Redbooks
ibm.com/redbooks

Monitoring and Managing the IBM Elastic Storage Server Using the GUI

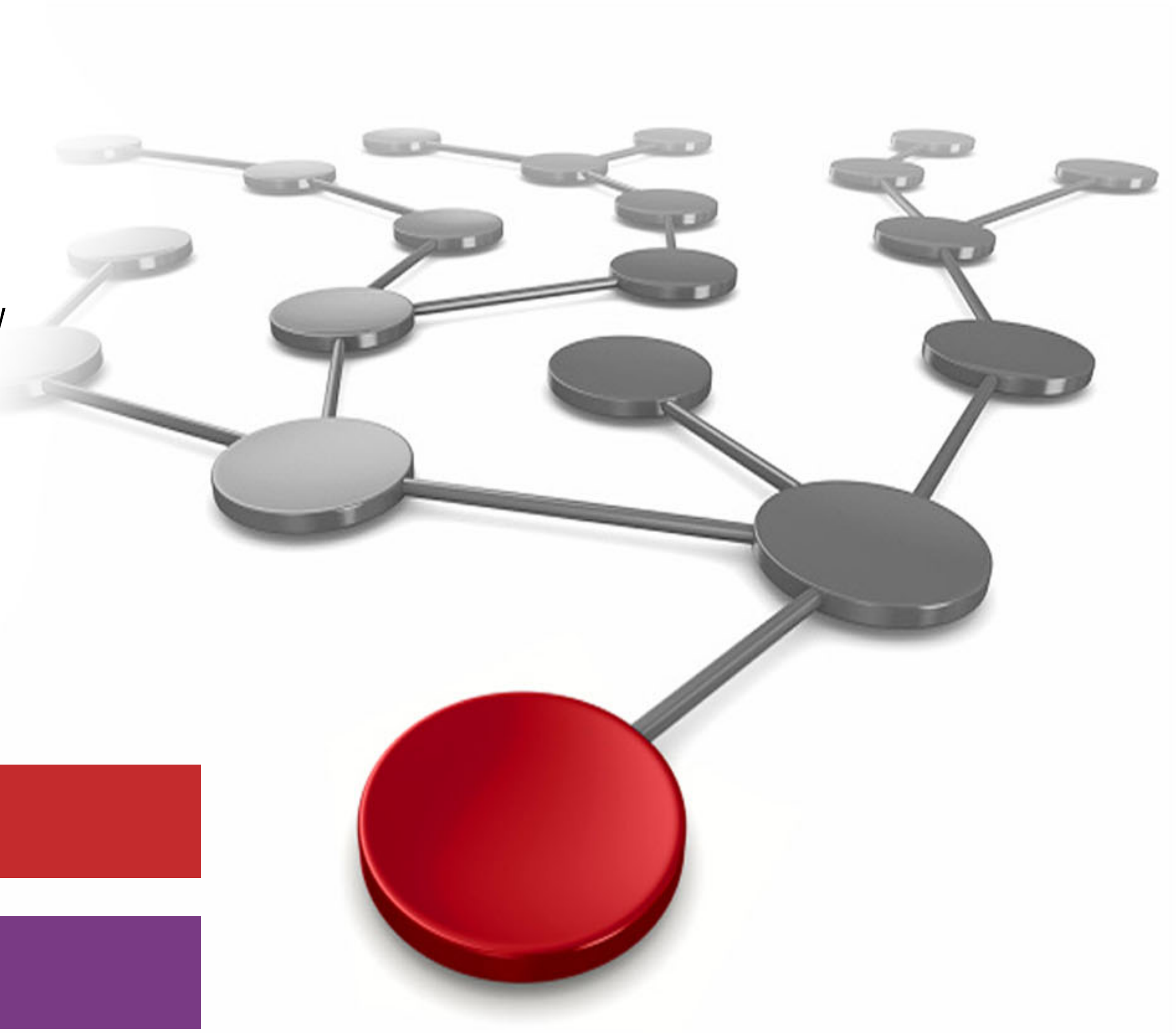
Markus Rohwedder

Alexander Wolf-Reber

Stefan Roth

Liju Joser

Przemyslaw Podfigurny



Cloud

Storage

IBM

Redpaper

International Technical Support Organization

Monitoring and Managing the IBM Elastic Storage Server Using the GUI

November 2019

REDP-5471-01

Note: Before using this information and the product it supports, read the information in “Notices” on page ix.

Second Edition (November 2019)

This edition applies to IBM Elastic Storage Server (ESS) version 5.3.4, which is based on IBM Spectrum Scale 5.0.3.

This document was created or updated on November 12, 2019.

Contents

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®
IBM Elastic Storage®
IBM Research™
IBM Spectrum®
Redbooks®
Redbooks (logo) ®
Storwize®
Tivoli®
WebSphere®

The following terms are trademarks of other companies:

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

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 IBM® Elastic Storage Server GUI provides an easy way to configure and monitor various features that are available with the IBM ESS system. It is a web application that runs on common web browsers, such as Chrome, Firefox, and Edge. The ESS GUI uses Java Script and Ajax technologies to enable smooth and desktop-like interfacing.

This IBM Redpaper publication provides a broad understanding of the architecture and features of the ESS GUI. It includes information about how to install and configure the GUI and in-depth information about the use of the GUI options. The primary audience for this paper includes experienced and new users of the ESS system.

For more 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, Poughkeepsie 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, such as 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, such as 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.

Przemyslaw Podfigurny is a Software Engineer in IBM Research and Development in Kelsterbach, Germany. He joined IBM in 2015 and worked as a developer on IBM Spectrum Scale GUI Backend, REST API components, and build setup. His primary interests include Java technologies, databases, distributed Linux environment, and big data. He holds a Master's degree in Software Engineering from the Wrocław University of Science and Technology.

Thanks to the following people for their contributions to this project:

Larry Coyne
International Technical Support Organization

Sandeep Ramesh
Dietmar Fischer
Andreas Koeninger
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:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

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.

This chapter provides a basic overview of the GUI and includes the following topics:

- 1.1, “ESS GUI architecture” on page 2
- 1.2, “Role-based access control with GUI users” on page 3
- 1.3, “Integration hub for configuration, health, and performance data” on page 3
- 1.4, “Support matrix” on page 4

1.1 ESS GUI architecture

Figure 1-1 shows the ESS GUI architecture.

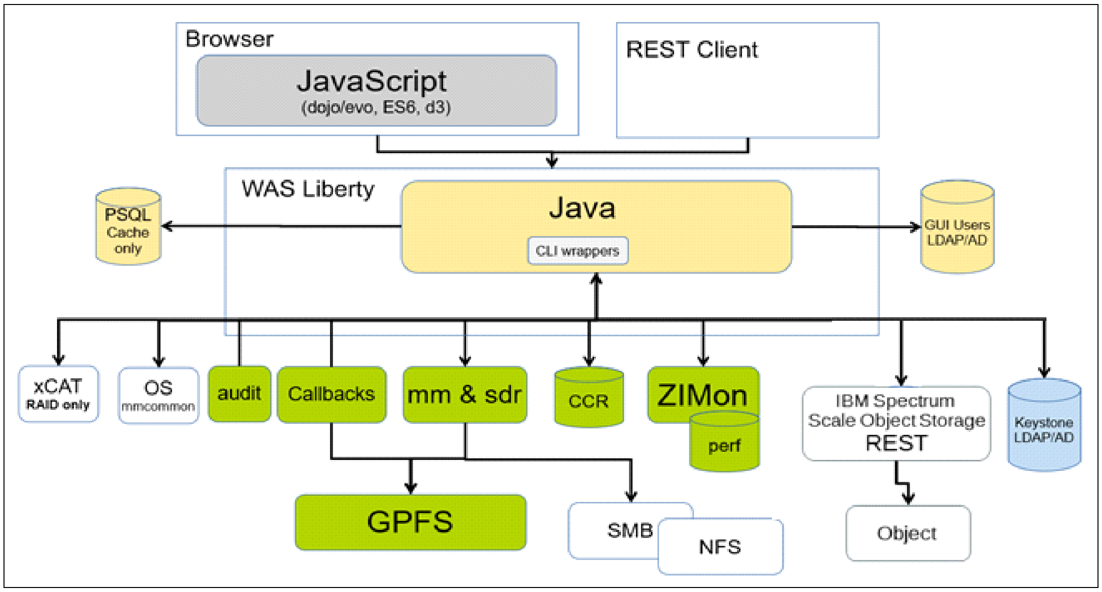


Figure 1-1 ESS GUI architecture

The ESS GUI runs on an IBM WebSphere® Liberty application server on one or more cluster nodes. The application servers provides the infrastructure for the GUI and REST API. Configuration information from the ESS cluster is cached in a database because some commands are resource-intense and user interaction with the GUI should not always trigger data refresh activities from the cluster. The GUI includes interfaces to many components in the cluster.

One GUI instance manages a single ESS cluster, but it can also contact GUI nodes from other clusters to exchange monitoring information through RESTful interface.

1.1.1 GUI node requirements

In contrast to generic IBM Spectrum Scale cluster, the selection of the ESS GUI node is restricted to the ESS Management Servers (EMS). The EMS server provides all necessary interfaces that are needed by the GUI to monitor. It also manages the ESS System and the cluster. On a cluster that uses ESS technology, the GUI needs access to the GNR command line interface (CLI), xCAT server, and hardware management console (HMC), if present.

Resource consumption

The resource consumption of the GUI service is considerably low. The memory consumption of the application server is limited to 512 MiB, and the memory limit of the GUI (including all child processes) is set to 2 GiB.

The GUI node also acts as the collector node for performance data. The collector process uses memory that is based on the number of elements, such as nodes or disks, and depends on collection frequency.

1.1.2 Network requirements

The GUI nodes must contact all nodes in the cluster. To connect to other clusters, you must establish an HTTPS connection among the local node with remote cluster nodes. The application server assumes that the ports 80 and 443 are available on the GUI node.

The next sections describe the use cases for the ESS GUI.

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 includes a built-in user database with which you can 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.

The GUI users are also used for the IBM Spectrum Scale management API (REST API) access.

For more information about GUI user management, see 5.12, “Configuring role-based access for GUI users” on page 80.

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 hardware details
- Edit rack components
- Configure hardware monitoring
- Monitor thresholds
- Monitor command audit logs
- Monitor file audit logs
- Monitor remote clusters
- Monitor nodes and networks in the cluster
- Manage IBM Spectrum Scale services

- Monitor storage pools
- Monitor NSDs
- Monitor virtual disks and physical disks
- Monitor declustered arrays
- Replace broken disks
- Run directed maintenance procedures
- 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
- Configure authentication method for NFS and SMB users
- Configure authentication method for GUI users
- Create and manage node classes
- 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 that is reported in the system
- Monitor system health events
- Enable and configure call home feature in the cluster
- Monitor Transparent Cloud Tiering service
- Manage Object Storage, and create object users and roles

1.4 Support matrix

In this section, we describe the operating systems and IBM Spectrum Scale release levels that support the GUI.

1.4.1 Operating system levels

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 operating systems and hardware platforms are supported in a cluster. The operating system of the GUI nodes is determined by the supported EMS servers. For more information about the supported software levels, see IBM Spectrum Scale RAID Frequently Asked Questions and Answers.

1.4.2 ESS GUI software requirements

ESS GUI software must meet the following requirements:

- The IBM Spectrum Scale that is installed in the cluster is at a minimum release level of 4.2.0.

  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.

- All packages that are installed on the GUI node are of the same underlying IBM Spectrum Scale release.

  For example, do not mix the IBM Spectrum Scale 5.0.3 GUI rpm with a 5.0.2 base rpm. However, GUI PTFs and fixes often can be applied without installing the corresponding PTF or fix of the base package. This feature is helpful if you want to resolve a GUI issue without changing anything on the base layer. The ESS software versions are not relevant for this compatibility aspect.

  Note: It is recommended to move to the latest PTF level that is available for the underlying IBM Spectrum Scale release.

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

2

Installing and configuring 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.

In this chapter, we describe how to install and configure the ESS GUI.

This chapter includes the following topics:

2.1 Enabling performance monitoring tools in ESS GUI

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

1. Generate performance collector in the EMS node. The EMS must be part of the ESS cluster and node name must be the node name that is 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 nodeclass` and `gss_ppc64 nodeclass` for performance monitoring, issue the following command:

   ```
   mmchnode --perfmon -N ems,gss_ppc64
   ```

   > **Note:** This example is applicable if the cluster consists of the EMS server and the ESS building blocks only. 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 data must be collected on a single node only. The system can automatically choose an appropriate node where the capacity sensors should run. If capacity collection is not enabled, you can turn on sensors GPFSFilesetQuota, GPFSFileset, GPFSPool, and GPFSDiskCapcin the Services Performance Monitoring Sensors page in the GUI. It is recommended to set the following data collection intervals for the sensors:

   – GPFSFilesetQuota = 3600
   – GPFSFileset = 300
   – GPFSPool = 300
   – GPFSDiskCap = 86400

   You can also use the following CLI commands to update the configuration and set periods for these sensors:

   – `mmperfmon config update GPFSFilesetQuota.restrict=@CLUSTER_PERF_SENSOR GPFSFilesetQuota.period=3600`

   – `mmperfmon config update GPFSFileset.restrict=@CLUSTER_PERF_SENSOR GPFSFileset.period=300`

   – `mmperfmon config update GPFSDiskCap.restrict=@CLUSTER_PERF_SENSOR GPFSDiskCap.period=86400`

   – `mmperfmon config update GPFSPool.restrict=@CLUSTER_PERF_SENSOR GPFSPool.period=300`

   > **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 by clicking **Files** → **Quota** for each file system, or you can use the **`mmchfs -Q`** and **`mmcheckquota`** commands.

4. Configure the sensors.

   Several GUI pages display performance data that is collected with the help of performance monitoring tools. If data is not collected, the GUI shows error messages, such as “No Data Available” or “Objects not found” in the performance charts. The GUI context-sensitive help that is available on various pages shows performance metric information. The GUI context-sensitive help also lists the sensor names.

The **Services** → **Performance Monitoring** page provides an option to configure the sensor and hints for collection periods and restriction of sensors to specific nodes.

You can also use the **mmperfmon config show** command to verify the sensor configuration. Use the **mmperfmon config update** command to adjust the sensor configuration to match your requirement.

The /opt/IBM/zimon/ZIMonSensors.cfg local file can be different on every node, and the system updates this file whenever a configuration change occurs. Therefore, this file must not be edited manually when the **mmperfmon config update** command or **Services** → **Performance Monitoring** in the GUI are used to modify the sensor configurations.

During the sensor configuration distribution process, the restrict clause is evaluated and the period for all sensors is set to 0 in the /opt/IBM/zimon/ZIMonSensors.cfg file on the nodes that did not match the restrict clause. You can check the local file to confirm that a restrict clause worked as intended.

5. Start sensors in the management server node and the I/O server nodes:

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

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

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

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

```
systemctl start pmcollector
```

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

```
 systemctl enable pmcollector
```

9. Enable and start gpfsgui:

```
systemctl enable gpfsgui
systemctl start gpfsgui
```

10. To access the GUI, open your web browser and navigate to https://<host name>:443. The GUI then starts, which might take a few minutes. After the initialization, the system setup wizard appears to complete the rest of the setup.

Configuring capacity-related sensors to run on a single-node

Several capacity-related sensors must run only on a single node as they collect data for a clustered file system; for example GPFSDiskCap, GPFSFilesetQuota, GPFSFileset, and GPFSPool.

It is possible to automatically assign restrict these sensors to a single node. In IBM Spectrum Scale 5.0.1 and later, capacity-related sensors are configured to automatically select a single node where the capacity collection occurs.

Use the **Services** → **Performance Monitoring** page to set appropriate periods for these sensors.

The GPFSDiskCap sensor includes a recommended period of 86400, which means once per day. As the GPFSDiskCap sensor runs **mmdf** command to get the capacity data, it is not recommended to use a value less than 10800 (every 3 hours).

To show fileset capacity information, it is necessary to enable quota for all file systems where fileset capacity must be monitored. For information about enabling quota, see the **-q** option in the **mmchfs** command and **mmcheckquota** command.

Checking the GUI and performance tool status

To check the GUI and performance tool status, complete the following steps:

1. Issue the systemctl status **gpfsgui** command to determine the GUI status, as shown in Example 2-1 Example 2-1.

   Example 2-1 Determining the GUI status using the systemctl status gpfsgui command

   ```
   systemctl status gpfsgui
   gpfsgui.service - IBM_Spectrum_Scale Administration GUI
   Loaded: loaded (/usr/lib/systemd/system/gpfsgui.service; disabled; vendor
   preset: disabled)
   Active: active (running) since Tue 2017-04-11 16:09:23 CEST; 1 day 22h ago Main
   PID: 1430 (java)
   Status: "GSS/GPFS GUI started" CGroup: /system.slice/gpfsgui.service
   oo1430 /usr/lpp/mmfs/java/jre/bin/java
   -XX:+HeapDumpOnOutOfMemoryError -Dcom.ibm.gpfs.platf...
   ```

2. Issue the **systemctl status pmcollector** and s**ystemctl status pmsensors** commands to determine the status of the performance tool.

   You can also check whether the performance tool backend can receive data by using the GUI or alternative by using a command line performance tool called zc. This tool is available in the `/opt/IBM/zimon` folder. Sample output is shown in Example 2-2.

   Example 2-2 Sample output of the zc tool

   ```
   echo "get metrics cpu_user last 1 bucket_size 60"|/opt/IBM/zimon/zc localhost
   1: node1.localnet.com|CPU|cpu_user
   2: node2.localnet.com|CPU|cpu_user
   3: node3.localnet.com|CPU|cpu_user
   Row   Timestampcpu_usercpu_usercpu_user 12017-04-13 14:50:004.328333null
   2.343333
   2  2017-04-13 14:51:003.492500null3.305000
   ```

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.

The ports that must be used to secure GUI are listed in Table 2-1.

Table 2-1 Firewall recommendations for GUI

Port Number	Functions	Protocol
47080	Management GUI	HTTP, localhost only
47443	Management GUI ESS management API	HTTPS, localhost only
80	Management GUI	HTTP
443	Management GUI ESS management API	HTTPS
4444	Management GUI	Localhost only
4739, 9085, and 9084	Performance monitoring collector	NA

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 open to receive events only if an older version than 4.2.3 of GPFS is used. It cannot be used to access the GUI. Port 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 gpfsgui service is started, and removed when it is stopped. Therefore, to access the GUI, ports (such as 443, 47443, and 47080) must be opened.

Port 4444 is accessible only from the localhost.

The update mechanism for iptables can be disabled by setting the variable **`UPDATE_IPTABLES`** to false, which is stored at: `/etc/sysconfig/gpfsgui`. You must restart the GUI for the changes to take effect.

The iptables rules that are necessary for the port forwarding and to bind the non-root users to the privileged ports are automatically checked every time when the GUI is started through the **`systemctl start gpfsgui`** command. The user does not have to configure anything manually for this.

2.3.2 Creating and using an HTTPS certificate to secure communications between GUI web server and web browsers

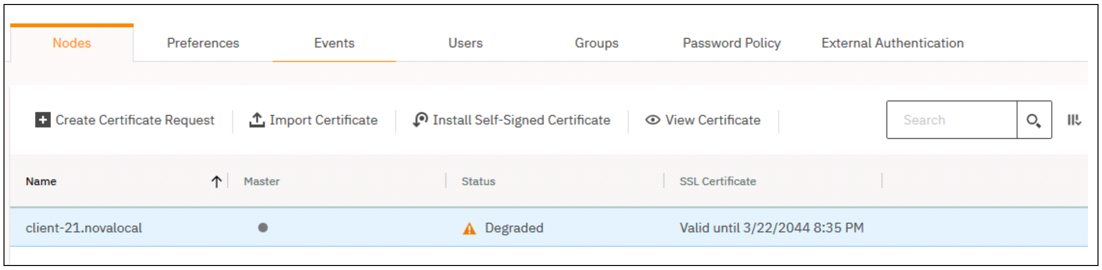
The ESS GUI supports self-signed and trusted certificates that are provided by a certificate authority (CA) to secure communications between the web server and web browser. During system setup, an initial self-signed certificate is created to use for secure connections between the GUI web servers and web browsers.

Based on the security requirements for your system, you can create a new self-signed certificate or install a signed certificate that is created by the certifying authority. Self-signed certificates can generate web browser security warnings and might not comply with organizational security guidelines.

The trusted certificates are created by a third-party certificate authority. These certificate authorities ensure that certificates have the required security level for an organization based on purchase agreements. Trusted certificates usually have higher security controls for encryption of data and do not cause browser security warnings. Trusted certificates are also stored in the WebSphere Liberty SSL keystore.

