HP Medical Archive solution

Software version: 8.1.0

audit message reference

Document release date: May 2010
Software release date: November 2009

Legal notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted rights legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Licensing

The use of HP products is governed by the terms and conditions of the applicable End User License Agreement (EULA).

Copyright notices

Trademark notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Microsoft, Windows, Windows NT, and Windows XP are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Contents

Intended audience 5
Prerequisites 5
Related documentation 5
Document conventions and symbols 6
Documentation updates 7
Subscription service 7
Support 7

1 Audit Message Overview 9
Overview of Auditing 9
Audit Log File Access 13
Audit Log Space Allocation 14

2 File and Message Format 15
Audit Log File Format 15
Audit Message Format 16

3 Message Reference 21
System Audit Messages 21
Object Storage Audit Messages 23
HTTP Protocol Audit Messages 24
DICOM Audit Messages 25
File System Gateway Audit Messages 26
External Audit Messages 27
Messages for Object Ingest, Retrieve, Modify, and Delete 28
Audit Message Reference 29

About this document

The Audit Management System (AMS) service stores audit messages of grid activity and events to a set of text log files. To enable you to read and analyze the audit trail, this document provides information on the structure and content of the text file log.

The objectives of this document are to:

- Describe how to access the current log file and archived logs
- Describe the text file format
- Provide a reference for common audit messages

Intended audience

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

Prerequisites

You are assumed to have a sound understanding of the nature of audited activities within the HP MAS system. To use the text log file, you are assumed to have access to the configured audit share on the Admin Node server hosting the AMS service.

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.

Related documentation

In addition to this guide, please refer to other documents for this product:

- *HP Medical Archive solution Release Notes* for 8.1.1
- *HP Medical Archive solution user guide*
- *HP Medical Archive solution DICOM Integration Guide*
- *HP Medical Archive solution Siemens Integration Guide*

- *HP Medical Archive solution DICOM Conformance Statement*
- *HP Medical Archive solution IHE Integration Statement*

These and other HP documents can be found on the HP documents web site:

http://www.hp.com/support/

Document conventions and symbols

Convention	Element
Medium blue text: Figure 1 http://www.hp.com	• Cross-reference links • E-mail addresses • Web site addresses
Bold	• Key names or key sequence • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes • Text typed into a GUI element, such as into a box
Italics	• Document titles • Text emphasis • You must supply a value for a variable in a GUI element.
`Monospace`	• File and directory names • Text displayed on the screen, such as system output and application messages • Command or reserved keyword in a CLI, API, program language, or operating system • Script or code example
`Italic monospace`	You must supply a value on the command line.
`Bold monospace`	• Text typed at the command line • Emphasis of file and directory names, system output, and code

NOTE Provides additional information.

RECOMMENDATION Provides guidance from HP for a best practice or for optimum performance.

△ CAUTION Caution messages appear before procedures which, if not observed, could result in loss of data or damage to equipment.

Documentation updates

The title page of this document contains the following identifying information:

- Software version number

  Indicates the software version.

- Document release date

  Changes each time the document is updated.

- Software release date

  Indicates the release date of this version of the software.

Subscription service

HP strongly recommends that customers sign up online using the Subscriber's choice web site:

http://www.hp.com/go/e-updates

- Subscribing to this service provides you with e-mail updates on the latest product enhancements, newest versions of drivers, and firmware documentation updates as well as instant access to numerous other product resources.
- After signing up, you can quickly locate your products under Product Category.

Support

You can visit the HP Software Support web site at:

http://www.hp.com/go/hpsoftwaresupport

HP Software Support Online provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts

- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

For more information about HP Passport, go to:

http://h20229.www2.hp.com/passport-registration.html

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)), 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 8 used in the HP MAS system release 8.1.

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.

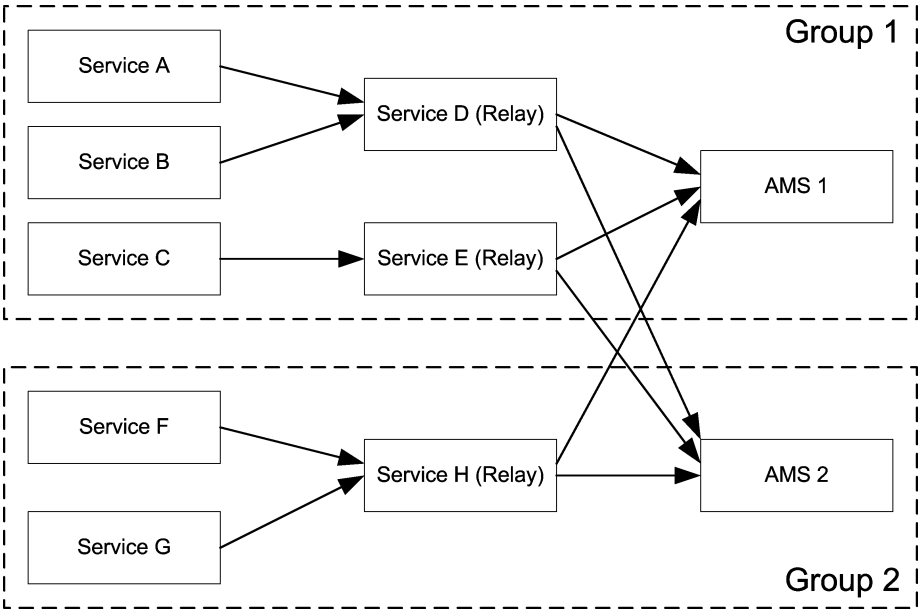

Figure 1 Audit Message Flow

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

Message Retention

After 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.

