
  Users can view objects and system configuration, but cannot configure, modify, or manage the system or its resources.

- **Data Access**
  Users can perform the following tasks:
  - Edit owner, group, and ACL of any file or path through the Access → File System ACL → Files and Directories page.
  - Edit owner, group, and ACL for a non-empty directory of a file system, fileset, NFS export, or SMB share.
  - Create and delete object containers through the Object → Accounts page.

- **Protocol Administrator**
  Users manage object storage and data export definitions of SMB and NFS protocols.

- **User Administrator**
  Users manage GUI users and user groups.

**Note:** Default groups are not created for the user role User Administrator in case the user is upgrading the ESS cluster from 4.2.0.x to a later release.
5.11.2 Managing GUI administrators in an external authentication server

By default, ESS uses an internal authentication repository for the GUI administrators. To use an external AD or LDAP server to manage the GUI administrators, perform the following steps:

1. Disable the internal user repository by performing the following steps:
   a. Access the server that is running the GUI and open the following file by using a text editor:
      
      /opt/ibm/wlp/usr/servers/gpfsgui/server.xml
   b. Comment out the feature FsccUserRepo, which is highlighted in boldface in Example 5-1.

      Example 5-1  Commenting out the FsccUserRepo feature on server.xml

      <server description="GSS GUI">
      <featureManager>
        <feature>jsp-2.2</feature>
        <feature>localConnector-1.0</feature>
        <feature>jdbc-4.0</feature>
        <feature>ssl-1.0</feature>
        <feature>servlet-3.0</feature>
        <!--<feature>usr:FsccUserRepo</feature>-->
        <feature>jndi-1.0</feature>
      </featureManager>
      [...]  

2. Configure the <ldapRegistry> element in the LDAP or AD repository. Depending on the type of the external server, the configuration element can have different attribute values. Sample configurations for AD and IBM Directory Server are given in Example 5-2.

      Example 5-2  Sample AD and IBM Directory Server configurations

      **Active Directory Server:**

      <ldapRegistry id="ldap">
        host="ldapserver.mycity.mycompany.com" port="389" ignoreCase="true"
        baseDN="cn=users,dc=adtest,dc=mycity,dc=mycompany,dc=com"
        bindDN="cn=testuser,dc=users,dc=adtest,dc=mycity,dc=mycompany,dc=com"
        bindPassword="testuserpwd"
        ldapType="Microsoft Active Directory"
        sslEnabled="false">
      </ldapRegistry>

      **IBM Directory Server:**

      <ldapRegistry id="ldap">
        host="ldapserver.mycity.mycompany.com" port="389" ignoreCase="true"
        baseDN="o=mycompany,c=us"
        ldapType="IBM Tivoli Directory Server"
        sslEnabled="false">
      </ldapRegistry>
3. Establish the LDAP group to GUI role mapping. After the GUI server was restarted, you must review the groups to roles mapping and add/remove group to role mappings as necessary.

4. View and modify the existing group to role mappings. You can view the existing groups by using the `lsusergrp` command. Adding groups can be done by using `mkusergrp`, and removing groups can be done by using `rmusergrp`.

   **Note:** The commands that are used to manage the GUI administrators are not available in the same path where all other IBM Spectrum Scale commands are located. The GUI user management commands are at the following location in the system:

   `/usr/lpp/mmfs/gui/cli`

Create a group to role mapping for initial access. For initial GUI access, you need to map one existing LDAP or AD group to the SecurityAdmin GUI role. Log on to the server that is hosting the GUI and run the following command, which maps the specified LDAP group to the GUI role SecurityAdmin:

```bash
# /usr/lpp/mmfs/gui/cli/mkusergrp LDAPGroup --role securityadmin
```

5. After the initial setup, any additional group mappings can be created through the GUI by using the **Create Group Mapping** option that is available in the **Access → GUI Access** window of the ESS GUI.

   **Note:** The GUI Access window is available only if an external authentication server is enabled to manage the GUI user authentication. If an internal user repository is used for GUI user authentication, the GUI displays GUI Users window to create and manage GUI users and user roles.
Troubleshooting options in GUI

The following troubleshooting options are available in the ESS GUI:

- View health status of components, such as file systems, NSD, and nodes.
- View details of the events reported in the system.
- View options to download logs, trace files, and dumps to know more about the issues reported in the system.
- View the directed maintenance procedures to fix certain events reported in the system.