Major web browsers trust the CA-certified certificates by default and therefore they can confirm that the certificate received by the GUI server can be trusted. You can either buy a signed certificate from a trusted third-party authority or create your own certificate and get it certified. You can use both self-signed and trusted certificates. However, using a trusted is the preferred way because the browser trusts this certificate automatically without any manual interventions.

You can use the **Services** → **GUI** page in the GUI to install and use the certificates (see Figure 2-1).



Name	Master	Status	SSL Certificate
client-21.novalocal	●	⚠ Degraded	Valid until 3/22/2044 8:35 PM

Figure 2-1 GUI to install and use certificates

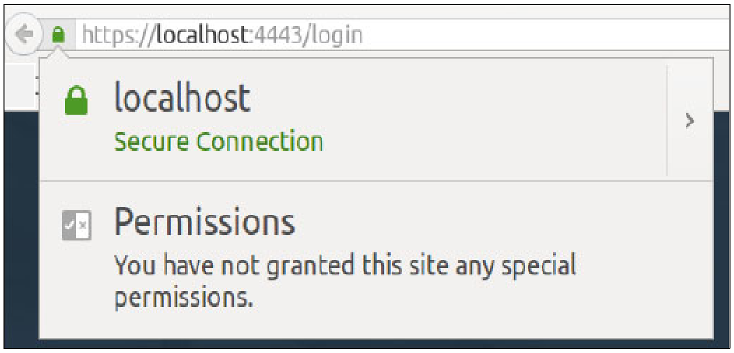
You can use the **Services** → **GUI** page in the GUI to complete the following steps:

1. Generate a self-signed certificate by using the Install **Self-Signed Certificate** option.
2. Generate a certificate request and install it after getting it certified by the CA by using the **Create Certificate Request** option.

   > **Note:** You can use new attributes for Subject Alternative Names, if the OpenSSL version on the GUI node is 1.1.1 or later.

3. Install an issued certificate by using the **Import Certificate** option.
4. View the details of the certificate that is applied on the local GUI node by using the **View Certificate** option.

When you export the certificate, you can see the certificate while accessing the GUI in the browser through HTTPS, as shown in Figure 2-2.



https://localhost:4443/login

localhost
Secure Connection

Permissions
You have not granted this site any special permissions.

Figure 2-2 SSL Certificate visible in the GUI

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 that are 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 GUI CLI commands; for example, **`mkuser`**, to create the first GUI user. The GUI CLI commands are located at /usr/lpp/mmfs/gui/cli on the GUI nodes.
- Bind to the privilege ports 80 (HTTP) and 443 (HTTPS). The iptables rule that is 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

Because 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 remote root access is disabled and sudo wrappers are used. On such a cluster, the GUI process still runs as root, but it issues SSH to other nodes using a user name for which sudo wrappers were configured.

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

1. Issue the **`mmchconfig sudoUser=gpfsadmin`** command to configure the user name.
2. Issue **`/usr/lpp/mmfs/gui/cli/runtask DAEMON_CONFIGURATION`** to refresh GUI configuration.

Passwordless SSH is 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 gpfsadmin@destination-node`. Therefore, it is not necessary to set up passwordless SSH between `gpfsadmin` users on any two nodes. The root user of the node where the GUI is running can do passwordless SSH to any other node by using the `gpfsadmin` user login. Therefore, unidirectional access from the GUI node to the remote nodes as `gpfsadmin` 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 following properties file:

```
/usr/lpp/mmfs/gui/conf/gpfsgui.properties
```

Because the properties file is not maintained over upgrades, modifications to this file must be reapplied when the GUI is upgraded. Typically, this file does not need to be updated. The important settings that can be modified in the properties file Table 2-2.

Table 2-2 Settings in the properties file

Setting	**Description**
KEEP_LOG_INTERVAL=168	Defines the number of hours the logs must be kept before they are discarded.
JDBC_DB_URL=jdbc:postgresql://localhost:5432/postgres	Sets the URL of the GUI owned postgres database.
MAX_ALLOWED_TIME_DIFF=60	Defines 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 proper 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.

Setting	Description
ZIMonAddress=localhost, ZIMonPort=9084	Sets 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	Specifies the current GPFS admin user. On a system with sudo wrappers enabled, it is automatically changed to a selected sudoUser.

2.7 Distributed 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.

These GUI preference files start with `_gui` and can be viewed by using the **`mmccr flist`** command. The local version of the GUI preferences is stored at `/var/lib/mmfs/gui`.

The distributed preferences contain various information that are needed in the distributed environment, such as user repository, LDAP and certificate settings, user account templates, policies, and thresholds.

Note: Distributed GUI preferences must not be edited manually.

You can also use the **Preferences** tab in the **Services** → **GUI** page to set the following options for the GUI node:

- Login message

  A message that can be displayed in the login page of the management GUI. Usually, this message is used to display some important information that must be shared with other users. For example, “Do not alter snapshot configuration”, “To get access to the system, please contact……”, and so on. You can specify only up to 160 characters in the message.

- Session timeout

  The system automatically logs out the user after a specified period of inactivity.

- Display cluster name on the banner

  You can enter a name for the cluster and display it on the banner.

Note: The settings made under the Preferences tab are stored centrally in CCR. Therefore, the settings that are made for one GUI node are applicable to all GUI nodes of the cluster.

3

Understanding the GUI options

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

- 3.1, “Login” on page 18
- 3.2, “Navigation” on page 19
- 3.3, “Header area” on page 20
- 3.4, “Understanding the features associated with a GUI page” on page 21

3.1 Login

The users who are created by using the **Access** → **GUI** → **Users** page can log in to the GUI (see Figure 3-1). When you log in for the first time after the installation, the GUI log-in window provides guidance about how to create the first GUI user.

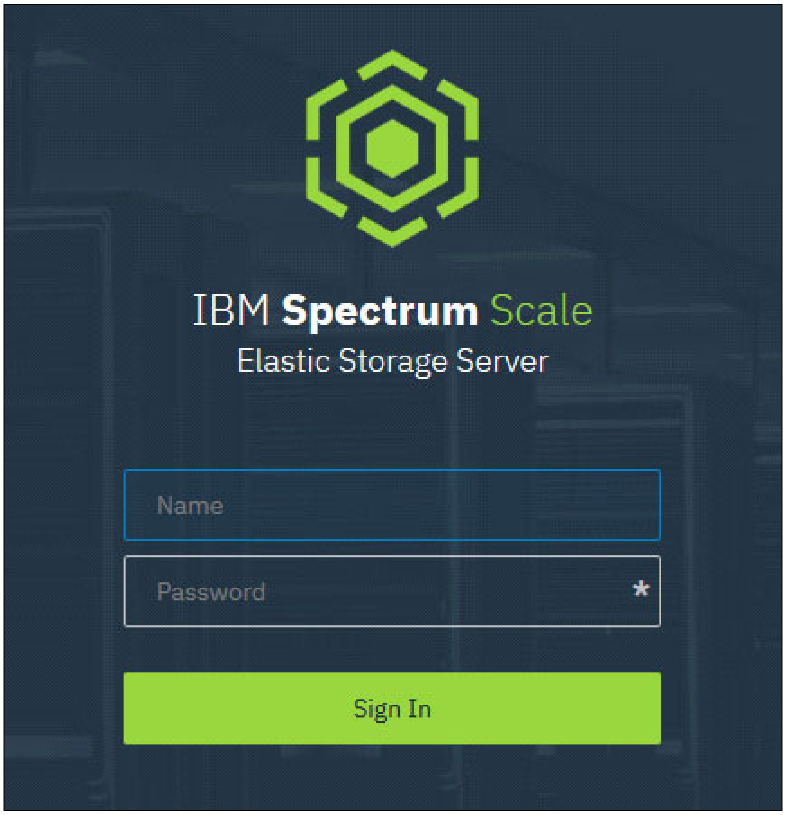


Figure 3-1 Login page

3.2 Navigation

You can navigate to the various GUI pages through the navigation menu on the left side of the GUI page (see 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.

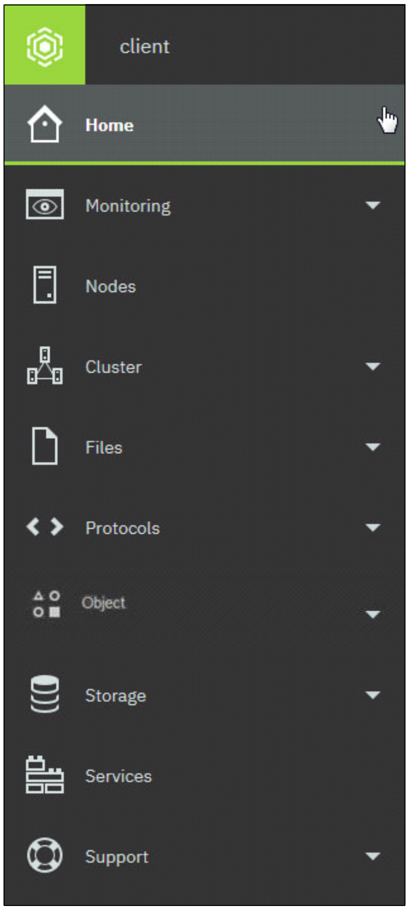


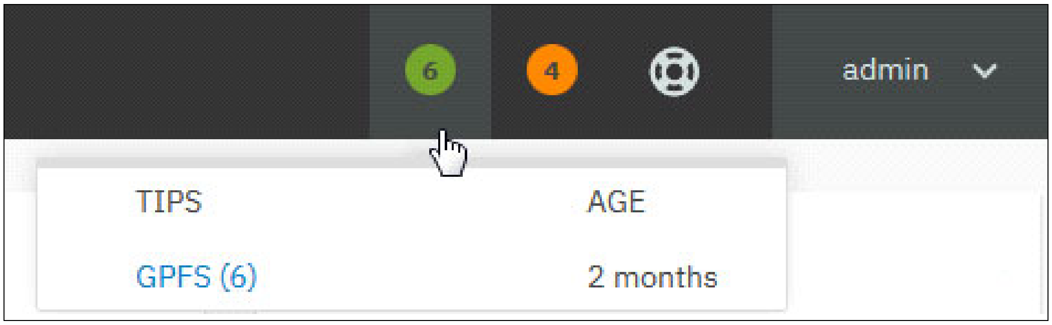
Figure 3-2 Navigation pane of the GUI

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:

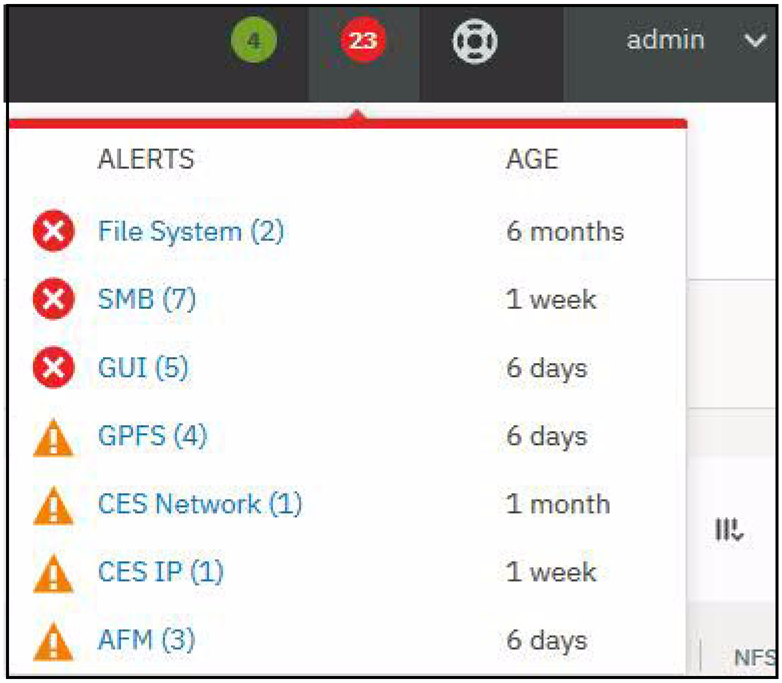
- List of events of type “tips”. The tips events give recommendations to the user to avoid certain issues in the future (see Figure 3-3).



TIPS	AGE
GPFS (6)	2 months

Figure 3-3 Tips menu

- 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.



	ALERTS	AGE
✖	File System (2)	6 months
✖	SMB (7)	1 week
✖	GUI (5)	6 days
⚠	GPFS (4)	6 days
⚠	CES Network (1)	1 month
⚠	CES IP (1)	1 week
⚠	AFM (3)	6 days

Figure 3-4 Health Status menu

- Link to the context-sensitive help page. This help file 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 placed in the upper right corner of the GUI page (see Figure 3-5 on page 21).

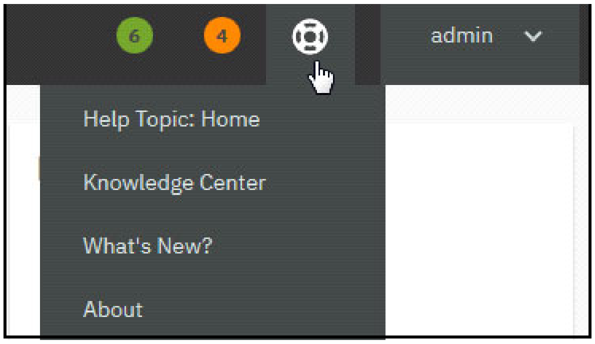


Figure 3-5 Help menu

- 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, log out, and provide feedback are available in the User menu (see Figure 3-6).

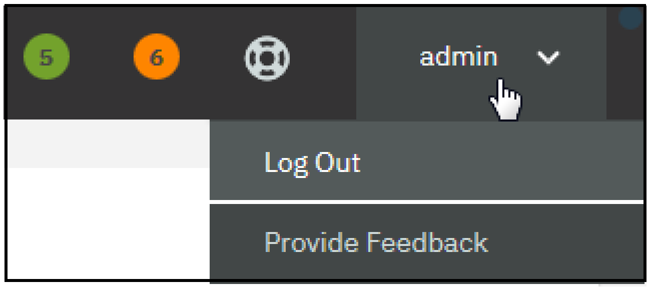


Figure 3-6 Log in menu

Connection indicators that show active data transfers between browser and the GUI server (blue light indicates “Loading”) and connection issues (yellow light indicates “Disconnected”), as shown in Figure 3-7.

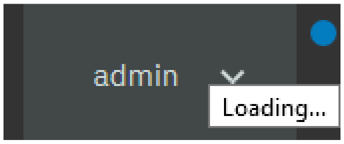


Figure 3-7 Connection indicator blue light indicates “Loading”

3.4 Understanding the features associated with a GUI page

The following levels of assistance are available for GUI users:

- 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.

- 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.

- IBM Knowledge Center

  This third level of information is 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.

4

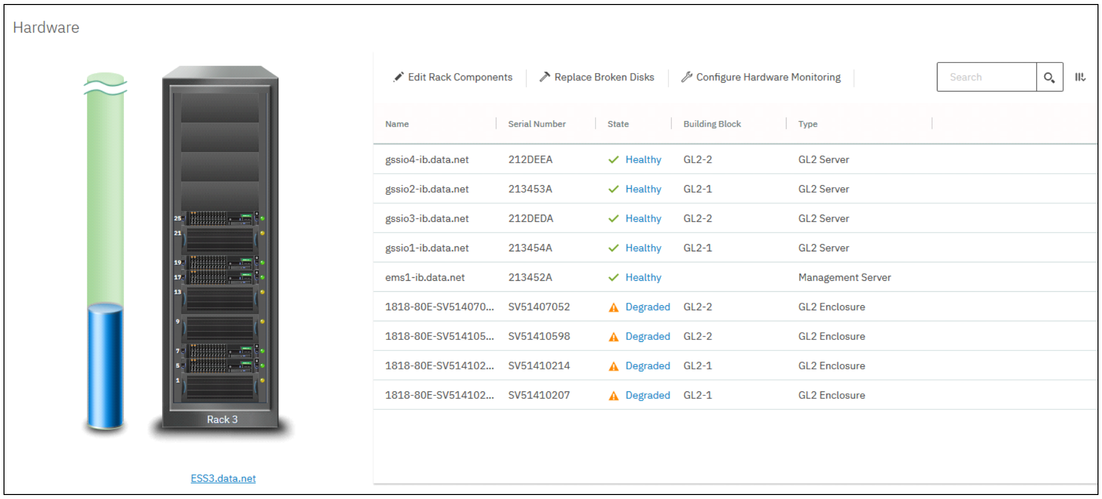
Monitoring options available in the GUI

In this chapter, we describe the various monitoring options that are available with the GUI. This chapter includes the following topics:

4.1 Monitoring hardware details

From the **Monitoring** → **Hardware** and **Monitoring** → **Hardware Details** pages 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.



Name	Serial Number	State	Building Block	Type
gssio4-ib.data.net	212DEEA	✓ Healthy	GL2-2	GL2 Server
gssio2-ib.data.net	213453A	✓ Healthy	GL2-1	GL2 Server
gssio3-ib.data.net	212DEDA	✓ Healthy	GL2-2	GL2 Server
gssio1-ib.data.net	213454A	✓ Healthy	GL2-1	GL2 Server
ems1-ib.data.net	213452A	✓ Healthy		Management Server
1818-80E-SV514070...	SV51407052	⚠ Degraded	GL2-2	GL2 Enclosure
1818-80E-SV514105...	SV51410598	⚠ Degraded	GL2-2	GL2 Enclosure
1818-80E-SV514102...	SV51410214	⚠ Degraded	GL2-1	GL2 Enclosure
1818-80E-SV514102...	SV51410207	⚠ Degraded	GL2-1	GL2 Enclosure

Figure 4-1 Hardware window in ESS GUI

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 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 on only the servers that are called as external management server (EMS) or management servers. In addition to GUI, the management server hosts the performance monitoring collectors and xCAT for hardware monitoring. You can configure only one xCAT per EMS node. If more than one EMS node exists in the ESS cluster, you can configure the GUI to connect to more than one xCAT to monitor the hardware details

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 of 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

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

4.1.4 Replace broken disks

If broken disks are in the Replaceable status, 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 Disks** and some other GUI pages.

4.1.5 Configure hardware monitoring

Use the **Configure Hardware Monitoring** option that is available in the **Monitoring** → **Hardware** page to configure hardware monitoring servers. The hardware monitoring server uses the xCAT software to monitor the health and status of the ESS server nodes. You can configure the connection to the monitoring server and test the connection to verify whether the communication works. You can configure up to 10 hardware monitoring servers based on the requirement.

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.

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

Table 4-1 Performance monitoring options available in ESS GUI

GUI window	Function
Monitoring → **Statistics**	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.
Monitoring → **Dashboards**	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.
Nodes	Provides an easy way to monitor the performance, health status, and configuration aspects of all available nodes in the ESS cluster.

GUI window	Function
Cluster → Network	Provides the performance details, health status, and configuration aspects of network components.
Files → File Systems	Provides a detailed view of the performance and health aspects of individual file systems.
Storage → NSDs	Provides a detailed view of the performance and health aspects of individual Network Shared Disks (NSDs).
Storage → Pools	Provides a detailed view of the performance and health aspects of storage pools.
Protocols → NFS Exports	Provides an overview of the performance aspects of the NFS export.
Protocols → SMB Shares	Provides an overview of the performance aspects of the SMB shares.
Files → Active File Management	Provides a detailed view of the configuration, performance, and health status of the Active File Management (AFM) cache relationship, AFM disaster recovery (AFM DR) relationship, and gateway nodes.
Files → Filesets	Provides a detailed view of filesets.
Files → Transparent Cloud Tiering	Provides insight into health, performance, and configuration of the Transparent Cloud Tiering feature.

The performance and capacity data are collected with the help of the following two components (see Figure 4-2 on page 27):

- 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 ages. The collector can run on any node in the system. You can configure multiple collectors in the system. To configure performance monitoring through GUI, a collector must be configured on each GUI node. The performance monitoring configuration for GUI is shown in Figure 4-2 on page 27.

