

NetCache™ 5.4

Guide to Messages and Log File Entries

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089 USA
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: <http://www.netapp.com>

Part number 215-00272
December 2002

Copyright and trademark information

Copyright information

Copyright © 1994–2003 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

Portions copyright © 1998–2001 The OpenSSL Project. All rights reserved.

No part of this book covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Portions of this product are derived from the Berkeley Net2 release and the 4.4-Lite-2 release, which are copyrighted and publicly distributed by The Regents of the University of California.

Copyright © 1980–1995 The Regents of the University of California. All rights reserved.

Portions of this product are derived from NetBSD, which is copyrighted by Carnegie Mellon University.

Copyright © 1994, 1995 Carnegie Mellon University. All rights reserved. Author Chris G. Demetriou.

Permission to use, copy, modify, and distribute this software and its documentation is hereby granted, provided that both the copyright notice and its permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

CARNEGIE MELLON ALLOWS FREE USE OF THIS SOFTWARE IN ITS “AS IS” CONDITION. CARNEGIE MELLON DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

Software derived from copyrighted material of The Regents of the University of California and Carnegie Mellon University is subject to the following license and disclaimer:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notices, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS

INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of the software were created by Netscape Communications Corp.

The contents of those portions are subject to the Netscape Public License Version 1.0 (the "License"); you may not use those portions except in compliance with the License. You may obtain a copy of the License at <http://www.mozilla.org/NPL/>.

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is Mozilla Communicator client code, released March 31, 1998.

The Initial Developer of the Original Code is Netscape Communications Corp. Portions created by Netscape are Copyright © 1998 Netscape Communications Corp. All rights reserved.

Software derived from copyrighted material of Network Appliance, Inc. is subject to the following license and disclaimer:

Network Appliance reserves the right to change any products described herein at any time, and without notice. Network Appliance assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Network Appliance. The use and purchase of this product do not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Network Appliance.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp and the Network Appliance design are registered trademarks of Network Appliance, Inc. in the United States, Canada, and the European Union. Network Appliance is a registered trademark of Network Appliance, Inc. in Monaco and a trademark of Network Appliance, Inc. in the United States and Canada. FAServer is a registered trademark of Network Appliance, Inc. in the United States and the European Union. NetCache is a registered trademark of Network Appliance, Inc. in the European Union and Japan, and a trademark of Network Appliance, Inc. in the United States. SnapCopy is a registered trademark of Network Appliance, Inc. in the European Union and a trademark of Network Appliance, Inc. in the United States. WAFL is a registered trademark of Network Appliance, Inc. in the United States, the European Union, and Canada. FilerView, SecureShare, SnapManager, SnapMirror and SnapRestore are registered trademarks of Network Appliance, Inc. in the United States. Data ONTAP is a trademark of Network Appliance, Inc. in the United States and Canada. Snapshot is a trademark of Network Appliance, Inc. in the United States and the European Union. NetApp—the Network Appliance Company is a registered trademark of Network Appliance, Inc. in the United States and other countries. ApplianceWatch, BareMetal, Center-to-Edge, ContentDirector, DataFabric, MultiStore, NearStore, SecureAdmin, Serving Data by Design, Smart SAN, SnapCache, SnapDrive, SnapVault, Vfiler, and Web Filer are trademarks of Network Appliance, Inc. in the United States.

Apple is a registered trademark and QuickTime is a trademark of Apple Computer, Inc. in the United States and/or other countries.

Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries.

RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

Network Appliance is a licensee of the CompactFlash and CF Logo trademarks.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

Network Appliance NetCache is certified RealSystem compatible.