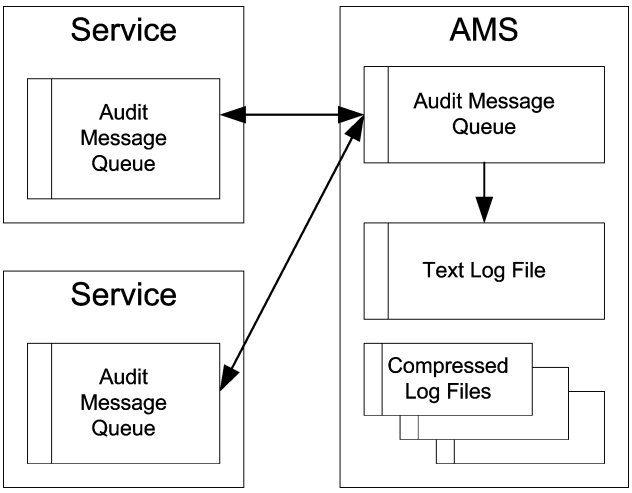

Figure 2 Audit Message Retention

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. The local message buffer at the audit relay service (ADC) and the AMS service each have an alarm (AMQS) associated with it, in the event the backlog becomes unusually large. 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. Audit logs are compressed when they are seven days old and are renamed `YYYY-MM-DD.txt.gz` (where the original date is preserved).

Over very long periods of time, this can result in the consumption of the storage available for audit logs on the server hosting the AMS service. After the audit directory on the AMS service is full, the oldest log files in the directory are automatically deleted until the directory contains less than its allocated storage. Depending upon the regulatory or administrative requirements of your enterprise, you may want 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 (page 18).

Message Level Filtering

The AMS service filters incoming audit messages based on settings made in Grid Management > Grid Configuration > Audit.

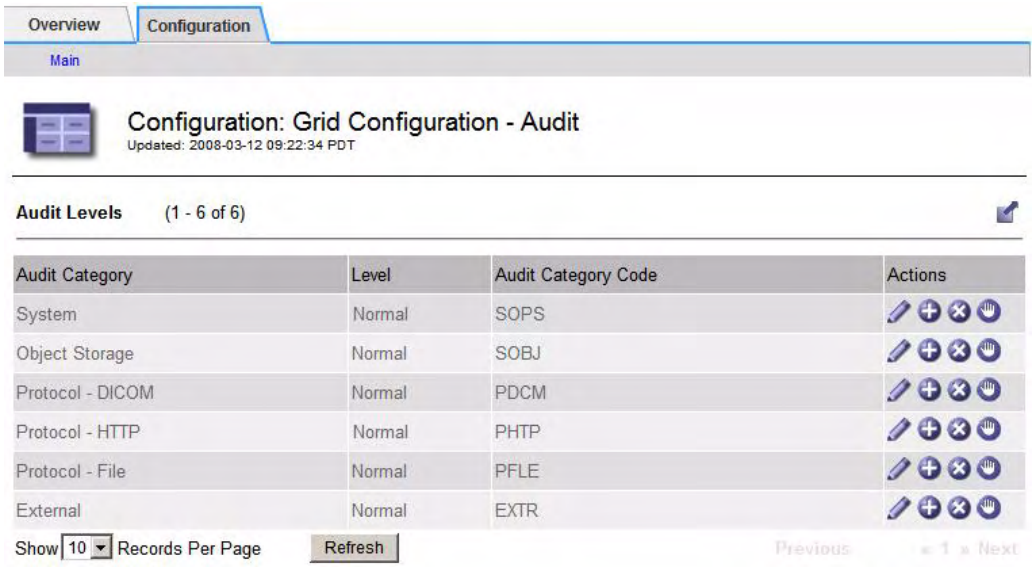

Figure 3 Default Audit Settings

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 Chapter 3, Message Reference for tables that sort the audit messages into the categories System Messages, Object Storage Messages, DICOM 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 HP MAS HTTP API.

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

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 an NFS or CIFS 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 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). That means that if you have one login authentication to access the managed file system of a secondary FSG service on a combined Admin/Gateway Node, and a different login to access the Audit Log on the same combined Admin/Gateway Node, you may not be able to have *both* file shares connected at the same time. You may be required to disconnect the secondary FSG share before you can connect to the Audit Log, and vice versa.

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.

After seven days, these archived log files are compressed, 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.

To access a 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. HP recommends "`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
- 50 GB for mysql database if it is required
- 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 this 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>
```

The script that manages audit log allocation reads the configuration information from the XML file. In order to meet specific customer requirements, you can configure the amount of space allocated to audit logs by editing the file `var-local-allocation.xml`. 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-DDTHH:MM:SS.UUUUUU where UUUUUU are microseconds), followed by a space.
- the audit message itself, enclosed within square brackets "[]" and beginning 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][UUID(CSTR):"FF09AF73-42
9D-4CEA-853B-30239279FE2A"][RSLT(FC32):SUCS][AVER(UI32):8]
[ATIM(UI64):1213920860692397][ATYP(FC32):FSWO][ANID(UI32):20946829][AMID(FC32):FSG
C][ATID(UI64):9502147098565145229][ASQN(UI64):2938511][ASES(UI64):1213829438271695
]]
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(UI
64):595448][UUID(CSTR):"25843BA6-ABFD-4257-A57F-1F5D57165490"][RSLT(FC32):SUCS][AV
ER(UI32):8][ATIM(UI64):1213920860710712][ATYP(FC32):FSTG][ANID(UI32):20946829][AMI
D(FC32):INGS][ATID(UI64):11495554162678525067][ASQN(UI64):2938512][ASES(UI64):1213
829438271695]]
2008-06-20T00:14:20.718929 [AUDT:[FPTH(CSTR):"/fsg/BM_Loadtesting_1/
CT_2400_1_f95788a8e6ffa4e932188541a1fb39d1/0/
3b6fdae2a429a68eb42c9212256caf95_1460"][FSIZ(UI64):532480][UUID(CSTR):"86E91656-47
88-4874-8F26-34F8ED7DAA0C"][RSLT(FC32):SUCS][AVER(UI32):8]
[ATIM(UI64):1213920860718929][ATYP(FC32):FSWO][ANID(UI32):20946829][AMID(FC32):FSG
C][ATID(UI64):2951277210434284714][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][U
UID(CSTR):"FF09AF73-429D-4CEA-853B-30239279FE2A"][RSLT(FC32)
:SUCS]
[AVER(UI32):8][ATIM(UI64):1213920860692397][ATYP(FC32):FSWO]
[ANID(UI32):20946829][AMID(FC32):FSGC][ATID(UI64):9502147098
565145229][ASQN(UI64):2938511][ASES(UI64):1213829438271695]]
```

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 3, 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 (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 (page 18).

