NetApp

Use an external syslog server

StorageGRID

NetApp
March 02, 2022

Table of Contents

Use an external syslog server

Considerations for external syslog server

Use the following guidelines to estimate the size of the external syslog server you need.

What is an external syslog server?

An external syslog server is a server outside of StorageGRID you can use to collect system audit information in a single location. Using an external syslog server enables you to configure the destinations of your audit information so you can reduce network traffic on your Admin Nodes and manage the information more efficiently. The types of audit information you can send to the external syslog server include:

- Audit logs containing the audit messages generated during normal system operation
- Security-related events such as logins and escalations to root
- Application logs that might be requested if it is necessary to open a support case to troubleshoot an issue you have encountered

How to estimate the size of the external syslog server

Normally, your grid is sized to achieve a required throughput, defined in terms of S3 operations per second or bytes per second. For example, you might have a requirement that your grid handle 1,000 S3 operations per second, or 2,000 MB per second, of object ingests and retrievals. You should size your external syslog server according to your grid's data requirements.

This section provides some heuristic formulas that help you estimate the rate and average size of log messages of various types that your external syslog server needs to be capable of handling, expressed in terms of the known or desired performance characteristics of the grid (S3 operations per second).

Use S3 operations per second in estimation formulas

If your grid was sized for a throughput expressed in bytes per second, you must convert this sizing into S3 operations per second to use the estimation formulas. To convert grid throughput, you must first determine your average object size, which you can do using the information in existing audit logs and metrics (if any), or by using your knowledge of the applications that will use StorageGRID. For example, if your grid was sized to achieve a throughput of 2,000 MB/second, and your average object size is 2 MB, then your grid was sized to be able to handle 1,000 S3 operations per second (2,000 MB / 2 MB).

> ⓘ The formulas for external syslog server sizing in the following sections provide common-case estimates (rather than worst-case estimates). Depending on your configuration and workload, you might see a higher or lower rate of syslog messages or volume of syslog data than the formulas predict. The formulas are meant to be used as guidelines only.

Estimation formulas for audit logs

If you have no information about your S3 workload other than number of S3 operations per second your grid is expected to support, you can estimate the volume of audit logs your external syslog server will need to handle using the following formulas, under the assumption that you leave the Audit Levels set to the default values (all categories set to Normal, except Storage, which is set to Error):

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

For example, if your grid is sized for 1,000 S3 operations per second, your external syslog server should be sized to support 2,000 syslog messages per second and should be able to receive (and typically store) audit log data at a rate of 1.6 MB per second.

If you know more about your workload, more accurate estimations are possible. For audit logs, the most important additional variables are the percentage of S3 operations that are PUTs (vs. GETS), and the average size, in bytes, of the following S3 fields (4-character abbreviations used in the table are audit log field names):

Code	Field	Description
SACC	S3 tenant account name (request sender)	The name of the tenant account for the user who sent the request. Empty for anonymous requests.
SBAC	S3 tenant account name (bucket owner)	The tenant account name for the bucket owner. Used to identify cross-account or anonymous access.
S3BK	S3 Bucket	The S3 bucket name.
S3KY	S3 Key	The S3 key name, not including the bucket name. Operations on buckets do not include this field.

Let's use P to represent the percentage of S3 operations that are PUTs, where $0 \leq P \leq 1$ (so for a 100% PUT workload, P = 1, and for a 100% GET workload, P = 0).

Let's use K to represent the average size of the sum of the S3 account names, S3 Bucket, and S3 Key. Suppose the S3 account name is always my-s3-account (13 bytes), buckets have fixed-length names like /my/application/bucket-12345 (28 bytes), and objects have fixed-length keys like 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Then the value of K is 90 (13+13+28+36).

If you can determine values for P and K, you can estimate the volume of audit logs your external syslog server will need to handle using the following formulas, under the assumption that you leave the Audit Levels set to the defaults (all categories set to Normal, except Storage, which is set to Error):

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

For example, if your grid is sized for 1,000 S3 operations per second, your workload is 50% PUTs, and your S3 account names, bucket names, and object names average 90 bytes, your external syslog server should be sized to support 1,500 syslog messages per second and should be able to receive (and typically store) audit log data at a rate of approximately 1 MB per second.

