StorageGRID® 9.0
Audit Message Reference

NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089 U.S.A.
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: http://www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-06836_A0
June 2012

Copyright and trademark information

Copyright information

Trademark information

Contents

1

Audit Message Overview

Overview of Auditing

As services in the grid perform various activities and process events, audit messages are generated to retain a record of grid activity. These messages are processed by the Audit Management System (AMS) service which is most commonly hosted by the Admin Node (reporting Admin Node in a High Capacity Admin Cluster (HCAC)) or Audit Node, and are stored in the form of text log files. This document provides information on the structure and content of the text log files to enable you to read and analyze the audit trail of grid activity.

Content of this guide is current with the audit software version 10 used in the StorageGRID system release 9.0.

Intended Audience

The guide is intended for administrators responsible for producing reports of network activity and usage that require analysis of the audit messages.

You are assumed to have a sound understanding of the nature of audited activities within the StorageGRID system. To use the text log file, you are assumed to have access to the configured audit share on the grid node hosting the AMS service (Admin Node or Audit Node).

This document assumes familiarity with many terms related to computer operations and programming, network communications, and operating system file operations. There is wide use of acronyms.

Audit Message Flow

Audit messages are generated internally by each grid service. All system services generate audit messages during normal system operation. These messages are sent to all connected AMS services for

processing and storage, so that each AMS service maintains a complete record of grid activity.

Some grid services can be designated as audit message relay services. They act as collection points to reduce the need for every service to send its audit messages to all connected AMS services. Notice in Figure 1 that each relay service must send messages to all AMS service destinations, whereas services can send messages to just one relay service.

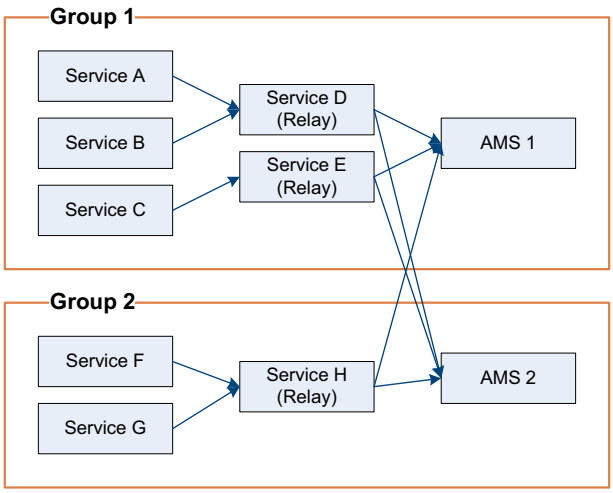

Figure 1: Audit Message Flow

Relay services are designated at the time the grid topology is configured. In a StorageGRID system, the ADC service is designated as the audit message relay.

Message Retention

Once an audit message is generated, it is stored on the local server of the originating service until it has been committed to all connected AMS services, or a designated audit relay service. The relays in turn store the message until it is committed at all AMS services. This process includes a confirmation (positive acknowledgment) to ensure no messages are lost.

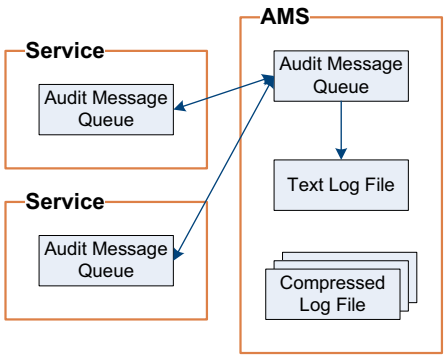

Figure 2: Audit Message Retention

Messages arrive at the AMS service and are stored in a queue pending confirmed write to the text log file audit.log. Confirmation of the arrival of messages is sent to the originating service (or audit relay) to permit the originator to delete its copy of the message.

Only after a message has been committed to storage at the AMS service can it be removed from the queue. In the event that the backlog becomes unusually large, the local message buffer at the audit relay service (ADC) and the AMS service each have an alarm (AMQS) associated with it. At times of peak activity, the rate at which audit messages are arriving may be faster than they can be relayed to the audit repository on the AMS service or committed to storage in the audit log file, causing a temporary backlog that will clear itself when grid activity declines.

Once a day the active audit log audit.log is saved to a file named for the date the file is saved (in the format YYYY-MM-DD.txt) and a new audit.log file is started. If, during a single day, more than one audit log is created, it is saved to a file named for the date the file is saved and appended with a number (in the format YYYY-MM-DD.txt.#). For example, 2010-04-23.txt.1. Subsequent audit messages generated on the same day are saved to a new audit log. This new audit log is saved with the same date as the other, but with the appended number incriminated by one; for example, 2010-04-23.txt.2.

Audit logs are compressed after one day and are renamed YYYY-MM-DD.txt.gz (where the original date is preserved). Audit logs files are saved to the /var/local/audit/export directory on the server that hosts the AMS service. Over time, this results in the consumption of storage allocated for audit logs on the server hosting the AMS service. A script monitors the audit log space consumption and deletes log files as necessary to free up space in the /var/local/audit/export directory. Audit log

files are deleted based on the date they were created with the oldest being deleted first.

Depending upon the regulatory or administrative requirements of your enterprise, you may decide to archive the compressed audit log files to some other media such as DVD, or into the grid itself.

Duplicate Messages

Audit messages are queued for storage by the AMS service. If grid communications are interrupted (for example, because of service failures or network interruptions), the status (that is, whether the message has been written to disk) of some audit messages may be in doubt. The grid takes a conservative approach in this case: all queued audit messages are resubmitted to the AMS service. This may result in duplicate messages in the audit logs.

If duplicate messages are a cause for concern, for example if the audit log is used for billing applications, you must detect and discard audit messages manually. To detect duplicate audit messages, use the audit sequence count number ASQN (duplicate messages will have the same ASQN). For more on ASQN, see "ASQN" on page 19.

Message Level Filtering

The AMS service and the HTTP audit feed filters incoming audit messages based on settings made in Grid Management ▶ Grid Configuration ▶ Audit.

For more information on the HTTP audit feed, see the *StorageGRID API Reference*.

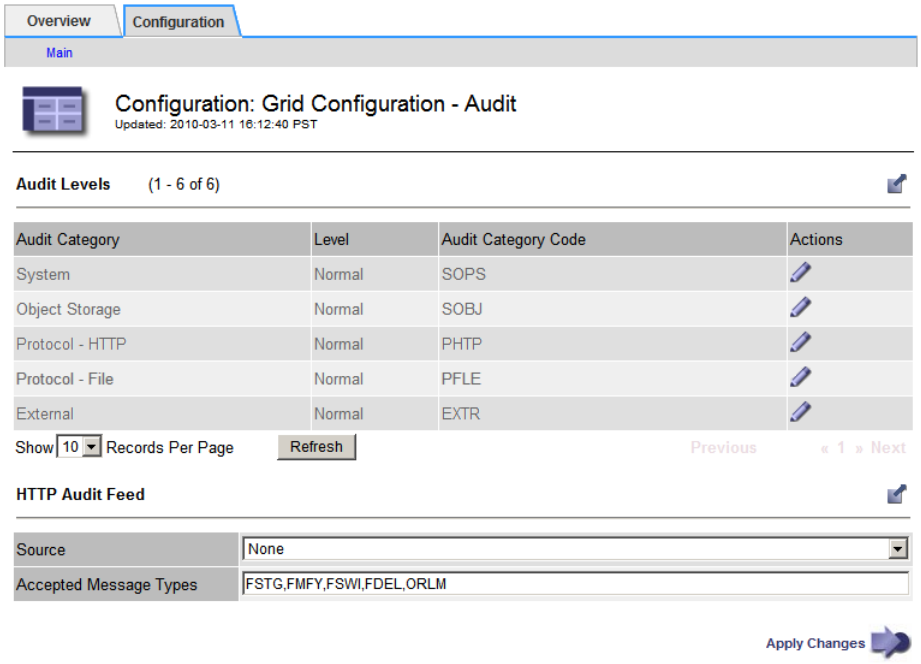

Figure 3: Default Audit Settings

Table 1: Audit Message Filter Levels

Level	Description
Off	No audit messages from the category are logged.
Error	Only error messages are logged; those for which the result code was not "successful" (SUCS).
Normal	Standard transactional messages are logged; all messages listed in this guide for the category.
Debug	Trace messages are logged; for troubleshooting only.

The messages included for any particular level in this table includes those that would be logged at the higher levels. Therefore, the Normal level includes all of the Error messages.

See the "Introduction" on page 45 in Chapter 4 for tables that sort the audit messages into the categories System Messages, Object Storage Messages, HTTP Messages, and File System Gateway Messages. The External category of audit message is only used by external custom applications that submit audit messages using the StorageGRID API.

NOTE Debug level messages are not included in this reference guide.

Change Audit Levels

1. Log in to the NMS MI using the Vendor account.
2. Go to **Grid Management ▶ Grid Configuration ▶ Audit ▶ Main**.
3. Click **Edit**  next to the audit category you want to configure.
4. Select an audit level from the list. See Table 1 above for a description of each level.
5. Click **Apply Changes**.

Audit Log File Access

The audit file share configured on the server hosting the AMS service contains the active audit.log file and any compressed audit log files. Depending upon the configuration at your site, you can access this file share with either a CIFS or NFS client.

Alternatively, if you have access to the command line of the server hosting the AMS service, you can access the text log file directly. Log on to the server using the user name and password as recorded in the Passwords.txt file. By default the text log file is stored at: /var/local/audit/export/audit.log

Access via Microsoft Windows

If you are using Windows to access network file shares, be aware that some versions of Windows do not support using two different logins (user name and password combinations) to access the same device (IP address).

Audit File Naming Convention

The active audit log file is named audit.log.

Once a day, the active audit log is closed and saved to an archived log file named YYYY-MM-DD.txt, where date stamp in the file name indicates when the file was archived. If more than one audit log file is manually created in a single day, subsequent files are named YYYY-MM-DD.txt.1, YYYY-MM-DD.txt.2, and so on.

These archived log files are compressed after one day, and saved to a file named YYYY-MM-DD.txt.gz, where the original date that the file was

created is preserved in the file name. Audit logs files are saved to the /var/local/audit/export directory on the server that hosts the AMS service.

Access Compressed Audit Log file

1. Make a local copy of the file to work with.
2. Decompress the file. This process requires a decompression utility. We suggest "7-Zip", which is a free download from:

   http://www.7-zip.org/
3. Decompress the file using the command **`gunzip filename`**

   The decompressed version of the file retains the same file name excluding the .gz extension.

Audit Log Space Allocation

If audit logs grow beyond the maximum allocated space (typically 50 GB), the oldest log files are automatically deleted. Depending on the regulatory or administrative requirements for the system, you may need to archive the compressed audit log files to other media such as DVD or into the grid itself before they are deleted automatically.

The maximum space allocated to audit logs is system-dependent. The directory used to store audit logs (/var/local) also holds application log files (for example, bycast.log), MySQL files if there is an NMS service but no CMS service on that grid node, core files, and other files such as upgrade files and fsg and arc state files.

At installation, space in /var/local is allocated as follows:

- 20 GB for application log files
- 66% of remaining space for audit logs
- 13% of remaining space for core files

The configuration information is captured in the XML file /var/local/install/var-local-allocation.xml. See below for an example:

```
<allocation>
  <total-size>59</total-size>
  <log>20</log>
  <mysql-ibdata>0</mysql-ibdata>
  <remaining>39</remaining>
  <core>5</core>
  <audit-export>26</audit-export>
</allocation>
```

Any changes you make to the file var-local-allocation.xml should take effect the next time the daily audit log rotation is executed shortly after midnight UTC.

2 File and Message Format

Audit Log File Format

The audit log file at the AMS service contains a collection of individual audit messages. Each audit message contains:

- the UTC time of the event that triggered the audit message (ATIM) in ISO 8601 format (that is, YYYY-MM-DD*T*HH:MM:SS.UUUUUU where UUUUUU are microseconds), followed by a space.
- the audit message itself, enclosed within square brackets "[]" and begin with "AUDT:". The message structure is discussed in more detail in the next section.

The following is part of a sample log file. Messages are wrapped within the boundaries shown, ending after the ASES attribute and double closing brackets "]]". The "\n" (line feed) characters at the end of each message are not shown.

```
2008-06-20T00:14:20.692397 [AUDT:[FPTH(CSTR):"/fsg/BM_
Loadtesting_1/CT_2400_1_f95788a8e6ffa4e932188541a1fb39d1/0/
3b6fdae2a429a68eb42c9212256caf95_1589"][FSIZ(UI64):532480][UU
ID(CSTR):"FF09AF73-429D-4CEA-853B-30239279FE2A"][RSLT(FC32)
:SUCS][AVER(UI32):9][ATIM(UI64):1213920860692397][ATYP(FC32):
FSWO][ANID(UI32):20946829][AMID(FC32):FSGC][ATID(UI64):950214
7098565145229][ASQN(UI64):2938511][ASES(UI64):121382943827169
5]]2008-06-20T00:14:20.710712[AUDT:[FPTH(CSTR):"/fsg/BM_
Loadtesting_1/MR_300_3_11d2c116ac44f55d8e1d79715ed317b1/2/
3a5f90e07362374e1b0087aaf8fb3706_161"][FLTP(FC32):DATA][FSIZ(
UI64):103425][FTIM(UI64):595448][UUID(CSTR):"25843BA6-ABFD-
4257-A57F-1F5D57165490"][RSLT(FC32):SUCS][AVER(UI32):9]
[ATIM(UI64):1213920860710712][ATYP(FC32):FSTG][ANID(UI32):209
46829][AMID(FC32):INGS][ATID(UI64):11495554162678525067][ASQN
(UI64):2938512][ASES(UI64):1213829438271695]]2008-06-
20T00:14:20.718929 [AUDT:[FPTH(CSTR):"/fsg/BM_Loadtesting_1/
CT_2400_1_f95788a8e6ffa4e932188541a1fb39d1/0/3b6fdae2a429
a68eb42c9212256caf95_1460"][FSIZ(UI64):532480][UUID(CSTR):"86
E91656-4788-4874-8F26-34F8ED7DAA0C"][RSLT(FC32):SUCS]
[AVER(UI32):9][ATIM(UI64):1213920860718929][ATYP(FC32):FSWO][
ANID(UI32):20946829][AMID(FC32):FSGC][ATID(UI64):295127721043
4284714][ASQN(UI64):2938513][ASES(UI64):1213829438271695]]
```

Audit Message Format

Audit messages exchanged within the grid include standard information common to all messages and specific content describing the event or activity being reported.

The following is a sample audit message as it might appear in the audit.log file:

```
2008-06-20T00:14:20.692397 [AUDT:[FPTH(CSTR):"/fsg/
BM_Loadtesting_1/CT_2400_1_f95788a8e6ffa4e932188541a1fb39d1/
0/3b6fdae2a429a68eb42c9212256caf95_1589"][FSIZ(UI64):532480]
[UUID(CSTR):"FF09AF73-429D-4CEA-853B-30239279FE2A"][RSLT
(FC32):SUCS][AVER(UI32):9][ATIM(UI64):1213920860692397][ATYP
(FC32):FSWO][ANID(UI32):20946829][AMID(FC32):FSGC][ATID(UI64
):9502147098565145229][ASQN(UI64):2938511][ASES(UI64):121382
9438271695]]
```

Each audit message is a string of attribute elements that are:

- Enclosed in square brackets “[ ]”
- Introduced by the string “AUDT”, indicating an audit message
- Without delimiters (no commas or spaces) between attributes
- Terminated by a line feed character (“\n”)

Each element includes an attribute code, a data type, and a value that are reported in this format:

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

where:

- ATTR is a four-character code for the attribute being reported. These attributes can either be related to event-specific messages (as described in Chapter 4 “Message Reference”), or may be attributes common to all audit messages (as described later in this chapter, on page 18).
- type is a four-character identifier of the programming data type of the value, such as UI64, FC32, and so on. For more information, see “Data Types” on page 17. The type is enclosed in brackets “( )”.
- value is the content of the attribute, typically a numeric or text value. Values always follow a colon “:”. Values of data type CSTR are surrounded by double quotes “ ”.

The number of attribute elements in the message depends on the event type of the message.

For a step-by-step description of how to interpret an audit message, see "Interpreting a Sample Audit Message" on page 19.

Data Types

The data types encountered in the audit messages are listed in Table 2.

Table 2: Data Types

Type	Description
UI32	Unsigned long integer (32 bits); it can store the numbers 0 to 4,294,967,295.
UI64	Unsigned double long integer (64 bits); it can store the numbers 0 to 18,446,744,073,709,551,615.
FC32	Four Character Constant; a 32-bit unsigned integer value represented as four ASCII characters such as: "ABCD".
IPAD	Used for IP addresses.
CSTR	A NetApp StorageGRID string; a variable length array of UTF-8 characters. Characters may be escaped using the conventions described in the *StorageGRID API Reference*. In brief, the most relevant escaping rules state: • characters may be replaced by their hexadecimal equivalents (in the format \xHH, where HH is the hexadecimal value representing the character) • double quotes are represented as \" • backslashes are represented as \\

Event-Specific Data

Following the opening "[AUDT:" container that identifies the message itself, the next set of attributes are items related to the event or action

described by the audit message. These attributes are highlighted in the sample message below:

```
2008-06-20T00:14:20.424035 [AUDT:[HSID(UI64):1027401556]
[OBNS(CSTR):"UUID"][OBPA(CSTR):"/"][OBNA(CSTR):"DDE2
5220-7049-403D-8B71-B9D884A00864"][CBID(UI64):0x210C9
CFC55EACDC6][UUID(CSTR):"DDE25220-7049-403D-8B71-
B9D884A00864"][RSLT(FC32):SUCS][AVER(UI32):9][ATIM(UI64
):1213920860424035][ATYP(FC32):HHEA][ANID(UI32):12885257][AM
ID(FC32):HTGM][ATID(UI64):9771581922913861059][ASQN(UI64):73
74859][ASES(UI64):1213662052895969]]
```

The event that these attributes describe is identified using the ATYP element described in "Common Elements" on page 18. The attributes for each event are described in Chapter 4: "Message Reference".

Common Elements

After the event-specific information is a set of elements common to all audit messages:

Table 3: Common Elements of Audit Messages

Code	Type	Description
AVER	UI32	Version — The version of the audit message. As the StorageGRID software evolves, new versions of services may incorporate new features in audit reporting. This field enables backward compatibility in the AMS to process messages from older versions of services.
ATYP	FC32	Event Type — A four-character identifier of the event being logged. This governs the "payload" content of the message — the attributes which are included.
ATIM	UI64	Timestamp — The time the event was generated that triggered the audit message, measured in microseconds since the operating system epoch (00:00:00 UTC on 1 January, 1970). Note that most available tools for converting the timestamp to local date and time are based on milliseconds. Rounding or truncation of the logged timestamp may be required. The human-readable time that appears at the beginning of the audit message in the audit.log file is the ATIM attribute in ISO 8601 format. (That is, the date and time is represented as YYYY-MM-DD*T*HH:MM:SS.UUUUUU, where the *T* is a literal string character indicating the beginning of the time segment of the date. UUUUUU are microseconds).
ATID	UI64	Trace ID — An identifier that is shared by the set of messages that were triggered by a single event.