Data Types

The data types encountered in the audit messages are:

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”.
IP32	Used for some IP addresses.[a]
CSTR	A string; a variable length array of UTF-8 characters. 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 \\ For more information on characters that may be escaped, contact HP Support.

a. The data type for IP addresses is either CSTR or IP32 depending on the audit message.

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 bolded in this sample message:

```
2008-06-20T00:14:20.424035 [AUDT:[HSID(UI64):1027401556]
[OBNS(CSTR):"UUID"][OBPA(CSTR):"/"]
[OBNA(CSTR):"DDE25220-7049-403D-8B71-B9D884A00864"][CBID(UI6
4):0x210C9CFC55EACDC6]
[UUID(CSTR):"DDE25220-7049-403D-8B71-B9D884A00864"]
[RSLT(FC32):SUCS][AVER(UI32):8][ATIM(UI64):1213920860424035]
[ATYP(FC32):HHEA][ANID(UI32):12885257][AMID(FC32):HTGM][ATID
(UI64):9771581922913861059][ASQN(UI64):7374859]
[ASES(UI64):1213662052895969]]
```

The event that these attributes describe is identified using the ATYP element described in Common Elements (page 18). The attributes for each event are described in Chapter 3, 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 HP MAS 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.
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 HP MAS 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):8][ATIM(UI64):1213920860718929]
[ATYP(FC32):FSWO][ANID(UI32):20946829][AMID(FC32):FSGC][ATID
(UI64):2951277210434284714][ASQN(UI64):2938513][ASES(UI64):1
213829438271695]]
```

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 (bolded in this example):

```
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):8][ATIM(UI64):1213920860718929]
[ATYP(FC32):FSWO][ANID(UI32):20946829][AMID(FC32):FSGC][ATID
(UI64):2951277210434284714][ASQN(UI64):2938513][ASES(UI64):1
213829438271695]]
```

The value of this attribute is FSWO. See Chapter 3, Message Reference 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 (page 57) 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):8][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 timestamp 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 (page 18)):

```
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):8][ATIM(UI64):1213920860718929]
[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 Message Reference

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 (page 11).