Estimation formulas for non-default audit levels

The formulas provided for audit logs assume the use of default audit level settings (all categories set to Normal, except Storage, which is set to Error). Detailed formulas for estimating the rate and average size of audit messages for non-default audit level settings are not available. However, the following table can be used to make a rough estimate of the rate; you can use the average size formula provided for audit logs, but be aware that it is likely to result in an over-estimate because the "extra" audit messages are, on average, smaller than the default audit messages.

Condition	Formula
Replication: Audit levels all set to Debug or Normal	Audit log rate = 8 x S3 operations Rate
Erasure coding: audit levels all set to Debug or Normal	Use same formula as for default settings

Estimation formulas for security events

Security events are not correlated with S3 operations and typically produce a negligible volume of logs and data. For these reasons, no estimation formulas are provided.

Estimation formulas for application logs

If you have no information about your S3 workload other than the number of S3 operations per second your grid is expected to support, you can estimate the volume of applications logs your external syslog server will need to handle using the following formulas:

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

So, for example, if your grid is sized for 1,000 S3 operations per second, your external syslog server should be sized to support 3,300 application logs per second and be able to receive (and store) application log data at a rate of about 1.2 MB per second.

If you know more about your workload, more accurate estimations are possible. For application logs, the most important additional variables are the data protection strategy (replication vs. erasure coding), the percentage of S3 operations that are PUTs (vs. GETs/other), and the average size, in bytes, of the following S3 fields (4-character abbreviations used in table are audit log field names):

Code	Field	Description
SACC	S3 tenant account name (request sender)	The name of the tenant account for the user who sent the request. Empty for anonymous requests.
SBAC	S3 tenant account name (bucket owner)	The tenant account name for the bucket owner. Used to identify cross-account or anonymous access.

Code	Field	Description
S3BK	S3 Bucket	The S3 bucket name.
S3KY	S3 Key	The S3 key name, not including the bucket name. Operations on buckets do not include this field.

Example sizing estimations

This section explains example cases of how to use the estimation formulas for grids with the following methods of data protection:

- Replication
- Erasure Coding

If you use replication for data protection

Let P represent the percentage of S3 operations that are PUTs, where $0 \leq P \leq 1$ (so for a 100% PUT workload, P = 1, and for a 100% GET workload, P = 0).

Let K represent the average size of the sum of the S3 account names, S3 Bucket, and S3 Key. Suppose the S3 account name is always my-s3-account (13 bytes), buckets have fixed-length names like /my/application/bucket-12345 (28 bytes), and objects have fixed-length keys like 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Then K has a value of 90 (13+13+28+36).

If you can determine values for P and K, you can estimate the volume of application logs your external syslog server will have to be able to handle using the following formulas.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

So, for example, if your grid is sized for 1,000 S3 operations per second, your workload is 50% PUTs, and your S3 account names, bucket names, and object names average 90 bytes, your external syslog server should be sized to support 1800 application logs per second, and will be receiving (and typically storing) application data at a rate of 0.5 MB per second.

If you use erasure coding for data protection

Let P represent the percentage of S3 operations that are PUTs, where $0 \leq P \leq 1$ (so for a 100% PUT workload, P = 1, and for a 100% GET workload, P = 0).

Let K represent the average size of the sum of the S3 account names, S3 Bucket, and S3 Key. Suppose the S3 account name is always my-s3-account (13 bytes), buckets have fixed-length names like /my/application/bucket-12345 (28 bytes), and objects have fixed-length keys like 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Then K has a value of 90 (13+13+28+36).

If you can determine values for P and K, you can estimate the volume of application logs your external syslog server will have to be able to handle using the following formulas.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

So, for example, if your grid is sized for 1,000 S3 operations per second, your workload is 50% PUTs, and your S3 account names, bucket names, and object names average 90 bytes, your external syslog server should be sized to support 2,250 application logs per second and should be able to receive and will be receive (and typically store) application data at a rate of 0.6 MB per second.