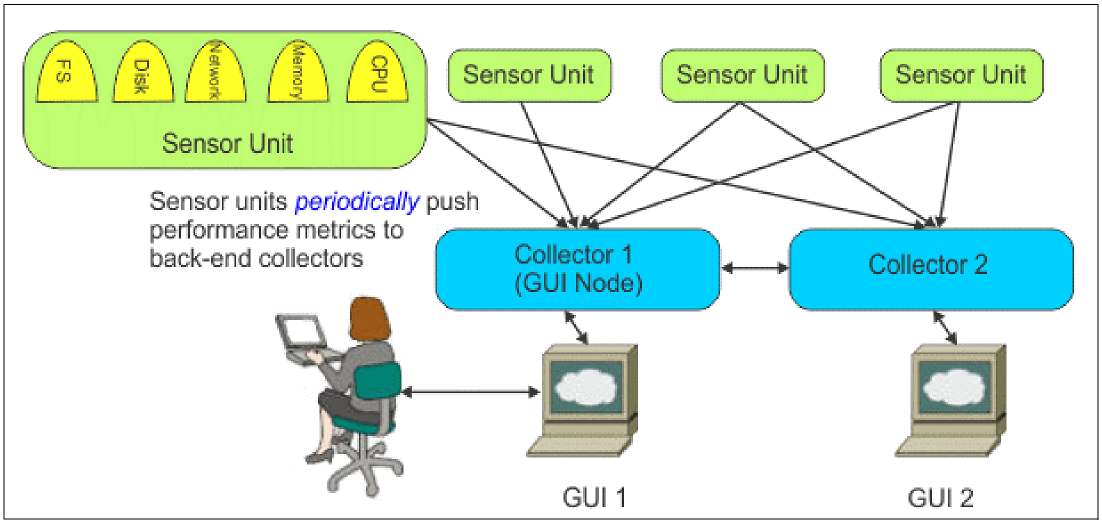


Figure 4-2 Performance monitoring configuration for GUI

You can use the **Services** → **Performance Monitoring** page to configure sensors. You can also use 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.

The performance monitoring tool installation can have a single collector or can consist of multiple collectors to increase the scalability or the fault-tolerance of the performance monitoring system. This latter configuration is referred to as “federation”.

You can configure the system to monitor the performance of the following functional areas in the system:

- Network
- InfiniBand 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 GUI Statistics page display options

The **Monitoring** → **Statistics** page is used for selecting the attributes that are based on which the performance of the system are monitored and comparing the performance that is based on the selected metrics. You can monitor the performance aspects of both local cluster and remote clusters. You can also use this page to monitor capacity.

The customized charts that are marked as favorite charts can be selected when you add widgets in the dashboard. You can display one or two charts at a time in the Statistics page.

The predefined performance charts and metrics help in investigating every node or any specific node that is collecting the metrics. Various configuration options that are available in the Statistics window of the management GUI are shown in Figure 4-3.

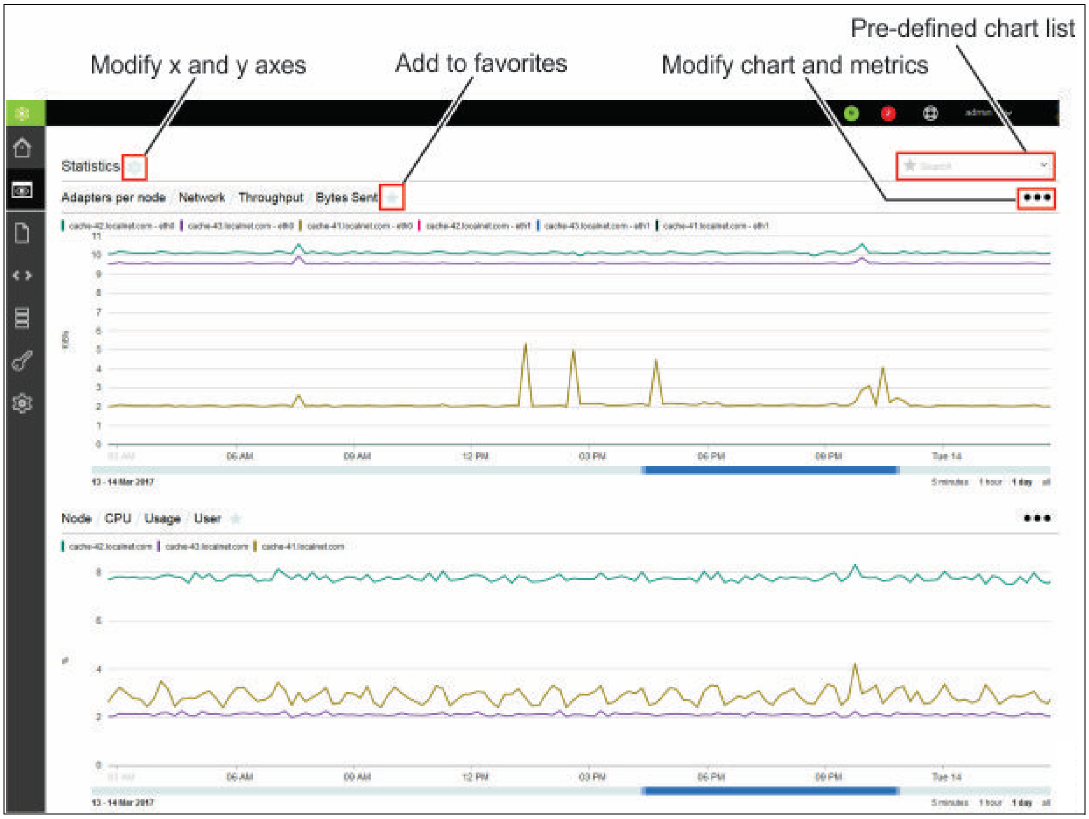


Figure 4-3 Statistics page in the ESS GUI

Predefined charts can be selected from a predefined chart list. You can add charts to this predefined list by clicking **Favorites**.

Performance charts display options

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.
- 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 that is 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.
- The Dashboard page helps to access all charts, which are 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 (see Figure 4-4).

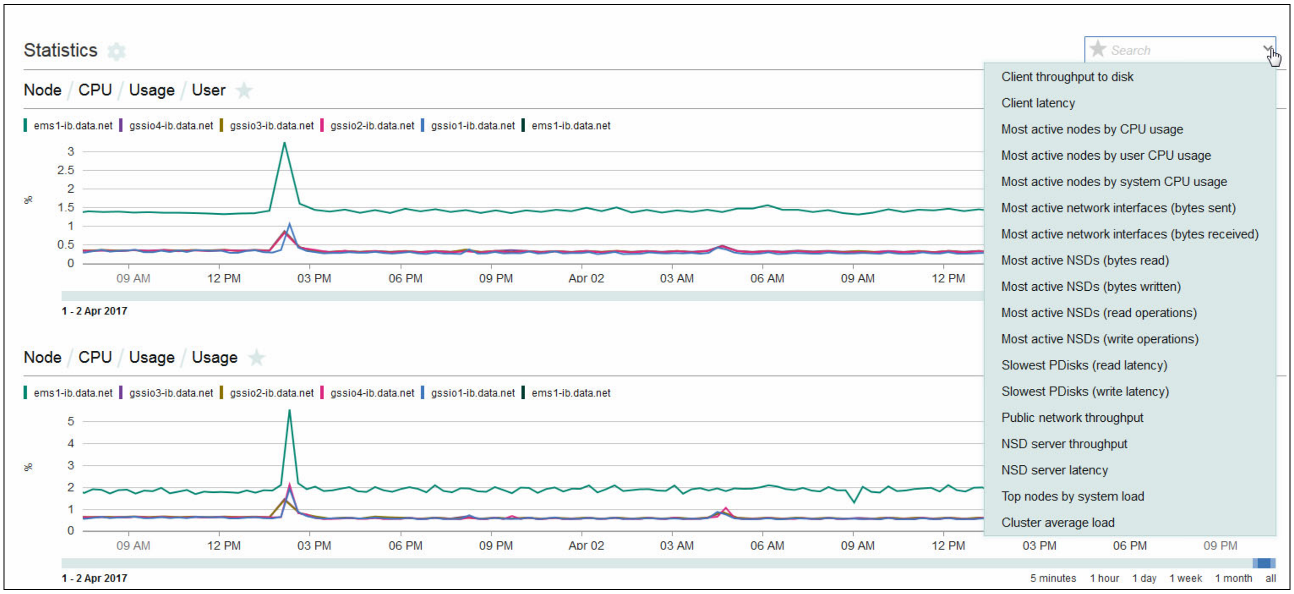
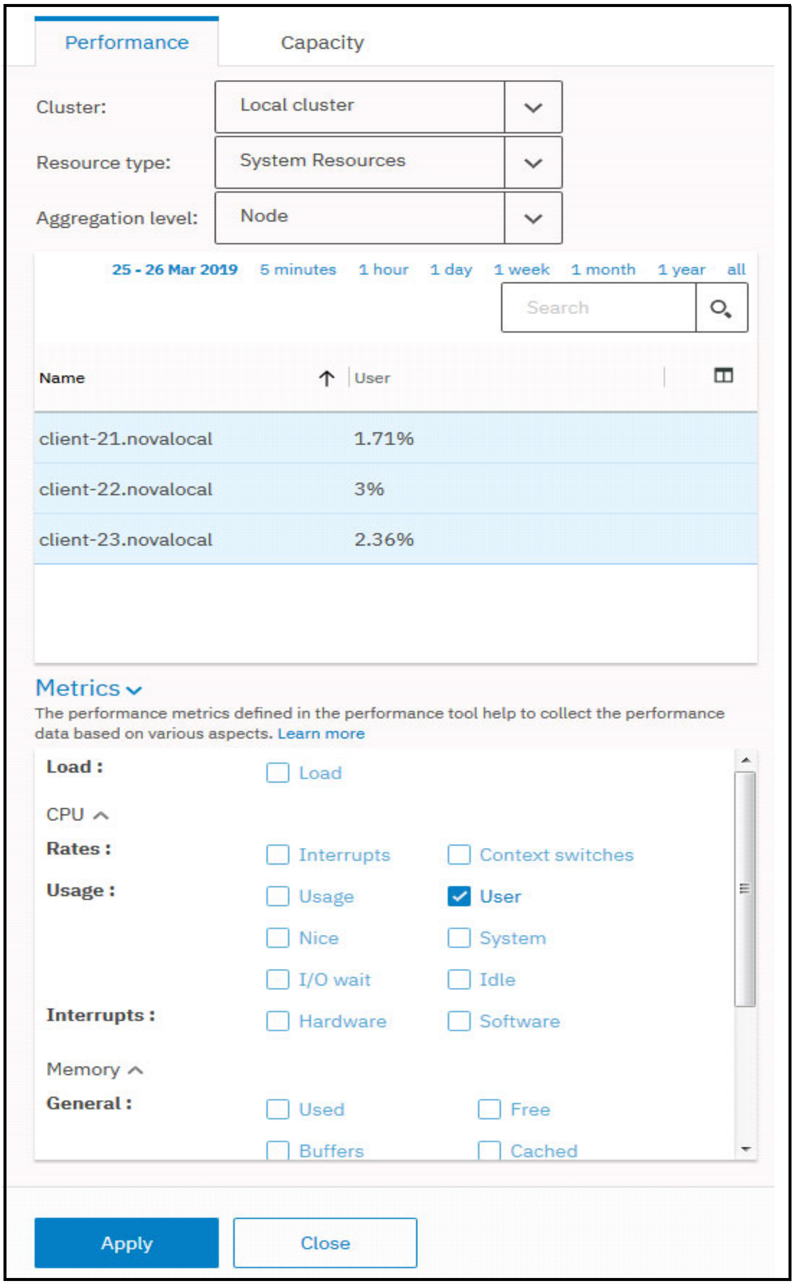


Figure 4-4   List of predefined charts in the Statistics window

Creating customized performance charts

Complete the following steps to create performance charts:

1. Click **Edit** in the menu to view the modification options. The performance and capacity options appear, as shown in Figure 4-5.



Cluster: Local cluster

Resource type: System Resources

Aggregation level: Node

Name	User
client-21.novalocal	1.71%
client-22.novalocal	3%
client-23.novalocal	2.36%

The performance metrics defined in the performance tool help to collect the performance data based on various aspects. Learn more

Load : □ Load

CPU

Rates : □ Interrupts □ Context switches

Usage : □ Usage ☑ User □ Nice □ System □ I/O wait □ Idle

Interrupts : □ Hardware □ Software

Memory

General : □ Used □ Free □ Buffers □ Cached

Figure 4-5 Options to create a performance chart on the Statistics page

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 whether you need to monitor performance of the local cluster or remote cluster from the **Cluster** field.

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

4.2.2 Using dashboard to view performance charts

The **Monitoring** → **Dashboard** page provides an easy-to-read, single-page, 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. 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

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

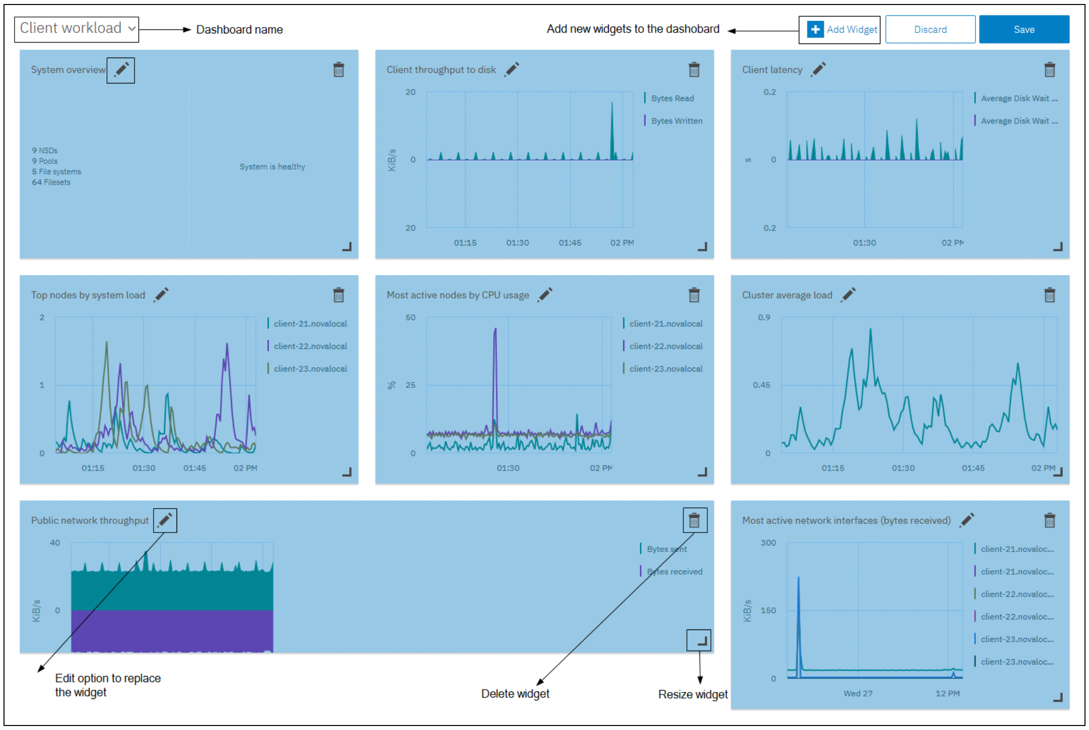


Figure 4-6 Dashboard page in the edit mode

4.2.3 Custom Dashboards

Select the **Create Dashboard** and **Delete Dashboard** options from the menu in the upper-right corner of the Dashboard page to create and delete dashboards. The dashboards are stored centrally in the cluster configuration repository (CCR). If several GUI nodes are configured in a cluster, all of the saved dashboards are available to all GUI users 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.

4.2.4 Display options

Select **Display Options** from the menu that is available in the upper-right corner of the Dashboard GUI page to change the display options.

4.2.5 Widget options

Several dashboard widgets can be added in a selected dashboard layout. Select the **Edit Widgets** option from the menu in 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.

4.3 Monitoring waiters

The metrics that are 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.

4.4 Monitoring capacity

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

The capacity details that are displayed in the GUI are obtained from the following sources:

- GPFS quota database. The system collects the quota details for users, groups, and filesets on a daily basis and stores them in the postgres database.
- Performance monitoring tool. The GUI queries the performance monitoring capacity and displays capacity data in various pages in the GUI.

Based on the source of the capacity information, different procedures must be performed to enable capacity and quota data collection.

For GPFS quota database and performance monitoring tool-based capacity and quota collection, you must use the **Files** → **Quotas** page to enable quota data collection per file system and enforce quota limit checking. Consider the following points if quota is not enabled for a file system:

- No capacity and inode data is collected for users, groups, and filesets.
- Quota limits for users, groups, and filesets cannot be defined.
- No alerts are sent, and the data writes are not restricted.

To enable capacity data collection from the performance monitoring tool, the `GPFSFilesetQuota` sensor must be enabled. For more information about how to enable the performance monitoring sensor for capacity data collection, see *Manual installation of IBM Spectrum Scale GUI in IBM Spectrum Scale: Concepts, Planning, and Installation Guide*.

4.4.1 Capacity data obtained from the GPFS quota database

The capacity and quota information collected from the GPFS quota database is displayed on the following pages in the management GUI:

- **Files** → **Quotas**

  Use quotas 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 page.

  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 possible in the command-line interface only.

  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 used capacity goes below the soft limit. If you set a hard limit quota, you cannot save data after the quota is reached. If the quota is exceeded, you must delete files or raise the quota limit to store more data.

  > **Note:** Consider the following points:
  >
  > - User or user group quotas for filesets are supported only if the Per Fileset option is enabled at the file system level. Use the command-line interface to set the option. For more information, see the man pages of the `mmcrfs` and `mmchfs` commands.
  > - You must unmount a file system to change the quota enablement method from per file system to per fileset or vice versa.

  You can set 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 fileset are 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.

  After reconfiguring quota settings, it is recommended to run the `mmcheckquota` command for the affected file system to verify the changes.

For more information about how to manage quotas, see *Managing GPFS quotas section in the IBM Spectrum Scale: Administration Guide.*

Capacity data from users, groups, and filesets with no quota limit set are not listed in the Quotas page. Use the **Files** → **User Capacity** page to see capacity information of such users and groups. Use the **Files** → **Filesets** page to view current and historic capacity information of filesets.

- **Files** → **User Capacity**

  The **Files** → **User Capacity** page provides predefined capacity reports for users and groups. While capacity information of file systems, pools, and filesets is available in the respective areas of the GUI, the **Files** → **User Capacity** page is the only place where information on used capacity per user or group is available.

  The User Capacity page depends on the quota accounting method of the file system. You must enable quota for a file system to display the user capacity data. If quota is not enabled, you can follow the fix procedure in the **Files** → **Quotas** page or use the `mmchfs <Device> -Q yes` CLI command to enable quota.

  Even if the capacity limits are not set, the User Capacity page shows data when the quota accounting is enabled, and users can start writing the data. In the Quotas page, only users and groups with quota limits defined are listed. The user and group capacity quota information is automatically collected once a day by the GUI.

  For users and user groups, you can see the total capacity and whether quotas are set for these objects. You can also see 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). Use the **Files** → **Quotas** page to change the quota limits.

4.4.2 Capacity data collected through the performance monitoring tool

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. When the IBM Spectrum Scale system is installed through the installation toolkit, the capacity data collection is configured by default. In other cases, you must enable capacity sensors manually.

If the capacity data collection is not configured correctly, you can use `mmperfmon` CLI command or the **Services** → **Performance Monitoring** → **Sensors** page.

The **Services** → **Performance Monitoring** → **Sensors** page allows you to view and edit the sensor settings. By default, the collection periods of capacity collection sensors are set to collect data with a period of up to one day. Therefore, it might take a while until the data is refreshed in the GUI.

The following sensors are collecting capacity related information and are used by the GUI:

- GPFSDiskCap

  NSD, Pool and File system level capacity. Uses the `mmdf` command in the background and typically runs once per day as it is resource intensive. Should be restricted to run on a single node only.

- GPFSPool

  Pool and file system level capacity. Requires a mounted file system and typically runs every 5 minutes. Should be restricted to run on a single node only.

- GPFSFilesetQuota

  Fileset capacity based on the quota collection mechanism. Typically, runs every hour. Should be restricted to run only on a single node.

- GPFSFileset

  Inode space (independent fileset) capacity and limits. Typically runs every 5 minutes. Should be restricted to run only on a single node.

- DiskFree

  Overall capacity and local node capacity. Can run on every node.

4.4.3 Capacity information for file systems, pools, NSDs, and filesets

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

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**

The Filesets grid and details depend on quota that is obtained from the GPFS quota database and the performance monitoring sensor GPFSFilesetQuota. If quota is disabled, the system displays a warning dialog in the Filesets page.