Table 3: Common Elements of Audit Messages (cont.)

Code	Type	Description
ANID	UI32	Node ID — The grid node ID assigned to the service that generated the message. Each service is allocated a unique identifier at the time the StorageGRID is configured and installed. This ID cannot be changed.
AMID	FC32	Module ID — A four-character identifier of the module ID that generated the message. This indicates the code segment within which the audit message was generated.
ASQN	UI64	Sequence Count — A counter that is incremented for each generated audit message on the grid node (ANID). This counter is reset to zero at service restart. It can be used for consistency checks to ensure that no audit messages have been lost.
ASES	UI64	Audit Session Identifier — Indicates the time at which the audit system was initialized after the service started up. This time value is measured in microseconds since the operating system epoch (00:00:00 UTC on 1 January, 1970). It can be used to identify which messages were generated during a given runtime session.

Interpreting a Sample Audit Message

The following is a sample audit message, as it might appear in the audit.log file:

```
2008-06-20T00:14:20.718929 [AUDT:[FPTH(CSTR):"/fsg/cifsshare/
CT_1200_1_5d/044a198def43f1_254"][FSIZ(UI64):532480][UUID
(CSTR):"86E91656-4788-4874-8F26-34F8ED7DAA0C"][RSLT(FC32)
:SUCS][AVER(UI32):9][ATIM(UI64):1213920860718929][ATYP(FC32)
:FSWO][ANID(UI32):20946829][AMID(FC32):FSGC][ATID(UI64):2951
277210434284714][ASQN(UI64):2938513][ASES(UI64):121382943827
1695]]
```

The audit message contains information about the event being recorded, as well as information about the audit message itself.

To identify which event is recorded by the audit message, look for the ATYP attribute (highlighted below):

```
2008-06-20T00:14:20.718929 [AUDT:[FPTH(CSTR):"/fsg/cifsshare/
CT_1200_1_5d/044a198def43f1_254"][FSIZ(UI64):532480][UUID
(CSTR):"86E91656-4788-4874-8F26-34F8ED7DAA0C"][RSLT(FC32):
SUCS][AVER(UI32):9][ATIM(UI64):1213920860718929][ATYP(FC32)
:FSWO][ANID(UI32):20946829][AMID(FC32):FSGC][ATID(UI64):295
1277210434284714][ASQN(UI64):2938513][ASES(UI64):12138294382
71695]]
```

The value of this attribute is FSWO. See Chapter 4 to discover that FSWO represents a File Swap Out event, which logs the removal of a file from the FSG local cache. The table in "FSWO — File Swap Out" on page 75 documents the attributes reported for FSWO. From this list you can discover, for example, that the UUID attribute in the audit message records the unique identifier of the file that was swapped out of the FSG cache:

```
2008-06-20T00:14:20.718929 [AUDT:[FPTH(CSTR):"/fsg/cifsshare/
CT_1200_1_5d/044a198def43f1_254"][FSIZ(UI64):532480]
[UUID(CSTR):"86E91656-4788-4874-8F26-34F8ED7DAA0C"]
[RSLT(FC32):SUCS][AVER(UI32):9][ATIM(UI64):1213920860718929]
[ATYP(FC32):FSWO][ANID(UI32):20946829][AMID(FC32):FSGC][ATID
(UI64):2951277210434284714][ASQN(UI64):2938513][ASES(UI64):1
213829438271695]]
```

To discover when the swap out event occurred, look at the UTC time-stamp at the beginning of the audit message. This value is a human-readable version of the ATIM attribute of the audit message itself (described in "Common Elements" on page 18):

```
2008-06-20T00:14:20.718929 [AUDT:[FPTH(CSTR):"/fsg/
cifsshare/CT_1200_1_5d/044a198def43f1_254"][FSIZ(UI64):53
2480][UUID(CSTR):"86E91656-4788-4874-8F26-34F8ED7DAA0C"]
[RSLT(FC32):SUCS][AVER(UI32):9][ATIM(UI64):1213920860718929
9][ATYP(FC32):FSWO][ANID(UI32):20946829][AMID(FC32):FSGC]
[ATID(UI64):2951277210434284714][ASQN(UI64):2938513][ASES(UI
64):1213829438271695]]
```

ATIM records the time, in microseconds, since the beginning of the Unix epoch. The value `1213920860718929` translates to Fri, 20 Jun 2008 00:14:20 UTC.

3

Audit Messages Related to Object Lifecycle

Audit messages generated as objects are ingested, retrieved, deleted, or modified

Introduction

This chapter lists the audit messages that are generated as objects are stored, retrieved, modified, and removed through FSGs. Audit messages are linked via the fields shown in Table 4. Also included in the following chapter are the audit messages that are generated when metadata for an object is updated, added, or deleted.

Table 4: Audit Traces for Ingest, Retrieval, and Deletion

Field Code	Field Name	Audit Messages Where Field Is Used
CBID	Object's internal identifier	ARCB (Archive Object Retrieve Begin) ARCE (Archive Object Retrieve End) AREM (Archive Object Remove) ASCE (Archive Object Store End) ATCE (Archive Object Store Begin) CBRB (Object Receive Begin) CBRE (Object Receive End) CBSB (Object Send Begin) CBSE (Object Send End) CDMD (CDMI DELETE Transaction) CDMG (CDMI GET Transaction) CDMP (CDMI POST Transaction) CDMU (CDMI PUT Transaction) HGEE (HTTP GET Transaction End) HGES (HTTP GET Transaction Start) HPUE (HTTP PUT Transaction End) ORLM (Object Rules Met) SCMT (Object Store Commit) SREM (Object Store Remove)
FPTH	Object's file path on the FSG	DCRE (Directory Create) DDEL (Directory Delete) FCRE (File Create) FDEL (File Delete) FMFY (File Modify) FSTG (File Store to Grid) FSWI (File Swap In) FSWO (File Swap Out) ORLM (Object Rules Met)

Table 4: Audit Traces for Ingest, Retrieval, and Deletion (cont.)

Field Code	Field Name	Audit Messages Where Field Is Used
UUID	Object's external identifier (content handle)	FDEL (File Delete) FMFY (File Modify) FRCV (File Recovery) **NOTE** File recovery is deprecated. FSTG (File Store to Grid) FSWI (File Swap In) FSWO (File Swap Out) HDEL (HTTP DELETE Transaction) HGEE (HTTP GET Transaction End) HGES (HTTP GET Transaction Start) HPUE (HTTP PUT Transaction End) ORLM (Object Rules Met)

Timing of Audit Messages

Because of factors such as timing differences between servers, object size, and network delays, the order of audit messages generated by the different services may vary from that shown in the examples given in this chapter. For example, a SCMT message may happen before a CBRB message although in practice object replication happens before object store.

Ingest

Table 5 lists the audit messages generated during ingest when:

- dual commit is enabled
- the ILM policy is the default (two copies on Storage Nodes)

Audit messages are listed in the order in which they are generated.

Table 5: Ingest Audit Messages (Objects Stored on LDRs)

Message (ATYP)	Name	Description	Trace	Page
FCRE	File Create	The CIFS or NFS client creates a file on the FSG.	FPTH	71
HPUS	HTTP PUT Transaction Start	Ingest starts: The FSG issues an HTTP PUT transaction to request that an LDR start receiving the object.		91
CBSB	Object Send Begin	Replication starts: The LDR starts copying the object to a second LDR.	CBID	58
CBRB	Object Receive Begin	The destination LDR starts receiving the object from the source LDR.	CBID	56
CBRE	Object Receive End	The destination LDR finishes receiving the object.	CBID	57
CBSE	Object Send End	Replication ends: The source LDR finishes sending the object.	CBID	60
SCMT	Object Store Commit	A copy of the object is stored on one LDR persistently.	CBID	101
SCMT	Object Store Commit	A copy of the object is stored in on one LDR (a second copy in this case).	CBID	101
HPUE	HTTP PUT Transaction End	The HTTP PUT transaction is done. Ingest is complete.	CBID, UUID	89
FSTG	File Store to Grid	A confirmation that the object has been stored in the grid.	FPTH, UUID	73
ORLM	Object Rules Met	The ILM policy for the object has been satisfied.	CBID	96

Dual Commit

Dual Commit forces two copies of the object to be stored on two LDRs on initial ingest. These initial copies are made without consulting the ILM policy and objects are simultaneously queued for ILM evaluation. During the ILM evaluation, additional copies may be made in different locations and the initial copies may be purged.

If Dual Commit is not enabled or cannot be achieved (dual commit is on a best effort basis), the set of CBSB, CBRB, CBRE, CBSE, and SCMT messages occurs after the HPUE and FSTG messages instead of before the HPUE message.

For more on dual commit, see the *Administrator Guide*.

ILM Policy Configuration

With the default ILM policy (Baseline 2 Copy Rule), the object is replicated once for a total of two copies stored in the grid on Storage Nodes. If the policy requires more than two copies, there will be an additional set of CBSB, CBRB, CBRE, CBSE, and SCMT messages for each extra copy stored into the grid.

For more information on ILM policies, see the *Administrator Guide*.

Archive Nodes

The series of audit messages generated when storing to an Archive Node is similar to that for Storage Nodes except that there is no SCMT (Store Object Commit) message and the messages ATCE (Archive Object Store Begin) and ASCE (Archive Object Store End) are generated for each copy stored to an Archive Node.

Example

The series of audit messages below is an example of what is recorded in the audit log when a CIFS or NFS client saves a file to an FSG. In this example, Dual Commit is enabled and the active ILM policy is the default Baseline 2 Copy Rule.

FCRE: File Create

```
2009-11-16T09:05:25.247642
[AUDT:[FPTH(CSTR):"/fsg/
2813211305523606116/DCED1BB6"]
[RSLT(FC32):SUCS][AVER(UI32):9][ATIM(UI64
):1258362325247642][ATYP(FC32):FCRE][ANI
D(UI32):20279463][AMID(FC32):FSGC][ATID(U
I64):9145857639040671064][ASQN(UI64):31][
ASES(UI64):1258358106696954]]
```

The FCRE message is generated to indicate that a file has been saved to an FSG. The message includes the file path.

HPUS: HTTP PUT Transaction Start

```
2009-11-16T09:05:45.593521
[AUDT:[HSID(UI64):3872333691][OBNS(CSTR):
"UUID"][OBPA(CSTR):"/"][OBNA(CSTR):""]
[RSLT(FC32):SUCS][AVER(UI32):9][ATIM(UI64
):1258362345593521][ATYP(FC32):HPUS][ANI
D(UI32):12410175][AMID(FC32):HTPM][ATID(U
I64):16003355865555441562][ASQN(UI64):485
][ASES(UI64):1258358101326338]]
```

The HPUS message indicates that the FSG is issuing an HTTP PUT request, asking an LDR to receive the object.

CBSB: Object Send Begin

```
2009-11-16T09:05:45.981944
[AUDT:[CNID(UI64):1258358101339053][CBID(
UI64):0x7B197F444E3BFB5E][CTDR(FC32):
PUSH][CTSR(UI32):12410175][CTDS(UI32)
:12913252][CTSS(UI64):0][CTES(UI64):18446
744073709551615][RSLT(FC32):SUCS][AVER(UI
32):9][ATIM(UI64):1258362345981944][ATYP(
FC32):CBSB][ANID(UI32):12410175][AMID(FC
32):RRTC][ATID(UI64):1177087108278797681
3][ASQN(UI64):488][ASES(UI64):125835810132
6338]]
```

The CBSB message indicates that the LDR has started to replicate the object to another LDR. The message contains the object's CBID and the node IDs of both LDRs. The transfer direction is PUSH.

CBRB: Object Receive Begin

```
2009-11-16T09:05:46.050470
[AUDT:[CNID(UI64):1258358104667221][CBID(
UI64):0x7B197F444E3BFB5E][CTDR(FC32):
PUSH][CTSR(UI32):12410175][CTDS(UI32)
:12913252][CTSS(UI64):0][CTES(UI64):18446
744073709551615][RSLT(FC32):SUCS][AVER(UI
32):9][ATIM(UI64):1258362346050470][ATYP(
FC32):CBRB][ANID(UI32):12913252][AMID(FC
32):RRET][ATID(UI64):11017619293499122116
][ASQN(UI64):488][ASES(UI64):125835810465
0566]]
```

The CBRB message indicates that the destination LDR has started receiving a copy of the object from the source LDR. The message contains the object's CBID and the node IDs of both LDRs. The transfer direction is PUSH.

CBSE: Object Send End

```
2009-11-16T09:05:46.052714
[AUDT:[CNID(UI64):1258358101339053][CBID(
UI64):0x7B197F444E3BFB5E][CTDR(FC32):
PUSH][CTSR(UI32):12410175][CTDS(UI32)
:12913252][CTSS(UI64):0][CTAS(UI64):1][RS
LT(FC32):SUCS][AVER(UI32):9][ATIM(UI64):1
258362346052714][ATYP(FC32):CBSE][ANID(U
I32):12410175][AMID(FC32):RRTC][ATID(UI64
):3515293953654630886][ASQN(UI64):489][AS
ES(UI64):1258358101326338]]
```

The CBSE message indicates that the source LDR has finished replicating the object to the destination LDR. The message contains the object's CBID and the node IDs of both LDRs. The transfer direction is PUSH.

CBRE: Object Receive End

```
2009-11-16T09:05:46.055744
[AUDT:[CNID(UI64):1258358104667221][CBID(
UI64):0x7B197F444E3BFB5E][CTDR(FC32):
PUSH][CTSR(UI32):12410175][CTDS(UI32)
:12913252][CTSS(UI64):0][CTAS(UI64):1][RS
LT(FC32):SUCS][AVER(UI32):9][ATIM(UI64):1
258362346055744][ATYP(FC32):CBRE][ANID(U
I32):12913252][AMID(FC32):RRET][ATID(UI64
):16614313605434897 89][ASQN(UI64):490][AS
ES(UI64):1258358104650566]]
```

The CBRE message indicates that the destination LDR has finished receiving the object from the source LDR. The message contains the object's CBID and the node IDs of both LDRs. The transfer direction is PUSH.

SCMT: Object Store Commit

```
2009-11-16T09:05:45.339347
[AUDT:[CBID(UI64):0x7B197F444E3BFB5E]
[RSLT(FC32):SUCS][AVER(UI32):9][ATIM(UI64
):1258362345339347][ATYP(FC32):SCMT][ANI
D(UI32):12410175][AMID(FC32):STOR][ATID(U
I64):8756220804619457372][ASQN(UI64):487]
[ASES(UI64):1258358101326338]]
```

The SCMT message indicates that a copy of the object has been stored on an LDR.

SCMT: Object Store Commit

```
2009-11-16T09:05:46.056045
[AUDT:[CBID(UI64):0x7B197F444E3BFB5E]
[RSLT(FC32):SUCS][AVER(UI32):9][ATIM(UI64
):1258362346056045][ATYP(FC32):SCMT][ANI
D(UI32):12913252][AMID(FC32):STOR][ATID(U
I64):1359201641142308 3751][ASQN(UI64):489
][ASES(UI64):1258358104650566]]
```

The SCMT message indicates that one copy of the object has been stored on an LDR. The message contains the object's internal identifier CBID.

HPUE: HTTP PUT Transaction End

```
2009-11-16T09:05:46.578280
[AUDT:[HSID(UI64):3872333691][OBNS(CSTR):
"UUID"][OBPA(CSTR):"/"][OBNA(CSTR):""]
[CBID(UI64):0x7B197F444E3BFB5E]
[UUID(CSTR):"32E0529C-9686-4D84-B7FA-
9986E648C102"][OBSP(CSTR):""]
[SPAR(UI64):5064106809552273418][RSLT(FC3
2):SUCS][CSIZ(UI64):6][BSIZ(UI64):8192][A
CBI(UI64):0][AUUI(CSTR):"00000000-0000-
0000-0000-000000000000"][AVER(UI32):9]
[ATIM(UI64):1258362346578280][ATYP(FC32):
HPUE][ANID(UI32):12410175][AMID(FC32):HT
PM][ATID(UI64):7027909393634635489][ASQN(
UI64):491][ASES(UI64):1258358101326338]]
```

The HPUE message indicates the end of the HTTP PUT transaction initiated by the FSG. The message contains the object's internal identifier CBID and external identifier UUID.

FSTG: File Stored to Grid

```
2009-11-16T09:05:46.595751
[AUDT:[FPTH(CSTR):"/fsg/
2813211305523606116/DCED1BB6"]
[FLTP(FC32):DATA][FSIZ(UI64):6][FTIM(UI64
):1011609][UUID(CSTR):"32E0529C-9686-
4D84-B7FA-9986E648C102"][FGRP
(UI32):10][RSLT(FC32):SUCS][AVER(UI32):9]
[ATIM(UI64):1258362346595751][ATYP(FC32):
FSTG][ANID(UI32):20279463][AMID(FC32):IN
GS][ATID(UI64):14277650515744879839][ASQN
(UI64):32][ASES(UI64):1258358106696954]]
```

The FSTG message confirms that the object has been stored in the grid. It includes the object's file path and the object's UUID used to access the object externally.

ORLM: Object Rules Met

```
2009-11-16T09:05:46.604676
[AUDT:[CBID(UI64):0x7B197F444E3BFB5E]
[RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][FGRP(UI32):10][FPTH(CS
TR):"/fsg/2813211305523606116/
DCED1BB6"][FSIZ(UI64):6][SPAR(UI64):50
64106809552273418][UUID(CSTR):"32E0529
C-9686-4D84-B7FA-9986E648C102"]
[LOCS(CSTR):"CLDI 12410175, CLDI
12913252"][RSLT(FC32):SUCS][AVER(UI32):9]
[ATYP(FC32):ORLM][ATIM(UI64):1258362346
604676][ATID(UI64):9013712031209070592][A
NID(UI32):13101936][AMID(FC32):BCMS][ASQN
(UI64):13][ASES(UI64):1258358082794702]]
```

Finally, the ORLM message indicates that the ILM policy has been satisfied for this object. The message includes the object's CBID and the name of the ILM rule that was applied.

Retrieval

Table 6 lists the audit messages generated when a CIFS or NFS client retrieves an object stored on an LDR. The messages are listed in the order in which they are generated.