For more information on configuring audit message levels and an external syslog server, see the following:

- Configure an external syslog server
- Configure audit messages and log destinations

Configure an external syslog server

If you want to save audit logs, application logs, and security event logs to a location outside of your grid, use this procedure to configure an external syslog server.

What you'll need
- You are signed in to the Grid Manager using a supported web browser.
- You have Maintenance or Root access permissions.
- You have a syslog server with the capacity to receive and store the log files. For more information, see Considerations for external syslog server.
- You have the correct server and client certifications if you plan to use TLS or RELP/TLS.

About this task
If you want to send audit information to an external syslog server, you must configure the external server first.

Sending audit information to an external syslog server enables you to:

- Collect and manage audit information such as audit messages, application logs, and security events more efficiently
- Reduce network traffic on your Admin Nodes because audit information is transferred directly from the various Storage Nodes to the external syslog server, without having to go through an Admin Node

> (!) When logs are sent to an external syslog server, single logs greater than 8192 bytes are truncated at the end of the message to conform with common limitations in external syslog server implementations.

> (i) To maximize the options for full data recovery in the event of a failure of the external syslog server, up to 20GB of local logs of audit records (localaudit.log) are maintained on each node.
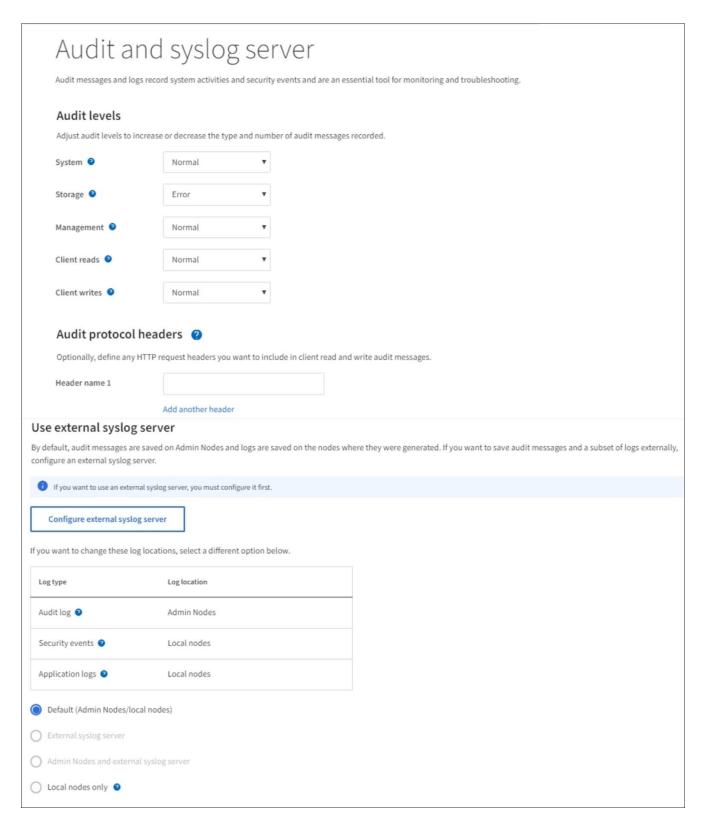
> ⓘ If the configuration options available in this procedure are not flexible enough to meet your requirements, additional configuration options can be applied using the private API `audit-destinations` endpoints. For example, it is possible to use different syslog servers for different groups of nodes.

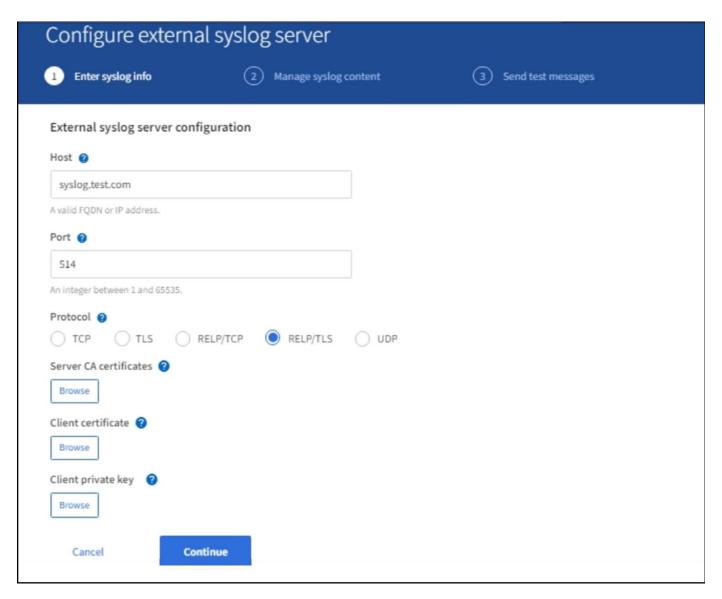## Access the syslog server configuration wizard