Table of Contents

	Preface	.ix
Chapter 1	Web access log	1
	About the Web access log	2
	Web access log headers.	4
	Order of headers in predefined formats in the Web access log.	14
	How data is displayed in the cs-username field	16
	x-transaction header entries in the Web access log.	17
	About logging HTTP headers received by the appliance.	20
	x-hiercode header entries	21
	WebWasher DynaBLocator codes	22
	SmartFilter transaction codes.	25
Chapter 2	x-note Header Entries in the Web access log	27
	x-note entries—explanation and actions	28
Chapter 3	Web Accelerator Logs.	51
	About Web server acceleration logs	52
Chapter 4	FTP transfer access log	53
	FTP transfer access log headers	54
Chapter 5	Streaming logs	57
	About the Streaming access log	59
	Streaming access log headers.	61
	sc-status header codes in the Streaming access log.	65
	About the Streaming details log	67
	Streaming details log headers.	68

	x-transaction codes in the Streaming details log	72
	x-action header codes (Streaming logs)	76
	x-action header values for pushed content	80
Chapter 6	x-status Header Entries (Streaming access log)	83
	About MMS and RTSP errors in the x-status header.	84
Chapter 7	NNTP access log	103
	About the NNTP access log	104
	NNTP access log headers.	105
	NNTP transaction codes	108
	x-error-msg header entries in the NNTP access log	109
Chapter 8	Messages log	115
	About the Messages log	116
	Subsystem (facility) information in the Messages log	118
	Severity levels in the Messages log.	120
Chapter 9	ICAP log	123
	About the ICAP 1.0 log.	124
	ICAP 1.0 log headers	125
Chapter 10	GRM logs	127
	About the GRM server access log	128
	GRM server access log headers	130
	About the GRM server details log	132
	GRM server details log headers	133
Chapter 11	DNS log.	137
	About the DNS log	138

	DNS log headers	139
Chapter 12	ContentDirector log	141
	About the ContentDirector log	142
Chapter 13	Confill Messages	143
	About CONFILL messages.	144
	CONFILL messages—explanations and actions	145
Chapter 14	CMS Log	153
	About the CMS log	154
	CMS log headers	155
	Index	157

Preface

About the Guide to Messages and Log File Entries

This guide provides information for the following supported NetCache platforms: C1100, C1105, C1200, C2100, C3100, and C6100. This guide describes the default and custom headers that can appear in the various NetCache appliance logs and the data that can appear in the header fields.

Use the information in this guide to

- ◆ Plan the headers that you need to include in your log files
This guide contains a topic that defines each header that is available for default, predefined, and custom logs (for example, a topic called Web access log headers). The information in this guide can help you determine how to configure your logs in the Appliance Manager. Use the Appliance Manager online Help for configuration details.
- ◆ Analyze your log files
You can view all log files in the Appliance Manager. Select Data tab > Log Files > Log File Name.

About the error messages described in this guide

This guide includes detailed descriptions of the error messages that can appear in specific headers in the following logs:

Log	Header name
Web access log	x-note header
NNTP access log	x-error-msg header
Streaming access log	x-status header
Streaming details log	x-status header

For each error that appears in a header field listed in the previous table, this guide contains the log file entry, an explanation, and an action for the administrator (labeled “Action”). For the error codes that appear in the Web access log and NNTP access log, the guide also includes an entry called Message Text in Browser. The Message Text in Browser is a string that Web and news end users see in their Web browsers when the error occurs. The message text typically includes an action for the end user to take (for example, “Retry the request” and “Contact your system administrator.”)

Example of an error message entry:

CACHE_FILL_WRITE_FILE

Message Text in Browser: Internal error. Contact your system administrator.

Explanation: An error occurred while the appliance was trying to send data to the client and cache the objects. The client did not receive the data, and the objects were not cached.

Action: Try sending the same request while performing a packet trace. Select Utilities > Diagnostics > Packet Trace in the Appliance Manager. Contact NetApp Technical Support for assistance.

Adherence to the extended log file format

Extended log file format defined: NetCache appliance log files adhere to the extended log file format conventions described by the World Wide Web Consortium (www.w3.org). The extended log file format enables you to add or delete log file headers so you can create customized log files that can be read by generic log analyzers.

Using the Appliance Manager custom log features, you can modify the log field set (the log header list of a given log format) to tailor most logs to your needs.

The Messages log is not customizable.

Extended log file format header prefixes: Extended log file format headers include a prefix that describes the transfer of information between devices. The NetCache appliance implementation of these extended log file format header prefixes are described in the following table.