Table 6: Retrieval Audit Messages (Objects Stored on LDRs)

Message (ATYP)	Name	Description	Trace	Page
HGES	HTTP Get Transaction Start	Retrieval starts: The FSG requests an object from an LDR.	UUID, CBID	83
CBSB	Object Send Begin	Replication starts: An LDR (source LDR) that has the object starts copying the object to the LDR contacted by the FSG (destination LDR).	CBID	58
CBRB	Object Receive Begin	The destination LDR starts receiving the object from the source LDR.	CBID	56
CBSE	Object Send End	Replication ends: The source LDR finishes sending the object.	CBID	60

Table 6: Retrieval Audit Messages (Objects Stored on LDRs) (cont.)

Message (ATYP)	Name	Description	Trace	Page
CBRE	Object Receive End	The destination LDR finishes receiving the object.	CBID	57
HGEE	HTTP Get Transaction End	Retrieval is complete.	UUID	81
FSWI	File Swap In	The object is transferred to the FSG cache.	FPTH, UUID	74

No audit messages are generated if the file is already in the FSG cache: the file is delivered directly from the file share without any interaction with the grid software.

No replication messages (CBSB, CBRB, CBSE, CBRE) are generated if the object happens to be stored on the LDR from which the FSG requested the file.

Archive Nodes

The series of audit messages generated when retrieving objects stored on Archive Nodes is similar to that for Storage Nodes except that the messages ARCB (Archive Object Retrieve Begin) and ARCE (Archive Object Retrieve End) are generated for each copy retrieved from an Archive Node.

Example

The example below shows the audit trail generated when a CIFS or NFS client retrieves a file via an FSG.

HGES: HTTP GET Transaction Start

```
2009-11-18T18:55:26.891578
[AUDT:[HSID(UI64):3293356933][OBNS(CSTR):
"UUID"][OBPA(CSTR):"/"]
[OBNA(CSTR):"40C38EE9-1A71-4239-8A92-
E144DB685265"][CBID(UI64):0x0000000000000
000][UUID(CSTR):"40C38EE9-1A71-4239-
8A92-E144DB685265"][RSLT(FC32):SUCS]
[AVER(UI32):9][ATIM(UI64):125857052689157
8][ATYP(FC32):HGES][ANID(UI32):12308368]
[AMID(FC32):HTGM][ATID(UI64):180781884706
87418669][ASQN(UI64):5527][ASES(UI64):125
8504501698866]]
```

Retrieval begins when the FSG sends an HTTP GET request to an LDR. This is captured by the HGES message. The message contains the objects's external identifier UUID.

CBSB: Object Send Begin

```
2009-11-18T18:55:26.891698
[AUDT:[CNID(UI64):1258504530873627][CBID(
UI64):0x7C2AF6B399D04A8D][CTDR(FC32):
PULL][CTSR(UI32):12812596][CTDS(UI32)
:19118342][CTSS(UI64):0][CTES(UI64):18446
744073709551615][RSLT(FC32):SUCS][AVER(UI
32):9][ATIM(UI64):1258570526891698][ATYP(
FC32):CBSB][ANID(UI32):12812596][AMID(FC
32):CSND][ATID(UI64):7686824200654128609]
[ASQN(UI64):5682][ASES(UI64):125850453047
5230]]
```

The LDR queries the CMS for the location of the object and pulls a copy from an LDR that has a copy. This is captured by the CBSB, CBRB, CBSE, and CBRE messages. These four messages contain the object's internal identifier CBID and the node IDs of the source and destination LDRs. The transfer direction is PULL.

CBRB: Object Receive Begin

```
2009-11-18T18:55:26.910872 [AUDT:
[CNID(UI64):1258504534708874][CBID(UI64):
0x7C2AF6B399D04A8D][CTDR(FC32):PULL]
[CTSR(UI32):12812596][CTDS(UI32):19118
342][CTSS(UI64):0][CTES(UI64):18446744073
709551615][RSLT(FC32):SUCS][AVER(UI32):9]
[ATIM(UI64):1258570526910872][ATYP(FC32):
CBRB][ANID(UI32):19118342][AMID(FC32):CR
EC][ATID(UI64):9085629854822413616][ASQN(
UI64):2][ASES(UI64):1258504534624729]]
```

CBSE: Object Send End

```
2009-11-18T18:55:26.891764
[AUDT:[CNID(UI64):1258504530873627][CBID(
UI64):0x7C2AF6B399D04A8D][CTDR(FC32):
PULL][CTSR(UI32):12812596][CTDS(UI32):
19118342][CTSS(UI64):0][CTAS(UI64):2][RSL
T(FC32):SUCS][AVER(UI32):9][ATIM(UI64):12
58570526891764][ATYP(FC32):CBSE][ANID(UI
32):12812596][AMID(FC32):CSND][ATID(UI64)
:5599813147267552139][ASQN(UI64):5683][AS
ES(UI64):1258504530475230]]
```

CBRE: Object Receive End

```
2009-11-18T18:55:26.911136
[AUDT:[CNID(UI64):1258504534708874][CBID(
UI64):0x7C2AF6B399D04A8D][CTDR(FC32):
PULL][CTSR(UI32):12812596][CTDS(UI32)
:19118342][CTSS(UI64):0][CTAS(UI64):2][RS
LT(FC32):SUCS][AVER(UI32):9][ATIM(UI64):1
258570526911136][ATYP(FC32):CBRE][ANID(U
I32):19118342][AMID(FC32):CREC][ATID(UI64
):12753436827658387817][ASQN(UI64):3][ASE
S(UI64):1258504534624729]]
```

HGEE: HTTP GET Transaction End

```
2009-11-18T18:57:02.171753
[AUDT:[HSID(UI64):3293356933][OBNS(CSTR):
"UUID"][OBPA(CSTR):"/"]
[OBNA(CSTR):"40C38EE9-1A71-4239-8A92-
E144DB685265"][CBID(UI64):0x7C2AF6B399
D04A8D][UUID(CSTR):"40C38EE9-1A71-
4239-8A92-E144DB685265"]
[OBSP(CSTR):""][SPAR(UI64):50641068095522
73418][RSLT(FC32):SUCS][AVER(UI32):9][ATI
M(UI64):1258570622171753][ATYP(FC32):HGE
E][ANID(UI32):12308368][AMID(FC32):HTGM][
ATID(UI64):17628435564272627690][ASQN(UI6
4):5528][ASES(UI64):1258504501698866]]
```

Retrieval ends when the HTTP GET transaction is done, as indicated by the HGEE message. This message contains the object's CBID and UUID.

FSWI: File Swap In

```
2009-11-18T18:57:02.192918
[AUDT:[FPTH(CSTR):"/fsg/asdfasdf/
asdfasdf.txt"][FSIZ(UI64):5][FTIM(UI64):10
6616][UUID(CSTR):"40C38EE9-1A71-4239-
8A92-E144DB685265"][FGRP(UI32):10]
[RSLT(FC32):SUCS][AVER(UI32):9][ATIM(UI64
):1258570622192918][ATYP(FC32):FSWI][ANID
(UI32):20216463][AMID(FC32):SWPI][ATID(UI
64):14282380356057899081][ASQN(UI64):12][
ASES(UI64):1258504671262329]]
```

The FSWI message indicates that the object's has been swapped into the FSG cache. The message contains the object's file path and UUID.

Deletion

Table 7 lists the audit messages that could be generated when a CIFS or NFS client attempts to remove a file from an FSG.

Table 7: Object Deletion Audit Messages

Message (ATYP)	Name	Description	Trace	Page
FMFY	File Modify	The file has been released from the FSG (the UUID is no longer associated with the file).	FPTH, UUID	72
FDEL	File Delete	The file has been deleted from the FSG directory tree.	FPTH	71
FRCV	File Recovery **NOTE** File recovery is deprecated.	The deleted file has been moved to the recovery area on the FSG.	UUID	72
HDEL	HTTP DELETE Transaction	The HTTP DELETE request issued by the FSG has been processed.	UUID	79
SREM	Object Store Remove	A copy of the object has been removed from an LDR.	CBID	102
ORLM	Object Rules Met	The ILM policy which has been re-evaluated for this object as a result of the removal is satisfied.	CBID	96

What messages are actually generated depends on how content protection is configured. The different scenarios are summarized in Figure 4. For more on content protection, see the *Administrator Guide*.

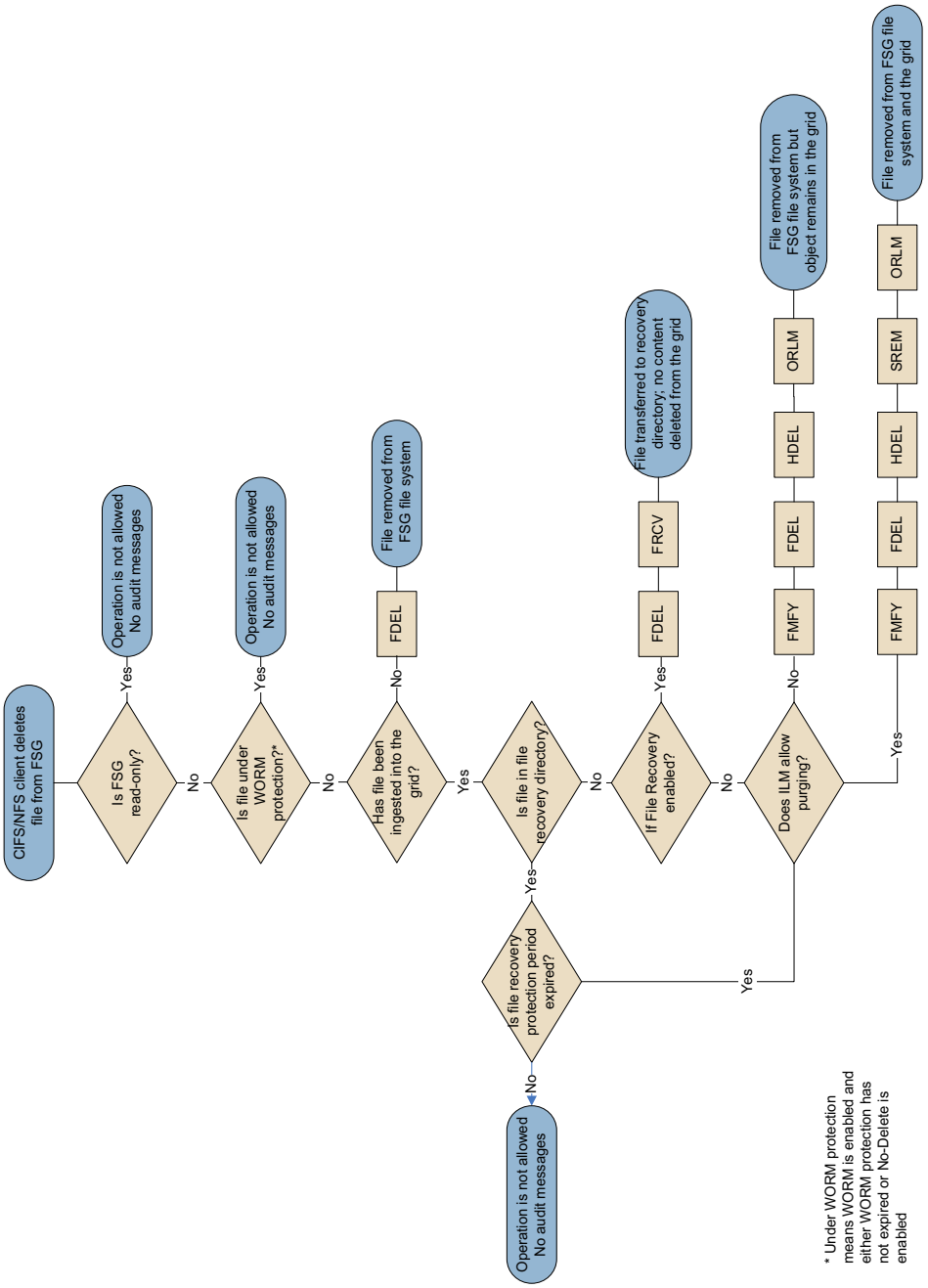

Figure 4: Delete Scenarios

Archive Nodes

The series of audit messages generated when deleting objects stored on Archive Nodes is similar to that for LDRs except that there is no SREM (Object Store Remove) message and there is an AREM (Archive Object Remove) message for each delete request sent from the Archive Node to the middleware software that manages nearline storage.

Example

The events that take place when a CIFS or NFS client removes a file via an FSG are summarized below. In this example, the ILM is configured to store two copies of all content on Storage Nodes when files are ingested and to purge files that are deleted through the FSG.

FMFY: File Modify

```
2009-11-20T00:28:22.588961
[AUDT:[FPTH(CSTR):"/fsg/delete/test.txt"]
[UUID(CSTR):"183B0049-181C-47D7-
A2BA-6F219B1DF51F"][FGRP(UI32):10]
[RSLT(FC32):SUCS][AVER(UI32):9][ATIM(UI64
):1258676902588961][ATYP(FC32):FMFY][ANI
D(UI32):20513440][AMID(FC32):FSGC][ATID(U
I64):9690443096488201053][ASQN(UI64):262]
[ASES(UI64):1258504675865797]]
```

When the CIFS or NFS client removes a file from the FSG, a FMFY message is generated to indicate that the UUID is no longer associated with this file. The message contains the object's file path and UUID.

FDEL: File Delete

```
2009-11-20T00:28:22.589013
[AUDT:[FPTH(CSTR):"/fsg/delete/test.txt"]
[UUID(CSTR):"183B0049-181C-47D7-
A2BA-6F219B1DF51F"][FGRP(UI32):10]
[RSLT(FC32):SUCS][AVER(UI32):9][ATIM(UI64
):1258676902589013][ATYP(FC32):FDEL][ANI
D(UI32):20513440][AMID(FC32):FSGC][ATID(U
I64):15801121656002088530][ASQN(UI64):263
][ASES(UI64):1258504675865797]]
```

The FDEL message indicates that the file entry has been deleted from the FSG directory tree. The file has not been deleted from the grid but it is no longer accessible through the FSG.

HDEL: HTTP DELETE

```
2009-11-20T00:28:42.839522 [AUDT:[HSID
(UI64):2957648831][OBNS(CSTR):"UUID"][OBP
A(CSTR):"/"][OBNA(CSTR):"183B0049-181C-
47D7-A2BA-6F219B1DF51F"][UUID(CSTR):
"183B0049-181C-47D7-A2BA-
6F219B1DF51F"][OBSP(CSTR):""][SPAR(UI64
):5064106809552273409][RSLT(FC32):SUCS][
AVER(UI32):9][ATIM(UI64):1258676922839522
][ATYP(FC32):HDEL][ANID(UI32):12812596][
AMID(FC32):HTDM][ATID(UI64):1457122272645
3359502][ASQN(UI64):23483][ASES(UI64):125
8504530475230]]
```

The HDEL message indicates that the HTTP DELETE request issued by the FSG has been processed. The message contains the object's UUID. The result "SUCS" indicates that the request to delete the object has been accepted. It does not indicate that the object has been purged from the grid. The object will be deleted from the grid only if the ILM policy is configured to purge objects when they are removed from the FSG.

SREM: Object Remove

```
2009-11-20T00:28:42.893144
[AUDT:[CBID(UI64):0xFD10DA170C262888]
[RSLT(FC32):SUCS][AVER(UI32):9][ATIM(UI64
):1258676922893144][ATYP(FC32):SREM][ANI
D(UI32):12812596][AMID(FC32):STOR][ATID(U
I64):11749638179726214582][ASQN(UI64):234
84][ASES(UI64):1258504530475230]]
```

The SREM message indicates that a copy of the object was removed from an LDR. The message contains the object's CBID. Because in this case there were two copies of the objects in the grid, two SREM messages are generated.

The UUID in the HDEL message and the CBID in the SREM message can be linked using the HPUE message that was generated when the object was ingested into the grid.

SREM: Object Remove

```
2009-11-20T00:28:42.917708
[AUDT:[CBID(UI64):0xFD10DA170C262888]
[RSLT(FC32):SUCS][AVER(UI32):9][ATIM(UI64
):1258676922917708][ATYP(FC32):SREM][ANID
(UI32):12308368][AMID(FC32):STOR][ATID(UI
64):8079966187988028241][ASQN(UI64):23610
][ASES(UI64):1258504501698866]]
```

ORLM: Object Rules Met

```
2009-11-20T00:28:42.934577 [AUDT:[CBID
(UI64):0xFD10DA170C262888][RULE(CSTR
):"Purge on Content Handle Release"][STAT
(FC32):PRGD][FGRP(UI32):10][FPTH(CSTR):"
/fsg/delete/test.txt"][FSIZ(UI64):6][SPAR
(UI64):5064106809552273409][UUID(CSTR):""]
[LOCS(CSTR):""][RSLT(FC32):SUCS][RSLT(FC32
):SUCS][AVER(UI32):9][ATYP(FC32):ORLM][A
TIM(UI64):1258676922934577][ATID(UI64):140
0275939407080561][ANID(UI32):13409607][AMI
D(FC32):BCMS][ASQN(UI64):3735][ASES(UI64):
1258504547020752]]
```

The ILM policy has been re-evaluated for this object. The ORLM message contains the name of the rule that was applied and the object's CBID.

Modification

If the grid configuration allows it, CIFS or NFS clients may modify content that has already been ingested into the grid. File modification consists of two events:

- the modified file is ingested
- the original file is deleted

The audit messages are essentially the same as those generated when a file is ingested, retrieved, and deleted except that a file modification does not generate any FCRE and FDEL messages.

Example

The example below lists the events that take place when a CIFS or NFS client modifies a file via an FSG. In this example:

- The original file is in the FSG cache, hence there are no replication messages associated with retrieval.
- Dual commit is applied.
- The ILM is configured to store two copies of all content on Storage Nodes on ingest and to purge files that are deleted through the FSG.

FMFY: File Modify

```
2009-11-20T00:56:13.684734 [AUDT:[FPTH
(CSTR):"/fsg/delete/modify.txt"][UUID
(CSTR):"9D7CD8B2-9D05-4314-9AD7-
38A9C6ED633E"][FGRP(UI32):10][RSLT(FC3
2):SUCS][AVER(UI32):9][ATIM(UI64):1258678
573684734]?[ATYP(FC32):FMFY][ANID(UI32):
20513440][AMID(FC32):FSGC][ATID(UI64):106
03826254378132696][ASQN(UI64):266][ASES(U
I64):1258504675865797]]
```

The FMFY message indicates that the UUID is no longer associated with this file. The message contains the object's file path and original UUID.