Steps

1. Select **CONFIGURATION** > **Monitoring** > **Audit and syslog server**.

Audit and syslog server

Audit messages and logs record system activities and security events and are an essential tool for monitoring and troubleshooting.

Audit levels

Adjust audit levels to increase or decrease the type and number of audit messages recorded.

System ❓	Normal ▼
Storage ❓	Error ▼
Management ❓	Normal ▼
Client reads ❓	Normal ▼
Client writes ❓	Normal ▼

Audit protocol headers ❓

Optionally, define any HTTP request headers you want to include in client read and write audit messages.

Header name 1	

Add another header

Use external syslog server

By default, audit messages are saved on Admin Nodes and logs are saved on the nodes where they were generated. If you want to save audit messages and a subset of logs externally, configure an external syslog server.

ℹ️ If you want to use an external syslog server, you must configure it first.

Configure external syslog server

If you want to change these log locations, select a different option below.

Log type	Log location
Audit log ❓	Admin Nodes
Security events ❓	Local nodes
Application logs ❓	Local nodes

- ⦿ Default (Admin Nodes/local nodes)
- ◯ External syslog server
- ◯ Admin Nodes and external syslog server
- ◯ Local nodes only ❓

2. From the Audit and syslog server page, select **Configure external syslog server**. If you have previously configured an external syslog server, select **Edit external syslog server**.

Enter syslog info

Configure external syslog server

1 Enter syslog info	2 Manage syslog content	3 Send test messages

External syslog server configuration

Host ❓

syslog.test.com

A valid FQDN or IP address.

Port ❓

514

An integer between 1 and 65535.

Protocol ❓

○ TCP   ○ TLS   ○ RELP/TCP   ◉ RELP/TLS   ○ UDP

Server CA certificates ❓

Browse

Client certificate ❓

Browse

Client private key ❓

Browse

Cancel   **Continue**

---

1. Enter a valid fully qualified domain name or an IPv4 or IPv6 address for the external syslog server in the **Host** field.

2. Enter the destination port on the external syslog server (must be an integer between 1 and 65535). The default port is 514.

3. Select the protocol used to send audit information to the external syslog server.

   TLS or RELP/TLS is recommended. You must upload a server certificate to use either of these options.

   Using certificates helps secure the connections between your grid and the external syslog server. For more information, see Use StorageGRID security certificates.

   All protocol options require support by, and configuration of, the external syslog server. You must choose an option that is compatible with the external syslog server.

   > ⓘ Reliable Event Logging Protocol (RELP) extends the functionality of the syslog protocol to provide reliable delivery of event messages. Using RELP can help prevent the loss of audit information if your external syslog server has to restart.

4. Select **Continue**.

5. If you selected **TLS** or **RELP/TLS**, upload the following certificates:

    ◦ **Server CA certificates**: One or more trusted CA certificates for verifying the external syslog server (in PEM encoding). If omitted, the default Grid CA certificate will be used. The file you upload here might be a CA bundle.

    ◦ **Client certificate**: The client certificate for authentication to the external syslog server (in PEM encoding).

    ◦ **Client private key**: Private key for the client certificate (in PEM encoding).

    > (i) If you use a client certificate you must also use a client private key. If you provide an encrypted private key, you must also provide the passphrase. There is no significant security benefit from using an encrypted private key because the key and passphrase must be stored; using an unencrypted private key, if available, is recommended for simplicity.

    a. Select **Browse** for the certificate or key you want to use.

    b. Select the certificate file or key file.

    c. Select **Open** to upload the file.