4.5 Monitoring system health

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

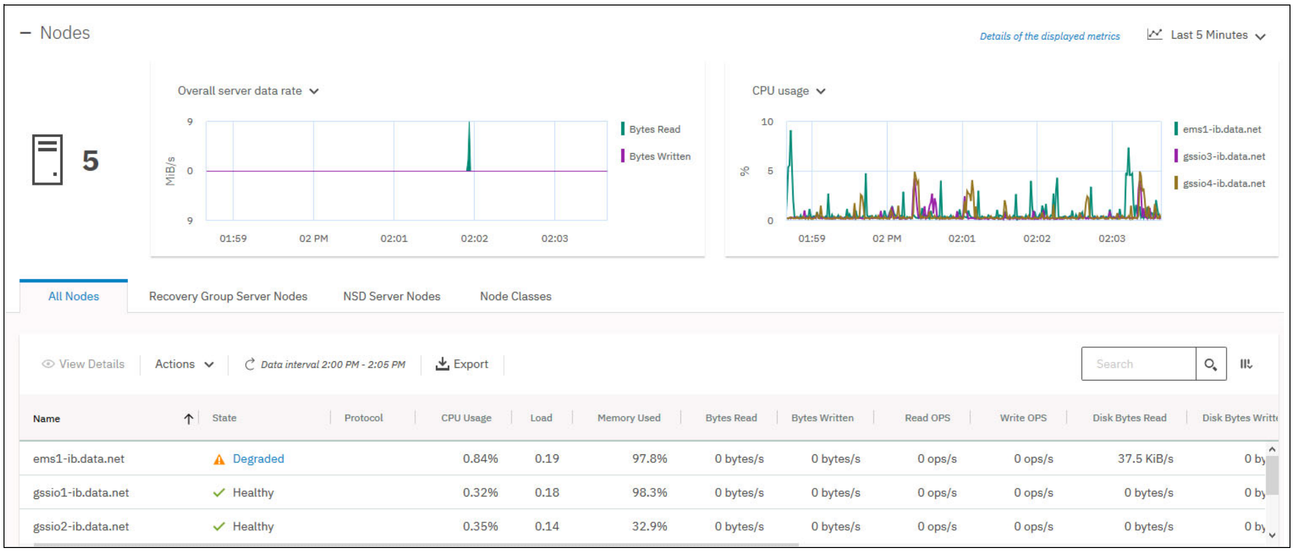
Table 4-2 System health monitoring options available in ESS GUI

GUI window	Functions
Monitoring → **Hardware**	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.
Monitoring → **Hardware Details**	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.
Monitoring → **Events**	Lists the events that are reported in the system. You can monitor and troubleshoot errors on your system on the Events page.
Monitoring → **Tips**	Lists the events of type “tips”. The tip events give recommendations to the user about certain events that might occur in the future.
Home	Provides the overall system health of the ESS system.

GUI window	Functions
Nodes	Displays the health status of nodes and lists the events reported at the node level.
Cluster → **Network**	Displays health status and configuration aspects of all available networks and interfaces that are part of the networks.
Files → **File Systems**	Displays the health status of file systems and lists the events reported at the file system level.
Files → **Filesets**	Displays the health status of filesets and lists the events reported at the fileset level.
Files → **Transparent Cloud Tiering**	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.
Files → **Active File Management**	Displays health status and lists events reported for AFM cache relationship, AFM disaster recovery (AFMDR) relationship, and gateway nodes.
Storage → **Pools**	Displays health status and lists events that are reported for storage pools.
Storage → **NSDs**	Displays health status of NSDs and lists the events that are reported at the NSD level.
Monitoring → **Command Audit Log**	Displays a record of various actions that are performed on the system. This record helps the system administrator to audit the commands and tasks that are performed by the administrators. These logs also can be used to troubleshoot issues that are reported in the system.
Health indicator that is available in the upper right corner of the GUI	Displays the number of events with warning and critical status that is specific to each component.
System overview widget in the **Monitoring** → **Dashboard** window	Displays the number of events that is reported against each component.
System health events widget in the **Monitoring** → **Dashboard** window	Provides an overview of the warning and error events that are reported in the system.
Timeline widget in the **Monitoring** → **Dashboard** window	Displays the events that are reported in a selected time frame on the selected performance chart.
Storage → **Declustered Arrays**	Displays the health information and properties of the declustered arrays and recovery groups.
Storage → **Physical Disks**	Displays the health information and properties of physical disks (PDisks).
Storage → **Virtual Disks**	Displays the health information and properties of virtual disks (VDisks).

4.6 Monitoring nodes

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



Name	State	Protocol	CPU Usage	Load	Memory Used	Bytes Read	Bytes Written	Read OPS	Write OPS	Disk Bytes Read	Disk Bytes Writt
ems1-ib.data.net	⚠ Degraded		0.84%	0.19	97.8%	0 bytes/s	0 bytes/s	0 ops/s	0 ops/s	37.5 KiB/s	0 by
gssio1-ib.data.net	✓ Healthy		0.32%	0.18	98.3%	0 bytes/s	0 bytes/s	0 ops/s	0 ops/s	0 bytes/s	0 by
gssio2-ib.data.net	✓ Healthy		0.35%	0.14	32.9%	0 bytes/s	0 bytes/s	0 ops/s	0 ops/s	0 bytes/s	0 by

Figure 4-7 Nodes window

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

4.6.1 Nodes tables

The following specific nodes tables 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 that is related to NSDs. If no NSD servers exist in the cluster, this table is not displayed.

- Protocol nodes

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

- Recovery group server nodes

  Shows all nodes that host the recovery groups and declustered arrays for ESS.

These tables can be customized individually by adding or removing columns by using the **Customize Columns** option.

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) was 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 occur briefly if a service is being restarted because of 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.

4.6.2 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 that is 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 following displayed time frame:

  - 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-day time frame

- A Nodes table that displays many different performance metrics. To find nodes with extreme values, you can sort the values that are 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, such as 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 information, see 5.2, "Mounting a file system through GUI" on page 65, and 5.3, "Unmounting a file system through GUI" on page 65.
- 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.

4.6.3 Creating and managing user-defined node classes

Node classes are used to group nodes. It helps you to select only the required set of nodes when you want to limit the scope of certain administrative tasks. The following types of node classes can be defined in the IBM Spectrum Scale system:

- System node classes
- User-defined node classes

The system node classes are hardcoded, but you can create user-defined node classes by using the **Nodes** → **Node Classes** → **Create Node Class** option in the ESS GUI. While creating a node class, consider the following points:

- The name of the new node class must be different from the name of the existing nodes or node classes.
- You can add individual nodes and other existing node classes in a new node class from the **All Nodes** and **Node Classes** tabs of the Create Node Class window.
- When you add an existing node class in the new node class, the nodes that are part of the existing node class become part of the new node class. When nodes are added or removed in the existing node class at a later time, those changes also are applied to the new node class.

Use the **Modify** option to change the node class name and nodes and node classes that are part of an existing node class. You cannot modify system node classes.

Use the **Delete** option to delete the user-defined node class. You cannot delete the system node classes.

4.7 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.

Transparent Cloud Tiering service features the following core functions (see Figure 4-8 on page 41):

- 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.

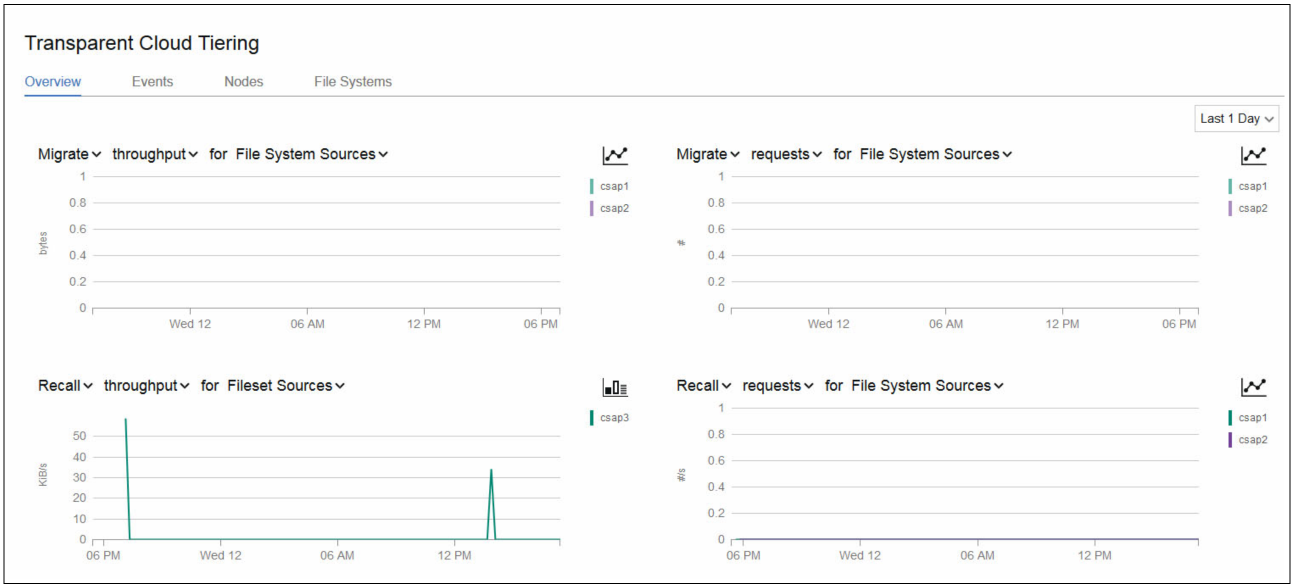


Figure 4-8 Transparent Cloud Tiering window

The **Files** → **Transparent Cloud Tiering** window provides performance and health details of the Transparent Cloud Tiering service through various charts that are available under the following 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 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.

4.8 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

The AFM GUI architecture is shown in Figure 4-9.

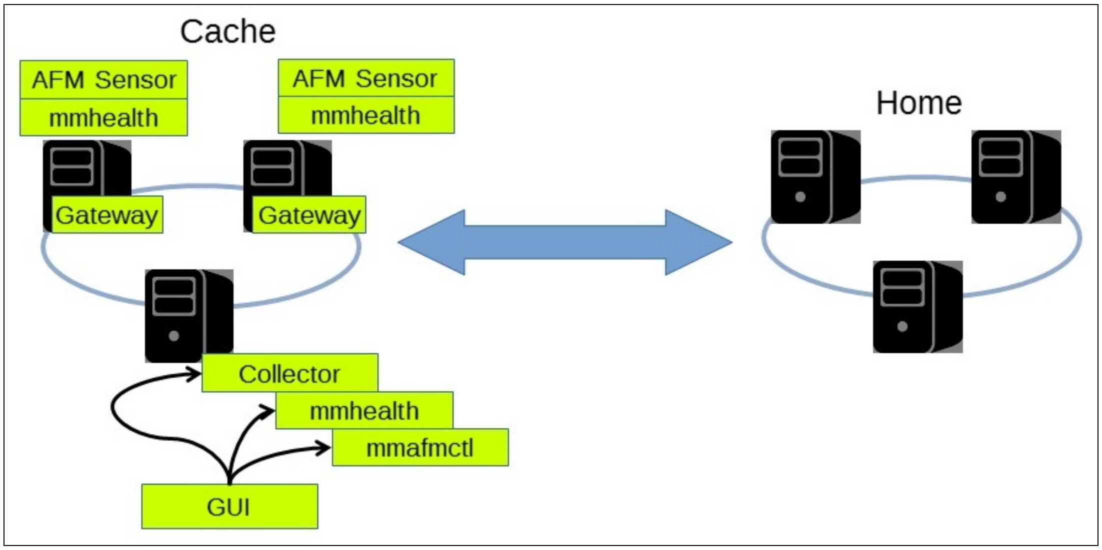
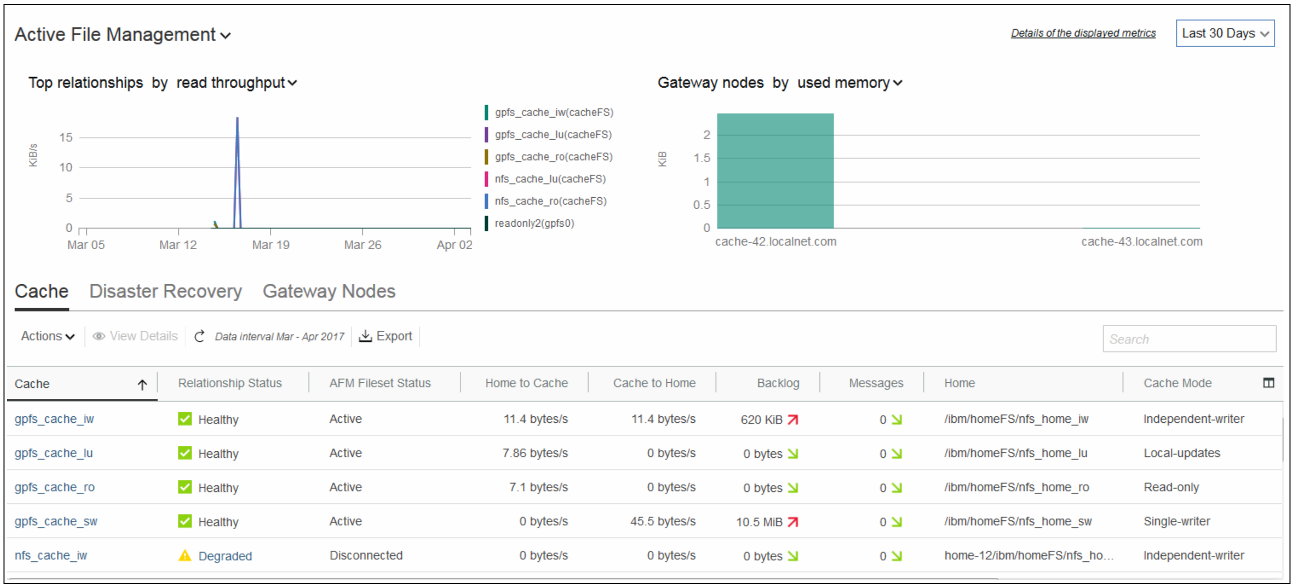


Figure 4-9 AFM GUI architecture

The Active File Management window in the GUI is shown in Figure 4-10.



Cache	Relationship Status	AFM Fileset Status	Home to Cache	Cache to Home	Backlog	Messages	Home	Cache Mode
gpfs_cache_iw	✓ Healthy	Active	11.4 bytes/s	11.4 bytes/s	620 KiB ↗	0 ↘	/ibm/homeFS/nfs_home_iw	Independent-writer
gpfs_cache_lu	✓ Healthy	Active	7.86 bytes/s	0 bytes/s	0 bytes ↘	0 ↘	/ibm/homeFS/nfs_home_lu	Local-updates
gpfs_cache_ro	✓ Healthy	Active	7.1 bytes/s	0 bytes/s	0 bytes ↘	0 ↘	/ibm/homeFS/nfs_home_ro	Read-only
gpfs_cache_sw	✓ Healthy	Active	0 bytes/s	45.5 bytes/s	10.5 MiB ↗	0 ↘	/ibm/homeFS/nfs_home_sw	Single-writer
nfs_cache_iw	⚠ Degraded	Disconnected	0 bytes/s	0 bytes/s	0 bytes ↘	0 ↘	home-12/ibm/homeFS/nfs_ho...	Independent-writer

Figure 4-10 Active File Management window

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 refresh intervals correspond 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-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-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, 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 the 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 that are reported for the AFM component.
    - Snapshots: Provides details of the snapshots that are available for the AFM fileset. The snapshots are taken for backup purposes. The snapshot that is 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 that is used for the queue.
    - Events: Provides details of the system health events that are reported for the AFM component.

- Snapshots: Provides details of the snapshots that are available for the AFM fileset. The snapshots that are taken in the AFM DR are called *recovery point objective (RPO) snapshots*. These peer snapshots are taken at the same time on the primary and the secondary sites.
- Gateway Nodes: Provides details of the nodes that are configured as gateway node in the AFM configuration.

4.8.1 Gateway nodes

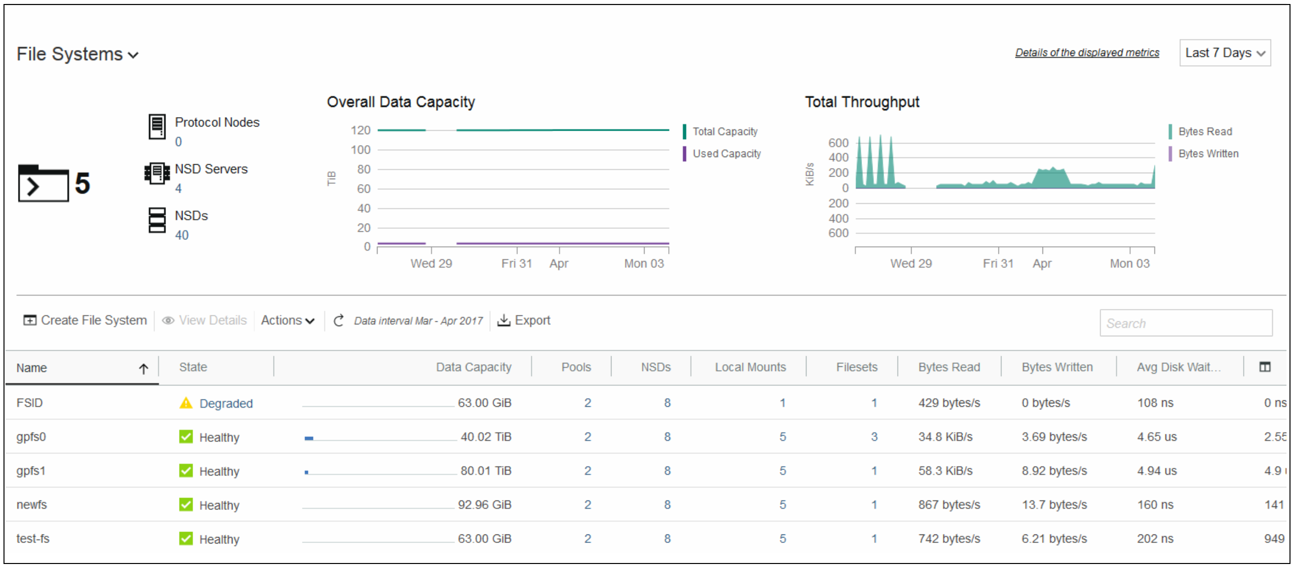
The details of gateway nodes are available under the following tabs. The same details are also available on the **Nodes** page:

- The Overview tab provides performance chart for the following information:
  - 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, such as 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 that are 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 must 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.

4.9 Monitoring file systems

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



Name	State	Data Capacity	Pools	NSDs	Local Mounts	Filesets	Bytes Read	Bytes Written	Avg Disk Wait...	
FSID	Degraded	63.00 GiB	2	8	1	1	429 bytes/s	0 bytes/s	108 ns	0 ns
gpfs0	Healthy	40.02 TiB	2	8	5	3	34.8 KiB/s	3.69 bytes/s	4.65 us	2.55
gpfs1	Healthy	80.01 TiB	2	8	5	1	58.3 KiB/s	8.92 bytes/s	4.94 us	4.9
newfs	Healthy	92.96 GiB	2	8	5	1	867 bytes/s	13.7 bytes/s	160 ns	141
test-fs	Healthy	63.00 GiB	2	8	5	1	742 bytes/s	6.21 bytes/s	202 ns	949

Figure 4-11 File Systems window

The following options are available to analyze the 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 that are displayed in the quick view are refreshed regularly. The refresh intervals depend on the following displayed time frames:

  - 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-day time frame

- A file systems table that displays many different performance metrics. To find file systems with extreme values, you can sort the values that are 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.

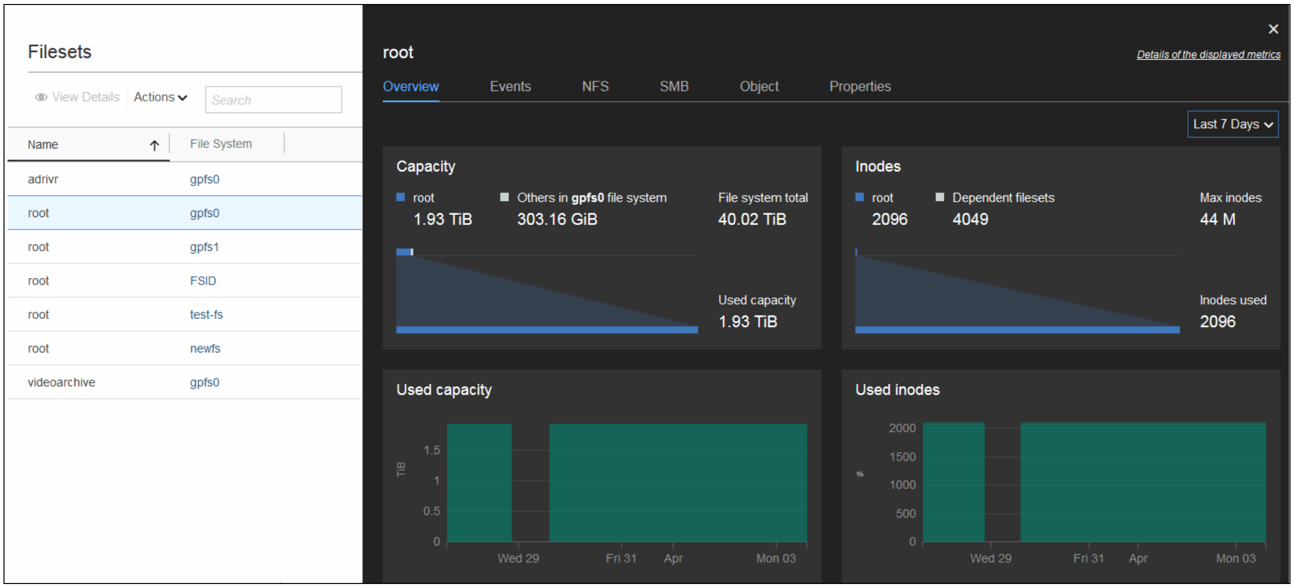
- A detailed view of the performance and health aspects of individual file systems. To see the detailed view, double-click the file system for which you need to view the details or select the file system and click **View Details**.