HPUS: HTTP PUT Transaction Start

```
2009-11-20T00:56:23.830562 [AUDT:[HSID
(UI64):1953223112][OBNS(CSTR):"UUID"][OBP
A(CSTR):"/"][OBNA(CSTR):""][RSLT(FC32)
:SUCS][AVER(UI32):9][ATIM(UI64):125867858
3830562][ATYP(FC32):HPUS][ANID(UI32):128
12596][AMID(FC32):HTPM][ATID(UI64):139331
755815272947][ASQN(UI64):26682][ASES(UI64
):1258504530475230]]
```

The HPUS message indicates that the FSG initiated an HTTP PUT transaction to store the modified object into the grid.

CBSB: Object Send Begin

```
2009-11-20T00:56:23.933709 [AUDT:[CNID
(UI64):1258504530882702][CBID(UI64):0xBD
0999B2C5F3AE64][CTDR(FC32):PUSH][CTSR(
UI32):12812596][CTDS(UI32):12308368][CTSS
(UI64):0][CTES(UI64):18446744073709551615
][RSLT(FC32):SUCS][AVER(UI32):9][ATIM(UI6
4):1258678583933709][ATYP(FC32):CBSB][AN
ID(UI32):12812596][AMID(FC32):RRTC][ATID(
UI64):17893246997946136197][ASQN(UI64):26
683][ASES(UI64):1258504530475230]]
```

The modified file is assigned a new CBID and is ingested into the grid. The CBSB, CBRB, CBRE, CBSE, and SCMT messages are issued.

CBRB: Object Receive Begin

```
2009-11-20T00:56:23.990903 [AUDT:[CNID
(UI64):1258504501727874][CBID(UI64):0xBD
0999B2C5F3AE64][CTDR(FC32):PUSH][CTSR(
UI32):12812596][CTDS(UI32):12308368][CTSS
(UI64):0][CTES(UI64):18446744073709551615
][RSLT(FC32):SUCS][AVER(UI32):9][ATIM(UI6
4):1258678583990903][ATYP(FC32):CBRB][AN
ID(UI32):12308368][AMID(FC32):RRET][ATID(
UI64):13577650088864879232][ASQN(UI64):26
554][ASES(UI64):1258504501698866]]
```

CBRE: Object Receive End

```
2009-11-20T00:56:24.005278 [AUDT:[CNID
(UI64):1258504501727874][CBID(UI64):0xBD
0999B2C5F3AE64][CTDR(FC32):PUSH][CTSR(
UI32):12812596][CTDS(UI32):12308368][CTSS
(UI64):0][CTAS(UI64):1][RSLT(FC32):SUCS][
AVER(UI32):9][ATIM(UI64):1258678584005278
][ATYP(FC32:CBRE][ANID(UI32):12308368][A
MID(FC32):RRET][ATID(UI64):92120411892149
3758][ASQN(UI64):26556][ASES(UI64):125850
4501698866]]
```

CBSE: Object Send End

```
2009-11-20T00:56:24.010737 [AUDT:[CNID
(UI64):1258504530882702][CBID(UI64):0xBD
0999B2C5F3AE64][CTDR(FC32):PUSH][CTSR(
UI32):12812596][CTDS(UI32):12308368][CTSS
(UI64):0][CTAS(UI64):1][RSLT(FC32):SUCS][
AVER(UI32):9][ATIM(UI64):1258678584010737
][ATYP(FC32):CBSE][ANID(UI32):12812596][
AMID(FC32):RRTC][ATID(UI64):1616174556717
1375742][ASQN(UI64):26685][ASES(UI64):125
8504530475230]]
```

SCMT: Object Store Commit

```
2009-11-20T00:56:23.945448 [AUDT:[CBID
(UI64):0xBD0999B2C5F3AE64][RSLT(FC32):
SUCS][AVER(UI32):9][ATIM(UI64):1258678583
945448][ATYP(FC32):SCMT][ANID(UI32):1281
2596][AMID(FC32):STOR][ATID(UI64):1387172
6619469938814][ASQN(UI64):26684][ASES(UI6
4):1258504530475230]]
```

SCMT: Object Store Commit

```
2009-11-20T00:56:24.005129 [AUDT:[CBID
(UI64):0xBD0999B2C5F3AE64][RSLT(FC32):
SUCS][AVER(UI32):9][ATIM(UI64):1258678584
005129][ATYP(FC32):SCMT][ANID(UI32):1230
8368][AMID(FC32):STOR][ATID(UI64):1346526
0864885248655][ASQN(UI64):26555][ASES(UI6
4):1258504501698866]]
```

HPUE: HTTP PUT Transaction End

```
2009-11-20T00:56:24.085345 [AUDT:[HSID
(UI64):1953223112][OBNS(CSTR):"UUID"][OBP
A(CSTR):"/"][OBNA(CSTR):""][CBID(UI64):
0xBD0999B2C5F3AE64][UUID(CSTR):"EE
AB6A4D-8BAB-48C5-80BE-B570246CD7
E6"][OBSP(CSTR):""][SPAR(UI64):5064106809
552273409][RSLT(FC32):SUCS][CSIZ(UI64):8]
[BSIZ(UI64):8192][ACBI(UI64):0][AUUI(CSTR
):"00000000-0000-0000-0000-000000000000"]
[AVER(UI32):9][ATIM(UI64):125867858408534
5][ATYP(FC32):HPUE][ANID(UI32):12812596]
[AMID(FC32):HTPM][ATID(UI64):111605998551
79846236][ASQN(UI64):26686][ASES(UI64):12
58504530475230]]
```

The HPUE message indicates the end of the HTTP PUT transaction for the modified file. The message contains the object's new CBID and UUID.

ORLM: Object Rules Met

```
2009-11-20T00:56:24.087497 [AUDT:[CBID
(UI64):0xBD0999B2C5F3AE64][RULE(CST
R):"Make 2 Copies"][STAT(FC32):DONE]
[FGRP(UI32):10][FPTH(CSTR):"/fsg/delete/
modify.txt"][FSIZ(UI64):6][SPAR(UI64):5064
106809552273409][UUID(CSTR):"EEAB6A4D
-8BAB-48C5-80BE-B570246CD7E6"][LOCS
(CSTR):"CLDI 12635027, CLDI 12752778"]
[RSLT(FC32):SUCS][AVER(UI32):9][ATYP(FC32)
:ORLM][ATIM(UI64):1258678584087497][ATID
(UI64):8510035149810021956][ANID(UI32):137
55142][AMID(FC32):BCMS][ASQN(UI64):5048][A
SES(UI64):1258504499181980]]
```

The ORLM message indicates that the ILM rule "Make 2 Copies" has been applied to the modified file and the ILM policy for this object is satisfied. The message contains the object's CBID.

FSTG: File Stored to Grid

```
2009-11-20T00:56:24.105927 [AUDT:[FPTH
(CSTR):"/fsg/delete/modify.txt"][FLTP
(FC32):DATA][FSIZ(UI64):8][FTIM(UI64):296
516][UUID(CSTR):"EEAB6A4D-8BAB-48C5-
80BE-B570246CD7E6"][FGRP(UI32):
10][RSLT(FC32):SUCS][AVER(UI32):9][ATIM(U
I64):1258678584105927][ATYP(FC32):FSTG][
ANID(UI32):20513440][AMID(FC32):INGS][ATI
D(UI64):10699542919573582238][ASQN(UI64):
267][ASES(UI64):1258504675865797]]
```

The FSTG message indicates that the modified file has been ingested. The message contains the file path and the object's UUID.

HDEL: HTTP DELETE

```
2009-11-20T00:56:33.840038 [AUDT:[HSID
(UI64):510828181][OBNS(CSTR):"UUID"][OBPA
(CSTR):"/"][OBNA(CSTR):"9D7CD8B2-9D05-
4314-9AD7-38A9C6ED633E"][UUID(CSTR):"9D
7CD8B2-9D05-4314-9AD7-38A9C6ED633E"
][OBSP(CSTR):""][SPAR(UI64):5064106809552
273409][RSLT(FC32):SUCS][AVER(UI32):9][AT
IM(UI64):1258678593840038][ATYP(FC32):HD
EL][ANID(UI32):12308368][AMID(FC32):HTDM]
[ATID(UI64):15796082304191793732][ASQN(UI
64):26566][ASES(UI64):1258504501698866]]
```

The HDEL message indicates that the HTTP DELETE transaction for the original file has been processed. The message contains the file's original UUID.

SREM: Object Store Remove

```
2009-11-20T00:56:33.856055 [AUDT:[CBID
(UI64):0x55E6C61C5F118A01][RSLT(FC32):
SUCS][AVER(UI32):9][ATIM(UI64):1258678593
856055][ATYP(FC32):SREM][ANID(UI32):1281
2596][AMID(FC32):STOR][ATID(UI64):9352765
557778359653][ASQN(UI64):26699][ASES(UI64
):1258504530475230]]
```

The SREM message indicates that a copy of the original file has been removed from an LDR. The message contains the object's old CBID. There are two SREM messages because there were two copies of the object in the grid.

SREM: Object Store Remove

```
2009-11-20T00:56:33.882293 [AUDT:[CBID
(UI64):0x55E6C61C5F118A01][RSLT(FC32):
SUCS][AVER(UI32):9][ATIM(UI64):1258678593
882293][ATYP(FC32):SREM][ANID(UI32):1230
8368][AMID(FC32):STOR][ATID(UI64):1388431
5135762521337][ASQN(UI64):26567][ASES(UI6
4):1258504501698866]]
```

ORLM: Object Rules Met

```
2009-11-20T00:56:33.897788 [AUDT:[CBID
(UI64):0x55E6C61C5F118A01][RULE(CSTR
):"Purge on Content Handle Release"][STAT
(FC32):PRGD][FGRP(UI32):10][FPTH(CSTR):"/
fsg/delete/test.txt"][FSIZ(UI64):6]
[SPAR(UI64):5064106809552273409][UUID(CS
TR):""][LOCS(CSTR):""][RSLT(FC32):SUCS][A
VER(UI32):9][ATYP(FC32):ORLM][ATIM(UI64
):1258678593897788][ATID(UI64):1735891906
0407322538][ANID(UI32):13755142][AMID(FC3
2):BCMS][ASQN(UI64):5049][ASES(UI64):1258
504499181980]]
```

The ORLM message indicates that the ILM rule "Purge on Content Handle Release" has been applied to the original file and the ILM policy for this object is satisfied. The message contains the object's old CBID.

Metadata Updates

Table 8 lists audit messages that may be generated when a StorageGRID API or CDMI client updates an object's metadata.

Table 8: Metadata Update Audit Messages

Message (ATYP)	Name	Description	Trace	Page
CDMU	CDMI PUT Transaction	The CDMI client makes a request to add or update an object's custom metadata.	COID, CBID	63
HGMD	HTTP GET Metadata	The StorageGRID API client requests all predefined and custom metadata for an object.	UUID	83
HPMD	HTTP PUT Metadata	The StorageGRID API client makes a request to add or update an object's custom metadata.	UUID	86
OMDU	Object Metadata Updated	Issued by the owner CMS after processing a custom metadata update for an ingested object.	CBID, UUID	95

Example

The example below lists the events that take place when a StorageGRID API client updates an object's metadata.

HGMD: HTTP GET Metadata

```
2010-11-20T00:56:13.684734 [AUDIT:[HSID
(UI64):195323112][OBNS(CSTR):"UUID"][OBPA
(CSTR):"/"][OBNA(CSTR):"EEABC-DBF-DFE436-
DK034-KD3601L3LN"][CBID(UI64):0xBD0999B
2C5F3AE64][UUID(CSTR):"EEABC-DBF-DFE436-
DK034-KD3601L3LN"][OBSP(CSTR):""][SPAR
(UI64):508738497389789078 3][RSLT(FC32)
:SUCS][AVER(UI32):10][ATIM(UI64):13468789
78][ATYP(FC32):HGMD][ANID(UI32):2027946
3][AMID(FC32):HTGM][ATID(UI64):9893048903
][ASQN(UI64):353][ASES(UI64):134351648685
563]]
```

The HGMD message indicates that the StorageGRID API client has made a request for an object's metadata in preparation for an update to the object's metadata.

HPMD: HTTP PUT Metadata

```
2009-11-20T00:56:23.830562 [AUDIT:[HSID
(UI64):195323112][OBNS(CSTR):"UUID"][OBPA
(CSTR):"/"][OBNA(CSTR):"EEABC-DBF-DFE436-
DK034-KD3601L3LN"][UUID(CSTR):"EEABC-DBF-
DFE436-DK034-KD3601L3LN"][OBSP(CSTR)
:""][SPAR(UI64):508738497389789078 3]
[RSLT(FC32):SUCS][AVER(UI32):10] [ATIM
(UI64):1346878978][ATYP(FC32):HPMD][ANI
D(UI32):20279463][AMID(FC32):HTPM] [ATID
(UI64):9893048903][ASQN(UI64):353] [ASES
(UI64):134351648685563]]
```

The HPMD message indicates that the StorageGRID API client has made a request to update an object's metadata.

OMDU: Object Metadata Updated

```
2010-11-20T00:56:23.933709 [AUDIT:[CBID
(UI64):0xBD0999B2C5F3AE64] [UUID(CSTR):
"EEABC-DBF-DFE436-DK034-KD3601L3LN"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI6
4):1346878978][ATYP(FC32):OMDU][ANID(UI
32):20279463][AMID(FC32):BCMS][ATID(UI64)
:9893048903][ASQN(UI64):353][ASES(UI64):1
34351648685563]]
```

The OMDU message indicates that the object's metadata has been successfully updated.

4

Message Reference

A comprehensive listing of generated audit messages

Introduction

This chapter provides detailed descriptions of event-specific audit messages, and the attributes reported for these messages. Each audit message is first listed in a table that groups related messages by the class of activity that the message represents. These groupings are useful both for understanding the types of activities that are audited, and for selecting the desired type of audit message filtering (as described in "Message Level Filtering" on page 10).

The audit messages are also listed alphabetically by their four-character codes (starting on page 51). This alphabetic listing facilitates finding information about a specific message of interest.

The four-character codes used throughout this chapter are the ATYP values found in the audit messages, as shown in the sample message below:

```
2008-06-20T00:14:20.718929 [AUDT:[FPTH(CSTR):"/fsg/cifsshare/
CT_1200_1_5d/044a198def43f1_254"][FSIZ(UI64):532480][UUID(CSTR)
:"86E91656-4788-4874-8F26-34F8ED7DAA0C"][RSLT(FC32):SUCS][AVER
(UI32):9][ATIM(UI64):1213920860718929][ATYP(FC32):FSWO][ANID
(UI32):20946829][AMID(FC32):FSGC][ATID(UI64):2951277210434284714
][ASQN(UI64):2938513][ASES(UI64):1213829438271695]]
```

System Audit Messages

This group of messages belong to the System audit category and are for events related to:

- The auditing system itself
- Grid node states
- Grid-wide task activity (grid tasks)
- Service backup operations
- File System Gateway (FSG) replication

Table 9: System Audit Messages

Code	Description	Page
BKSB	Backup Store Begin — A service has begun a backup operation.	55
BKSE	Backup Store End — A service has completed a backup operation.	56
ETAF	Security Authentication Failed — A connection attempt using Transport Layer Security (TLS) has failed.	66
ETCA	TCP/IP Connection Establish — An incoming or outgoing TCP/IP connection was successfully established.	67
ETCC	TCP/IP Connection Close — An established connection has been closed by either side of the connection (normally or abnormally).	68
ETCF	TCP/IP Connection Fail — An outgoing connection attempt failed at the lowest level, due to communication problems.	69
ETCR	TCP/IP Connection Refused — An incoming TCP/IP connection attempt was not allowed.	70
GNRG	GNDS Registration — A service has updated or registered information about itself in the grid.	76
GNUR	GNDS Unregistration — A service has unregistered information about itself from the grid.	76
GTED	Grid Task Ended — The CMN service has finished processing the grid task.	77
GTST	Grid Task Started — The CMN service has started to process the grid task.	77
GTSU	Grid Task Submitted — A grid task has been submitted to the CMN service.	78
IPMS	IP Mismatch — A session is accepted from a peer that has an unexpected IP address.	93
REND	Restoration End — An entity has completed the process of restoring private structured data from the grid	97
RPSB	Replication Session Begin — A service has begun a replication session to a secondary service.	98
RPSE	Replication Session End — A service has completed a replication session to a secondary service.	99
RSTA	Restoration Begin — An entity is starting the process of restoring private structured data from the grid	100
SADD	Security Audit Disable — Audit message logging has been turned off.	100
SADE	Security Audit Enable — Audit message logging has been turned on.	101
SYSD	Node Stop — A StorageGRID grid service has been gracefully stopped.	101

Table 9: System Audit Messages (cont.)