    A green check appears next to the certificate or key file name, notifying you that it has been uploaded successfully.

6. Select **Continue**.

Manage syslog content

Configure external syslog server

✓ Enter syslog info   ② Manage syslog content   ✓ Send test messages

Manage syslog content

☑ Send audit logs ❓

   Severity ❓ Informational (6) ▾   Facility ❓ local7 (23) ▾

☑ Send security events ❓

   Severity ❓ Passthrough ▾   Facility ❓ Passthrough ▾

☐ Send application logs ❓

   Severity ❓ Passthrough ▾   Facility ❓ Passthrough ▾

[Previous]   [Continue]

1. Select each type of audit information you want to send to the external syslog server.

   ○ **Send audit logs**: StorageGRID events and system activities

   ○ **Send security events**: Security events such as when an unauthorized user attempts to sign in or a user signs in as root

   ○ **Send application logs**: Log files useful for troubleshooting including:

     ▪ bycast-err.log

     ▪ bycast.log

     ▪ jaeger.log

     ▪ nms.log (Admin Nodes only)

     ▪ prometheus.log

     ▪ raft.log

     ▪ hagroups.log

2. Use the drop-down menus to select the severity and facility (type of message) for the category of audit information you want to send.

   If you select **Passthrough** for severity and facility, the information sent to the remote syslog server will receive the same severity and facility as it did when logged locally onto the node. Setting facility and severity can help you aggregate the logs in customizable ways for easier analysis.

a. For **Severity**, select **Passthrough** if you want each message sent to the external syslog to have the same severity value as it does in the local syslog.

For audit logs, if you select **Passthrough** the severity is 'info.'

For security events, if you select **Passthrough**, the severity values are generated by the linux distribution on the nodes.

For application logs, if you select **Passthrough**, the severities vary between 'info' and 'notice,' depending on what the issue is. For example, adding an NTP server and configuring an HA group gives a value of 'info,' while intentionally stopping the ssm or rsm service gives a value of 'notice.'

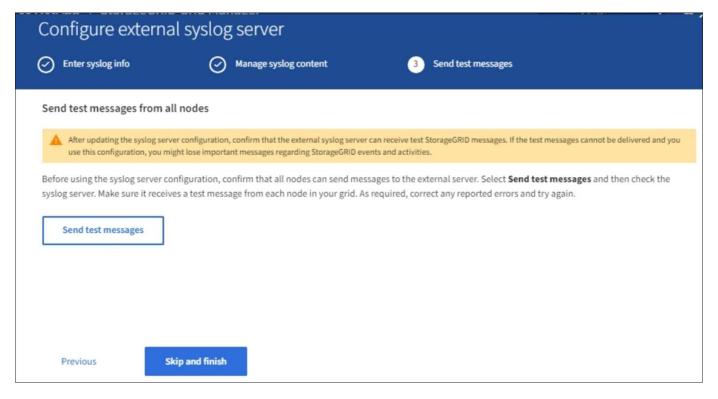b. If you do not want to use the passthrough value, select a severity value between 0 and 7.

The selected value will be applied to all messages of this type. Information about different severities will be lost when you choose to override severity with a fixed value.

Severity	Description
0	Emergency: System is unusable
1	Alert: Action must be taken immediately
2	Critical: Critical conditions
3	Error: Error conditions
4	Warning: Warning conditions
5	Notice: Normal but significant condition
6	Informational: Informational messages
7	Debug: Debug-level messages

c. For **Facility**, select **Passthrough** if you want each message sent to the external syslog to have the same facility value as it does in the local syslog.

For audit logs, if you select **Passthrough** the facility sent to the external syslog server is 'local7.'

For security events, if you select **Passthrough**, the facility values are generated by the linux distribution on the nodes.

For application logs, if you select **Passthrough**, the application logs sent to the external syslog server have the following facility values:

Application log	Passthrough value
bycast.log	user or daemon
bycast-err.log	user, daemon, local3, or local4
jaeger.log	local2
nms.log	local3
prometheus.log	local4
raft.log	local5
hagroups.log	local6

d. If you do not want to use the passthrough value, select the facility value between 0 and 23.