This chapter includes the following sections:

- Monitoring events
- Monitoring tip events
- Configuring event notifications
- Collecting diagnostic data through GUI
- Directed maintenance procedures
6.1 Monitoring events

You can primarily use the Monitoring → Events window to review the entire set of events that are reported in the ESS system.

The following filter options are available in the Events window:

- Current Issues displays all unfixed errors and warnings.
- Unread Messages displays all unfixed errors and warnings and information messages that are not marked as read.
- All Events displays every event, no matter if it is fixed or marked as read.

The Status icons help to quickly determine whether the event is informational, a warning, or an error. Click an event and select Properties from the Action menu to see the detailed information of that event. The event table displays the most recent events first.

6.1.1 Marking events as read

You can mark certain events as read to change the status of the event in the Events view. The status icons become gray if an error or warning is fixed or if it is marked as read.

6.1.2 Running fix procedure

Some issues can be resolved by running the Run Fix Procedure action. The Events page provides a recommendation for which fix procedure to run next. For more information, see 6.5, “Directed maintenance procedures” on page 71.

6.2 Monitoring tip events

You can monitor events of type “Tips” from the Monitoring → Tips window of the GUI. The tip events give recommendations to the user to avoid certain issues that might occur in the future. The system detects the entities with tip event as healthy. A tip disappears from the GUI when the problem behind the tip event is resolved.

Select Properties from the Actions menu to view the details of the tip. After you review the tip, decide whether it requires attention or can be ignored. Select Hide from the Actions menu to ignore the events that are not important and select Show to mark the tips that require attention.
6.3 Configuring event notifications

The system can use Simple Network Management Protocol (SNMP) traps and emails to notify you when significant events are detected. Any combination of these notification methods can be used simultaneously. Use the Settings → Event Notifications window in the GUI to configure event notifications (Figure 6-1).

![Event Notifications window]

Notifications are normally sent immediately after an event is raised.

6.3.1 Configuring email notifications

The email feature transmits operational and error-related data in the form of an event notification email. To configure an email server, complete these steps:

1. Click Settings → Event Notifications → Email Server.
2. Select Edit and then select Enable email notifications.
3. Enter the required settings and when you are ready, click OK.

Email notifications can be customized by setting a custom header and footer for the emails and customizing the subject by selecting and combining from the following variables:

- &message
- &messageId
- &severity
- &dateAndTime
Emails containing the quota reports and other events reported in the following functional areas are sent to the recipients:

- AFM and AFM DR
- Authentication
- CES network
- Transparent Cloud Tiering
- NSD
- File system
- GPFS
- GUI
- Hadoop connector
- iSCSI
- Keystone
- Network
- NFS
- Object
- Performance monitoring
- SMB
- Object authentication
- Node
- CES

In the email notification method, you can also define whether a recipient needs to get a report of events that are reported in the system. These reports are sent only once per day. Based on the seriousness of the issue, each event that is reported in the system gets a severity level associated with it.

To create email recipients, select **Email Recipients** from the Event Notifications window, and then click **Create Recipient**.

**Note:** You can change the email notification configuration or disable the email service at any time.

### 6.3.2 Configuring SNMP manager

SNMP is the standard protocol for managing networks and exchanging messages. The system can send SNMP messages that notify personnel about an event. You can use an SNMP manager to view the SNMP messages that the system sends.

With an SNMP manager, such as IBM Systems Director, you can view and act on the messages that the SNMP agent sends. The SNMP manager can send SNMP notifications, which are also known as traps, when an event occurs in the system. Click **Settings → Event Notifications → SNMP Manager** to configure SNMP managers for event notifications. You can specify a maximum of six SNMP managers.
In the SNMP mode of event notification, one SNMP notification (trap) with object identifier (OID) .1.3.6.1.4.1.2.6.212.10.0.1 is sent by the GUI for each event. Table 6-1 provides the SNMP objects included in the event notifications.