Code	Description	Page
SYST	Node Stopping—A StorageGRID grid service has initiated a graceful stop.	104
SYSU	Node Start—AStorageGRID grid service started; the nature of the previous shutdown is indicated in the message.	105

Object Storage Audit Messages

Object storage category audit messages represent events related to the storage and management of objects within the grid. These include:

- Object storage/retrieval
- Node-to-node transfer
- Verification

Table 10: Object Storage Audit Messages

Code	Description	Page
ARCB	Archive Object Retrieve Begin — The ARC service begins the retrieval of an object from archive media.	51
ARCE	Archive Object Retrieve End — The object has been retrieved from archive media, and the ARC service reports the status of the retrieval operation.	52
AREM	Archive Object Remove — A content block was successfully or unsuccessfully purged from an Archive Node.	53
ASCE	Archive Object Store End — A content block has been written to the archive media, and the ARC service reports the status of the write operation.	53
ATCE	Archive Object Store Begin — Storing a content block to archive media has started.	54
CBSB	Object Send Begin — The source entity initiated a node-to-node data transfer operation on a single piece of content.	58
CBSE	Object Send End — The source entity completed a node-to-node data transfer operation.	60
CBRB	Object Receive Begin — The destination entity initiated a node-to-node data transfer operation on a single piece of content.	56
CBRE	Object Receive End — The destination entity completed a node-to-node data transfer operation.	57
CRMP	Re-map CMS Content — All content owned by the source CMS service has been re-mapped to the destination CMS service as part of a Control Node hardware refresh.	64

Table 10: Object Storage Audit Messages

Code	Description	Page
LRMP	Re-Map LDR Content — All content on a source LDR has been re-mapped to the destination LDR as part of a Storage Node hardware refresh.	93
OHRP	Object Handle Repoint — Indicates that the object referenced by an object handle was changed.	93
OLST	Object Lost — A specific object was found to be missing from the grid by the CMS service that manages the object.	94
OMDU	Object Metadata Updated — Logs the result of an attempt to update custom metadata for an object.	95
ORLM	Object Rules Met — The object is stored where specified by the ILM rules.	96
SCMT	Object Store Commit — A content block was completely stored and verified, and can now be requested.	101
SREM	Object Store Remove — A content block was deleted from a node, and can no longer be requested directly.	102
SVRF	Object Store Verify Fail — A content block failed verification checks.	102
SVRU	Object Store Verify Unknown — Unexpected file(s) detected in the object store.	103

HTTP Protocol Audit Messages

HTTP Protocol audit messages (the Protocol – HTTP category) represent events related to interactions with internal and external system components using the HTTP protocol. These include:

- Session establishment/teardown
- Object storage
- Retrieval
- Query
- Metadata updates

Table 11: HTTP Protocol Audit Messages

Code	Description	Used By	Page
CDMD	CDMI DELETE Transaction — Logs a successful transaction to delete a data object.	CDMI client	61
CDMG	CDMI GET Transaction — Logs a successful transaction to read from a data object.	CDMI client	61

Table 11: HTTP Protocol Audit Messages

Code	Description	Used By	Page
CDMP	CDMI POST Transaction — Logs a successful transaction to create a new data object.	CDMI client	62
CDMU	CDMI PUT Transaction — Logs a successful transaction to add or update user metadata of a data object.	CDMI client	63
HDEL	HTTP DELETE Transaction — Logs a successful transaction to delete content.	StorageGRID API client FSG client	79
HGEE	HTTP GET Transaction End — A GET transaction to transfer content completed.	StorageGRID API client FSG client	81
HGES	HTTP GET Transaction Start — A request for a GET transaction to transfer content was initiated.	StorageGRID API client FSG client	83
HGMD	HTTP GET Metadata — A GET transaction to retrieve all predefined and custom metadata was initiated.	StorageGRID API client	83
HHEA	HTTP HEAD Transaction — Information about a piece of content was requested.	StorageGRID API client FSG client	84
HOPT	HTTP OPTIONS Transaction — Logs the result of a request for information about the transactions that can be performed on content.	StorageGRID API FSG client	86
HPMD	HTTP PUT Metadata — A PUT transaction to add or update custom metadata of an existing object was initiated.	StorageGRID API client	86
HPOE	HTTP POST Transaction End — A request for stored content completed.	StorageGRID API client	87
HPOS	HTTP POST Transaction Start — A query for stored content was initiated.	StorageGRID API client	88
HPUE	HTTP PUT Transaction End — A PUT transaction to transfer content completed.	StorageGRID API client FSG client	89
HPUS	HTTP PUT Transaction Start — A PUT transaction to transfer content was initiated.	StorageGRID API client FSG client	91

Table 11: HTTP Protocol Audit Messages

Code	Description	Used By	Page
HTSC	HTTP Session Close — A previously-established HTTP session was closed.	StorageGRID API and CDMI clients FSG client	91
HTSE	HTTP Session Establish — A remote host successfully established a session to the node.	StorageGRID API and CDMI clients FSG client	92

File System Gateway Audit Messages

This set of messages (the Protocol – File category) log activity related to interactions with external systems via the File System Gateway (FSG) interface to the grid.

Table 12: File System Gateway Audit Messages

Code	Description	Page
DCRE	Directory Create — Indicates that a new directory has been created on the volume shared by the FSG.	65
DDEL	Directory Delete — Indicates that an existing directory has been deleted on the volume shared by the FSG.	65
DRNM	Directory Rename — Indicates that an existing directory has been renamed on the volume shared by the FSG.	66
FCRE	File Create — Logs the addition of new files (not directories) to the FSG.	71
FDEL	File Delete — Logs deletion of a file from the FSG directory tree (not from the grid).	71
FMFY	File Modify — Logs ingested files that have been released from the FSG (modified or deleted).	72
FRCV	File Recovery — A file stored in the grid has been deleted, modified, or overwritten and the original file has been moved to the file recovery area on the FSG. **NOTE** File recovery is deprecated.	72
FRNM	File Rename — Logs changes to the name or path of an existing file.	72

Table 12: File System Gateway Audit Messages

Code	Description	Page
FSTG	File Store to Grid — Logs the storage of content from the FSG local cache to the grid.	73
FSWI	File Swap In — Logs the retrieval of a file from the grid to the FSG local cache.	74
FSWO	File Swap Out — Logs the deletion of a file from the FSG local cache (but not from the directory tree or grid).	75

As content is added to the grid via the FSG, the content is first stored locally in a cache on the FSG server. The FSG manages ingesting the content to the grid. The content in the cache can be purged if space is needed for new content, either inbound or outbound. As the cache content is changed, additional audit messages are logged.

Any changes made to the name or content of a file previously entered in the FSG are also logged, as are file deletions from the FSG.

External Audit Messages

It is possible to develop a custom application using the StorageGRID API that saves messages generated by an external application to the audit log file. These audit messages must follow the format of grid-generated messages, but the meaning of these messages and their codes are controlled by the external application. For more information on external audit messages, see the *StorageGRID API Reference*.

Table 13: External Audit Messages

Code	Description	Page
EXTL	External — Logs audit messages supplied by an external application via the StorageGRID API.	*StorageGRID API Reference*

Audit Message Reference

ARCB—Archive Object Retrieve Begin

When a request is made to retrieve content stored on archive media, this message is generated as the retrieval process begins.

Retrieval requests are processed immediately, but can be reordered to improve efficiency of retrieval from linear media such as tape.

Table 14: ARCB—Archive Object Retrieve Begin Fields

Code	Field	Description
CBID	Content Block ID	The unique identifier of the Content Block to be retrieved from the archive media.
RSLT	Result	Indicates the result of starting the archive retrieval process. Currently defined values are: SUCS — The content request was received and queued for retrieval.

This audit message marks the time of an archive object retrieval. It allows you to match the message with a corresponding ARCE end message to determine the duration of archived content retrieval, and whether the operation was successful.

ARCE—Archive Object Retrieve End

When an attempt to retrieve content from archive media completes, this message is generated. If successful, the message indicates that the data has been completely read from the archive location, and was successfully verified. Once content has been retrieved and verified, it is delivered to the requesting service.

Table 15: ARCE—Archive Object Retrieve End Fields

Code	Field	Description
CBID	Content Block ID	The unique identifier of the Content Block to be retrieved from the archive media.
VLID	Volume Identifier	The identifier of the volume on which the data was archived. If an archive location for the content is not found, a Volume ID of 0 is returned.
RSLT	Retrieval Result	The completion status of the archive retrieval process: SUCS — successful VRFL — failed (object verification failure) ARUN — failed (archive middleware unavailable) CANC — failed (retrieval operation cancelled) GERR — failed (general error)

Matching this message with the corresponding ARCB message can indicate the time taken to perform the archive retrieval. This message indicates whether the retrieval was successful, and in the case of failure, the cause of the failure to retrieve the content block.

AREM—Archive Object Remove

The Archive Object Remove audit message indicates that a content block was successfully or unsuccessfully purged from an Archive Node. If the result is successful, the Archive Node has successfully informed the archive middleware that an object location has been released by the grid. Whether the object is removed from archive media depends on the type of middleware and its configuration.

Table 16: AREM—Archive Object Remove Fields

Code	Field	Description
CBID	Content Block ID	The unique identifier of the Content Block to be retrieved from the archive media.
VLID	Volume Identifier	The identifier of the volume on which the data was archived.
RSLT	Retrieval Result	The completion status of the archive removal process: SUCS — successful ARUN — failed (archive middleware unavailable) GERR — failed (general error)

ASCE—Archive Object Store End

This message is generated after a content block is completely written to the archive location, optionally retrieved and verified, and the CMS notified of the location of the content block.

Table 17: ASCE—Archive Object Store End Fields

Code	Field	Description
CBID	Content Block Identifier	The identifier of the content block stored on the archive destination.
VLID	Volume Identifier	The unique identifier of the archive volume to which the data is written.

Table 17: ASCE—Archive Object Store End Fields (cont.)

Code	Field	Description
VREN	Verification Enabled	Indicates if verification is performed for content blocks. Currently defined values are: VENA — verification is enabled VDSA — verification is disabled
MCLS	Management Class	A string identifying the TSM Management Class to which the content block is assigned if applicable.
RSLT	Result	Indicates the result of archive process. Currently defined values are: SUCS — successful (archiving process succeeded) OFFL — failed (archiving is offline) VRFL — failed (object verification failed) ARUN — failed (archive middleware was unavailable) GERR — failed (general error)

This audit message means that the specified content block has been written to archive media. If the write fails, the result provides basic troubleshooting information about where the failure occurred. More detailed information about archive failures can be found by examining Archive Node attributes in the NMS MI.

ATCE—Archive Object Store Begin

This message indicates that writing a content block to archive media has started.

Table 18: ATCE—Archive Object Store Begin Fields

Code	Field	Description
CBID	Content Block ID	The unique identifier of the content block to be archived.
VLID	Volume ID	The unique identifier of the volume to which the content block is written. If the operation fails, a volume ID of 0 is returned.

Table 18: ATCE—Archive Object Store Begin Fields (cont.)

Code	Field	Description
RSLT	Result	Indicates the result of the transfer of the content block. Currently defined values are: SUCS — success (content block stored successfully) EXIS — ignored (content block was already stored) ISFD — failed (insufficient disk space) STER — failed (error storing the CBID) OFFL — failed (archiving is offline) GERR — failed (general error)

BKSB—Backup Store Begin

When a service begins a backup operation — storing private structured data to the grid — this message is generated.

Table 19: BKSB—Backup Store Begin Fields

Code	Field	Description
BKSI	Backup Session ID	The unique identifier of the backup session that is being started.
BKOI	Backup Source Entity	The type of entity that is performing the backup; typically one of: BFSG, BCMS, or BNMS.
BKEE	Entries to Backup	The number of entries (objects) the entity expects to include in this backup session. If the value is unknown, this field is set to zero (0).
RSLT	Backup Initiation Status	This field indicates status at the time the backup store was initiated: SUCS — The backup store started successfully.

This message marks the time of a backup session. It allows you to match the message with a corresponding BKSE end message to determine that backups are happening as planned and whether they are successful.

BKSE—Backup Store End

When a service completes a backup operation, this message is generated.

Table 20: BKSE—Backup Store End Fields

Code	Field	Description
BKSI	Backup Session ID	The unique identifier of the backup session that has been completed.
BKOI	Backup Source Entity	The type of entity that performed the backup; typically one of: BFSG, BCMS, or BNMS.
BKEA	Entries Backed Up	The actual number of entries (objects) that were included in this backup session. You can compare this to BKEE in the BKSB message.
UUID	Backup UUID	The Universal Unique IDentifier assigned to the backup by the grid. If the backup session fails or is aborted, this value is the NULL UUID.
RSLT	Backup Result	The completion status of the backup session: SUCS — The backup completed successfully. ABRT — The backup was aborted. FAIL — The backup failed before completion. STFL — The backup data could not be stored in the grid.

Matching this message with the corresponding BKSB message can indicate the time it took to perform the backup. This message indicates whether the backup was successful and the UUID of the backup data within the grid, should a restoration be needed.

CBRB—Object Receive Begin

During normal system operations, content blocks are continuously transferred between different nodes as data is accessed, replicated and retained. When transfer of a content block from one node to another is initiated, this message is issued by the destination entity.

Table 21: CBRB—Object Receive Begin Fields

Code	Field	Description
CNID	Connection Identifier	The unique identifier of the node-to-node session/connection.
CBID	Content Block Identifier	The unique identifier of the content block being transferred.

Table 21: CBRB—Object Receive Begin Fields (cont.)

Code	Field	Description
CTDR	Transfer Direction	Indicates if the CBID transfer was push-initiated or pull-initiated: PUSH — The transfer operation was requested by the sending entity. PULL — The transfer operation was requested by the receiving entity.
CTSR	Source Entity	The node ID of the source (sender) of the CBID transfer.
CTDS	Destination Entity	The node ID of the destination (receiver) of the CBID transfer.
CTSS	Start Sequence Count	Indicates the first sequence count requested. If successful, the transfer begins from this sequence count.
CTES	Expected End Sequence Count	Indicates the last sequence count requested. If successful, the transfer is considered complete when this sequence count has been received.
RSLT	Transfer Start Status	Status at the time the transfer was started: SUCS — Transfer started successfully.

This audit message means a node-to-node data transfer operation was initiated on a single piece of content, as identified by its Content Block Identifier. The operation requests data from "Start Sequence Count" to "Expected End Sequence Count". Sending and receiving nodes are identified by their node IDs. This information can be used to track system data flow, and when combined with storage audit messages, to verify replica counts.

CBRE—Object Receive End

When transfer of a content block from one node to another is completed, this message is issued by the destination entity.

Table 22: CBRE—Object Receive End Fields

Code	Field	Description
CNID	Connection Identifier	The unique identifier of the node-to-node session/connection.
CBID	Content Block Identifier	The unique identifier of the content block being transferred.

Table 22: CBRE—Object Receive End Fields (cont.)

Code	Field	Description
CTDR	Transfer Direction	Indicates if the CBID transfer was push-initiated or pull-initiated: PUSH — The transfer operation was requested by the sending entity. PULL — The transfer operation was requested by the receiving entity.
CTSR	Source Entity	The node ID of the source (sender) of the CBID transfer.
CTDS	Destination Entity	The node ID of the destination (receiver) of the CBID transfer.
CTSS	Start Sequence Count	Indicates the sequence count on which the transfer started.
CTAS	Actual End Sequence Count	Indicates the last sequence count successfully transferred. If the Actual End Sequence Count is the same as the Start Sequence Count, and the Transfer Result was not successful, no data was exchanged.
RSLT	Transfer Result	The result of the transfer operation (from the perspective of the sending entity): SUCS—transfer successfully completed; all requested sequence counts were sent. CONL — connection lost during transfer CTMO — connection timed-out during establishment or transfer UNRE — destination node ID unreachable CRPT — transfer ended due to reception of corrupt or invalid data (may indicate tampering)

This audit message means a node-to-node data transfer operation was completed. If the Transfer Result was successful, the operation transferred data from "Start Sequence Count" to "Actual End Sequence Count". Sending and receiving nodes are identified by their node IDs. This information can be used to track system data flow and to locate, tabulate, and analyze errors. When combined with storage audit messages, it can also be used to verify replica counts.

CBSB—Object Send Begin

During normal system operations, content blocks are continuously transferred between different nodes as data is accessed, replicated and

retained. When transfer of a content block from one node to another is initiated, this message is issued by the source entity.

Table 23: CBSB—Object Send Begin Fields

Code	Field	Description
CNID	Connection Identifier	The unique identifier of the node-to-node session/connection.
CBID	Content Block Identifier	The unique identifier of the content block being transferred.
CTDR	Transfer Direction	Indicates if the CBID transfer was push-initiated or pull-initiated: PUSH — The transfer operation was requested by the sending entity. PULL — The transfer operation was requested by the receiving entity.
CTSR	Source Entity	The node ID of the source (sender) of the CBID transfer.
CTDS	Destination Entity	The node ID of the destination (receiver) of the CBID transfer.
CTSS	Start Sequence Count	Indicates the first sequence count requested. If successful, the transfer begins from this sequence count.
CTES	Expected End Sequence Count	Indicates the last sequence count requested. If successful, the transfer is considered complete when this sequence count has been received.
RSLT	Transfer Start Status	Status at the time the transfer was started: SUCS — transfer started successfully.

This audit message means a node-to-node data transfer operation was initiated on a single piece of content, as identified by its Content Block Identifier. The operation requests data from “Start Sequence Count” to “Expected End Sequence Count”. Sending and receiving nodes are identified by their node IDs. This information can be used to track system data flow, and when combined with storage audit messages, to verify replica counts.

CBSE—Object Send End

When transfer of a content block from one node to another is completed, this message is issued by the source entity.

Table 24: CBSE—Object Send End Fields

Code	Field	Description
CNID	Connection Identifier	The unique identifier of the node-to-node session/connection.
CBID	Content Block Identifier	The unique identifier of the content block being transferred.
CTDR	Transfer Direction	Indicates if the CBID transfer was push-initiated or pull-initiated: PUSH — The transfer operation was requested by the sending entity. PULL — The transfer operation was requested by the receiving entity.
CTSR	Source Entity	The node ID of the source (sender) of the CBID transfer.
CTDS	Destination Entity	The node ID of the destination (receiver) of the CBID transfer.
CTSS	Start Sequence Count	Indicates the sequence count on which the transfer started.
CTAS	Actual End Sequence Count	Indicates the last sequence count successfully transferred. If the Actual End Sequence Count is the same as the Start Sequence Count, and the Transfer Result was not successful, no data was exchanged.
RSLT	Transfer Result	The result of the transfer operation (from the perspective of the sending entity): SUCS — Transfer successfully completed; all requested sequence counts were sent. CONL — connection lost during transfer CTMO — connection timed-out during establishment or transfer UNRE — destination node ID unreachable CRPT — transfer ended due to reception of corrupt or invalid data (may indicate tampering)

This audit message means a node-to-node data transfer operation was completed. If the Transfer Result was successful, the operation transferred data from “Start Sequence Count” to “Actual End Sequence Count”. Sending and receiving nodes are identified by their node IDs. This information can be used to track system data flow and to locate, tabulate, and analyze errors. When combined with storage audit messages, it can also be used to verify replica counts.

CDMD—CDMI Delete Transaction

When a CDMI client issues a DELETE transaction, a request is made to remove the specified data object. This message is issued by the server if the transaction is successful.

Table 25: CDMD—CDMI DELETE Transaction Fields

Code	Field	Description
CBID	Content Block Identifier	The unique identifier of the corresponding content block requested. If the CBID is unknown, this field is set to 0.
CSIZ	Content Size	The size of the object, in bytes.
CURI	CDMI URI	The URI to the object to be removed. Does not contain the /CDMI root.
HSID	Session Identifier	The unique identifier assigned to the HTTP session.
OBSP	Security Partition Name	The user-defined name for the security partition assigned to the data object. An empty string is returned if the object is not associated with a security partition.
COID	CDMI Object Identifier	A unique value assigned at creation time to identify an object.
SPAR	Security Partition ID	The unique identifier of the security partition assigned to the target object. Zero is returned if the object is not associated with a security partition. SPAR can be used to determine the security partition which an object is associated. See "Determine Security Partition or Replication Group ID for an Object" on page 80.
RSLT	Result Code	Result of the DELETE transaction. Result is always: SUCS — successful
TIME	Time	Total processing time for the request, in microseconds.

CDMG—CDMI GET Transaction

When a CDMI client issues a GET transaction, a request is made to read a data object. This message is issued by the server if the transaction is successful.

Table 26: CDMG—CDMI GET Transaction Fields

Code	Field	Description
CBID	Content Block Identifier	The unique identifier of the corresponding content block requested. If the CBID is unknown, this field is set to 0.

Table 26: CDMG—CDMI GET Transaction Fields (cont.)