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

- Overview: Provides an overview of the file system performance.
- Events: System health events that are 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. You can also perform the tasks, such as mount file system, unmount file system, and specify whether to automatically mount file system if GPFS daemon starts or prevent any mounts of this file system on selected nodes.
- Filesets: Details of the filesets that are part of the file system.
- NFS: Details of the NFS exports that are created in the file system.
- SMB: Details of the SMB shares that are 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.

4.10 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 (see Figure 4-12).



Name	File System
adrivr	gpfs0
root	gpfs0
root	gpfs1
root	FSID
root	test-fs
root	newfs
videoarchive	gpfs0

Capacity

root 1.93 TiB

Others in **gpfs0** file system 303.16 GiB

File system total 40.02 TiB

Used capacity 1.93 TiB

Inodes

root 2096

Dependent filesets 4049

Max inodes 44 M

Inodes used 2096

Figure 4-12 Filesets window in the detailed view

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.

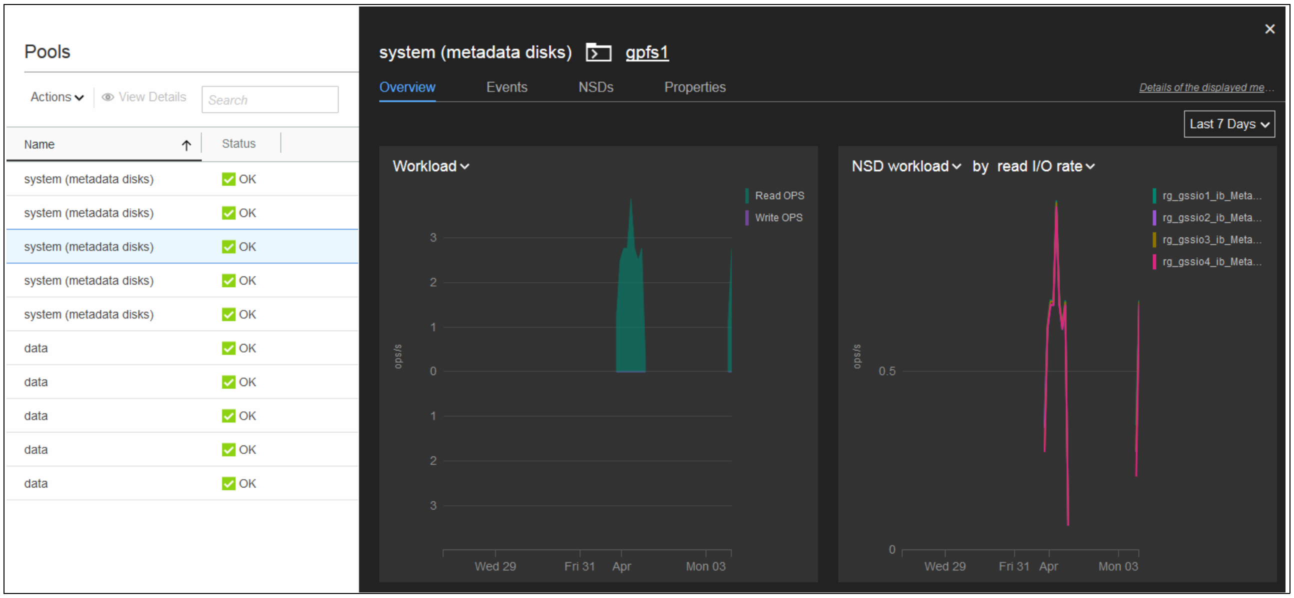
- An *overview* section that displays the fileset size and growth rates in graphical format. If you enabled quota accounting and the `GPFSFilesetQuota` sensor is active, you can view reports on fileset size distribution, absolute and relative growth, and growth rates by size range. You can change the observed time frame from the upper right corner of the display. The fileset display interacts with the filesets table so that selection in the graphical display correlates to the selection in the table.
- A detailed view of the performance and health aspects of individual filesets. To see the detailed view, you can 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 details 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 that are reported for the fileset.
  - NFS: Details of the NFS exports that are created in the fileset.
  - SMB: Details of the SMB shares that are 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.

4.11 Monitoring pools

The **Storage** → **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 (see Figure 4-13).



Name	Status
system (metadata disks)	✓ OK
system (metadata disks)	✓ OK
system (metadata disks)	✓ OK
system (metadata disks)	✓ OK
system (metadata disks)	✓ OK
data	✓ OK
data	✓ OK
data	✓ OK
data	✓ OK
data	✓ OK

Figure 4-13 Pools window in the detailed view

The systems pool contains metadata for the entire 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. Click the **Refresh** button above the table to refresh the table with more recent data.

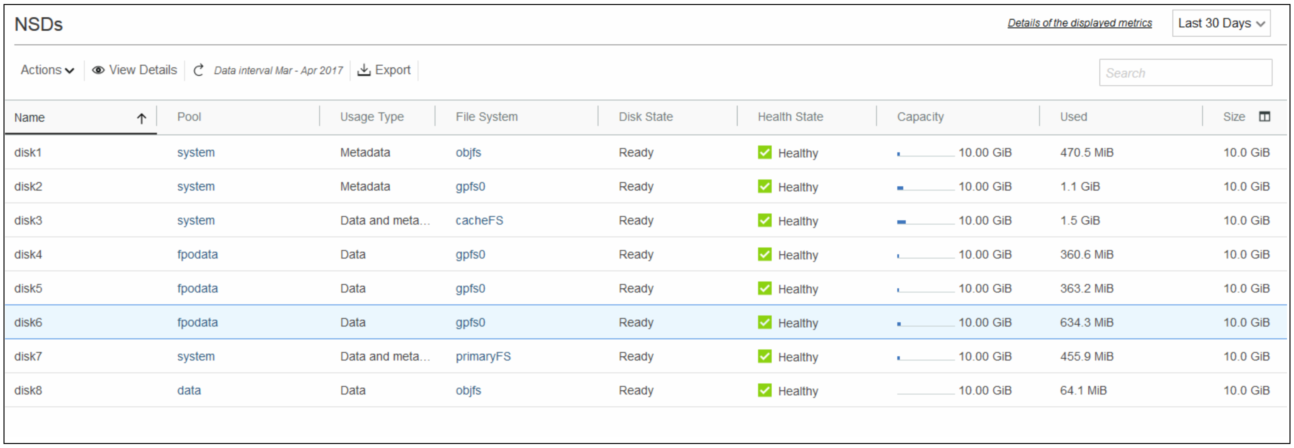
- A detailed view of the performance and health aspects of individual pools. To see the detailed view, double-click the pool for which you need to view the details or select the pool and click **View Details**.

  The detailed performance view helps to drill-down to various performance aspects. The following performance details 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 that are reported for the file system.
  - NSDs: Details of the NSDs that are part of the file system.
  - Properties: Overview of the pool's properties.

4.12 Monitoring NSDs

The **Storage** → **NSDs** page provides an easy way to monitor the performance, health status, and configuration aspects of the all Network Shared Disks (NSDs) that are available in the ESS cluster (see Figure 4-14 on page 49).



NSDs

Details of the displayed metrics
Last 30 Days
Actions
View Details
Data interval Mar - Apr 2017
Export
Search

Name	Pool	Usage Type	File System	Disk State	Health State	Capacity	Used	Size
disk1	system	Metadata	objfs	Ready	✓ Healthy	10.00 GiB	470.5 MiB	10.0 GiB
disk2	system	Metadata	gpfs0	Ready	✓ Healthy	10.00 GiB	1.1 GiB	10.0 GiB
disk3	system	Data and meta...	cacheFS	Ready	✓ Healthy	10.00 GiB	1.5 GiB	10.0 GiB
disk4	fpodata	Data	gpfs0	Ready	✓ Healthy	10.00 GiB	360.6 MiB	10.0 GiB
disk5	fpodata	Data	gpfs0	Ready	✓ Healthy	10.00 GiB	363.2 MiB	10.0 GiB
disk6	fpodata	Data	gpfs0	Ready	✓ Healthy	10.00 GiB	634.3 MiB	10.0 GiB
disk7	system	Data and meta...	primaryFS	Ready	✓ Healthy	10.00 GiB	455.9 MiB	10.0 GiB
disk8	data	Data	objfs	Ready	✓ Healthy	10.00 GiB	64.1 MiB	10.0 GiB

Figure 4-14 NSDs window

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 that are 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 can 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 details can be obtained from each tab of the detailed view:

  – Overview: Overview of the NSD performance details.

  – Events: System health events that are reported for the NSD.

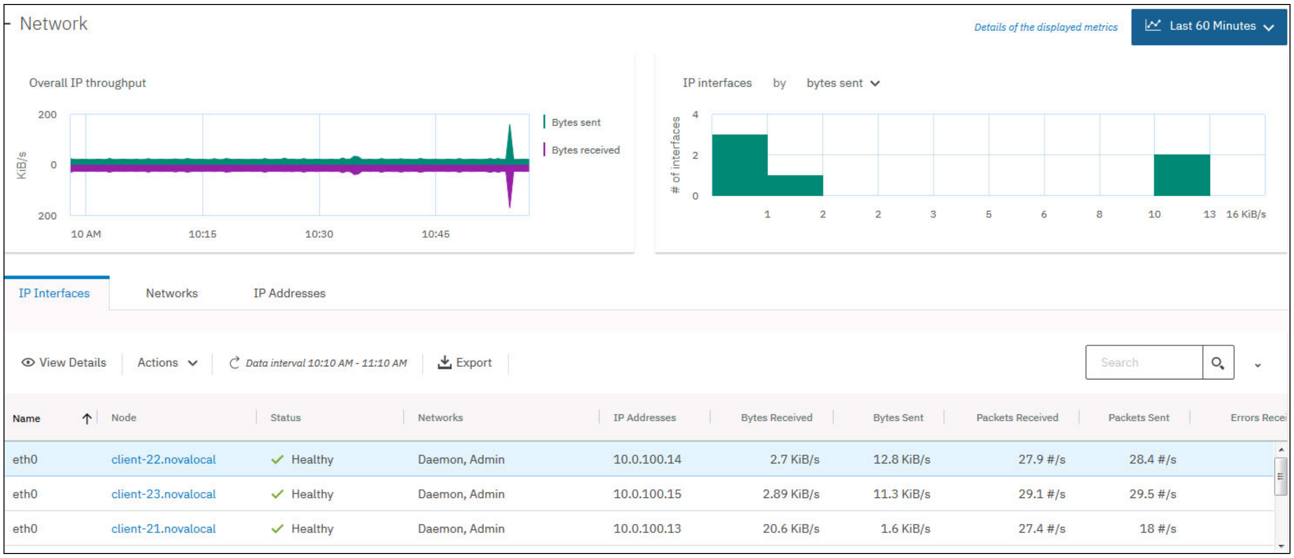
  – Nodes: Details of the nodes that serve the NSDs.

  – 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.

4.13 Monitoring networks by using GUI

The **Cluster** → **Network** page (see Figure 4-15) provides an easy way to monitor the performance, health status, and configuration aspects of all available networks and their interfaces that are part of the networks.



Name	Node	Status	Networks	IP Addresses	Bytes Received	Bytes Sent	Packets Received	Packets Sent	Errors Recei
eth0	client-22.novalocal	✓ Healthy	Daemon, Admin	10.0.100.14	2.7 KiB/s	12.8 KiB/s	27.9 #/s	28.4 #/s	
eth0	client-23.novalocal	✓ Healthy	Daemon, Admin	10.0.100.15	2.89 KiB/s	11.3 KiB/s	29.1 #/s	29.5 #/s	
eth0	client-21.novalocal	✓ Healthy	Daemon, Admin	10.0.100.13	20.6 KiB/s	1.6 KiB/s	27.4 #/s	18 #/s	

Figure 4-15 Network page

A dedicated network is used within the cluster for certain operations. For example, the system uses the administration network when an administration command is issued. It is also used for sharing administration-related information. This network is used for node-to-node communication within the cluster.

The daemon network is used for sharing file system or other resources data. Remote clusters also establish communication path through the daemon network. Similarly, the dedicated network types like CES network and external network can also be configured in the cluster.

The performance of network is monitored by monitoring the data transfer managed through the respective interfaces. The following types of network interfaces can be monitored through the GUI:

- IP interfaces on Ethernet and InfiniBand adapters.
- Remote Direct Memory Access (RDMA) interfaces on InfiniBand adapters with Open Fabrics Enterprise Distribution (OFED) drivers.

The GUI retrieves performance data from the performance monitoring tool. The IP-adapter-based metrics are taken from the Network sensor and the RDMA metrics are taken from the InfiniBand sensor. If no performance data appears in the GUI, verify that the monitoring tool is correctly set up and that these two sensors are enabled.

The Network page also exposes adapters and IPs that are not bound to a service to provide a full view of the network activity on a node.

The details of the networks and their components can be obtained both in graphical and tabular formats. The Network page provides the following options to analyze the performance and status of networks and adapters:

- A quick view that gives graphical representation of overall IP throughput, overall RDMA throughput, IP interfaces by bytes sent and received, and RDMA interfaces by bytes sent and received. You can access this view by selecting the expand button that is next to the title of the page. You can close this view if not required.

  Graphs in the overview are refreshed regularly. The refresh intervals of the top three entities are depended on the following displayed time frames:

  - Every minute for the 5-minutes time frame
  - Every 15 minutes for the 1-hour time frame
  - Every 6 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-day time frame

  If you click a block in the IP interfaces charts, the corresponding details are displayed in the IP interfaces table. The table is filtered by the IP interfaces that are part of the selected block. You can remove the filter by clicking the link that appears above the table header row.

- A table that provides the following performance metrics that are available under the following tabs of the table:

  - IP Interfaces: Shows all network interfaces that are part of the Ethernet and InfiniBand networks in the cluster. To view performance details in graphical format or to see that the events reported against the individual adapter, select the adapter in the table and then select **Actions** → **View Details**.

  - RDMA Interfaces: Shows the details of the InfiniBand RDMA networks that are configured in the cluster. To view performance details in graphical format or to see that the events reported against the individual adapter, select the adapter in the table and then select **Actions** → **View Details**.

    The system displays the RDMA Interfaces tab only if there are RDMA interfaces available.

  - Networks: Shows all networks in the cluster and provides information on network types, health status, and number of nodes and adapters that are part of the network.

  - IP Addresses: Lists all IP addresses that are configured in the cluster.

  To find networks or adapters with extreme values, you can sort the values that are displayed in the tables 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. Click the **Refresh** button that is above the table to refresh the table content with more recent data.

- A detailed view of performance aspects and events reported against each adapter. To access this view, select the adapter in the table and then select **Actions** → **View Details**. The detailed view is available for both IP and RDMA interfaces.

4.14 Monitoring remote cluster through GUI

The ESS GUI can monitor and manage a single cluster. Cluster setups exist in which multiple clusters exchange data through AFM or cross cluster mounts. To provide consolidated monitoring of multiple clusters by using the ESS GUI, monitoring information can be exchanged among GUI nodes of different clusters.

By establishing a connection between the GUI nodes, both the clusters can monitor the other cluster. To enable remote monitoring capability among clusters, the release-level of the GUI nodes that are communicating with each other must be 5.0.0 or later.

To establish a connection with the remote cluster, complete the following steps:

1. Complete the following steps on the local cluster to raise the access request:
   a. Click **Cluster** → **Remote Connections**.
   b. Select the **Request Access** option that is available under the Outgoing Requests tab to raise the request for access.
   c. In the Request Remote Cluster Access dialog, enter an alias for the remote cluster name and specify the GUI nodes to which the local GUI node must establish the connection.
   d. If you know the credentials of the security administrator of the remote cluster, you also can add the user name and password of the remote cluster administrator and skip step 2.
   e. Click **Send** to submit the request.
2. Complete the following steps on the remote cluster to grant access:
   a. When the request for connection is received in, the GUI displays the details of the request in the **Cluster** → **Remote Connections** → **Incoming Requests** page.
   b. Select Grant Access to grant the permission and establish the connection.

Now, the requesting cluster GUI can monitor the remote cluster. To enable both clusters to monitor each other, repeat the procedure with reversed roles through the respective GUIs.

> **Note:** Only the GUI user with Security Administrator role can grant access to the remote connection requests.

You can see the details of the connections established with the remote clusters under the Remote Cluster tab.

The remote cluster monitoring options that are available in the GUI are listed in Table 4-3.

Table 4-3 . Remote cluster monitoring options available in GUI

GUI option	Description
Home	The Remote clusters grouping shows the following details: ► Number of remote clusters that are connected to the resource cluster. ► Number of file systems that are mounted on the local nodes. ► Number of local nodes on which the remote file systems are mounted.
Files → File Systems	The grid view provides the following remote cluster monitoring details: ► Whether the file system is mounted on a remote cluster. ► Capacity information. ► Number of local nodes on which the file system is mounted. ► Performance details. ► Pools, NSDs, filesets, and snapshots.
Files → File Systems → View Details → Remote Nodes	Provides the details of the remote cluster nodes where the local file system
Files → Filesets	The Remote Fileset column in the filesets grid shows whether the fileset belongs to a remote file system. The fileset table also displays the same level of details for both remote and local filesets; for example, capacity, parent file system, inodes, AFM role, and snapshots.
Files → Active File Management	When remote monitoring is enabled, you can view the following AFM details: ► On home and secondary, you can see the AFM relationships configuration, health status, and performance values of the Cache and Disaster Recovery grids. ► On the Overview tab of the detailed view, the available home and secondary inodes are available. ► On the Overview tab of the detailed view, the details such as NFS throughput, IOPs, and latency details are available, if the protocol is NFS.
Files → Quotas	When remote monitoring is enabled, you can view quota limits, capacity, and inode information for users, groups, and filesets of a file system that is mounted from a remote cluster. The user and group name resolution of the remote cluster is used in this view. It is not possible to change quota limits on a file system that is mounted from a remote cluster.

GUI option	Description
Cluster → **Remote Connections**	Provides the following options: ▸ Send a connection request to a remote cluster. ▸ Grant or reject the connection requests received from remote clusters. ▸ View the details of the remote clusters that are connected to the local cluster.
Monitoring → **Statistics** and **Monitoring** → **Dashboard**	You can create customized performance charts to monitor the remote cluster performance. For more information, see "Monitoring performance of the remote cluster".

Monitoring performance of the remote cluster

You can monitor the performance of the remote cluster with the help of performance monitoring tools that are configured in the remote and local clusters. The performance details that are collected in the remote cluster is shared with the local cluster by using REST APIs.

After establishing the connection with the remote cluster by using the **Cluster** → **Remote Connections** page, you can access the performance details of the remote cluster from the following GUI pages:

- **Monitoring** → **Statistics**
- **Monitoring** → **Dashboard**
- **Files** → **File Systems**

To monitor performance details of the remote cluster in the Statistics page, you must create customized performance charts by completing the following steps:

1. Access the edit mode by clicking the icon that is available in the upper right corner of the performance chart and select **Edit**.
2. In the edit mode, select the remote cluster to be monitored from the Cluster field. You can select the l**ocal cluster** or **remote cluster** from this field.
3. Select **Resource** type. The data is taken from this area to create the performance analysis.
4. Select **Aggregation level.** This level determines the level at which the data is aggregated. The aggregation levels that are available for selection varies based on the resource type.
5. Select the entities that must be graphed. The table lists all entities that are available for the chosen resource type and aggregation level. When a metric is selected, you can also see the selected metrics in the same grid and use methods, such as sorting, filtering, or adjusting the time frame to select the entities that you want to select.
6. Select **Metrics**. These metrics are the type of data that must be included in the performance chart. The list of metrics that is available for selection varies based on the resource type and aggregation type.
7. Click **Apply** to create the customized chart.