Table 6-1  SNMP objects included in event notifications

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.4.1.2.6.212.10.1.1</td>
<td>Cluster ID</td>
<td>317908494245422510</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2.6.212.10.1.2</td>
<td>Entity type</td>
<td>SERVER, FILESYSTEM</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2.6.212.10.1.3</td>
<td>Entity name</td>
<td>gss-11, fs01</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2.6.212.10.1.4</td>
<td>Component</td>
<td>SMB, AUTHENTICATION</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2.6.212.10.1.5</td>
<td>Severity</td>
<td>SEVERE, WARN, INFO</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2.6.212.10.1.6</td>
<td>Date and time</td>
<td>17.02.2016 13:27:42.516</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2.6.212.10.1.7</td>
<td>Event name</td>
<td>MS1014</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2.6.212.10.1.8</td>
<td>Message</td>
<td>At least one CPU of &quot;gss-11&quot; is failed</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2.6.212.10.1.9</td>
<td>Reporting node</td>
<td>The node where the problem is reported</td>
</tr>
</tbody>
</table>

Understanding the SNMP OID ranges

Table 6-2 provides the description of the SNMP OID ranges.

Table 6-2  SNMP OID ranges

<table>
<thead>
<tr>
<th>OID range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.4.1.2.6.212</td>
<td>IBM Spectrum Scale</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2.6.212.10</td>
<td>ESS GUI</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2.6.212.10.0.1</td>
<td>ESS GUI event notification (trap)</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2.6.212.10.1.x</td>
<td>ESS GUI event notification parameters (objects)</td>
</tr>
</tbody>
</table>

The traps for the core IBM Spectrum Scale and the trap objects are not included in the SNMP notifications that are configured through the ESS GUI.

Example for SNMP traps

Example 6-1 shows the SNMP event notification that is sent when performance monitoring sensor is shut down on a node.

Example 6-1  Event notification for sense shutdown

```
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::enterprises.2.6.212.10.0.1
SNMPv2-MIB::enterprises.2.6.212.10.1.1 = STRING: "317908494245422510"
SNMPv2-MIB::enterprises.2.6.212.10.1.2 = STRING: "NODE"
SNMPv2-MIB::enterprises.2.6.212.10.1.3 = STRING: "gss-11"
SNMPv2-MIB::enterprises.2.6.212.10.1.4 = STRING: "PERFMON"
SNMPv2-MIB::enterprises.2.6.212.10.1.5 = STRING: "ERROR"
SNMPv2-MIB::enterprises.2.6.212.10.1.6 = STRING: "18.02.2016 12:46:44.839"
SNMPv2-MIB::enterprises.2.6.212.10.1.7 = STRING: "pmsensors_down"
```
SNMPv2-SMI::enterprises.2.6.212.10.1.8 = STRING: "pmsensors service should be started and is stopped"
SNMPv2-SMI::enterprises.2.6.212.10.1.9 = STRING: "gss-11"

Example 6-2 shows the SNMP event notification that is sent for an SNMP test message.

Example 6-2  Event notification for test message

SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.2.6.212.10.0.1
SNMPv2-SMI::enterprises.2.6.212.10.1.1 = STRING: "317908494245422510"
SNMPv2-SMI::enterprises.2.6.212.10.1.2 = STRING: "CLUSTER"
SNMPv2-SMI::enterprises.2.6.212.10.1.3 = STRING: "UNKNOWN"
SNMPv2-SMI::enterprises.2.6.212.10.1.4 = STRING: "GUI"
SNMPv2-SMI::enterprises.2.6.212.10.1.5 = STRING: "INFO"
SNMPv2-SMI::enterprises.2.6.212.10.1.6 = STRING: "18.02.2016 12:47:10.851"
SNMPv2-SMI::enterprises.2.6.212.10.1.7 = STRING: "snmp_test"
SNMPv2-SMI::enterprises.2.6.212.10.1.8 = STRING: "This is a SNMP test message."
SNMPv2-SMI::enterprises.2.6.212.10.1.9 = STRING: "gss-11"

SNMP MIBs

The SNMP Management Information Base (MIB) is a collection of definitions that define the properties of the managed objects.

The ESS GUI MIB OID range starts with 1.3.6.1.4.1.2.6.212.10. The OID range .1.3.6.1.4.1.2.6.212.10.0.1 denotes ESS GUI event notification (trap), and .1.3.6.1.4.1.2.6.212.10.1.x denotes ESS GUI event notification parameters (objects). Use the text shown in Example 6-3 to configure the ESS GUI MIB.

Example 6-3  Text that is used to configure ESS GUI MIB

IBM-SPECTRUM-SCALE-GUI-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    NOTIFICATION-TYPE,
    Counter64,
    enterprises
    FROM SNMPv2-SMI
DisplayString
    FROM RFC1213-MIB;

ibmSpectrumScaleGUI MODULE-IDENTITY
LAST-UPDATED "201607080000Z"    -- July 08, 2016
ORGANIZATION "International Business Machines Corp."
CONTACT-INFO ""
DESCRIPTION "Definition of Spectrum Scale GUI Notifications for Spectrum Scale product.
These objects are subject to modification by IBM as product specifications require."