The audit messages are also listed alphabetically by their four-character codes (starting on Audit Message Reference (page 29)). 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 this sample message:

```
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):7][ATIM(UI64):1213920860718929]
[ATYP(FC32):FSWO][ANID(UI32):20946829][AMID(FC32):FSGC][ATID(UI64):2951277210
434284714][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 4 System Audit Messages

Code	Description	See
BKSB	Backup Store Begin—A service has begun a backup operation.	page 32
BKSE	Backup Store End—A service has completed a backup operation.	page 32
ETAF	Security Authentication Failed—A connection attempt using Transport Layer Security (TLS) has failed.	page 49
ETCA	TCP/IP Connection Establish—An incoming or outgoing TCP/IP connection was successfully established.	page 50
ETCC	TCP/IP Connection Close—An established connection has been closed by either side of the connection (normally or abnormally).	page 51
ETCF	TCP/IP Connection Fail—An outgoing connection attempt failed at the lowest level, due to communication problems.	page 52
ETCR	TCP/IP Connection Refused—An incoming TCP/IP connection attempt was not allowed.	page 53
GNRG	GNDS Registration—A service has updated or registered information about itself in the grid.	page 58
GNUR	GNDS Unregistration—A service has unregistered information about itself from the grid.	page 58
GTED	Grid Task Ended—The CMN service has finished processing the grid task.	page 59
GTST	Grid Task Started—The CMN service has started to process the grid task.	page 60
GTSU	Grid Task Submitted—A grid task has been submitted to the CMN service.	page 60
IPMS	IP Mismatch—A session is accepted from a peer that has an unexpected IP address.	page 71
REND	Restoration End—An entity has completed the process of restoring private structured data from the grid	page 74
RPSB	Replication Session Begin—A service has begun a replication session to a secondary service.	page 74
RPSE	Replication Session End—A service has completed a replication session to a secondary service.	page 75
RSTA	Restoration Begin—An entity is starting the process of restoring private structured data from the grid	page 76
SADD	Security Audit Disable—Audit message logging has been turned off.	page 76
SADE	Security Audit Enable—Audit message logging has been turned on.	page 77
SYSD	Node Stop—The HP MAS grid service has been gracefully stopped.	page 77
SYST	Node Stopping—The HP MAS grid service has initiated a graceful stop.	page 80
SYSU	Node Start—The HP MAS grid service started; the nature of the previous shutdown is indicated in the message.	page 80

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 5 Object Storage Audit Messages

Code	Description	See
ARCB	Archive Object Retrieve Begin—The ARC service begins the retrieval of an object from archive media.	page 29
ARCE	Archive Object Retrieve End—The object has been retrieved from archive media, and the ARC service reports the status of the retrieval operation.	page 29
AREM	Archive Object Remove—A content block was successfully or unsuccessfully purged from a Tape Node.	page 30
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.	page 30
ATCE	Archive Object Store Begin—Storing a content block to archive media has started.	page 31
CBSB	Object Send Begin—The source entity initiated a node-to-node data transfer operation on a single piece of content.	page 35
CBSE	Object Send End—The source entity completed a node-to-node data transfer operation.	page 36
CBRB	Object Receive Begin—The destination entity initiated a node-to-node data transfer operation on a single piece of content.	page 33
CBRE	Object Receive End—The destination entity completed a node-to-node data transfer operation.	page 34
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.	page 37
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.	page 72
OHRP	Object Handle Repoint—Indicates that the object referenced by an object handle was changed.	page 72
OLST	Object Lost—A specific object was found to be missing from the grid by the CMS service that manages the object.	page 72
ORLM	Object Rules Met—The object is stored where specified by the ILM rules.	page 73
SCMT	Object Store Commit—A content block was completely stored and verified, and can now be requested.	page 77

Table 5 Object Storage Audit Messages

Code	Description	See
SREM	Object Store Remove—A content block was deleted from a node, and can no longer be requested directly.	page 78
SVRF	Object Store Verify Fail—A content block failed verification checks.	page 78
SVRU	Object Store Verify Unknown—Unexpected file(s) detected in the object store.	page 79

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/breakdown
- Object storage
- Retrieval
- Query

Table 6 HTTP Protocol Audit Messages

Code	Description	See
HCPE	HTTP PUT C–STORE End—A PUT transaction for a DICOM object was completed.	page 61
HCPS	HTTP PUT C–STORE Start—A PUT transaction for a DICOM object was initiated.	page 62
HDEL	HTTP DELETE Transaction—Logs the result of a request to delete content.	page 63
HGEE	HTTP GET Transaction End—A GET transaction to transfer content to an HTTP client completed.	page 64
HGES	HTTP GET Transaction Start—A request for a GET transaction to transfer content to an HTTP client was initiated.	page 65
HHEA	HTTP HEAD Transaction—Information about a piece of content was requested by an HTTP client.	page 65
HOPT	HTTP OPTIONS Transaction—Logs the result of a request for information about the transactions that can be performed on content.	page 66
HPOE	HTTP POST Transaction End—An HTTP client completed a query for stored content.	page 67
HPOS	HTTP POST Transaction Start—An HTTP client initiated a query for stored content.	page 68
HPUE	HTTP PUT Transaction End—A PUT transaction to transfer content from an HTTP client completed.	page 68

Table 6 HTTP Protocol Audit Messages

Code	Description	See
HPUS	HTTP PUT Transaction Start—A PUT transaction to transfer content from an HTTP client was initiated.	page 70
HTSC	HTTP Session Close—An HTTP client closed a previously-established HTTP session.	page 70
HTSE	HTTP Session Establish—A remote host successfully established an HTTP session to the node.	page 71

DICOM Audit Messages

The Protocol – DICOM audit messages log activity related to interactions with external systems using the DICOM protocol. These include:

- Association establishment
- C–STORE
- C–FIND
- C–MOVE
- N–ACTION (storage commitment)

Table 7 DICOM Audit Messages

Code	Description	See
CDAD	DICOM Study Add—A new study (not previously recorded by the CMS) or a new instance (image) has been added to a known study.	page 37
DASC	DICOM Association Close—An established DICOM association with a remote host closed.	page 38
DASE	DICOM Association Establish—A successful inbound or outbound DICOM association was established with a remote host.	page 38
DASF	DICOM Association Fail—An association attempt failed (remote host cannot process the DICOM protocol, or the request was rejected).	page 39
DCFE	DICOM C–FIND End—A remote DICOM host completed a query for DICOM-related content.	page 40
DCFS	DICOM C–FIND Start—A remote DICOM host initiated a query for DICOM-related content.	page 41
DCME	DICOM C–MOVE End—A remote DICOM host completed a transfer of DICOM instances to a remote Application Entity.	page 42
DCMS	DICOM C–MOVE Start—A remote DICOM host initiated a transfer of DICOM instances to a remote Application Entity.	page 43

Table 7 DICOM Audit Messages

Code	Description	See
DCMT	DICOM Storage Commitment—A remote DICOM host initiated an operation to check if content was previously stored.	page 43
DCPE	DICOM C–STORE End—A transfer of content between hosts over a DICOM association has completed.	page 44
DCPS	DICOM C–STORE Start—A transfer of content between hosts over a DICOM association has started.	page 45
DCSF	DICOM C–STORE Fail—A transfer of content between hosts over a DICOM association has failed.	page 47

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 8 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.	page 46
DDEL	Directory Delete—Indicates that an existing directory has been deleted on the volume shared by the FSG.	page 48
DRNM	Directory Rename—Indicates that an existing directory has been renamed on the volume shared by the FSG.	page 48
FCRE	File Create—Logs the addition of new files (not directories) to the FSG.	page 54
FDEL	File Delete—Logs deletion of a file from the FSG directory tree (not from the grid).	page 54
FMFY	File Modify—Logs ingested files that have been released from the FSG (modified or deleted).	page 55