Code	Field	Description
CSIZ	Content Size	The size of the retrieved object, in bytes.
HSID	Session Identifier	The unique identifier assigned to the HTTP session.
CURI	CDMI URI	The URI to the data object. Does not contain the /CDMI root.
OBSP	Security Partition Name	The user-defined name for the security partition assigned to the data object. An empty string is returned if the object is not associated with a security partition.
COID	CDMI Object Identifier	A unique value assigned at creation time to identify an object.
SPAR	Security Partition ID	The unique identifier of the security partition assigned to the target object. Zero is returned if the object is not associated with a security partition. SPAR can be used to determine the security partition which an object is associated. See "Determine Security Partition or Replication Group ID for an Object" on page 80.
RSLT	Result Code	Result of the GET transaction. Result is always: SUCS — successful
TIME	Time	Total processing time for the request, in microseconds.

CDMP—CDMI POST Transaction

When a CDMI client issues a POST transaction, a request is made to create a new data object. This message is issued by the server if the transaction is successful.

Table 27: CDMP—CDMI POST Transaction Fields

Code	Field	Description
CBID	Content Block Identifier	The unique identifier of the corresponding content block requested. If the CBID is unknown, this field is set to 0.
CSIZ	Content Size	The size of the original content stored, in bytes.
HSID	Session Identifier	The unique identifier assigned to the HTTP session.
CURI	CDMI URI	The URI to the data object. Does not contain the /CDMI root.
OBSP	Security Partition Name	The user-defined name for the security partition assigned to the data object. An empty string is returned if the object is not associated with a security partition.

Table 27: CDMP—CDMI POST Transaction Fields (cont.)

Code	Field	Description
COID	CDMI Object Identifier	A unique value assigned at creation time to identify an object.
SPAR	Security Partition ID	The unique identifier of the security partition assigned to the target object. Zero is returned if the object is not associated with a security partition. SPAR can be used to determine the security partition which an object is associated. See "Determine Security Partition or Replication Group ID for an Object" on page 80.
RSLT	Result Code	Result of the POST transaction. Result is always: SUCS — successful
TIME	Time	Total processing time for the request, in microseconds.

CDMU—CDMI PUT Transaction

When a CDMI client initiates a PUT transaction, a request is made to add or update all of the user metadata of a data object. This message is issued by the server if the transaction is successful.

Table 28: CDMU—CDMI PUT Transaction Fields

Code	Field	Description
CBID	Content Block Identifier	The unique identifier of the corresponding content block requested. If the CBID is unknown, this field is set to 0.
CSIZ	Content Size	The size of the original content stored, in bytes.
HSID	Session Identifier	The unique identifier assigned to the HTTP session.
CURI	CDMI URI	The URI to the data object. Does not contain the /CDMI root.
OBSP	Security Partition Name	The user-defined name for the security partition assigned to the data object. An empty string is returned if the object is not associated with a security partition.
COID	CDMI Object Identifier	A unique value assigned at creation time to identify an object.
SPAR	Security Partition ID	The unique identifier of the security partition assigned to the target object. Zero is returned if the object is not associated with a security partition. SPAR can be used to determine the security partition which an object is associated. See "Determine Security Partition or Replication Group ID for an Object" on page 80.

Table 28: CDMU—CDMI PUT Transaction Fields (cont.)

Code	Field	Description
RSLT	Result Code	Result of the PUT transaction. Result is always: SUCS — successful
TIME	Time	Total processing time for the request, in microseconds.

CRMP—Re-Map CMS Content

This message indicates that a Re-Map CMS Metadata grid action was processed by a CMS: all content owned by the source CMS service has been re-mapped to the destination CMS service as part of a Control Node hardware refresh.

Table 29: CRMP — Re-Map CMS Content

Code	Field	Description
SNID	Source CMS	The node ID of the original CMS service that previously owned the metadata.
DNID	Destination CMS	The node ID of the new CMS service that now owns the metadata.
RSLT	Result	This field has the value 'SUCS'. RSLT is a mandatory message field but is not relevant for this particular message.

The Re-Map CMS Metadata grid action is triggered during a Control Node hardware refresh procedure which causes a new CMS service to own everything that was previously owned by another CMS service. On receiving a Re-Map CMS Metadata grid action, a CMS service records the remapping of node IDs and immediately acts as if metadata previously on the original CMS service is now on the new CMS service. The CMS service issues this audit message after it successfully processes the Re-Map CMS Metadata grid action.

DCRE—Directory Create

When a new directory is created on the volume shared by the File System Gateway, this message is issued.

Table 30: DCRE—Directory Create Fields

Code	Field	Description
FPTH	File Path	Indicates the complete path and name of the directory that has been created.
RSLT	Result	Indicates the result of creating the directory. Currently defined values are: SUCS — The directory was created successfully.

This audit message means that a new directory has been created at a specific location.

DDEL—Directory Delete

When a directory is deleted on the volume shared by the File System Gateway, this message is issued.

Table 31: DCRE—Directory Delete Fields

Code	Field	Description
FPTH	File Path	Indicates the complete path and name of the directory that has been deleted.
RSLT	Result	Indicates the result of deleting the directory. Currently defined values are: SUCS — The directory was deleted successfully.

This audit message means that a directory has been deleted at a specific location.

DRNM—Directory Rename

When a directory is renamed on the volume shared by the File System Gateway, this message is issued.

Table 32: DCRE—Directory Rename Fields

Code	Field	Description
OLDP	Original File Path	The complete path and name of the (original) directory being renamed.
NEWP	New File Path	The complete path and name being assigned to the directory.
RSLT	Result	Indicates the result of renaming the directory. Currently defined values are: SUCS — The directory was renamed successfully.

This audit message means that a directory has been renamed and now resides at a different location and/or has a new file name.

ETAF—Security Authentication Failed

A connection attempt using Transport Layer Security (TLS) has failed.

Table 33: ETAF—Security Authentication Failed Fields

Code	Field	Description
CNID	Connection Identifier	The unique grid identifier for the TCP/IP connection over which the authentication failed.
RUID	User Identity	A service dependent identifier representing the identity of the remote user.
RSLT	Reason Code	The reason for the failure: SCNI — Secure connection establishment failed. CERM — Certificate was missing. CERT — Certificate was invalid. CERE — Certificate was expired. CERR — Certificate was revoked. CSGN — Certificate signature was invalid. CSGU — Certificate signer was unknown. UCRM — User credentials were missing. UCRI — User credentials were invalid. UCRU — User credentials were disallowed. TOUT — Authentication timed out.

When a connection is established to a secure service that uses TLS, the credentials of the remote entity are verified using the TLS profile and additional logic built into the service. If this authentication fails due to invalid, unexpected, or disallowed certificates or credentials, an audit message is logged. This enables queries for unauthorized access attempts and other security-related connection problems.

The message could result from a remote entity having an incorrect configuration, or from attempts to present invalid or disallowed credentials to the system. This audit message should be monitored to detect attempts to gain unauthorized access to the system.

ETCA—TCP / IP Connection Establish

When a connection to a service running on a node is permitted, this message is generated.

Table 34: ETCA—TCP / IP Connection Establish Fields

Code	Field	Description
SEID	Service Identifier	The unique identifier of the service to which the connection was established. Values of interest include: • HING: HTTP Ingest Service • HCLN: HTTP Query/Retrieve Service • NCON: Neighbor Connection Service
CNDR	Connection Direction	Indicates whether the connection was opened by the grid node or by a remote host: INBO — Connection initiated by a remote host, which connected to the node. OUTB — Connection initiated by the grid node, which connected to a remote host.
SVIP	Destination Service Port	The port the connection was established to.
DAIP	Destination IP Address	The IP address the connection was established to.
SAIP	Source IP Address	The IP address the connection was established from.
CNID	Connection Identifier	The unique identifier of the connection.
RSLT	Result Code	Connection status: SUCS — connection successfully established

This audit message means an incoming or outgoing TCP/IP connection was successfully established. This does *not* indicate the corresponding user was permitted to use the service — only that they were not rejected. Typically, each service implements additional authentication mechanisms specific to the service type (HTTP).

This message can be used to report on external hosts communicating with the system, and to correlate higher level protocol messages back to the IP address initiating the activity. The "Connection Identifier" field allows correlation of audit messages related to actions performed during a session.

ETCC—TCP / IP Connection Close

When the system on either side of an established connection closes the connection (either normally or abnormally), this message is generated.

Table 35: ETCC—TCP / IP Connection Close Fields

Code	Field	Description
CNID	Connection Identifier	The unique identifier of the connection.
INIE	Initiating Entity	The entity causing the connection to be closed: LOCL — the node closed the connection RMOT — the remote entity closed the connection
RSLT	Result Code	Why the connection was closed: SUCS — connection closed at an expected point LOST — connection closed by the remote entity at an unexpected point UNEX — connection closed by the remote entity at an unexpected point TOUT — connection timed-out and was closed

This audit message means a TCP/IP connection was closed. When this message is generated, the corresponding connection ID no longer exists, and the associated TCP/IP connection is no longer established.

This message can be used to detect problems within the system, such as network issues over a WAN, or interoperability problems between systems. The "Connection Identifier" field allows correlation of audit messages related to actions performed during a session.

ETCF—TCP / IP Connection Fail

When an attempt to establish a connection to a remote service fails during establishment, this message is generated.

Table 36: ETCF—TCP / IP Connection Fail Fields

Code	Field	Description
SEID	Service Identifier	The unique identifier of the service to which the connection was attempted. Values of interest include: • HING: HTTP Ingest Service • HCLN: HTTP Query/Retrieve Service • NCON: Neighbor Connection Service
CNDR	Connection Direction	Indicates whether the connection was opened by the grid node or by a remote host: INBO — connection initiated by a remote host connecting to the node OUTB — connection initiated by the grid node, attempting a connection to a remote host
SVIP	Destination Service Port	The port to which the connection attempt was made.
DAIP	Destination IP Address	The IP address to which the connection attempt was made.
SAIP	Source IP Address	The IP address from which the connection attempt was made.
CNID	Connection Identifier	The unique identifier of the attempted connection.
RSLT	Result Code	Why the attempted connection failed: IPAR — inbound IP address was not from allowed range CRFU — outgoing connection refused by remote host UNRE — destination (remote host) unreachable ATHF — TCP/IP connection level authentication failure

This audit message means an outgoing or incoming connection attempt failed at the lowest level, due to communication problems - the corresponding service was unable to access the remote host, and the TCP/IP connection was not established.

This message can be used to detect system problems such as configuration errors where content is being pushed to unreachable hosts, or where routing problems result in inaccessibility of hosts. The message can also be used to report on the hosts to which content was pushed. The “Connection Identifier” field allows correlation of audit messages related to actions performed during a session.

ETCR—TCP / IP Connection Refused

The Connection Refused Audit Message indicates that an incoming TCP/IP connection attempt was not allowed.

If the node refuses a connection, this message is generated. Failures of inbound connections can result from a variety of reasons, which are described in the entry below for the Result field.

Table 37: ETCR—TCP / IP Connection Refused Fields

Code	Field	Description
SEID	Service Identifier	The unique identifier of the service to which the connection was attempted. Values of interest include: • HING: HTTP Ingest Service • HCLN: HTTP Query/Retrieve Service • NCON: Neighbor Connection Service
CNDR	Connection Direction	Indicates that the connection was opened by a remote host: INBO — connection initiated by a remote host connecting to the node
SVIP	Destination Service Port	The port to which the connection attempt was made.
DAIP	Destination IP Address	The IP address to which the connection attempt was made (remote IP address).
SAIP	Source IP Address	The IP address from which the connection attempt was made (local IP address).
CNID	Connection Identifier	The unique identifier of the attempted connection.
RSLT	Result Code	Why the attempted connection was refused: IPAR — inbound IP address was not from allowed range ATHF — TCP/IP connection level authentication failure

For incoming connections, this audit message means that a connection was not successfully established at the lowest level due to a security violation. When this message is received, the corresponding user was not able to access the service and the TCP/IP Connection was closed. The most common reporting use of this message is to detect unauthorized attempts to access services running on the system from foreign IP address that have not been explicitly given access to the service.

FCRE—File Create

This message is created when a new file (not a directory) is created on the FSG.

Table 38: FCRE—File Create Fields

Code	Field	Description
FPTH	File Path	The complete path and name of the file that has been created.
RSLT	Result	Indicates the result of creating the file. Currently defined values are: SUCS — file created successfully.

This audit message means a new file entry has been added to the FSG directory tree. The content of the file resides on the local FSG cache, and the process of storing it within the grid has initiated.

See also "Ingest" on page 23.

FDEL—File Delete

When an existing file entry in the FSG is deleted, this logs the deletion.

Table 39: FDEL—File Delete Fields

Code	Field	Description
FPTH	File Path	The complete path and name of the file that has been deleted.
UUID	Universal Unique ID	The identifier of the original version of the file within the grid.
FGRP	Replication Group	The FSG replication group identifier of the FSG on which the operation occurred.
RSLT	Result	Indicates the result of deleting the file. Currently defined values are: SUCS — file deleted successfully

This audit message means an existing file entry has been deleted from the FSG directory tree. The content of the file residing within the grid is not affected, however the file becomes inaccessible through the FSG.

Deleting a directory triggers an audit message for each enclosed file that is deleted.

See also "Deletion" on page 34.

FMFY—File Modify

The FMFY message indicates that the indicated UUID is no longer associated with the file identified in the message. This can occur when an existing file is modified (such that the original file is overwritten), or when the file is deleted.

Table 40: FMFY—File Modify Fields

Code	Field	Description
FPTH	File path	The complete path and name of the file being modified.
UUID	Universal Unique ID	The identifier of the original version of the file within the grid.
FGRP	Replication Group	The FSG replication group identifier of the FSG on which the operation occurred.
RSLT	Result	Indicates the result of modifying the file. Currently defined values are: SUCS — file modified successfully

If file purging is not enabled for the grid, the original content of the modified file is retained within the grid, but can no longer be accessed through the FSG. The content is available through other direct grid interfaces via a query on object metadata.

If file purging is enabled, the original content of the file is deleted as needed to free grid storage.

See also "Modification" on page 38.

FRCV—File Recovery

NOTE File recovery is deprecated and no longer supported.

The File Recovery audit message indicates that a file stored in the grid has been deleted, modified, or overwritten and the original file has been moved to the file recovery area on the FSG.

Table 41: FRCV—File Recovery Fields

Code	Field	Description
OLDP	Original file path	The complete path and name of the original file that was modified or deleted.

Table 41: FRCV—File Recovery Fields (cont.)

Code	Field	Description
NEWP	New file path	The complete path and name of the file that was created in the file recovery area.
UUID	Universal Unique ID	The identifier of the original version of the file within the grid.
RSLT	Result	Indicates the result of renaming the file. Currently defined values are: SUCS—The recovery file was successfully created in the file recovery area. GERR—A general error occurred attempting to create the recovery file. The recovery file was not created.

File recovery must be enabled in the NMS MI for the file to be moved to the file recovery area and for this message to be generated.

See also "Deletion" on page 34.

FRNM—File Rename

When an existing file entry in the FSG is renamed, this logs the change.

Table 42: FRNM—File Rename Fields

Code	Field	Description
OLDP	Original file path	The complete path and name of the (original) file being renamed.
NEWP	New file path	The complete path and name being assigned to the file.
RSLT	Result	Indicates the result of renaming the file. Currently defined values are: SUCS—file renamed successfully

An existing file entry in the FSG directory tree is changing. The content of the file residing within the grid is not affected.

FSTG—File Store to Grid

When new content is stored via the FSG, the content is cached locally by the FSG server and is copied into the grid. When the grid confirms it has stored the copy (and is processing it under its business rules for replication), this message is issued.

Table 43: FSTG—File Store to Grid Fields

Code	Field	Description
FPTH	File path	The complete path and name of the file being stored.
FLTP	File Type	Indicates the type of object storage, as processed by the grid's file type detection.
UUID	Universal Unique ID	The identifier of the file content within the grid.
FSIZ	File size	Indicates the size of the file in bytes.
FTIM	Operation Time	Indicates the total time required to store the file in microseconds.
FGRP	Replication Group	The FSG replication group identifier of the FSG on which the operation occurred.
RSLT	Result Code	The result of the storage operation: SUCS — Successfully stored. FTER — Failed extended type verification (will be re-ingested as a generic object). TOUT — Failed due to timeout. ERRC — Failed due to lost connection. GERR — A general error occurred while storing content.

If a failure is logged, the FSG initiates a new storage attempt. Retries continue until successful.

See also "Ingest" on page 23.

FSWI—File Swap In

A file has been retrieved from the grid for storage in the FSG local cache. Content still resides in the grid.

Table 44: FSWI—File Swap In Fields

Code	Field	Description
FPTH	File path	The complete path and name of the file added to the FSG local cache.
UUID	Universally Unique ID	The identifier of the file content within the grid.

Table 44: FSWI—File Swap In Fields (cont.)

Code	Field	Description
RSLT	Result Code	The result of the file retrieve operation: SUCS — Successfully retrieved. TOUT — Failed due to timeout. ERRC — Failed due to lost connection. GERR — A general error occurred while retrieving the content.
FSIZ	File size	Indicates the size of the file in bytes.
FTIM	Operation Time	Indicates the total time required to retrieve the file in microseconds.
FGRP	Replication Group	The FSG replication group identifier of the FSG on which the operation occurred.

The original content of the file (along with its associated path and file name metadata) is retained within the grid at the UUID provided.

This message indicates that a file not stored in the FSG local cache has been accessed using the FSG. That access may be for the purpose of modification, in which case the FMFY message should also appear in the audit log.

See also "Retrieval" on page 29.

FSWO—File Swap Out

A file has been purged from the FSG local cache. Content still resides in the grid and can be accessed using the FSG.

Table 45: FSWO—File Swap Out Fields

Code	Field	Description
FPTH	File path	The complete path and name of the file dropped from the FSG local cache.
UUID	Universal Unique ID	The identifier of the file content within the grid.
RSLT	Result	Indicates the result of the swap out operation. Currently defined values are: SUCS — File successfully swapped out.
FSIZ	File Size	Indicates the size of the file in bytes.

The original content of the file (along with its associated path and file name metadata) is retained within the grid at the UUID provided. The FSG interface can be used to retrieve the content from the grid.

GNRG—GNDS Registration

The CMN service generates this audit message when a service has updated or registered information about itself in the grid.

Table 46: GNRG—GNDS Registration

Code	Field	Description
RSLT	Result	The result of the update request: • SUCS — Successful • SUNV— Service Unavailable • GERR — Other failure
GNID	Node ID	The node ID of the service that initiated the update request
GNTP	Device Type	The node's device type (for example, BLDR for an LDR)
GNDV	Device Model version	The string identifying the node's device model version in the DMDL bundle.
GNGP	Group	The group to which the node belongs (in the context of link costs and service-query ranking).
GNIA	IP Address	The node's IP address.