After creating the customized performance chart, you can mark it as favorite charts so that they are displayed on the Dashboard page.

If a file system is mounted on the remote cluster nodes, the performance details of such remote cluster nodes are available in the Remote Nodes tab of the detailed view of file systems in the **Files** → **File Systems** page.

4.15 Monitoring thresholds

You can configure the IBM Spectrum Scale to raise events when certain thresholds are reached. Use the **Monitoring** → **Thresholds** page to define or modify thresholds for the data that is collected through the performance monitoring sensors.

You can set the following types of threshold levels for data collected through performance monitoring sensors:

- Warning level

  When the data that is monitored reaches the warning level, the system raises an event with severity Warning. When the observed value exceeds the current threshold level, the system removes the warning.

- Error level

  When the data that is monitored reaches the error level, the system raises an event with severity Error. When the observed value exceeds the current threshold level, the system removes the error state.

Certain types of thresholds are predefined in the system. The following predefined thresholds are available:

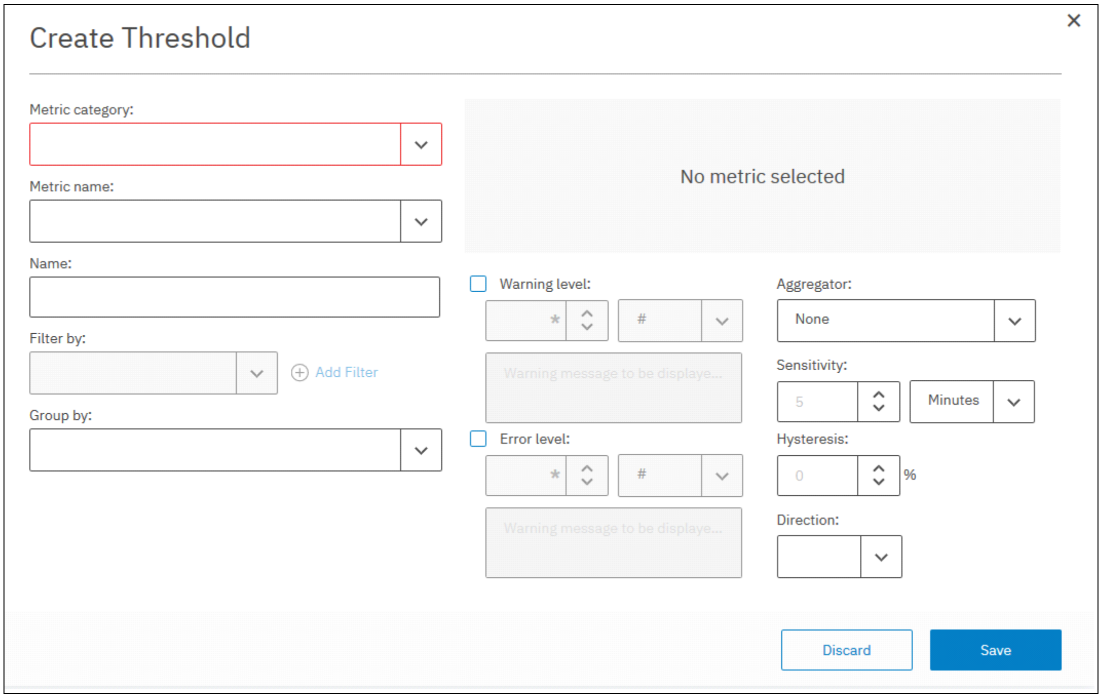
- Inode utilization at the fileset level
- Data pool capacity utilization
- Metadata pool capacity utilization
- Free memory utilization

Apart from the predefined thresholds, you can create user-defined thresholds for the data that is collected through the performance monitoring sensors.

You can use the **Monitoring** → **Thresholds** page in the GUI and the `mmhealth` command to manage predefined and user-defined thresholds.

Defining thresholds

Use the **Create Thresholds** option (see Figure 4-16) to define user-defined thresholds or to modify the predefined thresholds.



Aggregator: None

Sensitivity: 5 Minutes

Hysteresis: 0 %

Direction:

Figure 4-16 Create Threshold dialog

You can use the **Use as Template** option that is available in the Actions menu to use a defined threshold as the template to create a threshold. You can specify the following details in a threshold rule:

- Metric category

  Lists all performance monitoring sensors that are enabled in the system and thresholds that are derived by performing certain calculations on certain performance metrics. These derived thresholds are referred as *measurements*. The measurements category provides the flexibility to edit certain predefined threshold rules. The following measurements are available for selection:

  - `Fileset_inode`

    Inode capacity utilization at the fileset level. This level is calculated as shown in the following example:

    ```
    (sum(gpfs_fset_allocInodes)-sum(gpfs_fset_freeInodes))/sum(gpfs_fset_maxInod
    es)
    ```

  - `DataPool_capUtil`

    Data pool capacity utilization, which is calculated as shown in the following example:

    ```
    (sum(gpfs_pool_total_dataKB)-sum(gpfs_pool_free_dataKB))/sum(gpfs_pool_total
    _dataKB)
    ```

- `MetaDataPool_capUtil`

  Metadata pool capacity utilization, which is calculated as shown in the following example:

  ```
  (sum(gpfs_pool_total_metaKB)-sum(gpfs_pool_free_metaKB))/sum(gpfs_pool_total
  _metaKB)
  ```

- `FsLatency_diskWaitRd`

  File system latency for the read operations. Average disk wait time per read operation on the IBM Spectrum Scale client:

  ```
  sum(gpfs_fs_tot_disk_wait_rd)/sum(gpfs_fs_read_ops)
  ```

- `FsLatency_diskWaitWr`

  File system latency for the write operations. Average disk wait time per write operation on the IBM Spectrum Scale client:

  ```
  sum(gpfs_fs_tot_disk_wait_wr)/sum(gpfs_fs_write_ops)
  ```

- `SMBNodeLatency_read`

  SMB read latency at the node level:

  ```
  avg(op_time)/avg(op_count)
  ```

- `SMBNodeLatency_write`

  SMB write latency at the node level:

  ```
  avg(op_time)/avg(op_count)
  ```

- `NFSNodeLatency_read`

  NFS read latency at the node level:

  ```
  sum(nfs_read_lat)/sum(nfs_read_ops)
  ```

- `NFSNodeLatency_write`

  NFS write latency at the node level:

  ```
  sum(nfs_write_lat)/sum(nfs_write_ops)
  ```

- Metric name

  The list of performance metrics that are available under the selected performance monitoring sensor or the measurement.

- Name

  User-defined name of the threshold rule.

- Filter by

  Defines the filter criteria for the threshold rule.

- Group by

  Groups the threshold values by the selected grouping criteria. If you select a value in this field, you must select an aggregator criterion in the **Aggregator** field. By default, there is no grouping, which means that the thresholds are evaluated based on the finest available key.

- Warning level

  Defines the threshold level for warning events to be raised for the selected metric. When the warning level is reached, the system raises an event with severity Warning. You can customize the warning message to specify the user action that is required to fix the issue.

- Error level

  Defines the threshold level for error events to be raised for the selected metric. When the error level is reached, the system raises an event with severity “Error”. You can customize the error message to specify the user action that is required to fix the issue.

- Aggregator

  When grouping is selected in the Group by field, an aggregator must be chosen to define the aggregation function. When the Rate aggregator is set, the grouping is automatically set to the finest available grouping.

- Sensitivity

  Defines the sample interval value. If a sensor is configured with interval period greater than 5 minutes, the sensitivity is set to the same value as sensors period. The minimum value allowed is 120 seconds. If a sensor is configured with interval period less than 120 seconds, the `--sensitivity` is set to 120 seconds.

- Hysteresis

  Defines the percentage of the observed value that must be under or over the current threshold level to switch back to the previous state. The default value is 0 percent. Hysteresis is used to avoid frequent state changes when the values are close to the threshold. The level must be set according to the volatility of the metric.

- Direction

  Defines whether the events and messages are sent when the value that is being monitored exceeds or goes below the threshold level.

You can also edit and delete a threshold rule.

Threshold configuration: A scenario

The user wants to configure a threshold rule to monitor the maximum disk capacity usage. The values against each field of the Create Threshold dialog and their respective functionality are listed in Table 4-4.

Table 4-4 Threshold rule configuration: A sample scenario

GUI fields	Value and functions
Metric Category	GPFSDiskCap Specifies that the threshold rule is going to be defined for the metrics that belong to the GPFSDiskCap sensor.
Metric name	Total Capacity The threshold rule is going to be defined to monitor the threshold levels of total capacity usage.
Name	Total capacity threshold By default, the performance monitoring metric name is used as the threshold rule name. Here, the default value is overwritten with “Total capacity threshold”.
Filter by	Cluster The values are filtered at the cluster level.

GUI fields	Value and functions
Group by:	File System Groups the selected metric by file system.
Aggregator	Maximum When maximum capacity exceeds the threshold level, the system raises the event. If the following values are selected, the nature of the threshold rule changes: ▶ Sum: When the sum of the metric values exceeds the threshold levels, the system raises the events. ▶ Average: When the average value exceeds the average, the system raises the events. ▶ Maximum: When the maximum value exceeds maximum level, the system raises the events. ▶ Minimum: When the minimum value exceeds the sum of or goes below the threshold levels, the system raises the events. ▶ Rate: When the rate exceeds the threshold value, the system raises the events. Rate is only added for the “finest” group by clause. If we wanted to get a rate for a “partial key”, this function is not supported; that is, when Rate is selected, the system automatically selects the best possible values in the grouping field.
Warning level	9 GiB The system raises an event with severity Warning when the total capacity usage exceeds 9 GiB.
Error level	10 GiB The system raises an event with severity level Error when the total capacity usage exceeds 10 GiB.
Sensitivity	24 hours The threshold value is being monitored once in a day.
Hysteresis	50% If the value is reduced below 4.5 GiB, the warning state is removed. Similarly, if the value is reduced below 5 GiB, the error state is removed.
Direction	High When the value that is being monitored exceeds the threshold limit, the system raises an event.

4.16 Monitoring physical disks

The **Storage** → **Physical Disks** page displays health information and properties of physical disks. This page also provides capacity information and allows to run a procedure to replace one or more broken disks.

4.17 Monitoring virtual disks

The **Storage** → **Virtual Disks** page displays health information and properties of virtual disks. An NSD must be created for each vdisk to make it usable within a file system.

Some declustered arrays are used for internal purposes. Such arrays do not store any user data and they are called log arrays. The log arrays are not displayed by default, but you can display them by selecting **Show All Disks** option. Use the **Hide Log Disks** option to hide the log disks from the view.

4.18 Monitoring declustered arrays

Use the **Storage** → **Declustered Array** page in the ESS GUI to view the details of the declustered arrays that are configured in the system.

Use the View Details option that is available in the Actions menu to view more details of a declustered array. The following details are available in the detailed view:

- Events reported against the selected declustered array and for the corresponding recovery group.
- Recovery group server nodes that serve the physical disks of the corresponding recovery group.
- Physical disks that are included in the declustered array.
- Virtual disks that are created within the declustered array.
- Recovery groups to which the pdisks of the declustered array belong.

Some declustered arrays are used for internal purposes. Such arrays do not store any user data and they are called log arrays. The log arrays are not displayed by default, but you can display them by selecting the **Show All Disks** option from the **Virtual Disks** tab of the detailed view. You can access the detailed view of a declustered array by selecting the **View Details** option from the **Actions** menu.

You can use the **Replace Broken Disks** option to start the directed maintenance procedure to replace the physical disks that are in the replaceable status.

You can create a declustered array together with its member pdisks and its containing recovery group by using the **`mmchrecoverygroup`** command. You can also create a declustered array by using the **`mmaddpdisk`** command to add pdisks to a declustered array that does not yet exist in a recovery group. In an mmvdsik-enabled system, you need to use the **`mmvdisk`** command instead of **`mmchrecoverygroup`** and **`mmaddpdisk`** commands to create a recovery group.

You can create a declustered array together with its member pdisks and its containing recovery group by using the **`mmvdisk`** command.

A declustered array can be deleted by deleting its last member pdisk, or by deleting the recovery group in which it resides. Any vdisk NSDs and vdisks within the declustered array must already have been deleted. There are no explicit commands to create or delete declustered arrays.

4.19 Monitoring command audit log

The audit log maintains a record of various actions that are performed on the system. This log helps the system administrator to audit the commands and tasks that are performed by the administrators. These logs can also be used to troubleshoot issues that are reported in the system.

You can monitor the command audit log from the **Monitoring** → **Command Audit Log** page.

You can use the **`Copy Command and Arguments`** option from the **Actions** menu to copy the command and arguments that are used in an operation.

5

Configuring and managing ESS by using the GUI

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

5.1 Creating file systems

Use the Create File System option that is available in the **Files** → **File Systems** page to launch the wizard that assists you to create a file system.

On an ESS System, the Create File System wizard guides you through several steps that result in the creation of VDisks, NSDs, pools, the file system (including all settings), and a default placement policy.

The GUI expects that recovery groups and declustered arrays exist to create a file system.

The GUI detects whether the underlying system has mmvdisk-enabled recovery groups and automatically applies the correct commands to create a file system. In an environment that includes GNR- based storage and traditional NSD storage, the GUI creates file systems on the GNR-based storage only.

You can specify the following details while creating the file system through GUI:

- The file system name.
- The storage pool configuration.

  Storage pools provide storage for the file system. You can create a system pool and multiple data pools for a file system. A system pool can be used for storing metadata, data, or both. The data pool can be used only for storing data. You can also specify the following details for a pool:

  – A RAID code can be selected for each storage pool that is applied to all underlying vdisks.

  – Declustered arrays that provide storage to the pools.
- Pool size data availability settings

  Define the default replication policy for the file system by specifying the number of data and metadata copies that are required. You can later change the number of copies of data and metadata through the CLI by using the `mmchfs` command.

  You also must define the failure groups of NSDs and certain attributes that are important for the failure group definition.
- Adapt the file system to the expected data and workload by specifying the following details:

  – Size of each inode
  – Maximum number of inodes for the root fileset
  – Data and metadata block size
- Mount point and automatic mode of the file system.
- Whether to enable quota for the file system. If yes, whether the user and group quota definitions must be set at the file system level or at the individual fileset level.
- Adapt the file system to the environment and external dependencies:

  – Maximum number of IBM Spectrum Scale client nodes that can access the file system concurrently.

  – Whether to enable DMAPI for the file system.

  – The IBM Spectrum Scale release with which the file system features are compatible.

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 one of the following windows in the GUI to mount or unmount a file system:

- **Files** → **File Systems**
- **Files** → **File Systems** → **View Details** → **Nodes**
- **Nodes** → **View Details** → **File Systems**

The GUI has the following options that are 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 must be mounted.
- Prevent or allow file systems from mounting on individual nodes.

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

  a. Go to the **Nodes** page.

  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 must 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 one of the following windows in the GUI to mount or unmount a file system:

- **Files** → **File Systems**
- **Files** → **File Systems** → **View Details** → **Nodes**
- **Nodes** → **View Details** → **File Systems**

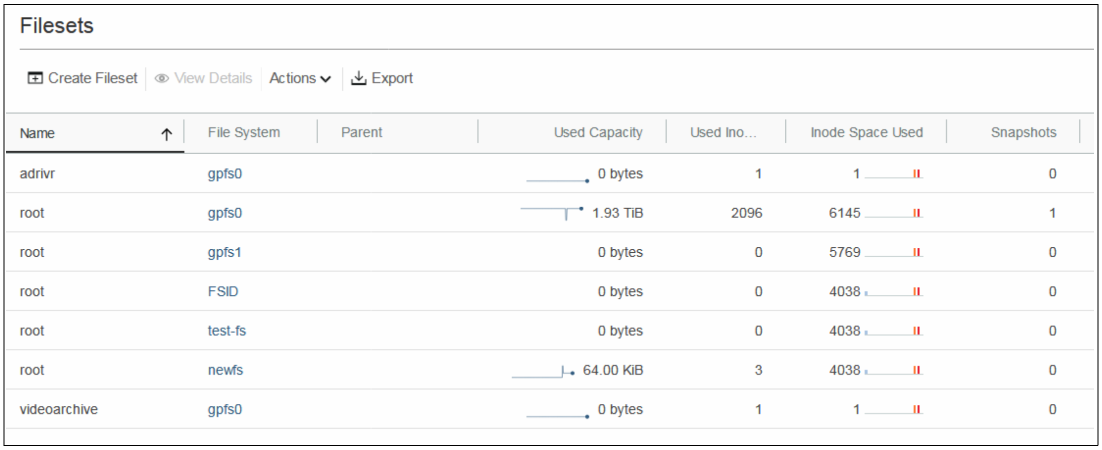
You can use the following unmount features that are supported in the GUI:

- 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 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 complete 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, such as *lsof* and *fuser*, for this goal.

5.4 Creating filesets

Use the **Files** → **Filesets** window in the GUI (see Figure 5-1) to create, manage, and monitor the filesets.



Name	File System	Parent	Used Capacity	Used Ino...	Inode Space Used	Snapshots
adrivr	gpfs0		0 bytes	1	1	0
root	gpfs0		1.93 TiB	2096	6145	1
root	gpfs1		0 bytes	0	5769	0
root	FSID		0 bytes	0	4038	0
root	test-fs		0 bytes	0	4038	0
root	newfs		64.00 KiB	3	4038	0
videoarchive	gpfs0		0 bytes	1	1	0

Figure 5-1 Filesets window

Use the **Files** → **Filesets** → **Create Fileset** option to create a fileset. You can create 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. When Quota data collection is enabled, the GUI also provides information on fileset size and growth rates.

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 a file system or fileset data and the data then recovered from the snapshot if the production data becomes unavailable.

> **Note:** Consider the following characteristics of snapshots:
>
> - Snapshots are read-only. You can change only the normal and active files and directories, not 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 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**.

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 features 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

An example of the values that are specified for these parameters is provided in Table 5-1.

Table 5-1 Example for retention period

Snapshot deletion time	**Frequency**	**Minute**	**Number of most recent snapshots**	**Keep latest snapshots for**			
				Hours	**Days**	**Weeks**	**Months**
2:30 AM	Hourly	1	2	2	6	2	3

Based on this retention rule, the snapshots that are listed in Table 5-2 are created and retained on March 20, 2016 at 06:10 AM.

Table 5-2 Example of time stamp of snapshots that are retained based on the retention policy

Time stamp	Condition based on which snapshot is retained
December 31 (Thursday, 23:01 AM)	Keep the latest snapshot for last 3 months
January 31 (Sunday, 23:01 AM)	Keep the latest snapshot for last 3 months
February 29 (Monday, 23:01 AM)	Keep the latest snapshot for last 3 months
March 5 (Saturday, 23:01 AM)	Keep the latest snapshot for last 2 weeks
March 12 (Saturday, 23:01 AM)	Keep the latest snapshot for last 2 weeks
March 14 (Monday, 23:01 AM)	Keep the latest snapshot for last 6 days
March 15 (Tuesday, 23:01 AM)	Keep the latest snapshot for last 6 days
March 16 (Wednesday, 23:01 AM)	Keep the latest snapshot for last 6 days
March 17 (Thursday, 23:01 AM)	Keep the latest snapshot for last 6 days
March 18 (Friday, 23:01 AM)	Keep the latest snapshot for last 6 days
March 19 (Saturday, 23:01 AM)	Keep the latest snapshot for last 6 days
March 20 (Sunday, 1:01 AM)	Keep two most recent snapshots.
March 20 (Sunday, 2:01 AM)	Keep two most recent snapshots

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, enter the path of the file system or independent fileset for which you need to create snapshots.
4. In the **Snapshot name** field, enter 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, enter 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 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 provided. The default snapshot ID is generated at the creation time by using the following format:

```
@GMT-yyyy.MM.dd-HH.mm.ss
```

If this option is provided and the `@GMT-date-time` format is omitted, this snapshot is not identifiable by Windows VSS and the file restore is not possible by using that method. Avoid white spaces, double and single quotation marks, 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 effect 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 also enable quota on file systems, set grace time defaults, and trigger a quota database repair action.

You can create and modify quotas. 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. Use the GUI to manage capacity-related quotas only. The inode-related quota management is possible in the command-line interface only.

You also 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 cannot 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: Consider the following points about quotas:

- User or user group quotas for filesets are supported only if the Per Fileset option is enabled at the file system level.
- You must 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 must 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 are 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 the limit is changed at the file system or fileset level.