FRNM	File Rename—Logs changes to the name or path of an existing file.	page 55
FSTG	File Store to Grid—Logs the storage of content from the FSG local cache to the grid.	page 56
FSWI	File Swap In—Logs the retrieval of a file from the grid to the FSG local cache.	page 57
FSWO	File Swap Out—Logs the deletion of a file from the FSG local cache (but not from the directory tree or grid).	page 57

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 HP MAS HTTP 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.

Messages for Object Ingest, Retrieve, Modify, and Delete

This section lists the audit messages that are generated as objects are ingested, retrieved, modified, or deleted through a FSG.

Table 9 Audit Messages for Object Ingest, Retrieve, Modify, and Delete

Scenario	Message
File is created	FCRE
File is modified before it has been ingested into the grid	No audit message generated
File is deleted before it has been ingested into the grid	FDEL
File is ingested into the grid	HPUS HPUE FSTG
File that has been ingested into the grid is modified	FMFY for the original object UUID HDEL for the original object HPUS HPUE for the new object FSTG for the new object UUID
File that has been ingested into the grid is deleted	FMFY FDEL HDEL
File is moved	FRNM
CHRI (Content Handle Release Inhibit) is enabled and file that has been ingested into the grid is modified	FMFY for the original object UUID HPUS HPUE for the new object FSTG for the new object UUID
CHRI is enabled and file that has been ingested into the grid is deleted	FMFY FDEL
Content that is cached is retrieved	No audit message generated
Content that is not cached is retrieved	HGES HGEE FSWI

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 10 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. After content has been retrieved and verified, it is delivered to the requesting service.

Table 11 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 a Tape Node. If the result is successful, the Tape 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 12 AREM—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.
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 13 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 13 ASCE—Archive Object Store End Fields *(continued)*

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 Tape 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 14 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.
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 15 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 16 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 17 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.
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 18 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.
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 19 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 20 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.

CDAD — DICOM Study Add

When a new DICOM study ID is ingested, or when new images are added to an existing study, this logs the addition.

Table 21 CDAD—DICOM Study Add Fields

Code	Field	Description
STDY	Study Instance UID	The unique DICOM study identifier.
SIMC	Number of Images	The number of instances (images) in the study.
RSLT	Result	Indicates the result of the operation that added the study or image and notified the CMS of the addition. Current values are: SUCS—operation was successful

This audit message appears for each new study instance (image) that is added to the grid. As a new study appears, the message indicates the new study is now known to the grid. As images are added to the study, the message appears with the new count of images.

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 22 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.

DASC — DICOM Association Close

When an established DICOM association with a remote host is closed, this message is issued.

Table 23 DASC—DICOM Association Close Fields

Code	Field	Description
ASID	Association Identifier	The unique identifier assigned to the DICOM association.
RSLT	Closing State	Indicates how the association closed: SUCS—closed normally without errors TOUT—timed-out by the node due to inactivity ERRC—lost connection ABRT—aborted COMP—suitable presentation context could not be negotiated GERR—general data processing error

This audit message means the DICOM association specified by the Association Identifier is no longer established. The DASC message always corresponds with a previous DASE (Association Establish) message. DASC should be monitored to determine if there are excessive problems during attempts to establish an association. Problems could indicate communications or interoperability issues related to DICOM implementation.

DASE — DICOM Association Establish

When a DICOM association is established between a node and a host, this message is issued.

Table 24 DASE—DICOM Association Establish Fields

Code	Field	Description
CNID	Connection Identifier	The unique identifier assigned to the connection over which the DICOM association was established.
ASID	Association Identifier	The unique identifier assigned to the DICOM association.
DIDR	Association Direction	Indicates whether the association was opened by the grid node or by a remote host: INBO—initiated by a remote host connecting to the grid node OUTB—initiated by the grid node connecting to a remote host

Table 24 DASE—DICOM Association Establish Fields *(continued)*

Code	Field	Description
RMAE	External Application Entity	The Application Entity Title of the remote device.
GRAE	Grid Application Entity	The Application Entity Title of the grid.
RSLT	Result	Indicates the result of opening the association. Currently defined values are: SUCS—association was opened successfully

This audit message means a successful inbound or outbound DICOM association was established with a remote host. It can be used to track hosts communicating with the system via DICOM.

The Grid Application Entity field allows identification of related configuration and coerce tag profiles, if applicable. The Association Identifier can be used to trace the progress of a single transaction, such as a C-MOVE or a C-FIND, from initiation to completion.

DASF—DICOM Association Fail

When an attempt by a DICOM service to establish an association fails, this message is issued. This can occur if the remote host cannot process the DICOM protocol, or when either side of the communication rejects the association request.

Table 25 DASF—DICOM Association Fail Fields

Code	Field	Description
CNID	Connection Identifier	The unique identifier assigned to the connection over which the DICOM association was established.
DIDR	Association Direction	Indicates whether the association was opened by the grid node or by a remote host: INBO—initiated by a remote host connecting to the grid node OUT—initiated by the grid node connecting to a remote host

Table 25 DASF—DICOM Association Fail Fields *(continued)*

Code	Field	Description
RMAE	External Application Entity	The Application Entity Title of the remote device (if unknown, this field contains a null string).
GRAE	Grid Application Entity	The Application Entity Title of the grid.
RSLT	Failure Code	Reason for the failure: ERRC—connection closed by remote host before an association could be established ABRT—aborted TOUT—timeout period expired REJT—association rejected PERM—calling AE Title denied permission to connect CONF—unexpected AE Title for called entity COMP—suitable presentation context could not be negotiated GERR—unknown data received from remote host

This audit message should be monitored to determine if there are repetitive or excessive problems during attempts to establish an association. Problems could indicate communications or interoperability issues related to DICOM implementation, or incorrectly configured external DICOM devices.

The result codes for PERM and CONF depend on whether the association is inbound (INBO) or outbound (OUTBO). For example, if the association is inbound, the calling AE is the remote host, and PERM refers to the AE title of the remote host. If the association is outbound, the grid is the calling AE, and PERM refers to the AE title of the grid.

The Grid Application Entity field allows identification of related configuration and coerce tag profiles, if applicable.

DCFE — DICOM C–FIND End

When a DICOM association completes a C–FIND operation to query available content, this message is issued.

Table 26 DCFE—DICOM C–FIND End Fields

Code	Field	Description
ASID	Association Identifier	The unique identifier assigned to the DICOM association.