-- Revision log, in reverse chronological order

REVISION "201607080000Z"    -- July 08, 2016
DESCRIPTION "Version 0.2."
::= { ibmGPFS 10 }

-- ibmGPFS is copied from GPFS MIB (/usr/lpp/mmfs/data/GPFS-MIB.txt)
ibm OBJECT IDENTIFIER ::= { enterprises 2 }
ibmProd OBJECT IDENTIFIER ::= { ibm 6 }
ibmGPFS OBJECT IDENTIFIER ::= { ibmProd 212 }

ibmSpectrumScaleGuiNotification OBJECT IDENTIFIER ::= { ibmSpectrumScaleGUI 0}
ibmSpectrumScaleGuiEventObject OBJECT IDENTIFIER ::= { ibmSpectrumScaleGUI 1}

--- *************************************************************************
-- IBM Spectrum Scale GUI Scalar object declarations - accessible for notifications
--- *************************************************************************

ibmSpectrumScaleGuiEventCluster OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION
"The cluster where the notification occurred."
 ::= { ibmSpectrumScaleGuiEventObject 1 }

ibmSpectrumScaleGuiEventEntityType OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION
"The type of entity for which the notification occurred."
 ::= { ibmSpectrumScaleGuiEventObject 2 }

ibmSpectrumScaleGuiEventEntityName OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION
"The name of the entity for which the notification occurred."
 ::= { ibmSpectrumScaleGuiEventObject 3 }

ibmSpectrumScaleGuiEventComponent OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION
"The component for which the notification occurred."
 ::= { ibmSpectrumScaleGuiEventObject 4 }

ibmSpectrumScaleGuiEventSeverity OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION
"The severity."
 ::= { ibmSpectrumScaleGuiEventObject 5 }

ibmSpectrumScaleGuiEventTime OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION
   "A representation of the date and time when the notification occurred."
::= { ibmSpectrumScaleGuiEventObject 6 }

ibmSpectrumScaleGuiEventName OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION
   "The event name."
::= { ibmSpectrumScaleGuiEventObject 7 }

ibmSpectrumScaleGuiEventMessage OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..1492))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION
   "The human readable message of the notification."
::= { ibmSpectrumScaleGuiEventObject 8 }

ibmSpectrumScaleGuiEventReportingNode OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION
   "The node that reported the event."
::= { ibmSpectrumScaleGuiEventObject 9 }

ibmSpectrumScaleGuiNotificationEvent NOTIFICATION-TYPE
OBJECTS {
   ibmSpectrumScaleGuiEventCluster,
   ibmSpectrumScaleGuiEventEntityType,
   ibmSpectrumScaleGuiEventEntityName,
   ibmSpectrumScaleGuiEventComponent,
   ibmSpectrumScaleGuiEventSeverity,
   ibmSpectrumScaleGuiEventTime,
   ibmSpectrumScaleGuiEventName,
   ibmSpectrumScaleGuiEventMessage,
   ibmSpectrumScaleGuiEventReportingNode
}
STATUS current
DESCRIPTION
   "This notification indicates a Health event as reported by the Spectrum
Scale GUI."
::= { ibmSpectrumScaleGuiNotification 1 }

END
6.4 Collecting diagnostic data through GUI

IBM Support might ask you to collect logs, trace files, and dump files from the system to help resolve a problem. You can perform this task from the management GUI or by using the `gpfs.snap` command. Use the Settings → Diagnostic Data window in the ESS GUI to collect details of the issues reported in the system.

The entire set of diagnostic data available in the system helps analyzing all kinds of ESS issues. Depending on the data selection criteria, these files can be large (gigabytes) and might take an hour to download. The diagnostic data is collected from each individual node in a cluster. In a cluster with hundreds of nodes, downloading the diagnostic data might take a long time and the downloaded file can be large.