5.7 Information Lifecycle Management

The Information Lifecycle Management (ILM) feature that is available in the ESS system facilitates automated tiered storage management. As part of the ILM, you must 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 pool with high performance storage and the non-frequently accessed files on a less expensive pool.

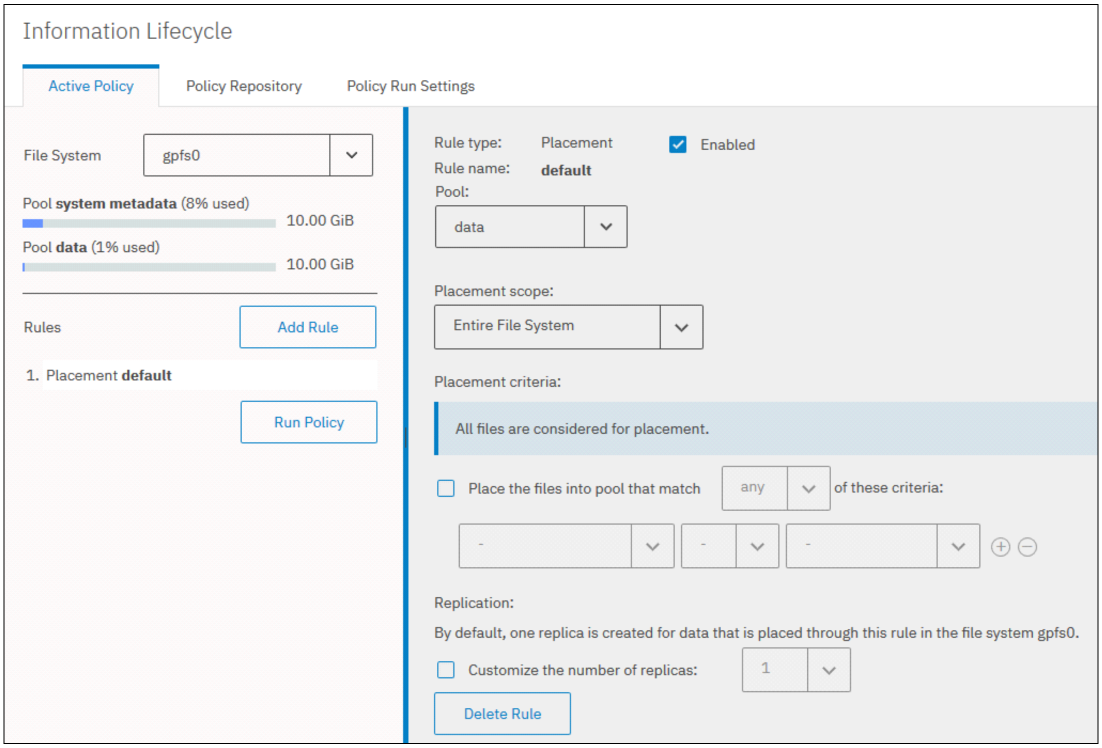
A *policy* is a set of rules that describes the lifecycle of user data that is based on the file's attributes. Each rule defines an operation or definition, such as placing new files into different pools or migrating files from one pool to another pool.

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.

ILM rules include the following main functions:

- 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, such as tape

The Information Lifecycle window is shown in Figure 5-2.



Information Lifecycle

File System: gpfs0

Pool **system metadata** (8% used) 10.00 GiB

Pool **data** (1% used) 10.00 GiB

Rules

1. Placement **default**

Rule type: Placement ☑ Enabled

Rule name: **default**

Pool: data

Placement scope: Entire File System

Placement criteria:

All files are considered for placement.

□ Place the files into pool that match any of these criteria:

Replication:

By default, one replica is created for data that is placed through this rule in the file system gpfs0.

□ Customize the number of replicas: 1

Figure 5-2 Information Lifecycle window

The active policy of a file system is available on the **Files** → **Information Lifecycle** → **Active Policy** window. Use the GUI to create more policies for a file system that can be applied manually by editing the existing active policy or creating a policy and applying 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 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.

Complete the following steps to create and apply a policy:

1. Click **Files** → **Information Lifecycle**.
2. Select **Policy Repository**.
3. Click **Create Policy** and specify the required details.

   The policy is created. Next, you must add rules in the policy that manage the files in the system. Complete the following steps:

   a. 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 supports only the option 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.

   b. 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.

4. After editing the policy details, click **Apply Changes**.
5. 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 from 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, such as encryption, exclusion, and list, you must manually edit the SQL policy text by using the text editor.

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

5.7.3 Defining the policy run settings

You can define some of the policy run parameters that are used every time the ILM policy is run from the Information Lifecycle page in the GUI.

> **Note:** The policy run settings that you set in the GUI are applicable when the policy execution is triggered by the default threshold callback or when the Run Policy action in the GUI is used. These parameters are not applicable when a custom callback script is registered or when you run the policy by using the **`mmapplypolicy`** command in the CLI.

You can specify the following details that determine the policy run characteristics:

- Node that run the policies

  The ILM policy can run parallel on multiple nodes. The following types of nodes are available:

  – Nodes of a node class.

  – Default helper nodes. Nodes can be marked as helper nodes by using the **`defaultHelperNodes`** parameter of the **`mmchconfig`** command.

  – Manager nodes. These nodes are nodes from which file system managers and token managers are selected.

  – Individual nodes.

- Local work directory

  The directory to be used for temporary storage during policy execution. This local directory, such as `/tmp`, is used on each helper node. A significant amount of temporary storage is required if the file system or directories contain many files.

- Global work directory

  A global directory to be used for temporary storage during policy execution. The specified directory must exist within a shared file system. It must also be mounted and available for writing and reading from each of the nodes. The use of a global work directory causes high performance and fault-tolerant protocols during policy execution.

- File selection algorithm. The following algorithm types are available:
  - Exact

    Sorts all the candidate files by weight, then serially considers each file from the highest weight to the lowest weight by choosing feasible candidates for migration, deletion, or listing according to any applicable rule LIMITs and current storage-pool occupancy.
  - Fast

    Uses a combination of statistical, heuristic, and parallel computing methods to favor higher weight candidate files, but the set of chosen candidates might be different than the exact method.
  - Best

    Chooses the optimal method based on the rest of the input parameters.
- Average number of CPU cores per node.

  The number of threads and sort pipelines that each node runs during the parallel inode scan and policy evaluation.
- Number of threads per policy scan.

  The number of threads is created and dispatched within each **`mmapplypolicy`** process during the directory scan phase. The default is 24.
- Number of threads for policy execution.

  The number of threads that are created and dispatched within each **`mmapplypolicy`** process during the policy execution phase. The default value is 24.
- Maximum number of files per batch.

  Specifies how many files are passed for each invocation of the EXEC script. The default value is 100. If the number of files exceeds the value that is specified, the use of the **`mmapplypolicy`** command starts the external program multiple times.

5.7.4 Log files

The policy executions that are started by using the Run Policy action logs the details in the `/var/log/cnlog/ilm` directory.

The policy executions can also be triggered based on a threshold that is managed by the callback handler, which is installed on the GUI node. Such policy execution details are logged in the `/var/adm/ras` directory and the `/var/adm/ras/mmfs.log` file.

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 5-3.

Table 5-3 Storage management options

GUI option	Functions
Storage → Pools	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.

GUI option	Functions
Storage → NSDs	Provides an easy way to monitor the performance, health status, and configuration aspects of the all Network Shared Disks (NSDs) that are available in the ESS cluster.
Storage → Physical Disks	Displays health information, capacity details, and properties of physical disks (PDisks) and the corresponding declustered arrays. This page also provides a procedure to replace one or more broken disks and replace disks.
Storage → Virtual Disks	Displays health information and properties of logical volumes (VDisks) and the corresponding declustered arrays.
Storage → Declustered Arrays	Provides the details of the declustered arrays that are configured in the system.

5.9 Managing access control lists

Use the **File → 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 often 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 wanted 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` can modify ACLs of files and directories in the **Files → File System ACLs** window.

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

Users with `DataAccess` role can 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 can 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

The options that are available to configure, monitor, and manage the data exports through the NFS, SMB, and Object protocols are listed in Table 5-4.

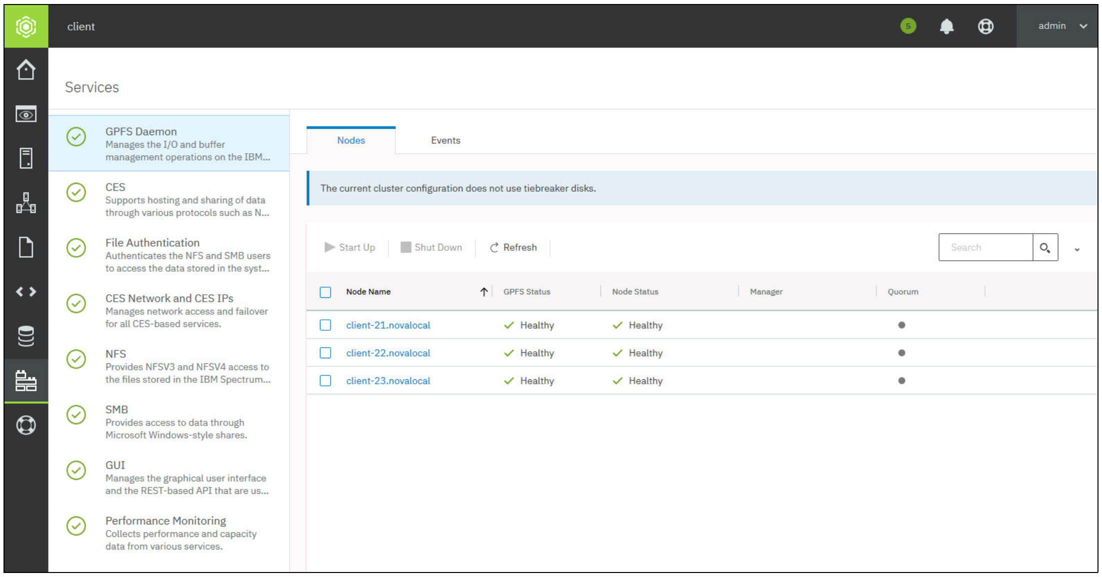
Table 5-4 GUI options available for monitoring and managing protocol data exports

GUI page	Functions
Protocols → NFS Exports	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.
Services → NFS	Specify NFS server settings and start or stop NFS services.
Protocols → SMB Shares	Create and manage SMB shares. Protocols pages are displayed in the GUI only when the protocol feature is enabled on the cluster.
Services → SMB	Specify SMB server settings and start or stop SMB services.
Object → Accounts	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.
Object → Users	Create object users.
Object → Roles	Define roles for the object users.
Services → Object	View and change the object service status. You can also define object administrator who can manage accounts in the Object Storage.

5.11 Managing IBM services

An IBM Spectrum Scale setup comprises various services. You can monitor, configure, and manage them through the newly introduced Services page in the IBM Spectrum Scale 5.0.3 management GUI. This page acts as the single place where you can view all the supported services, health status of each service. It also provides certain configuration options for some of the services.

The Services page in the GUI is shown in Figure 5-3.



GPFS Daemon
Manages the I/O and buffer management operations on the IBM...

CES
Supports hosting and sharing of data through various protocols such as N...

File Authentication
Authenticates the NFS and SMB users to access the data stored in the syst...

CES Network and CES IPs
Manages network access and failover for all CES-based services.

NFS
Provides NFSV3 and NFSV4 access to the files stored in the IBM Spectrum...

SMB
Provides access to data through Microsoft Windows-style shares.

GUI
Manages the graphical user interface and the REST-based API that are us...

Performance Monitoring
Collects performance and capacity data from various services.

The current cluster configuration does not use tiebreaker disks.

□	Node Name ↑	GPFS Status	Node Status	Manager	Quorum
□	client-21.novalocal	✓ Healthy	✓ Healthy		●
□	client-22.novalocal	✓ Healthy	✓ Healthy		●
□	client-23.novalocal	✓ Healthy	✓ Healthy		●

Figure 5-3 Services page

The IBM Spectrum Scale services that can be managed through the Services page in the GUI are described next.

5.11.1 GPFS daemon

The GPFS daemon performs all I/O operations and buffer management for GPFS. You can perform the following actions from the GPFS Daemon section:

- Start and shut down the GPFS services on the nodes.
- Monitor the status of GPFS service and the nodes on which the GPFS service is configured.
- Monitor the events that are raised against the GPFS service.

5.11.2 CES

The cluster export service (CES) provides highly available file and object services by using NFS, SMB, and Object protocols. The nodes that support these protocol services are referred as *CES nodes*. You can perform the following actions from the CES section:

- Stop CES service on a node when you are suspending the node.
- Start CES service on a node when you are resuming the node.
- Suspend and resume CES nodes.
- Monitor the status of the CES nodes and the protocol services that are hosted on the node.
- Monitor the events that are raised against the CES service.

5.11.3 CES network and CES IPs

This service provides the details of the nodes that are part of the CES network. You can perform the following actions from the CES network section:

- View all of the nodes that are part of the CES network.
- Add CES IP addresses by using the Add CES IP option that is available under the Addresses section.
- Monitor the events that are raised against the CES network service.
- Select the distribution policy to be used for assigning the CES IP address.

5.11.4 NFS

You must configure the NFS services on the system to use NFS protocol for data transfer between client and the IBM Spectrum Scale system. You can use NFSv3, NFSv4, or both to use for communication between server and client. You can perform the following actions from the NFS section:

- Start and Stop NFS service.
- Monitor the health status of the NFS service that is configured on the CES nodes.
- View the events that are raised against the NFS service.
- Configure the lease lifetime, domain, and NFS protocol version at the NFS server level.

5.11.5 SMB

You can monitor the SMB service and change global SMB configuration parameters from the GUI.

The following options are available under the respective tabs in the SMB section:

- SMB Service Status

  View the details and health status of the SMB service that is configured in the CES nodes. You can also start and stop the SMB service.
- Events

  Displays the events that are raised against the SMB service.
- Settings

  Provides options to configure the disk free quota, specify server description, set SMB server encryption node, and specify whether to restrict anonymous access.

5.11.6 Object

You must enable and start the object services to use the Object Storage facility.

You can monitor start and stop object services on all or individual CES nodes from the Object section in the Services page. In addition, object specific events and object administrator credential settings can be managed from this section.

5.11.7 File authentication

Use the File Authentication section to configure an authentication method or view the existing authentication method that is used for NFS and SMB users. You can also view the events that are reported against the authentication configuration.

The following file user authentication methods are available to authenticate the user:

Active Directory Uses Microsoft Active Directory as the authentication server. This method is used if you must authenticate SMB users to access the data through SMB shares. When you select AD as the authentication server, you must configure an ID mapping method to map the user IDs from the external domain with a set of internal user IDs.

LDAP Uses an LDAP server to authenticate users. This method is the ideal method to authenticate the NFS protocol users to access the data through the NFS exports.

NIS The NIS-based authentication is useful in NFS-only environment where NIS acts as an ID mapping server and used for netgroups. When file access is configured with NIS, SMB access cannot be enabled.

User-defined The user can select the authentication and ID mapping methods of their choice. It is the responsibility of the administrator of the client system to manage the authentication and ID mapping for file access to the IBM Spectrum Scale system.

5.11.8 Object authentication

The Object Authentication section shows the object user authentication configuration details and the events that are raised against the object authentication service in the cluster.

5.11.9 Hadoop connector

The IBM Spectrum Scale system provides access to the Hadoop Distributed File System Transparency (HDFS) clients. You can monitor the status of the HDFC transparency service from the Hadoop Connector section of the Services page.

5.11.10 GUI

The GUI service manages the GUI and REST APIs that are used to configure, monitor, and manage the IBM Spectrum Scale system. You can perform the following actions from the GUI section:

- Monitor the GUI node configuration in the cluster.
- Configure a login message. This message appears in the login page of the GUI, which is typically used to display some important information that must be shared with the users who are attempting to log in.
- Configure session timeout.
- Create an SSL certificate request.
- Install a self-signed certificate or a certificate that is issued by the certificate authority.
- View the certificate information of the GUI node.
- View the issues that are raised against the GUI service in the cluster.

- Manage GUI users, groups, and their password policy.
- Assign user roles for the GUI users.
- Configure an LDAP-based external configuration method for the GUI users.

For more information about the GUI user management, see 5.12.1, “Managing GUI users locally in the ESS system” on page 80.

5.11.11 Performance monitoring

The performance monitoring tool collects metrics from various components of the IBM Spectrum Scale system and provides performance information.

The Performance Monitoring section in the Services page organizes the monitoring and configuration aspects of performance monitoring under the following tabs:

- Nodes: Provides the nodes on which performance monitoring is enabled. You can also see the health status of these nodes and the performance monitoring sensors that are enabled on the node.
- Sensors: Lists all the sensors that are available with the IBM Spectrum Scale system and provides the option to edit the sensor configuration. By using the Edit option, you can modify the data collection intervals and the scope of data collection. The data can be collected at the all nodes, node group, or individual node level.
- Collectors: Provides the health status of the performance monitoring collector that is configured in the system.
- Events: Lists all events that are raised against the performance monitoring component.

5.11.12 File auditing

The file auditing logs data access to the files. Each file operation is generated as a local event on the node that serves the file operation.

The following details are available in the File Auditing section:

- Nodes: Provides file auditing service status per node.
- File Systems: Provides file auditing service status per file system and node.
- Events: Lists the events that are reported against the file auditing service.

5.11.13 Message queue

The message queue collects and stores events that are published by the producers that are running on nodes in an IBM Spectrum Scale cluster. This service provides a scalable infrastructure for file auditing services.

5.12 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 locally within the system and 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. Internal and external authentication methods can be configured in the system.

5.12.1 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 **Services** → **GUI** 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 default user groups are available:

- Administrator

  Manages all functions on the system, except those functions that deal 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.

When you log in to the system for the first time after the installation, the system shows how to create the first GUI 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 the password of the individual users or all the users that are created in the system. If the password is set as `expired`, the users is 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.

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 functions 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 by using the **Files** → **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 by using 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.

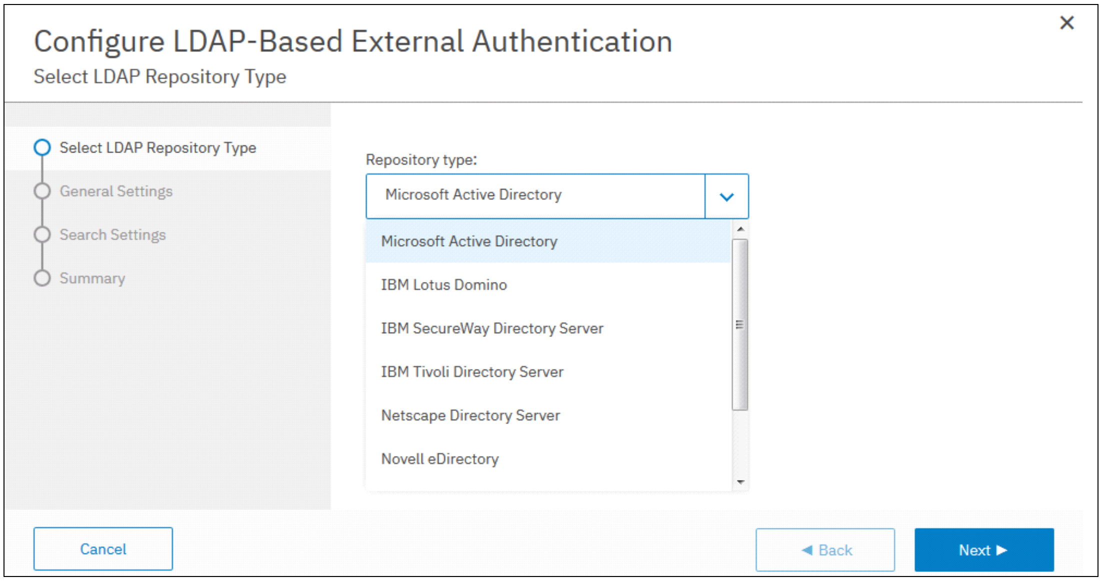
> **Note:** Default groups are not created for the user role User Administrator if the user is upgrading the ESS cluster from 4.2.0.x to a later release.

5.12.2 Managing GUI administrators in an external authentication server

By default, the IBM Spectrum Scale uses an internal authentication repository for the GUI administrators. You can configure an external authentication server either through GUI or CLI.

Configuring external authentication by using GUI

Use the **Configure External Authentication** option that is available under the **External Authentication** tab of **Services** → **GUI** page to configure an external LDAP-based authentication method for authenticating the GUI users, as shown in Figure 5-4. The Configure LDAP-Based External Authentication wizard assists to configure the external authentication method.