This message is generated whenever a node updates its entry in the Grid Nodes Bundle.

GNUR—GNDS Unregistration

The CMN service generates this audit message when a service has unregistered information about itself from the grid.

Table 47: GNUR—GNDS Unregistration

Code	Field	Description
RSLT	Result	The result of the update request: • SUCS — Successful • SUNV— Service Unavailable • GERR — Other failure
GNID	Node ID	The node ID of the service that initiated the update request

This message is generated whenever a node removes its entry in the Grid Nodes Bundle.

GTED—Grid Task Ended

This audit message indicates that the CMN service has finished processing the specified grid task and has moved the task to the Historical table. If the result is SUCS, ABRT, or ROLF, there will be a corresponding Grid Task Started audit message. The other results indicate that processing of this grid task never started.

Table 48: GTED—Grid Task Ended Fields

Code	Field	Description
TSID	Task ID	This field uniquely identifies a generated grid task and allows the task to be managed over its lifecycle. **NOTE** The Task ID is assigned at the time that a grid task is generated, not the time that it is submitted. It is possible for a given task to be submitted multiple times, and in this case the Task ID field is not sufficient to uniquely link the Submitted, Started, and Ended audit messages.
RSLT	Result	The final status result of the task: • SUCS — The task completed successfully. • ABRT — The task was aborted without a rollback error. • ROLF — The task was aborted and was unable to complete the rollback process. • CANC — The task was cancelled by the user before it was started. • EXPR — The task expired before it was started. • IVLD — The task was invalid. • AUTH — The task was unauthorized. • DUPL — The task was rejected as a duplicate.

GTST—Grid Task Started

This audit message indicates that the CMN has started to process the specified grid task. The audit message immediately follows the Grid Task Submitted message for tasks initiated by the internal Grid Task Submission service and selected for automatic activation. For tasks

submitted into the Pending table, this message is generated when the user starts the task.

Table 49: GTST—Grid Task Started Fields

Code	Field	Description
TSID	Task ID	This field uniquely identifies a generated grid task and allows the task to be managed over its lifecycle. **NOTE** The Task ID is assigned at the time that a grid task is generated, not the time that it is submitted. It is possible for a given task to be submitted multiple times, and in this case the Task ID field is not sufficient to uniquely link the Submitted, Started, and Ended audit messages.
RSLT	Result	The result. This field has only one value: • SUCS — The task was started successfully.

GTSU—Grid Task Submitted

This audit message indicates that a grid task has been submitted to the CMN.

Table 50: GTSU—Grid Task Submitted Fields

Code	Field	Description
TSID	Task ID	Uniquely identifies a generated grid task and allows the task to be managed over its lifecycle. **NOTE** The Task ID is assigned at the time that a grid task is generated, not the time that it is submitted. It is possible for a given task to be submitted multiple times, and in this case the Task ID field is not sufficient to uniquely link the Submitted, Started, and Ended audit messages.
TTYP	Task Type	The type of task.
TVER	Task Version	A number indicating the version of the task.
TDSC	Task Description	A human readable description of the task.
VATS	Valid After Timestamp	The earliest time (UINT64 microseconds from January 1, 1970 - Unix time) at which the task is valid.

Table 50: GTSU—Grid Task Submitted Fields (cont.)

Code	Field	Description
VBTS	Valid Before Timestamp	The latest time (UINT64 microseconds from January 1, 1970 - Unix time) at which the task is valid.
TSRC	Source	The source of the task: • TXTB — The task was submitted through the NMS interface as a signed text block • GRID — The task was submitted though the internal Grid Task Submission Service.
ACTV	Activation Type	The type of activation: • AUTO — The task was submitted for automatic activation • PEND — The task was submitted into the pending table. This is the only possibility for the 'TXTB' source.
RSLT	Result	The result of the submission: • SUCS — The task was submitted successfully. • FAIL — The task has been moved directly to the historical table

HDEL—HTTP DELETE Transaction

When an FSG or StorageGRID API client issues a DELETE transaction, a request is made to remove the specified stored content, and this message is issued by the server.

Table 51: HDEL—HTTP DELETE Transaction Fields

Code	Field	Description
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.
OBNS	Object Namespace	The namespace within which the object to be removed resides.
OBPA	Object Path	The path to the object to be removed.
OBNA	Object Name	The name of the object to be removed.
UUID	Content UUID	The Universal Unique IDentifier assigned to the content requested for removal.
OBSP	Security Partition Name	The user-defined name for the security partition assigned to the target object. An empty string is returned if the object is not associated with a security partition.

Table 51: HDEL—HTTP DELETE Transaction Fields (cont.)

Code	Field	Description
SPAR	Security Partition ID	The unique identifier of the security partition assigned to the target object. Zero is returned if the object is not associated with a security partition. SPAR can be used to determine the security partition or FSG replication group to which an object is associated. See "Determine Security Partition or Replication Group ID for an Object" on page 80.
RSLT	Result Code	Result of the DELETE transaction: SUCS — successful ERRS — session closed or lost while the DELETE transaction was being performed CTNF — content to be deleted not found BRQT — malformed DELETE transaction GERR — general error processing content

This audit message indicates the result of a request to delete content. If the specified content exists, it can be identified via the "Content UUID" field (which contains the same value as OBNA, given that deletion occurs in the UUID namespace). If deletion occurs via the FSG, the FMFY message ("FMFY — File Modify" on page 72) can be used to identify the file name. The "Result Code" field can be used to determine when errors occurred. See also "Deletion" on page 34.

Determine Security Partition or Replication Group ID for an Object

Use the security partition ID number listed in the SPAR field to determine the security partition or FSG replication group to which an object is associated. For more information on security partitions, see the *Administrator Guide*.

Procedure

1. Obtain the security partition ID as listed in the SPAR field.

   For example, `[SPAR(UI64):5064106809552273409]`

   NOTE If security partitioning is disabled for the grid, SPAR is zero.

2. Convert the security partition ID to a hexadecimal.

   For example, 5064106809552273409 becomes 0x4647525000000001.

3. Interpret the result of the conversion to a hexadecimal.

   The first eight numbers determine the character code:

   - FGRP (FSG Replication Group) — 0x46475250
   - HTTP (HTTP Security Partition) — 0x48545450

   The remainder of the hexadecimal number is the partition identifier or the FSG replication group.

   For example:

   - 0x4647525000000001 means that FSG replication group 1 is associated with security partition ID 5064106809552273409.
   - 0x485454500000001 means that security partition identifier 1 is associated with the security partition ID 325742710709288961.

4. For objects ingested via an HTTP client go to **Grid Management ▶ HTTP Management ▶ Security Partitions ▶ Overview ▶ Main** and under **Partitions** determine the Partition Identifier associated with the Partition Number as determined in step 3 above.

   — or —

   For objects ingested via an FSG replication group go to **Grid Management ▶ FSG Management ▶ Overview ▶ Main** and under **File System Gateway Groups** determine the FSG Node associated with the FGS Replication Group as determined in step 3 above.

HGEE—HTTP GET Transaction End

When an FSG or StorageGRID API client completes a GET transaction to transfer content from the HTTP server to the FSG or StorageGRID API client, this message is issued.

Table 52: HGEE—HTTP GET Transaction End Fields

Code	Field	Description
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.
OBNS	Object Namespace	The namespace within which the requested object resides.
OBPA	Object Path	The path to the requested object.
OBNA	Object Name	The name of the requested object.
CBID	Content Block Identifier	The unique identifier of the corresponding content block requested. If the CBID is unknown, this field is set to 0.

Table 52: HGEE—HTTP GET Transaction End Fields (cont.)

Code	Field	Description
UUID	Content UUID	The Universal Unique IDentifier corresponding to the requested content. If the UUID is unknown, this field is set to the NULL UUID.
OBSP	Security Partition Name	The user-defined name for the security partition assigned to the target object. An empty string is returned if the object is not associated with a security partition.
SPAR	Security Partition ID	The unique identifier of the security partition assigned to the target object. Zero is returned if the object is not associated with a security partition. SPAR can be used to determine the security partition or FSG replication group to which an object is associated. See "Determine Security Partition or Replication Group ID for an Object" on page 80.
RSLT	Result Code	Result of the GET transaction: SUCS — successful TOUT — timed-out due to inactivity ERRS — session closed or lost while the GET transaction was being performed CTNF — content to be transferred not found or generated (404) error CVRF — content to be transferred failed validation AUTH — transaction terminated due to authorization failure GERR — general error processing content

This audit message means a transfer of content to an FSG or StorageGRID API client completed. It can be monitored to determine the content sent to particular systems. The "Result Code" field can be used to determine when errors occurred.

See also "Retrieval" on page 29.

HGES—HTTP GET Transaction Start

When an FSG or StorageGRID API client initiates a GET transaction to transfer content from the HTTP server to the FSG or StorageGRID API client, this message is issued.

Table 53: HGES—HTTP GET Transaction Start Fields

Code	Field	Description
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.
OBNS	Object Namespace	The namespace within which the requested object resides.
OBPA	Object Path	The path to the requested object.
OBNA	Object Name	The name of the requested object.
CBID	Content Block Identifier	The unique identifier of the corresponding content block requested. If the CBID is unknown, this field is set to 0.
UUID	Content UUID	The Universal Unique IDentifier corresponding to the requested content. If the UUID is unknown, this field is set to the NULL UUID.
RSLT	Result Code	Status at the time the request for the GET transaction was initiated: SUCS — GET transaction successfully initiated BRQT — GET transaction malformed

This audit message means a request for transfer of content to an FSG or StorageGRID API client has been initiated. It can be monitored to determine the content sent to particular systems.

See also "Retrieval" on page 29.

HGMD—HTTP GET Metadata

When a StorageGRID API client initiates a GET transaction to retrieve all predefined and custom metadata for an object, this message is issued.

Table 54: HGMD—HTTP GET Metadata

Code	Field	Description
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.

Table 54: HGMD—HTTP GET Metadata (cont.)

Code	Field	Description
OBNS	Object Namespace	The namespace within which the requested object resides.
OBPA	Object Path	The path to the requested object.
OBNA	Object Name	The name of the requested object.
CBID	Content Block Identifier	The unique identifier of the corresponding content block requested. If the CBID is unknown, this field is set to 0.
UUID	Content UUID	The Universal Unique IDentifier corresponding to the requested content. If the UUID is unknown, this field is set to the NULL UUID.
OBSP	Security Partition Name	The user-defined name for the security partition assigned to the target object. An empty string is returned if the object is not associated with a security partition.
SPAR	Security Partition ID	The unique identifier of the security partition assigned to the target object. Zero is returned if the object is not associated with a security partition. SPAR can be used to determine the security partition or FSG replication group to which an object is associated. See "Determine Security Partition or Replication Group ID for an Object" on page 80.
RSLT	Result Code	Status at the time the request for the GET transaction was initiated: SUCS — successful CTNF — specified content was not found, or generated (404) error ERRS — session closed or lost while the GET transaction was being performed GERR — general error processing content

HHEA—HTTP HEAD Transaction

When an FSG or StorageGRID API client initiates a HEAD transaction to request information about stored content, this message is issued.

Table 55: HHEA—HTTP HEAD Transaction Fields

Code	Field	Description
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.
OBNS	Object Namespace	The namespace within which the requested object resides.

Table 55: HHEA—HTTP HEAD Transaction Fields (cont.)

Code	Field	Description
OBPA	Object Path	The path to the requested object.
OBNA	Object Name	The name of the requested object.
CBID	Content Block Identifier	The unique identifier of the corresponding content block about which information is being requested. If the CBID is unknown, this field is set to 0.
UUID	Content UUID	The Universal Unique IDentifier corresponding to the content about which information is being requested. If the UUID is unknown, this field is set to the NULL UUID.
OBSP	Security Partition Name	The user-defined name for the security partition assigned to the target object. An empty string is returned if the object is not associated with a security partition.
SPAR	Security Partition ID	The unique identifier of the security partition assigned to the target object. Zero is returned if the object is not associated with a security partition. SPAR can be used to determine the HTTP security client or FSG replication group to which an object is associated. See "Determine Security Partition or Replication Group ID for an Object" on page 80.
RSLT	Result Code	Result of the HEAD transaction: SUCS — successful CTNF — specified content was not found, or generated (404) error AUTH — transaction terminated due to authorization failure ERRS — session closed or lost while the HEAD transaction was being performed BRQT — HEAD transaction malformed GERR — general error processing content

This audit message means information about a given piece of content was requested by an FSG or StorageGRID API client. It can be monitored to determine the content inspected by clients. The "Result Code" field can be used to determine when errors occurred.

HOPT—HTTP OPTIONS Transaction

This message is issued when an FSG or StorageGRID API client initiates an OPTIONS transaction to discover which HTTP transactions can be performed on the server.

Table 56: HOPT—HTTP OPTIONS Transaction Fields

Code	Field	Description
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.
OBNS	Object Namespace	The namespace within which the specified object resides.
OBPA	Object Path	The path to the specified object.
OBNA	Object Name	The name of the specified object.
RSLT	Result Code	Result of the OPTIONS transaction: SUCS — successful ERRS — session closed or lost while the OPTIONS transaction was being performed AUTH — transaction terminated due to authorization failure BRQT — OPTIONS transaction malformed GERR — general error processing content

This audit message indicates the result of a request for information about the transactions that can be performed on content. The OPTIONS transaction is typically performed to discover if content can be deleted, created, and so on.

HPMD—HTTP PUT Metadata

When a StorageGRID API client initiates a PUT transaction to add or update the custom metadata of an existing object, this message is issued.

Table 57: HPMD—HTTP PUT Metadata

Code	Field	Description
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.
OBNS	Object Namespace	The namespace within which the requested object resides.
OBPA	Object Path	The path to the requested object.

Table 57: HPMD—HTTP PUT Metadata (cont.)

Code	Field	Description
OBNA	Object Name	The name of the requested object.
UUID	Content UUID	The Universal Unique IDentifier corresponding to the requested content. If the UUID is unknown, this field is set to the NULL UUID.
OBSP	Security Partition Name	The user-defined name for the security partition assigned to the target object. An empty string is returned if the object is not associated with a security partition.
SPAR	Security Partition ID	The unique identifier of the security partition assigned to the target object. Zero is returned if the object is not associated with a security partition. SPAR can be used to determine the HTTP security partition or FSG replication group to which an object is associated. See "Determine Security Partition or Replication Group ID for an Object" on page 80.
RSLT	Result Code	Status at the time the request for the PUT transaction was initiated: SUCS — successful CTNF — specified content was not found, or generated (404) error ERRS — session closed or lost while the PUT transaction was being performed BRQT — PUT transaction malformed GERR — general error processing content FNOP — permission to modify metadata denied because the request includes read-only metadata

HPOE—HTTP POST Transaction End

When a POST transaction initiated by a StorageGRID API client to query available content completes, this message is issued.

Table 58: HPOE—HTTP POST Transaction End Fields

Code	Field	Description
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.
OBNS	Object Namespace	The namespace within which the query is performed.
RSFD	Results Found	The number of found objects matching the query.

Table 58: HPOE—HTTP POST Transaction End Fields (cont.)

Code	Field	Description
RSLT	Result Code	Result of the POST query operation: SUCS — successful TOUT — timed-out due to inactivity ERRS — session closed or lost while the POST transaction was being performed CMLF — malformed query parameters received from client AUTH — transaction terminated due to authorization failure BRQT — invalid POST query (bad request) GERR — general error processing content

This audit message means a StorageGRID API client has initiated and completed queries about the grid or about objects stored in the grid, or has submitted user-supplied audit messages. If the query cannot be started (HPOS fails), then no HPOE message is generated. HPOE can be monitored to determine the content being queried. The "Result Code" field can be used to determine when errors occurred.

The time between the "HTTP POST Transaction Start" and "HTTP POST Transaction End" audit messages tells you how long particular query operations are taking to complete.

HPOS—HTTP POST Transaction Start

When a POST transaction is initiated by a StorageGRID API client to query available content, this message is issued.

Table 59: HPOS—HTTP POST Transaction Start Fields

Code	Field	Description
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.
OBNS	Object Namespace	The namespace within which the query is performed.
RSLT	Result Code	Status at the time the request for the POST transaction was initiated: SUCS — POST transaction initiated successfully BRQT — failure (bad request, usually malformed POST transaction)

This audit message means a StorageGRID API client initiated a query about the grid or about objects stored in the grid, or has submitted a user-supplied audit message. It can be monitored to determine the content being queried or the audit message submitted.

The time between the "HTTP POST Transaction Start" and "HTTP POST Transaction End" audit messages tells you how long particular query operations are taking to complete.

HPUE—HTTP PUT Transaction End

When an FSG or StorageGRID API client completes a PUT transaction to transfer content from the FSG or StorageGRID API client to the HTTP server (the node), this message is issued.

Table 60: HPUE—HTTP PUT Transaction End Fields

Code	Field	Description
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.
OBNS	Object Namespace	The namespace within which the stored object was handled.
OBPA	Object Path	The path used to store the object.
OBNA	Object Name	The name of the stored object.
CBID	Content Block Identifier	The identifier of the corresponding content block for the successfully-stored content. If the store operation was not successful, this field is set to 0.
UUID	Content UUID	The Universal Unique IDentifier assigned to the successfully stored content. If the UUID was not specified, or the store operation failed, this field is set to the NULL UUID.
CSIZ	Content Size	The size of the original content stored, in bytes.
OBSP	Security Partition Name	The user-defined name for the security partition assigned to the target object. An empty string is returned if the object is not associated with a security partition.
SPAR	Security Partition ID	The unique identifier of the security partition assigned to the target object. Zero is returned if the object is not associated with a security partition. SPAR can be used to determine the HTTP security partition or FSG replication group to which an object is associated. See "Determine Security Partition or Replication Group ID for an Object" on page 80.
BSIZ	Object Size	The size of the managed fixed content object (after compression and encryption), in bytes.

Table 60: HPUE—HTTP PUT Transaction End Fields (cont.)

Code	Field	Description
ACBI	Associated CBID	The identifier of the Associated content block (if applicable). This will be non-zero if the ingested object was split into two content blocks in order to support de-duplication. Associated objects are referenced through their UUID, and this UUID may be re-pointed by the CMS to a different CBID after the content has been ingested.
AUUI	Associated UUID	The identifier of the Associated content block (if applicable). This contains a value if the ingested object was split into two content blocks in order to support de-duplication. Otherwise this field is set to the NULL UUID.
RSLT	Result Code	The result of the PUT transaction: SUCS — successful TOUT — timed-out due to inactivity ERRS — session closed or lost while the PUT transaction was being performed CMLF — malformed content received from the client STER — storing the content failed AUTH — transaction terminated due to authorization failure CANC — cancelled by client GERR — general error processing content

This audit message means a transfer of content from an FSG or StorageGRID API client completed. If content was successfully stored, the CBID and/or UUID fields identify it.