Header prefix	Description
c	Client
s	Server (NetCache)
r	Remote (origin server)
cs	Client to server (client to NetCache)
sc	Server to client (NetCache to client)
sr	Server to remote server (NetCache to origin server)
rs	Remote server to server (origin server to NetCache)

Header prefix	Description
x	Application-specific identifier (NetCache specific)
-	Fields that are unknown or not implemented

The NetCache appliance implementation of these headers is slightly different than that described in the extended log file format working draft. In that draft, the server header describes the origin server, whereas the remote header describes a proxy. Because NetCache acts as a server to the client, the server header in NetCache logs describes the NetCache appliance, and the remote header describes the origin server.

About this chapter

This chapter describes the Web access log and provides details about the data that can appear in the header fields in the Web access log. See also Chapter 2, “x-note Header Entries in the Web Access Log,” on page 27, which provides a reference to each error message that can appear in the x-note header field of the Web access log.

Topics in this chapter

This chapter contains the following topics:

- ◆ “About the Web access log” on page 2
- ◆ “Web access log headers” on page 4
- ◆ “Order of headers in predefined formats in the Web access log” on page 14
- ◆ “How data is displayed in the cs-username field” on page 16
- ◆ “x-transaction header entries in the Web access log” on page 17
- ◆ “About logging HTTP headers received by the appliance” on page 20
- ◆ “x-hiercode header entries” on page 21
- ◆ “WebWasher DynaBLocator codes” on page 22
- ◆ “SmartFilter transaction codes” on page 25

About the Web access log

Description of the Web access log

The Web access log records information about client HTTP, FTP, and Gopher transactions conducted through the NetCache appliance. Entries in the Web access log can include a variety of headers, including the IP address of the client, the URL requested, a timestamp, the object size, the transaction type (whether the object was a cache hit or a miss), and the number of milliseconds that the transfer required. It can also show how each object was resolved.

When to use the Web access log

Use the Web access log if you want to know any of the following:

- ◆ The requests that NetCache has serviced
- ◆ Whether a request was a cache hit or a cache miss
- ◆ How long a certain request took
- ◆ The HTTP result code for a request
- ◆ The hierarchical route that NetCache used to service the request

Excerpt from a Web access log

The following is an excerpt from a Web access log (Common Log Format):

```
10.34.26.6 - - [12/Aug/2000:17:35:11 00000] "GET
http://www.netapp.com/jobs/ HTTP/1.0" 200 9824
10.34.26.6 - - [12/Aug/2000:17:35:11 00000] "GET
http://www.netapp.com/images/main_careers_3.gif HTTP/1.0" 200 954
10.34.26.6 - - [12/Aug/2000:17:35:11 00000] "GET
http://www.netapp.com/images/sub_careers_1a.gif HTTP/1.0" 200 1017
10.34.26.6 - - [12/Aug/2000:17:35:11 00000] "GET
http://www.netapp.com/images/sub_careers_1b.gif HTTP/1.0" 200 1424
10.34.26.6 - - [12/Aug/2000:17:35:11 00000] "GET
http://www.netapp.com/images/sub_careers_3a.gif HTTP/1.0" 200 886
10.34.26.6 - - [12/Aug/2000:17:35:11 00000] "GET
http://www.netapp.com/images/sub_careers_2a.gif HTTP/1.0" 200 1034
10.34.26.6 - - [12/Aug/2000:17:35:11 00000] "GET
http://www.netapp.com/images/sub_careers_4a.gif HTTP/1.0" 200 756
10.34.26.6 - - [12/Aug/2000:17:35:11 00000] "GET
http://www.netapp.com/images/sub_careers_5a.gif HTTP/1.0" 200 918
```

```
10.34.26.6 - - [12/Aug/2000:17:35:11 00000] "GET
http://www.netapp.com/images/sub_careers_6a.gif HTTP/1.0" 200 809
10.34.26.6 - - [12/Aug/2000:17:35:11 00000] "GET
http://www.netapp.com/images/sub_careers_7a.gif HTTP/1.0" 200 742
10.34.26.6 - - [12/Aug/2000:17:35:11 00000] "GET
http://www.netapp.com/images/sub_careers_8a.gif HTTP/1.0" 200 624
```

Web access log headers

The following table describes each header that can appear in the Web access log and shows the Web access log formats that are applicable to each header.