Configure LDAP-Based External Authentication

Select LDAP Repository Type

Repository type: Microsoft Active Directory

Select LDAP Repository Type
General Settings
Search Settings
Summary
Microsoft Active Directory
IBM Lotus Domino
IBM SecureWay Directory Server
IBM Tivoli Directory Server
Netscape Directory Server
Novell eDirectory
Cancel
◀ Back
Next ▶

Figure 5-4 Configure LDAP-Based External Authentication wizard

The user credentials are stored in an external repository. You can store the user credentials in the following repository types:

- Microsoft Active Directory
- IBM Lotus Domino
- IBM SecureWay Directory Server
- IBM Tivoli® Directory Server
- Netscape Directory Server
- Novell eDirectory
- Sun Java System Directory Server
- Custom (for example, OpenLdap)

Follow the wizard to complete the authentication service.

Use the **Test Connection** option that is available under the **External Authentication** tab to find out whether a user credential is available in the internal or external repository.

Configuring external authentication by using CLI

Complete the following steps to configure external authentication by using the CLI:

1. Create your AD or LDAP configuration by issuing the **`mkldap`** command at the following location: `/usr/lpp/mmfs/gui/cli/mkldap`.

   The use of this command writes the configuration automatically to `/opt/ibm/wlp/usr/servers/gpfsgui/ldap.xml`, which is then distributed across all GUI nodes. For secure AD or LDAP connection, ensure that the keystores are present on the respective GUI nodes.

   The **`mkldap`** command accepts the parameters that are listed in Table 5-5.

   Table 5-5 mkldap command parameters

Parameter	Description
id	Unique ID of the LDAP configuration.
--host	The IP address or host name of the LDAP server.
--baseDn	BaseDn string for the repository.
--bindDn	BindDn string for the authentication user.
--bindPassword	Password of the authentication user.
--port	Port number of the LDAP. Default is 389 or 636 over SSL.
--type	Repository type, such as Microsoft Active Directory, ids, domino, secureway, iplanet, netscape, edirectory, or custom. Default value is Microsoft Active Directory.
--connectTimeout	Maximum time for establishing a connection with the LDAP server. Default value is 1m.
--searchTimeout	Maximum time for an LDAP server to respond before a request is canceled. Default value is 1m.
--keystore	Location with file name of the keystore file (.jks, .p12, or .pfx).
--keystorePassword	Password of the keystore.
--truststore	Location with file name of the truststore file (.jks, .p12, or .pfx).
--truststorePassword	Password of the truststore.
--userFilter	User filter for the LDAP repository.
--userIdMap	User ID map for the LDAP repository.
--groupFilter	Group filter for the LDAP repository.
--groupIdMap	Group ID map for the LDAP repository.
--groupMemberIdMap	Group member ID map for the LDAP repository.

   Example for standard AD:

```
mkldap myad --host 9.155.106.19 --bindDn
CN=Administrator,CN=Users,DC=mydomain,DC=local
```

```
--baseDn CN=Users,DC=mydomain,DC=local
```

Example for secure AD:

```
mkldap mysecuread --host 9.155.106.19 --bindDn
CN=Administrator,CN=Users,DC=mydomain,DC=local
```

```
--baseDn CN=Users,DC=mydomain,DC=local --keystore /tmp/ad.jks
```

If you specify multiple AD or LDAP servers, you might encounter a problem that a user with the same user name exists in multiple user repositories. This user cannot log in. To prevent this situation, you can specify LDAP filters for User Principal Names (UPN) for a selected server configuration.

Example for a scenario where UPN filters are enabled:

```
mkldap myfilteredad --host 9.155.106.19 --bindDn
CN=Administrator,CN=Users,DC=mydomain,DC=local
```

```
--baseDn CN=Users,DC=mydomain,DC=local --userFilter
"(&(userPrincipalName=%v)(objectcategory=person))"
```

```
--groupFilter "(&(cn=%v)(objectcategory=group))" --userIdMap
"*:userPrincipalName"
```

```
--groupIdMap "*:cn" --groupMemberIdMap "memberOf:member"
```

2. Map an existing AD or LDAP group to the SecurityAdmin GUI role, as shown in the following example:

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

   Now you can log in with your AD or LDAP user and create more group mappings through the GUI on the **Services** → **GUI** → **Users** page by using the **Create Group Mapping** option.

   If you want to remove the existing configurations, use the **rmldap** command. To see all specified LDAP configurations, issue the **lsldap** command.

   > **Note:** Configurations that are managed by **mkldap** and **rmldap** commands are not overwritten during the upgrade. That is, you do not need to back up the configuration data.

6

Troubleshooting options in GUI

The following troubleshooting options are available in the ESS GUI:

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

This chapter includes the following topics:

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.

6.1.1 Event deduplication

The events are raised against the respective component; for example, GPFS, NFS, SMB, and so on. Some of these events might occur multiple times in the system. Such events are grouped under the **Event Groups** tab and the number of occurrences of the events are indicated in the **Occurrences** column. The **Individual Events** tab lists all the events irrespective of the multiple occurrences.

6.1.2 Event Filtering

The following filter options by event type are available as a drop-down list in the Events page:

- Current Issues displays all unfixed errors and warnings.
- Notices displays all transient messages of type “notice” that were not marked as read.
- Current State displays all events that define the current state of the entities, and excludes notices and historic events.
- All Events displays all messages, even historic messages and messages that are marked as read. This filter is not available in the Event Groups view because of performance implications.

A graphical view of events that are reported against each component is available. Clicking the graph displays only the relevant events in the grid view. That is, clicking a portion in the graphical view applies the corresponding filter on the search action and fetches only the relevant data in the events table.

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.

6.1.3 Marking events as read

You can mark events of type Notices 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.

6.1.4 Running fix procedure

Some issues can be resolved by running the **Run Fix Procedure** action. For more information, see 6.6, “Directed maintenance procedures” on page 93.

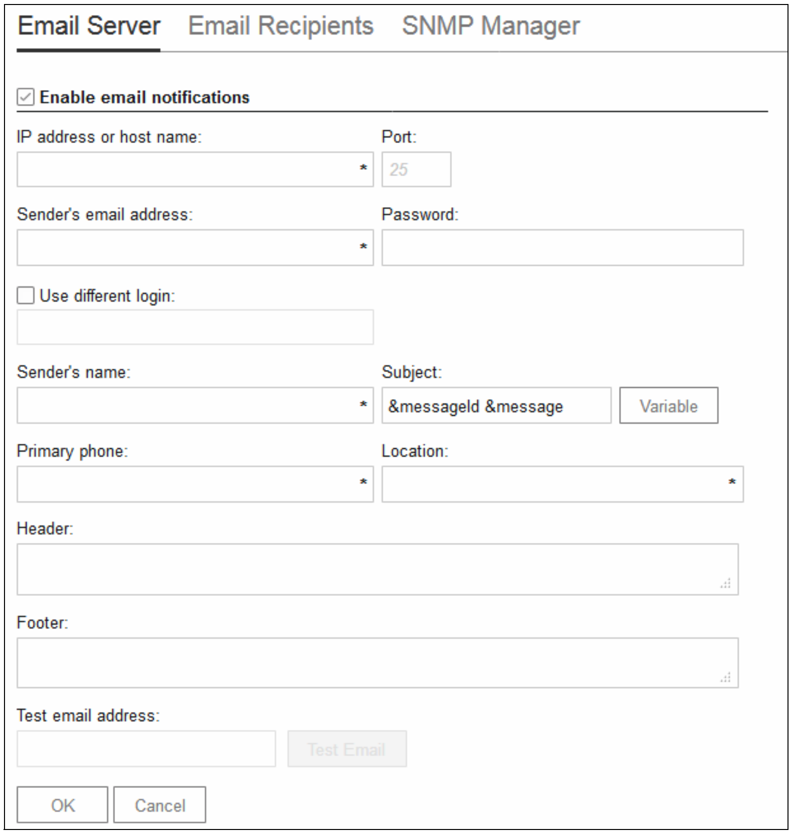
6.2 Monitoring tip events

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 **Monitoring** → **Event Notifications** window in the GUI to configure event notifications (see Figure 6-1).



☑ Enable email notifications

Port: 25

Subject: &messageId &message

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 the following steps:

1. Click **Monitoring** → **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
- &cluster
- &component

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

By using the email notification method, you can also define whether a recipient must receive 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 is assigned a severity level.

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 **Monitoring** → **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. The SNMP objects that are included in the event notifications are listed in Table 6-1.

Table 6-1 SNMP objects included in event notifications

OID	Description	Examples
.1.3.6.1.4.1.2.6.212.10.1.1	Cluster ID	317908494245422510
.1.3.6.1.4.1.2.6.212.10.1.2	Entity type	NODE, FILESYSTEM
.1.3.6.1.4.1.2.6.212.10.1.3	Entity name	gss-11, fs01
.1.3.6.1.4.1.2.6.212.10.1.4	Component	NFS, FILESYSTEM, NSD
.1.3.6.1.4.1.2.6.212.10.1.5	Severity	INFO, TIP, WARNING, ERROR
.1.3.6.1.4.1.2.6.212.10.1.6	Date and time	17.02.2016 13:27:42.516
.1.3.6.1.4.1.2.6.212.10.1.7	Event name	nfs active
.1.3.6.1.4.1.2.6.212.10.1.8	Message	NFS service is now active
.1.3.6.1.4.1.2.6.212.10.1.9	Reporting node	Node where the problem is reported

Understanding the SNMP OID ranges

The SNMP OID ranges are listed in Table 6-2.

Table 6-2 SNMP OID ranges

OID range	Description
.1.3.6.1.4.1.2.6.212	IBM Spectrum Scale
.1.3.6.1.4.1.2.6.212.10	ESS GUI
.1.3.6.1.4.1.2.6.212.10.0.1	ESS GUI event notification (trap)
.1.3.6.1.4.1.2.6.212.10.1.x	ESS GUI event notification parameters (objects)

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 on page 90 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-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: "NODE"
SNMPv2-SMI::enterprises.2.6.212.10.1.3 = STRING: "gss-11"
SNMPv2-SMI::enterprises.2.6.212.10.1.4 = STRING: "PERFMON"
SNMPv2-SMI::enterprises.2.6.212.10.1.5 = STRING: "ERROR"
SNMPv2-SMI::enterprises.2.6.212.10.1.6 = STRING: "18.02.2016 12:46:44.839"
SNMPv2-SMI::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).While configuring SNMP, use the MIB file that is available at the following location of each GUI node:

```
/usr/lpp/mmfs/gui/IBM-SPECTRUM-SCALE-GUI-MIB.txt
```

6.4 Collecting diagnostic data through GUI

IBM Support might request that you 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 **Support** → **Diagnostic Data** window in the ESS GUI to collect details of the issues reported in the system.

The entire set of diagnostic data that is available in the system helps to analyze all types 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 individual nodes 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.

It is always better to reduce the size of the log file as you might need to send it to IBM Support to help fix the issues. You can reduce the size of the diagnostic data file by reducing the scope. The following options are available to reduce the scope of the diagnostic data:

- Include only affected functional areas
- Include only affected nodes
- Reduce the number of days for which the diagnostic data needs to be collected

The following three modes are available in the GUI to select the functional areas of the diagnostic data:

- Standard diagnostics

  The data that is collected in the standard diagnostics consists of the configuration, status, log files, dumps, and traces in the following functional areas:

  - Core IBM Spectrum Scale
  - Network
  - GUI
  - NFS
  - SMB
  - Object
  - Authentication
  - Cluster export services (CES)
  - Crash dumps

  You can download the diagnostic data for these functional areas at the following levels:

  - All nodes
  - Specific nodes
  - All nodes within one or more node classes

- Deadlock diagnostics

  The data that is collected in this category consists of the minimum amount of data that is needed to investigate a deadlock problem.

- Performance diagnostics

  The data that is collected in this category consists of the system performance details that are collected from performance monitoring tools. You can use this option only if it is requested by the IBM Support.

> **Note:** Instead of collecting the diagnostic data again, you can also use the diagnostic data that Is collected in the past. You can analyze the relevance of the historic data based on the date on which the issue is reported in the system. Ensure to delete the diagnostic data that is no longer needed to save disk space.

6.5 Configuring Call Home using GUI

The Call Home feature provides a communication channel that automatically notifies the IBM Service personnel about the issues reported in the system. You can also manually upload diagnostic data files and associate them with a PMR through the GUI.

You can use the Call Home page in the GUI to perform the following tasks:

- Enable the Call Home feature on the cluster.
- Select one or more Call Home nodes that share the data with the IBM Support.
- Specify the contact information to be used by the IBM Support if any issues occur.

- Specify the proxy information that is needed to create a communication channel between the Call Home nodes and IBM support.
- Test connection with the IBM server.

Collecting and sharing data with IBM Support

Call Home shares support information and your contact information with IBM on a scheduled basis. IBM Support monitors the details that are shared by Call Home and takes necessary action on any issues or potential issues.

Enabling Call Home reduces the response time for the IBM Support to address any issues. Call Home automatically shares data with the IBM support based on a schedule. The GUI does *not* support to change the data gathering and sharing schedules.

You can also manually upload the diagnostic data that is collected through the **Support** → **Diagnostic Data** page in the GUI to share the diagnostic data to resolve a Problem Management Record (PMR). To upload data manually, perform the following steps:

1. Go to **Support** → **Diagnostic Data**.
2. Collect diagnostic data based on the requirement. You can also use the previously collected data for the upload.
3. Select the relevant data set from the **Previously Collected Diagnostic Data** section and then, right-click and select **Upload to PMR**.
4. Select the PMR to which the data must be uploaded and then, click **Upload.**

6.5.1 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 that are related to incoming requests from the browser. Check this log if the GUI displays the following error message: `Server was unable to process request`.

6.6 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 that are reported in the system.

The available DMPs and the corresponding events are listed in Table 6-3.

Table 6-3 Directed maintenance procedures available for events

DMP	Event ID
Replace disks	gnr_pdisk_replaceable
Update enclosure firmware	enclosure_firmware_wrong
Update drive firmware	drive_firmware_wrong
Update host-adapter firmware	adapter_firmware_wrong
Start NSD	disk_down
Start GPFS daemon	gpfs_down
Increase fileset space	node_error_high and inode_warn_high
Start performance monitoring collector service	pmcollector_down
Start performance monitoring sensor service	pmsensors_down
Activate AFM performance monitoring sensors	afm_sensors_inactive
Activate NFS performance monitoring sensors	nfs_sensors_inactive
Activate SMB performance monitoring sensors	smb_sensors_inactive
Configure NFS sensor	nfs_sensors_not_configured
Configure SMB sensor	smb_sensors_not_configured
Mount file systems	unmounted_fs_check
Start GUI service on remote node	gui_down
Repair a failed GUI refresh task	gui_refresh_task_failed

6.7 Troubleshooting issues with capacity data displayed in the GUI

Because of the effect that capacity data collection can have on the system, different capacity values are collected on a different schedule and are provided by different system components. The following issues can arise from the multitude of schedules and subsystems that provide capacity data:

- Capacity in the file system view and the total amount of the capacity for pools and volumes view do not match.

  The capacity data in the file system view is collected every 10 minutes by performance monitoring collector, but the capacity data for pools and Network Shared Disks (NSD) are not updated. By default, NSD data is collected only once per day by performance monitoring collector and it is cached.

  Clicking the refresh icon gathers the last two records from performance monitoring tool and it displays the last record values if they are not null. If the last record includes null values, the system displays the previous value. If the values of both records are null, the system displays N/A and the option to display a time chart is disabled. The last update date is the record date that is fetched from performance monitoring tool if the values are not null.

- Capacity in the file system view and the total amount of used capacity for all filesets in that file system do not match.

  Differences exist in the collection schedule and collection mechanism that contribute to the fact that the fileset capacities do not add up to the file system used capacity:

  – Scheduling differences

    Capacity information that is shown for filesets in the GUI is collected once per hour by performance monitoring collector and displayed on the Filesets page. When you click the refresh icon, you get the information of the last record from performance monitoring.

    If the last two records have null values, you receive a “Not collected” warning for used capacity. The file system capacity information on the file systems view is collected every 10 minutes by performance monitoring collector. When you click the refresh icon, you receive the information of the last record from performance monitoring.

  – Data collection differences

    Quota values show the sum of the size of all files and are reported asynchronously. The quota reporting does not consider metadata, snapshots, or capacity that cannot be allocated within a subblock. Therefore, the sum of the fileset quota values can be lower than the data shown in the file system view.

    You can use the CLI command **`mmlsfileset`** with the **`-d`** and **`-ioptions`** to view capacity information. The GUI does not provide a means to display these values because of the effect performance effect on data collection.

- The sum of all fileset inode values on the view quota window does not match the number of inodes that are displayed on the file system properties window.

  The quota value accounts for only user-created inodes while the properties for the file system also display inodes that are used internally. Refresh the quota data to update these values.

- No capacity data shown on a new system or for a newly created file system

  Capacity data can appear with a delay of up to 1 day. The capacity data for file systems, NSDs, and pools is collected once a day because this operation is resource-intensive.

  Line charts do not show a line if only a single data point exists. You can use the hover function to see the first data point in the chart.

- The management GUI displays negative fileset capacity or an extremely high used capacity, such as millions of Petabytes or 4000000000 used inodes.

  This problem can be seen in the quota and filesets views. This problem is caused when the quota accounting is out of sync. To fix this error, issue the **mmcheckquota** command. This command recounts inode and capacity usage in a file system by user, user group, and fileset, and writes the collected data into the database. It also checks quota limits for users, user groups, and filesets in a file system. Running this command can affect performance of I/O operations.

- No capacity data is displayed on the performance monitoring charts.

  Verify whether the sensors (as described in 4.4.1, “Capacity data obtained from the GPFS quota database” on page 33) are enabled correctly. Ensure prerequisites are met. For example, quota is enabled for the GPFSFIlesetQuota sensor, or file systems are mounted on the nodes where the GPFSPools sensor runs.

For more information about how to enable the performance monitoring sensor for capacity data collection, see *Manual installation of IBM Spectrum Scale GUI in IBM Spectrum Scale: Concepts, Planning, and Installation Guide*.

A

GUI limitations

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

- The GUI is supported on an EMS server only.
- Up to 1000 nodes are supported.
- The GUI supports a subset of the CLI functionality. More 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 manages a single cluster. A GUI instance can monitor a subset of performance and system health of remote clusters after creating a connection between the local and remote cluster GUI.
- In an IBM Spectrum Scale and ESS mixed support environment, the ESS GUI must manage the entire cluster to display the ESS-specific pages in the GUI.
- The GUI supports IBM Spectrum Scale release 4.2.0.0 or later. Issue the **`mmlsconfig`** command to see the value that is set for the `minReleaseLevel` attribute.

  Use the **`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 **`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 50.3 GUI rpm with a 5.0.2 base rpm. However, GUI PTFs and fixes often can be applied without installing the corresponding PTF or fix of the base package. This feature is helpful if you want to remove a GUI issue without changing anything on the base layer.

Related publications

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

IBM Redbooks

The following IBM Redbooks publications provide more information about the topics in this document. Note that some publications that are referenced in this list might be available in softcopy only:

- *Introduction Guide to the IBM Elastic Storage Server*, REDP-5253
- *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

The following publications are also relevant as further information sources:

- *Elastic Storage Server Version 5.1 Problem Determination Guide*, SA23-1457
- *Elastic Storage Server Version 5.1 Quick Deployment Guide*, SC27-8580
- *IBM Spectrum Scale RAID Version 4 Release 2.3 Administration*, SC27-6658

Online resources

The following websites are also relevant as further information sources:

- Elastic Storage Server (ESS) Knowledge Center:

  https://www.ibm.com/support/knowledgecenter/SSYSP8/sts_welcome.html

- Examples for GUI issues and their resolutions:

  https://www.ibm.com/support/knowledgecenter/STXKQY_5.0.3/com.ibm.spectrum.scale.v5r03.doc/bl1pdg_GUI_issues.htm

- IBM Spectrum Scale GUI quick reference:

  https://www.ibm.com/support/knowledgecenter/STXKQY_5.0.3/com.ibm.spectrum.scale.v5r03.doc/bl1ins_quickrefforgui.htm

- IBM Spectrum Scale GUI videos:

  https://www.youtube.com/playlist?list=PLS7mekU2kxDrWbtK5AiVGPyF94xTv02xN

- IBM Spectrum Scale RAID concepts:

  https://www.ibm.com/support/knowledgecenter/SSYSP8_5.3.4/com.ibm.spectrum.scale.raid.v5r03.adm.doc/bl1adv_introduction.htm

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

REDP-5471-01

ISBN 0738458198

Printed in U.S.A.