DIDR	C–FIND Direction	Indicates whether the C–FIND was initiated by the grid node or by a remote host: INBO—initiated by a remote host
ROOT	DICOM Query Root	The query root specified in the C–FIND.

Table 26 DCFE—DICOM C–FIND End Fields *(continued)*

Code	Field	Description
LEVL	DICOM Query Level	The query level specified in the C–FIND.
RSFD	Results Found	The number of DICOM objects found matching the query.
RSLT	Result Code	The result of the C–FIND operation: SUCS—successful CANC—cancelled by the Service Class User GERR—general error processing the C–FIND command

This audit message means a remote DICOM host initiated and completed a query for DICOM-related content. It can be monitored to determine the content being queried. The “Result Code” field can be used to determine when errors occur.

The time interval between the C–FIND Start and C–FIND End audit messages tells you how long the related C–FIND operations are taking to complete.

DCFS — DICOM C–FIND Start

When a DICOM association initiates a C–FIND operation to query available content, this message is issued.

Table 27 DCFS – DICOM C–FIND Start Fields

Code	Field	Description
ASID	Association Identifier	The unique identifier assigned to the DICOM association.
DIDR	C–FIND Direction	Indicates whether the C–FIND was initiated by the grid node or by a remote host: INBO—initiated by a remote host
ROOT	DICOM Query Root	The query root specified in the C–FIND.
LEVL	DICOM Query Level	The query level specified in the C–FIND.
RSLT	Result	Indicates the result of starting the C-FIND operation. Currently defined values are: SUCS—C-FIND was started successfully.

This audit message means a remote DICOM host initiated a query for DICOM-related content. It can be monitored to determine the content being queried.

The time interval between the C–FIND Start and C–FIND End audit messages tells you how long the related C–FIND operations are taking to complete.

DCME — DICOM C–MOVE End

When a DICOM association completes a C–MOVE operation to query and retrieve found content over a second association, this message is issued.

Table 28 DCME—DICOM C–MOVE End Fields

Code	Field	Description
ASID	Association Identifier	The unique identifier assigned to the DICOM association.
DIDR	C–MOVE Direction	Indicates whether the C–MOVE was initiated by the grid node or by a remote host: INBO—initiated by a remote host
ROOT	DICOM Query Root	The query root specified in the C–MOVE.
LEVL	DICOM Query Level	The query level specified in the C–MOVE.
SAET	Source Application Entity (AE) Title	The source AE-Title for the C–MOVE operation.
DAET	Destination AE-Title	The destination AE-Title for the C–MOVE operation.
RSFD	Results Found	The number of DICOM objects retrieved matching the query.
RSLT	Result Code	The result of the C–MOVE operation: SUCS—successful CANC—cancelled by the Service Class User GERR—general error processing the C–MOVE command

This audit message means a remote DICOM host initiated and completed a C–MOVE operation to transfer DICOM content. It can be monitored to determine the content being queried/transferred. The “Result Code” field can be used to determine when errors occur.

The time interval between the C–MOVE Start and C–MOVE End audit messages tells you how long the related C–MOVE operations are taking to complete.

DCMS — DICOM C–MOVE Start

When a DICOM association initiates a C–MOVE operation to query and transfer DICOM content over a second association, this message is issued.

Table 29 DCMS—DICOM C–MOVE Start Fields

Code	Field	Description
ASID	Association Identifier	The unique identifier assigned to the DICOM association.
DIDR	C–MOVE Direction	Indicates whether the C–MOVE was initiated by the grid node or by a remote host: INBO—initiated by a remote host
ROOT	DICOM Query Root	The query root specified in the C–MOVE.
LEVL	DICOM Query Level	The query level specified in the C–MOVE.
SAET	Source Application Entity (AE) Title	The source AE-Title for the C–MOVE operation.
DAET	Destination AE-Title	The destination AE-Title for the C–MOVE operation.
RSLT	Result	Indicates the result of starting the C-MOVE operation. Currently defined values are: SUCS—successful.

This audit message means a remote DICOM host initiated a C–MOVE operation to transfer DICOM instances to a remote Application Entity.

The time interval between the C–MOVE Start and C–MOVE End audit messages tells you how long the related C–MOVE operations are taking to complete.

DCMT — DICOM Storage Commitment

When a DICOM association initiates a Storage Commitment operation to determine if content has been successfully received and stored, this message is issued.

Table 30 DCMT—DICOM Storage Commitment Fields

Code	Field	Description
ASID	Association Identifier	The unique identifier assigned to the DICOM association.
DIDR	Storage Commitment Direction	Indicates whether the Storage Commit operation was initiated by the grid node or by a remote host: INBO—initiated by a remote host
ISTR	Items Requested	The number of items requested for storage verification.

Table 30 DCMT—DICOM Storage Commitment Fields *(continued)*

Code	Field	Description
ISTS	Items Stored	The number of items requested for verification which have been successfully stored.
ISTN	Items not Stored	The number of items requested for verification which have *not* been successfully stored.
RSLT	Result Code	Result of the Storage Commitment operation: SUCS—successful GERR—an error occurred during Storage Commitment processing

This audit message means that a Storage Commitment operation was initiated (usually by a remote DICOM host) to check whether content has been previously stored. It can be used to discover situations where a discrepancy exists between content storage requests and what was in fact successfully stored.

DCPE — DICOM C–STORE End

When a DICOM association completes a C–STORE operation to transfer content from one host to another, this message is issued.

Table 31 DCPE—DICOM C–STORE End Fields

Code	Field	Description
ASID	Association Identifier	The unique identifier assigned to the DICOM association.
DIDR	C–STORE Direction	Indicates whether the C–STORE was initiated by the grid node or by a remote host: INBO—initiated by a remote host OUTB—initiated by the node
STUG	Study Instance UID	The Study Identifier of the data being transferred.
SERG	Series Instance UID	The Series Identifier of the data being transferred.
IMGG	SOP Instance UID	The Image Identifier of the data being transferred.
STCL	SOP Class	The SOP Class of the instance.
STTX	Transfer Syntax	The Transfer Syntax of the instance.
CBID	Content Block Identifier	The identifier of the content block being transferred.

Table 31 DCPE—DICOM C–STORE End Fields *(continued)*

Code	Field	Description
CSIZ	Content Size	The size of the original content stored, in bytes.
BSIZ	Object Size	The size of the managed fixed content object (after compression and encryption) in bytes.
RSLT	Result Code	The result of the C–STORE operation: SUCS—successful CANC—cancelled CBNM—CBID associated with the image did not contain metadata, or had invalid metadata in the CMS CSDI—extraction error while processing incoming C-STORE transaction data TOUT—timed-out due to inactivity COMP—presentation contexts not accepted ERRC—lost connection ERFH—failure message sent by remote application entity CTNF—content to be transferred was not found CVRF—content to be transferred failed verification GERR—general error processing content

This audit message means a transfer of content between hosts over a DICOM association completed. The message can be monitored to determine the content sent to particular systems. The “Result Code” field can be used to determine when errors occurred.

DCPS — DICOM C–STORE Start

When a DICOM association initiates a C–STORE operation to transfer content from one host to another, this message is issued.

Table 32 DCPS—DICOM C–STORE Start Fields

Code	Field	Description
ASID	Association Identifier	The unique identifier assigned to the DICOM association.
DIDR	C–STORE Direction	Indicates whether the C–STORE was initiated by the grid node or by a remote host: INBO—initiated by a remote host OUTB—initiated by the node
STUG	Study Instance UID	The Study Identifier of the data being transferred.
SERG	Series Instance UID	The Series Identifier of the data being transferred.
IMGG	SOP Instance UID	The Image Identifier of the data being transferred.

Table 32 DCPS—DICOM C–STORE Start Fields *(continued)*

Code	Field	Description
STCL	SOP Class	The SOP Class of the instance.
STTX	Transfer Syntax	The Transfer Syntax of the instance.
CBID	Content Block Identifier	The identifier of the content block being transferred.