Header	Description	Default	Common	Netscape extended	Squid	Custom
bytes	Total number of bytes NetCache delivered to the client.	X	—	—	X	X
cached	Status code indication whether the object was cached, where 1 = cached and 0 = not cached	—	—	—	—	X
c-dns	Client's fully qualified domain name (FQDN). Reporting the FQDN can result in a performance penalty because of the latency associated with the DNS lookup.	—	—	—	—	X
c-ip	Client IP address	X	X	X	X	X
cs-method	HTTP request method NetCache received from the client	X	—	—	X	X

Header	Description	Default	Common	Netscape extended	Squid	Custom
cs(Referer)	Logs the information contained in the request header field that the client delivered to the appliance. This header functions as a wildcard. You can replace the header in parentheses, Referer in this case, with any header. See “About logging HTTP headers received by the appliance” on page 20 for more details.	—	—	—	—	X
cs-uri	URL accessed, for example: http://abc/hello?there	X	—	—	X	X
cs-uri-query	Query portion of URL (the portion after the “?” in the URL), for example: http://abc/hello?“there”	—	—	—	—	X
cs-uri-stem	Stem portion of URL, for example: http://abc/hello	—	—	—	—	X

Header	Description	Default	Common	Netscape extended	Squid	Custom
cs-username	This field is an alternative to the x-username field. For Windows authentication methods (Kerberos and NTLM), the cs-username field precedes the user name with the domain name (the x-username field does not include the domain name). For the local database and RADIUS and LDAP, the cs-username field includes only a user name (like the x-username field). See “How data is displayed in the cs-username field” on page 16.	—	—	—	—	X
date	GMT date when the transaction ended, in YYYY-MMM-DD format	—	—	—	—	X
r-dns	Origin server’s fully qualified domain name	—	—	—	—	X
r-ip	Origin server’s IP address	—	—	—	—	X

Header	Description	Default	Common	Netscape extended	Squid	Custom
rs(Content-Type)	Logs the information contained in the header that the origin server delivered to the appliance. This header functions as a wildcard. You can replace the header in parentheses, Content-Type in this case, with any header. See “About logging HTTP headers received by the appliance” on page 20 for more details.	X	—	—	X	X
rs-status	Response status code NetCache received from the origin server	—	—	X	—	X
sc-comment	HTTP response NetCache sent to the client (For example, when NetCache returns 200 OK, the OK portion of the response code is the comment.)	—	—	—	—	X
sc-status	HTTP response code that NetCache returned to the client, for example, 401	—	X	X	—	X
time	GMT time when the client connection ended, in HH:MM:SS format; indicates the client disconnection time	—	—	—	—	X

Header	Description	Default	Common	Netscape extended	Squid	Custom
time-taken	Time for a transaction, expressed as <seconds>.<milliseconds>	X	—	—	—	X
x-age	Time since the object was last verified with the origin server (in seconds)	—	—	—	—	X
x-authmethod	Method used to authenticate the user or, if authentication failed, the method that was used to try to authenticate the user.	—	—	—	—	X
x-client-port	Client-side port number of the client connection	—	—	—	—	X
x-connect-time	Total time NetCache required to connect to the origin server (in seconds and milliseconds)	—	—	—	—	X
x-cs-bodylength	Length of the body (the object excluding the header) NetCache received from the client	—	—	X	—	X
x-cs-headerlength	Length of the header NetCache received from the client (in bytes)	—	—	X	—	X
x-dnslookup-time	Total time NetCache required to perform the DNS lookup (in seconds and milliseconds)	—	—	—	—	X

Header	Description	Default	Common	Netscape extended	Squid	Custom
x-domain	For Windows authentication methods, shows the domain name. For non-Windows authentication methods, shows information about the authentication server, for example, for LDAP, it could show the LDAP server IP address.	—	—	—	—	X
x-elapsed-seconds	Time for a transaction, expressed in seconds only, (milliseconds are not counted)	—	—	X	—	X
x-elapsed-milliseconds	Time for a transaction expressed in milliseconds	—	—	—	X	X
x-hiercode	NetCache hierarchy code/peer IP address See “x-hiercode header entries” on page 21 for details.	X	—	—	X	X
x-hiername	Name of the hierarchy forwarding rule that was executed.	—	—	—	—	X
x-localtime	NetCache local time, in DD/MMM/YYYY:HH:MM:SS GGGG format (where GGGG is the time differential from GMT)	—	X	X	—	X