This audit message can be monitored to determine the content sent to particular systems. The "Result Code" field can be used to determine when errors occurred.

See also "Ingest" on page 23.

HPUS—HTTP PUT Transaction Start

When an FSG or StorageGRID API client initiates a PUT transaction to transfer content from the FSG or StorageGRID API client to the HTTP server (the node), this message is issued.

Table 61: HPUS—HTTP PUT Transaction Start Fields

Code	Field	Description
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.
OBNS	Object Namespace	The namespace within which the stored object should be handled.
OBPA	Object Path	The path to use when storing the object.
OBNA	Object Name	The name of the object to store.
RSLT	Result Code	The status at the time the request for the PUT transaction was initiated: SUCS — PUT transaction initiated successfully BRQT — malformed PUT transaction

This audit message means a transfer of content from an FSG or StorageGRID API client has initiated. It can be monitored to determine the content stored using HTTP.

See also "Ingest" on page 23.

HTSC—HTTP Session Close

When an FSG, StorageGRID API, or CDMI client finishes communicating with a remote host and closes the previously-established HTTP session, this message is issued.

Table 62: HTSC—HTTP Session Close Fields

Code	Field	Description
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.

Table 62: HTSC—HTTP Session Close Fields (cont.)

Code	Field	Description
RSLT	Result Code	Why the session was closed: SUCS — session closed normally, without errors TOUT — timed-out by the node, due to inactivity ERRC — lost the connection over which the session was established ERRT — session terminated due to an error occurring on a transaction AUTH — session terminated due to a failed transaction authorization GERR — a general error occurred, causing the session to close

This audit message means an FSG or StorageGRID API client closed a previously-established HTTP session. "HTTP Session Close" always corresponds with a previously-issued "HTTP Session Establish" message.

This message should be monitored to determine if there are any repetitive or excessive problems in attempting to establish a session. This could indicate potential communications or interoperability problems related to FSG or StorageGRID API client or server implementations.

HTSE—HTTP Session Establish

When an FSG, StorageGRID API, CDMI client establishes an HTTP session, this message is issued.

Table 63: HTSE—HTTP Session Establish Fields

Code	Field	Description
CNID	Connection Identifier	The unique identifier for the connection over which the HTTP session was established.
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.
OBCL	Client Name	The user-defined security partition client name assigned to the client certificate. An empty string is returned if the client has not been defined.
RSLT	Result Code	Status at the time the session was established: SUCS — session successfully established.

IPMS — IP Mismatch

The ADE generates this audit message whenever a session is accepted from a peer that has an unexpected IP address.

Table 64: IPMS—IP Mismatch

Code	Field	Description
RSLT	Result	This field has the value 'NONE'
NOID	Node ID	The node ID of the peer node.
IADR	IP Address	The actual IP address from which the node is connecting.
EXIP	Expected IP Address	The expected IP address for this node.

It is normal for this audit message to be generated when servers are added to a grid (including when the grid is first installed) or when a server is moved to a di61fferent IP address. If this message is seen outside the context of such a maintenance procedure, it should be investigated as a potential security breach.

LRMP—Re-Map LDR Content

This message indicates that a Re-Map LDR Content grid action was processed by the sending CMS. The message specifies the old location and the new location of objects moved by the Storage Node hardware refresh process.

Table 65: LRMP—Re-Map LDR Content Fields

Code	Field	Description
SNID	Source LDR	The node ID of the original LDR.
DNID	Destination LDR	The node ID of the new LDR for objects previously stored on the original LDR.
RSLT	Result	This field has the value 'SUCS'. RSLT is a mandatory message field but is not relevant for this particular message.

OHRP—Object Handle Repoint

This message is generated when the content handle of an object (UUID) is updated to reference a different object (CBID).

When the CMS service determines that two objects ingested into the grid are identical, it repoints the content handle (UUID) of one of them so that both content handles refer to the same object (CBID). The CMS service repoints content handles as part of the GE Optimized Store (deduplication) feature

NOTE Deduplication and the GE Optimized Store are deprecated and no longer supported.

Table 66: OHRP—Object Handle Repoint Fields

Code	Field	Description
RCHN	Repointed Content Handle	The content handle (UUID) of the object that was pointed to another CBID.
OCBI	Original CBID	The CBID that the content handle pointed to originally.
RCBI	Repointed CBID	The CBID that the content handle points to after the operation is complete.
RSLT	Result	This field has the value 'SUCS'. RSLT is a mandatory message field but is not relevant for this particular message.

When a content handle is updated to point to a different CBID, the original CBID will no longer have any content handles pointing to it. Depending on the retention rules for the grid, the CBID may be deleted from the system.

OLST—Object Lost

This message is generated when the CMS service detects that an object is missing from the grid. This happens when the CMS service finds that all of the recorded locations for the object specified by the ILM rules no longer exist. The CMS service learns that a location no longer exists in a number of ways:

- A range of CBIDs for a specific Storage Node or Archive Node is indicated as being lost, either via a grid-task or directly from the console of the node.
- A Storage Node or Archive Node, on being told by the CMS service that it should already have a particular object stored, finds that it does not actually have the object stored, causing a notification to the CMS.
- A Storage Node detects that an object is corrupt, causing a notification to the CMS service.

- Using CMS-driven foreground verification, a CMS service discovers that a location that was supposed to exist on a Storage Node does not.

Table 67: OLST—Object Lost Fields

Code	Field	Description
CBID	Content Block Identifier	The CBID of the lost object.
RSLT	Result	This field has the value 'NONE'. RSLT is a mandatory message field but is not relevant for this particular message. The use of 'NONE' rather than 'SUCS' is so that this message will not be filtered

OMDU—Object Metadata Updated

This message is generated by the owner CMS after processing a metadata update for an ingested object.

Table 68: OMDU—Object Metadata Updated

Code	Field	Description
CBID	Content Block Identifier	The unique identifier of the corresponding content block requested. If the CBID is unknown, this field is set to 0.
UUID	Content UUID	The Universal Unique IDentifier corresponding to the requested content. If the UUID is unknown, this field is set to the NULL UUID.
RSLT	Result Code	Status at the time the request for the transaction was completed: SUCS — successful FNOP — permission to modify metadata denied because the request includes read-only metadata

ORLM—Object Rules Met

This message is generated when the ILM rules for the object have been achieved for the current epoch, that is, the object is stored where specified by the ILM rules.

Table 69: ORLM—Object Rules Met Fields

Code	Field	Description
CBID	Content Block Identifier	The CBID of the object.
RULE	Rules Label	The human-readable label given to the ILM rule that applied to this object.
FGRP	Replication Group	The FSG replication group identifier of the FSG on which the operation occurred. The value for FGRP is 0 if the file was not ingested through an FSG.
FPTH	File Path	The complete path to and name of the object at the time of original ingest (for example, if the file is renamed, object metadata is not updated and FPTH in ORLM does not reflect the updated file name). The value for FGRP is "" if the file was not ingested through an FSG.
FSIZ	File size	Indicates the size of the file in bytes.
UUID	Associated UUID	The identifier of the file content within the grid. The value for UUID is "" if the object does not have a UUID, content handle has been released
SPAR	Security Partition ID	The unique identifier of the security partition assigned to the target object. Zero is returned if the object is not associated with an HTTP security partition. SPAR can be used to determine the HTTP security partition or FSG replication group to which an object is associated. See "Determine Security Partition or Replication Group ID for an Object" on page 80.
LOCS	Locations	The content locations of objects within the grid. The value for LOCS is "" if the object has no locations (for example, it has been purged).
STAT	Status	The status of ILM operation DONE—The object has dropped permanently out of the replication system. DFER—The object has been marked for future ILM re-evaluation. PRGD—The object has been purged entirely from the grid. NLOC—The object was purged from the grid without the CMS being involved. This typically happens when ingest fails.

Table 69: ORLM—Object Rules Met Fields (cont.)

Code	Field	Description
RSLT	Result	The result of the ILM operation. SUCS—The ILM operation was successful.

The ORLM audit message can be issued a number of times for a single object. For instance, it is issued whenever one of the following events take place:

- the ILM for the object is satisfied forever
- the ILM for the object is satisfied for this epoch
- the ILM has completely purged the content
- the owner CMS service has transferred ownership of the object to another CMS service and the new owner CMS service re-evaluates the content
- a copy of the object was found to be corrupt by the LDR background verification and the owner CMS re-evaluates the content

See also "Ingest" on page 23 and "Deletion" on page 34.

REND—Restoration End

This message indicates that an entity has completed the process of restoring private structured data from the grid.

Table 70: RSTE—Restoration End Fields

Code	Field	Description
RSSE	Restoration Source Entity	The type of entity performing the restoration. Typically a Node Type field, such as BCMS or BFSG. This must match the entity specified for the matching Restoration Begin.
RENE	Entries Restored	The number of entries/objects for the entity restored in the operation that has completed.
UUID	Restoration UUID	The UUID that the restoration data was retrieved from.
RSLT	Restoration result	The completion status of the restoration: SUCS—The restoration operation completed successfully. ABRT—The restoration operation was aborted. FAIL—The restoration operation failed.

This audit message is used to determine when an entity on the grid completes a restoration operation. This could include the NMS, CMS, FSG and other entities. See also "RSTA — Restoration Begin" on page 100.

RPSB—Replication Session Begin

This message is generated when a service begins a replication session (replicating private structured data to a secondary service).

Table 71: RPSB — Replication Session Begin Fields

Code	Field	Description
RPSI	Replication Session ID	The unique identifier of the replication session being started.
RPPI	Previous Session ID	The identifier of the previous replication session (if one exists); zero otherwise.
RPSE	Replication Source Entity	The node ID of the service that is generating the replication session.
RPDE	Replication Destination Entity	The node ID of the service that is accepting the replication session.
RPSC	Start Sequence Count	The replication sequence count of FSG transactions at which the session starts or resumes.
RSSS	Session Start Reason	The status of the replication session: NEWS — A new session is being established. CONT — A new session is being established that continues after a previous session. RSUM — A previous session is being resumed.
RSLT	Operation Result	The result of the replication operation: SUCS — The replication session started successfully.

This message indicates a replication session is either starting or being resumed. It identifies the primary (originating) and secondary (accepting) services by their node IDs. Both the source and destination services report this message.

RPSE—Replication Session End

This message is generated when a service completes a replication session.

Table 72: RPSE—Replication Session End Fields

Code	Field	Description
RPSI	Replication Session ID	The unique identifier of the replication session that has ended.
RPPI	Next Session ID	The identifier of the next replication session (if known). If the next session ID is not known, this value is zero (0).
RPSE	Replication Source Entity	The node ID of the service that is generating the replication session.
RPDE	Replication Destination Entity	The node ID of the service that is accepting the replication session.
RPSC	End Sequence Count	The replication sequence count of FSG transactions that would be the next value (in a resumed session).
RSSS	Session End Reason	The completion status of the replication session: SUCS — The replication session was closed successfully. UNEX — The session was closed unexpectedly. PAUS — The session was paused (the FSG was shut down). CKPT — The session was stopped for a checkpoint such as a backup. A new session handles remaining replication.
RSLT	Session Result	The result of the replication session: SUCS — The replication session completed successfully. FAIL — The replication session did not complete successfully.

Matching this message with the corresponding RPSB message can indicate the time it took to perform the replication. This message indicates whether the replication session closed normally. Both the source and destination services report this message.

RSTA—Restoration Begin

This message indicates that an entity is starting the process of restoring private structured data from the grid.

Table 73: RSTA—Restoration Begin Fields

Code	Field	Description
RSSE	Restoration Source Entity	The type of entity performing the restoration. This is typically a Node Type field, such as BCMS or BFSG.
UUID	Restoration UUID	The UUID that the restoration data was retrieved from.
RSLT	Result	The status at the time the restoration began: SUCS—The restoration started successfully.

This audit message is used to determine when an entity on the grid starts a restoration operation. This could include the NMS, CMS, FSG and other entities. See also "REND—Restoration End" on page 97.

SADD—Security Audit Disable

This message indicates the originating service (node ID) has turned off audit message logging; audit messages are no longer being collected or delivered.

Table 74: SADD—Security Audit Disable Fields

Code	Field	Description
AETM	Enable Method	The method used to disable the audit.
AEUN	User Name	The user name that executed the command to disable audit logging.
RSLT	Result	This field has the value 'NONE'. RSLT is a mandatory message field but is not relevant for this particular message. The use of 'NONE' rather than 'SUCS' is so that this message will not be filtered

The message implies that logging was previously enabled, but has now been disabled. This is typically only used during bulk ingest to improve system performance. Following the bulk activity, auditing is restored (SADE) and the capability to disable auditing is then permanently blocked.

SADE—Security Audit Enable

This message indicates that the originating service (node ID) has restored audit message logging; audit messages are again being collected and delivered.

Table 75: SADE—Security Audit Enable Fields

Code	Field	Description
AETM	Enable Method	The method used to enable the audit.
AEUN	User Name	The user name that executed the command to enable audit logging.
RSLT	Result	This field has the value 'NONE'. RSLT is a mandatory message field but is not relevant for this particular message. The use of 'NONE' rather than 'SUCS' is so that this message will not be filtered

The message implies that logging was previously disabled (SADD) but has now been restored. This is typically only used during bulk ingest to improve system performance. Following the bulk activity, auditing is restored and the capability to disable auditing is then permanently blocked.

SCMT—Object Store Commit

Grid content is not made available or recognized as being stored until it has been committed — meaning it has been stored persistently. Persistently-stored content has been completely written to disk, and has passed related integrity checks. When a content block is committed to storage, this message is issued.

Table 76: SCMT—Object Store Commit Fields

Code	Field	Description
CBID	Content Block Identifier	The unique identifier of the content block committed to permanent storage.
RSLT	Result Code	Status at the time the object was stored to disk: SUCS — object successfully stored

This message means a given content block has been completely stored and verified, and can now be requested. It can be used to track data flow within the system.

SREM—Object Store Remove

This message is issued when grid content is removed from persistent storage and is no longer accessible through regular grid APIs. The content may still exist on the server for a period of time, for example in a "garbage" directory.

Table 77: SREM—Object Store Remove Fields

Code	Field	Description
CBID	Content Block Identifier	The unique identifier of the content block deleted from permanent storage.
RSLT	Result Code	Indicates the result of the content removal operations. Currently defined values are: SUCS — content removed from persistent storage

This audit message means a given content block has been deleted from a node and can no longer be requested directly. The message can be used to track the flow of deleted content within the system.

SVRF—Object Store Verify Fail

This message is issued whenever a content block fails the verification process.

Each time content is read from or written to disk, several verification and integrity checks are performed to ensure the data sent to the requesting user is identical to the data originally ingested into the system. If any of these checks fail, the system automatically quarantines the corrupt data to prevent it from being retrieved again.

Table 78: SVRF—Object Store Verify Fail Fields

Code	Field	Description
CBID	Content Block Identifier	The unique identifier of the content block which failed verification.

Table 78: SVRF—Object Store Verify Fail Fields (cont.)

Code	Field	Description
RSLT	Result Code	Verification failure type: CRCF — cyclic redundancy check (CRC) failed HMAC — hash-based message authentication code (HMAC) check failed EHSH — unexpected encrypted content hash PHSH — unexpected original content hash SEQC — incorrect data sequence on disk PERR — invalid structure of disk file DERR — disk error

NOTE This message should be monitored closely. Content verification failures can indicate attempts to tamper with content or impending hardware failures.

To determine what operation triggered the message, look at the value of the AMID (Module ID) field. For example, the value of SVFY indicates that the message was generated by the Storage Verifier module, that is, background verification, and the value STOR indicates that the message was triggered by content retrieval.

SVRU—Object Store Verify Unknown

The LDR storage component continuously scans all files in the object store to schedule content verification. If it detects a file or directory does not match expected naming conventions, it moves the unexpected file(s) to the quarantine directory, where they can be manually removed.

When an unknown or unexpected file is detected in the object store and moved to the quarantine directory, this message is issued.

Table 79: SVRU—Object Store Verify Unknown Fields

Code	Field	Description
FPTH	File Path	The full path to the unexpected file's original location.

Table 79: SVRU—Object Store Verify Unknown Fields (cont.)

Code	Field	Description
RSLT	Result	This field has the value 'NONE'. RSLT is a mandatory message field but is not relevant for this particular message. The use of 'NONE' rather than 'SUCS' is so that this message will not be filtered

NOTE The "SVRU - Object Store Verify Unknown" audit message should be monitored closely. It means unexpected files were detected in the object store. This situation should be investigated immediately to determine how the files were created, as it can indicate attempts to tamper with content or impending hardware failures.

SYSD—Node Stop

When a StorageGRID grid service is stopped gracefully, this message is generated to indicate the shutdown was requested. Typically this message is sent only after a subsequent restart as the audit message queue is not cleared prior to shutdown. Look for the SYST message, sent at the beginning of the shutdown sequence, if the service has not restarted.

Table 80: SYSD—Node Stop Fields

Code	Field	Description
RSLT	Clean Shutdown	The nature of the shutdown: SUCS—System was cleanly shutdown.

The message does not indicate if the host server is being stopped, only the reporting service. The RSLT of a SYSD cannot indicate a "dirty" shutdown, as the message is only generated by "clean" shutdowns.

SYST—Node Stopping

When a StorageGRID grid service is stopped gracefully, this message is generated to indicate the shutdown was requested and that the grid service has initiated its shutdown sequence. SYST can be used to determine if the shutdown was requested, before the service is restarted (unlike SYSD, which is typically sent after the service restarts.)

Table 81: SYST—Node Stopping Fields

Code	Field	Description
RSLT	Clean Shutdown	The nature of the shutdown: SUCS — System was cleanly shutdown.

The message does not indicate if the host server is being stopped, only the reporting service. The RSLT of a SYST cannot indicate a "dirty" shutdown, as the message is only generated by "clean" shutdowns.

SYSU—Node Start

When a StorageGRID grid service is restarted, this message is generated to indicate if the previous shutdown was clean (commanded) or disorderly (unexpected).

Table 82: SYSU—Node Start Fields

Code	Field	Description
RSLT	Clean Shutdown	The nature of the shutdown: SUCS — System was cleanly shut down. DSDN — System was not cleanly shut down. VRGN — System was started for the first time after server installation (or re-installation)

The message does not indicate if the host server was started, only the reporting service.

This message can be used to:

- Detect discontinuity in the audit trail.
- Determine if a service is failing during operation (as the distributed nature of the grid can mask these failures). The Server Manager restarts a failed service automatically.