6.4.1 GUI logs

Run `gpfs.snap -N GUI_MGMT_SERVERS` or use the Settings → Collect Diagnostic Data window in the GUI to access the GUI logs to analyze GUI problems. These logs are available at the following location:

/var/log/cnlog/mgtsrv/

The following main log files are available:

- `mgtsrv-system-log-x` (most important)
  Logs everything that runs in background processes such as refresh tasks.
- `mgtsrv-trace-log-x`
  Logs everything that is directly triggered by the GUI user, such as starting an action, clicking a button, and running a GUI CLI command.
- `wlp-messages.log`
  Covers the underlying WebSphere Liberty server. The log is mostly relevant during the start-up phase.
- `gpfsgui_trc.log`
  Logs problems related to incoming requests from the browser. Check this log if the GUI displays the following error message: Server was unable to process request.

6.5 Directed maintenance procedures

The directed maintenance procedures (DMPs) assist you to repair a problem when you select Run Fix Procedure on a selected event from the Monitoring → Events page. DMPs are present for only a few events reported in the system.

Table 6-3 provides details about the available DMPs and the corresponding events.

<table>
<thead>
<tr>
<th>DMP</th>
<th>Event ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replace disks</td>
<td>gnr_pdisk_replaceable</td>
</tr>
<tr>
<td>Update enclosure firmware</td>
<td>enclosure_firmware_wrong</td>
</tr>
<tr>
<td>Update drive firmware</td>
<td>drive_firmware_wrong</td>
</tr>
<tr>
<td>DMP</td>
<td>Event ID</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Update host-adapter firmware</td>
<td>adapter_firmware_wrong</td>
</tr>
<tr>
<td>Start NSD</td>
<td>disk_down</td>
</tr>
<tr>
<td>Start GPFS daemon</td>
<td>gpfs_down</td>
</tr>
<tr>
<td>Increase fileset space</td>
<td>node_error_high and inode_warn_high</td>
</tr>
<tr>
<td>Synchronize Node Clocks</td>
<td>time_not_in_sync</td>
</tr>
<tr>
<td>Start performance monitoring collector service</td>
<td>pmcollector_down</td>
</tr>
<tr>
<td>Start performance monitoring sensor service</td>
<td>pmsensors_down</td>
</tr>
</tbody>
</table>
GUI limitations

The Elastic Storage Server (ESS) GUI has the following limitations:

- The GUI supports RHEL 7.x and SUSE Linux Enterprise Server 12.x on Intel x86, Power (Big or Little Endian), and IBM Z platforms.
- Up to 1000 nodes are supported.
- The GUI supports a subset of the CLI functionality. Additional capabilities will be added in the future releases of the product.
- The Object management pages do not support configurations with Keystone V2 API.
- One GUI instance supports a single cluster.
- In an IBM Spectrum Scale and ESS mixed support environment, the ESS GUI must manage the whole cluster to display the ESS-specific pages in the GUI.
- The GUI is not supported on the cluster that runs on IBM Spectrum Scale releases earlier than 4.2.0.0. The GUI supports IBM Spectrum Scale release 4.2.0.0 or later. Issue the \texttt{mmlsconfig} command to see the value that is set for the \texttt{minReleaseLevel} attribute. Use the \texttt{mmchconfig release=LATEST} command and restart the GUI to make the management GUI fully operational at the new code level.
  
  Because changing the minimum release level affects the cluster behavior, see the \texttt{mmchconfig} command man page and other related topics before you make this configuration change.

- All IBM Spectrum Scale packages that are installed on the GUI node must be of the same release. For example, do not mix the 4.2.3 GUI rpm with a 4.2.2 base rpm. However, GUI PTFs and fixes can usually be applied without having to install the corresponding PTF or fix of the base package. This feature is helpful if you just want to get rid of a GUI issue without changing anything on the base layer.
Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document. Note that some publications referenced in this list might be available in softcopy only.

- *Monitoring Overview for IBM Spectrum Scale and IBM Elastic Storage Server*, REDP-5418

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

ibm.com/redbooks

Other publications

These publications are also relevant as further information sources:

- *IBM Spectrum Scale RAID Version 4 Release 2.3 Administration*, SC27-6658

Online resources

These websites are also relevant as further information sources:

- Elastic Storage Server (ESS) Knowledge Center
- Examples for GUI issues and their resolutions
- IBM Spectrum Scale GUI quick reference
- IBM Spectrum Scale GUI videos
  https://www.youtube.com/playlist?list=PLS7mekU2kxDrWbtK5AIVGPyF94xTv02xN
- IBM Spectrum Scale RAID concepts

Help from IBM

IBM Support and downloads
ibm.com/support

IBM Global Services
ibm.com/services