RSLT	Result	Indicates the result of starting the C-STORE operation. Currently defined values are: SUCS—C-STORE started successfully.

This audit message means a transfer of content between hosts over a DICOM association has started. The message can be monitored to determine the content sent to particular systems.

DCRE — Directory Create

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

Table 33 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.

DCSF — DICOM C–STORE Fail

When an association to perform a requested C–STORE cannot be established, or the information required to establish an association to perform a C–STORE cannot be located, the C–STORE operation cannot be initiated, and this message is issued.

Table 34 DCSF—DICOM C–STORE Fail Fields

Code	Field	Description
SVIP	Destination Service Port	The destination port for the C–STORE operation. If unknown, this field is omitted from the audit message output.
DAIP	Destination IP Address	The destination IP address for the C–STORE operation. If unknown, this field is omitted from the audit message output.
RMAE	External Application Entity (AE)	The AE-Title of the destination device. If unknown, this field is omitted from the audit message output.
DIDR	C–STORE Direction	Indicates whether the C–STORE was initiated by the grid node or by a remote host: OUTB—initiated by the node
STUG	Study Instance UID	The Study Identifier of the data being transferred. If unknown, this field is omitted from the audit message output.
SERG	Series Instance UID	The Series Identifier of the data being transferred. If unknown, this field is omitted from the audit message output.
IMGG	SOP Instance UID	The Image Identifier of the data being transferred. If unknown, this field is omitted from the audit message output.
STCL	SOP Class	The SOP Class of the instance. If unknown, this field is omitted from the audit message output.
CBID	Content Block Identifier	The identifier of the content block being transferred.
RSLT	Result Code	Why the C–STORE was unable to complete: CBLK—the CBID associated with the image could not be referenced ASOF—an association could not be established for the C-STORE request.

This audit message means a transfer of content between hosts over a DICOM association failed. This can be symptomatic of network problems, or indicate attempts to send data to systems that do not support the image SOP Class.

If the attempt could be initiated but the transfer failed, a DCSF message is not generated. Instead, there is a DCPS (DCPS—DICOM C–STORE Start (page 45)) and DCPE (DCPE—DICOM C–STORE End (page 44)) pair of messages which indicate the start and end of the transfer, with result codes that identify the cause of the failure.

The audit message does not include the ASID field which uniquely identifies the DICOM association of the transaction. To trace the entire transaction, the DCSF (DICOM C-STORE Fail) message can be linked to the corresponding DCMS/DCME (DICOM C-MOVE Start/End) message using the ATID (trace ID) field. DCMS/DCME can in turn can be linked to the associated DASE (DICOM Association Open) message using the ASID (association ID) field, which in turn can be linked to the correct ETCA (Connection Establish) message using the CNID (connection ID) field

DDEL — Directory Delete

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

Table 35 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 36 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 37 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 38 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: • DING: DICOM Ingest Service • DCLN: DICOM Query/Retrieve Service • 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 (DICOM, HTTP etc.).

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 39 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 40 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: • DING: DICOM Ingest Service • DCLN: DICOM Query/Retrieve Service • 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.

When a remote client needs to communicate with a service running on a node, it attempts to create a connection to that node. If the node refuses the 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 41 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: • DING: DICOM Ingest Service • DCLN: DICOM Query/Retrieve Service • 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 42 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 Messages for Object Ingest, Retrieve, Modify, and Delete (page 28).

FDEL — File Delete

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

Table 43 FDEL—File Delete Fields

Code	Field	Description
FPTH	File Path	The complete path and name of the file that has been deleted.
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 Messages for Object Ingest, Retrieve, Modify, and Delete (page 28).

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 44 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.
RSLT	Result	Indicates the result of modifying the file. Currently defined values are: SUCS — file modified successfully

The FMFY audit message is generated regardless of the CHRI content protection setting.

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 Messages for Object Ingest, Retrieve, Modify, and Delete (page 28).

FRNM — File Rename

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

Table 45 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.

See also Messages for Object Ingest, Retrieve, Modify, and Delete (page 28).

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 46 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.
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 Messages for Object Ingest, Retrieve, Modify, and Delete (page 28).

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 47 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.
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.

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.

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 48 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 49 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 (for example, 32-dicom).
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 50 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 51 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. 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 52 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 53 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.
VBTS	Valid Before Timestamp	The latest time (UINT64 microseconds from January 1, 1970 - Unix time) at which the task is valid.

Table 53 GTSU—Grid Task Submitted Fields *(continued)*

Code	Field	Description
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

HCPE — HTTP PUT C–STORE End

An object can be stored into the /DICOM namespace over an established HTTP session by initiating a PUT transaction to process and store the content as a DICOM object in the grid. When DICOM object storage has completed, this message is issued.

Table 54 HCPE—HTTP PUT C–STORE End Fields

Code	Field	Description
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.
STUG	Study Instance UID	The Study Identifier of the data being stored.
SERG	Series Instance UID	The Series Identifier of the data being stored.
IMGG	SOP Instance UID	The Image Identifier of the data being stored.
STCL	SOP Class	The SOP Class of the instance.
STTX	Transfer Syntax	The Transfer Syntax of the instance.
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.

Table 54 HCPE—HTTP PUT C–STORE End Fields *(continued)*

Code	Field	Description
CSIZ	Content Size	The size of the original content stored, in bytes.
BSIZ	Object Size	The size of the managed fixed content object (after compression and encryption), in bytes.
RSLT	Result Code	The result of the DICOM Store operation: SUCS—successful TOUT—timed-out due to inactivity ERRS—session closed or lost while the PUT transaction was being performed CVRF—content to be transferred failed verification GERR—general error processing content

This audit message means a transfer of content between hosts over an HTTP session completed. This message is generated prior to, and in addition to, the "HTTP PUT Transaction End" audit message.

HCPS — HTTP PUT C–STORE Start

An object can be stored into the /DICOM namespace over an established HTTP session by initiating a PUT transaction to process and store the content as a DICOM object in the grid. When DICOM object storage has been initiated, this message is issued.

Table 55 HCPS—HTTP PUT C–STORE Start Fields

Code	Field	Description