The selected value will be applied to all messages of this type. Information about different facilities will be lost when you choose to override facility with a fixed value.

Facility	Description
0	kern (kernel messages)
1	user (user-level messages)
2	mail
3	daemon (system daemons)
4	auth (security/authorization messages)
5	syslog (messages generated internally by syslogd)
6	lpr (line printer subsystem)
7	news (network news subsystem)
8	UUCP
9	cron (clock daemon)
10	security (security/authorization messages)
11	FTP

Facility	Description
12	NTP
13	logaudit (log audit)
14	logalert (log alert)
15	clock (clock daemon)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Select **Continue**.

Send test messages

Before starting to use an external syslog server, you should request that all nodes in your grid send test messages to the external syslog server. You should use these test messages to help you validate your entire log collection infrastructure before you commit to sending data to the external syslog server.

> ⚠️ Do not use the external syslog server configuration until you confirm that the external syslog server received a test message from each node in your grid and that the message was processed as expected.

1. If you do not want to send test messages and you are certain your external syslog server is configured properly and can receive audit information from all the nodes in your grid, select **Skip and finish**.

   A green banner appears indicating your configuration has been saved successfully.

2. Otherwise, select **Send test messages**.

   Test results continuously appear on the page until you stop the test. While the test is in progress, your audit messages continue to be sent to your previously configured destinations.

3. If you receive any errors, correct them and select **Send test messages** again. See Troubleshooting the external syslog server to help you resolve any errors.

3. Wait until you see a green banner indicating all nodes have passed testing.

4. Check your syslog server to determine if test messages are being received and processed as expected.

   > ℹ️ If you are using UDP, check your entire log collection infrastructure. The UDP protocol does not allow for as rigorous error detection as the other protocols.

5. Select **Stop and finish**.

   You are returned to the **Audit and syslog server** page. A green banner appears notifying you that your syslog server configuration has been saved successfully.

> ℹ️ Your StorageGRID audit information is not sent to the external syslog server until you select a destination that includes the external syslog server.

Select audit information destinations

You can specify where security event logs, application logs, and audit message logs are sent.

> ℹ️ For more information on StorageGRID software logs, see StorageGRID software logs.

1. On the Audit and syslog server page, select the destination for audit information from the listed options:

Option	Description
Default (Admin nodes/local nodes)	Audit messages are sent to the audit log (`audit.log`) on the Admin Node, and security event logs and application logs are stored on the nodes where they were generated (also referred to as "the local node").
External syslog server	Audit information is sent to an external syslog server and saved on the local node. The type of information sent depends upon how you configured the external syslog server. This option is enabled only after you have configured an external syslog server.
Admin Node and external syslog server	Audit messages are sent to the audit log (`audit.log`) on the Admin Node, and audit information is sent to the external syslog server and saved on the local node. The type of information sent depends upon how you configured the external syslog server. This option is enabled only after you have configured an external syslog server.
Local nodes only	No audit information is sent to an Admin Node or remote syslog server. Audit information is saved only on the nodes that generated it. **Note**: StorageGRID periodically removes these local logs in a rotation to free up space. When the log file for a node reaches 1 GB, the existing file is saved, and a new log file is started. The rotation limit for the log is 21 files. When the 22nd version of the log file is created, the oldest log file is deleted. On average about 20 GB of log data is stored on each node.

> ℹ️ Audit information generated on every local node is stored in `/var/local/log/localaudit.log`

2. Select **Save**. Then, select OK to accept the change to the log destination.

3. If you selected either **External syslog server** or **Admin Nodes and external syslog server** as the destination for audit information, an additional warning appears. Review the warning text.

> ℹ️ You must confirm that the external syslog server can receive test StorageGRID messages.

4. Confirm that you want to change the destination for audit information by selecting **OK**.

A green banner appears notifying you that your audit configuration has been saved successfully.

New logs are sent to the destinations you selected. Existing logs remain in their current location.

Related information

Audit message overview

Configure audit messages and log destinations

System audit messages

Object storage audit messages

Management audit message

Client read audit messages

Administer StorageGRID