HSID	Session Identifier	The unique identifier assigned to the HTTP session established to the node.
STUG	Study Instance UID	The Study Identifier of the data being stored.
SERG	Series Instance UID	The Series Identifier of the data being stored.
IMGG	SOP Instance UID	The Image Identifier of the data being stored.
STCL	SOP Class	The SOP Class of the instance.
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.
STTX	Transfer Syntax	The Transfer Syntax of the instance
RSLT	Result Code	Status at the time the PUT operation was initiated: SUCS—C–STORE transaction successfully initiated

This audit message means a transfer of content between hosts over an HTTP session has been initiated. This message is generated after, and in addition to, the "HTTP PUT Transaction Start" audit message.

HDEL — HTTP DELETE Transaction

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

Table 56 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 HTTP Security Partition assigned to the target object. An empty string is returned if the object is not associated with a HTTP Security Partition.
SPAR	Security Partition ID	The unique identifier of the HTTP Security Partition assigned to the target object. Zero is returned if the object is not associated with a HTTP Security Partition.
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 (page 55)) can be used to identify the file name. The "Result Code" field can be used to determine when errors occurred.

See also Messages for Object Ingest, Retrieve, Modify, and Delete (page 28).

HGEE — HTTP GET Transaction End

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

Table 57 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.
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 HTTP Security Partition assigned to the target object. An empty string is returned if the object is not associated with a HTTP Security Partition.
SPAR	Security Partition ID	The unique identifier of the HTTP Security Partition assigned to the target object. Zero is returned if the object is not associated with a HTTP Security Partition.
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 HTTP 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.

HGES — HTTP GET Transaction Start

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

Table 58 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 HTTP client has been initiated. It can be monitored to determine the content sent to particular systems.

HHEA — HTTP HEAD Transaction

When an HTTP client initiates a HEAD transaction to request information about stored content, this message is issued.

Table 59 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.
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.

Table 59 HHEA—HTTP HEAD Transaction Fields *(continued)*

Code	Field	Description
OBSP	Security Partition Name	The user-defined name for the HTTP Security Partition assigned to the target object. An empty string is returned if the object is not associated with a HTTP Security Partition.
SPAR	Security Partition ID	The unique identifier of the HTTP Security Partition assigned to the target object. Zero is returned if the object is not associated with a HTTP Security Partition.
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 HTTP 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 HTTP client initiates an OPTIONS transaction to discover which HTTP transactions can be performed on the server.

Table 60 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.

HPOE — HTTP POST Transaction End

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

Table 61 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.
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 an HTTP 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 an HTTP client to query available content, this message is issued.

Table 62 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 an HTTP 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 HTTP client completes a PUT transaction to transfer content from the HTTP client to the HTTP server (the node), this message is issued.

Table 63 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 HTTP Security Partition assigned to the target object. An empty string is returned if the object is not associated with a HTTP Security Partition.

Table 63 HPUE—HTTP PUT Transaction End Fields *(continued)*

Code	Field	Description
SPAR	Security Partition ID	The unique identifier of the HTTP Security Partition assigned to the target object. Zero is returned if the object is not associated with a HTTP Security Partition.
BSIZ	Object Size	The size of the managed fixed content object (after compression and encryption), in bytes.
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 HTTP 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 Messages for Object Ingest, Retrieve, Modify, and Delete (page 28).

HPUS — HTTP PUT Transaction Start

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

Table 64 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 HTTP client has initiated. It can be monitored to determine the content stored using HTTP.

See also Messages for Object Ingest, Retrieve, Modify, and Delete (page 28).

HTSC — HTTP Session Close

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

Table 65 HTSC—HTTP Session Close Fields

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

HTSE—HTTP Session Establish

When an HTTP client establishes an HTTP session, this message is issued.

Table 66 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 HTTP 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 67 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 different 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 68 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.

Table 69 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 Tape Node is indicated as being lost, either via a grid-task or directly from the console of the node.

- A Storage Node or Tape 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 70 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

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 71 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.
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.
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 these 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

REND — Restoration End

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

Table 72 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 (page 76).

RPSB — Replication Session Begin

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

Table 73 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.

Table 73 RPSB — Replication Session Begin Fields *(continued)*

Code	Field	Description
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 74 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 75 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 (page 74).

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 76 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 77 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 78 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 79 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

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.

When a content block fails the verification process, this message is issued.

Table 80 SVRF—Object Store Verify Fail Fields

Code	Field	Description
CBID	Content Block Identifier	The unique identifier of the content block which failed verification.
RSLT	Result Code	Verification failure type: CRCF—content CRC checks failed HMAC—content HMAC checks 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 The “SVRF - Object Store Verify Fail” audit message should be monitored closely. It means a given content block failed verification checks, which can indicate attempts to tamper with content or impending hardware failures.

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 81 SVRU—Object Store Verify Unknown Fields

Code	Field	Description
FPTH	File Path	The full path to the unexpected file's original location.
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 an HP MAS 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 82 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 an HP MAS 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 83 SYST—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 SYST cannot indicate a “dirty” shutdown, as the message is only generated by “clean” shutdowns.

SYSU — Node Start

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

Table 84 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.