Header	Description	Default	Common	Netscape extended	Squid	Custom
x-last-modified	Last-modified time specified in the Last-Modified header	—	—	—	—	X
x-last-verify	Time this object was last verified	—	—	—	—	X
x-note	Miscellaneous NetCache error codes See Chapter 2, “x-note Header Entries in the Web Access Log,” on page 27 for details about the error codes.	X	—	—	—	X
x-protocol	Protocol used during the connection	—	—	—	—	X
x-max-age	Maximum age of the object	—	—	—	—	X
x-remote-id	Not implemented; appears as a “-”	—	X	X	X	X
x-request-line	Entire request method line (in quotation marks), for example: "GET http://abc/content HTTP/1.0"	—	X	X	—	X
x-rs-contentlength	Length of the object that NetCache received from the origin server (in bytes, as specified by the Content-Length header)	—	—	X	—	X

Header	Description	Default	Common	Netscape extended	Squid	Custom
x-rs-headerlength	Length of the header that NetCache received from the origin server (in bytes)	—	—	X	—	X
x-sc-contentlength	Length of the object that NetCache delivered to the client (in bytes, as specified by the Content-Length header)	—	X	X	—	X
x-sc-headerlength	Length of the header that NetCache delivered to the client (in bytes)	—	—	X	—	X
x-smartfilter-categories	SmartFilter category code that is associated with a URL, for example: Sex = sx See “SmartFilter transaction codes” on page 25.	—	—	—	—	X
x-smartfilter-result	SmartFilter result code, where 1 = denied and 0 = allowed	—	—	—	—	X
x-sr-bodylength	Length of the body that NetCache received from the origin server (in bytes)	—	—	X	—	X
x-sr-headerlength	Length of the header that NetCache delivered to the origin server (in bytes)	—	—	X	—	X

Header	Description	Default	Common	Netscape extended	Squid	Custom
x-timestamp	Number of seconds since the UNIX epoch—January 1, 1970, for example: 963873698.73 Indicates when the client connection ended	X	—	—	X	X
x-transaction	Transaction or reply code, for example: HIT/200 See “x-transaction header entries in the Web access log” on page 17 for more information.	X	—	—	X	X
x-username	User name given for proxy authenticated requests. See also cs-username.	X	X	X	—	X
x-wwfilter-categories	WebWasher DynaBlocator category code that is associated with a URL, for example: Sex = sx See “WebWasher DynaBLocator codes” on page 22.	—	—	—	—	X
x-wwfilter-result	WebWasher DynaBLocator result code, where 1 = denied and 0 = allowed	—	—	—	—	X

Header	Description	Default	Common	Netscape extended	Squid	Custom
x-uri-path	Relative URL path name, that is, the URL without the protocol specifier and host name, for example: /abc/content	—	—	—	—	X

Order of headers in predefined formats in the Web access log

About predefined formats	For the Web access log, you can choose from several predefined formats that determine the headers that are in the log and the order in which those headers appear in the log. You must define a custom log if you want the headers to appear in an order that is different from the order provided by a predefined log format.
Web access log default format headers, in order	The Web access log default format includes the following headers, in the order shown: - x-timestamp - time-taken - c-ip - x-transaction - bytes - cs-method - cs-uri - x-username - x-hiercode - rs(Content-Type) “About logging HTTP headers received by the appliance” on page 20 - x-note
Common log format headers, in order	The Common log format includes the following headers, in the order shown: - c-ip - x-remote-id - x-username - x-localtime - x-request-line - sc-status - x-sc-contentlength

**Netscape extended
format headers, in
order**

The Netscape extended format includes the following headers, in the order shown:

c-ip
x-remote-id
x-username
x-localtime
x-request-line
sc-status
x-sc-contentlength
rs-status
x-rs-contentlength
x-cs-bodylength
x-sr-bodylength
x-cs-headerlength
x-sc-headerlength
x-sr-headerlength
x-rs-headerlength
x-elapsed-seconds

**Squid native format
headers, in order**

The squid native format specifies the following field order:

x-timestamp
x-elapsed-milliseconds
c-ip
x-transaction
bytes
cs-method
cs-uri
x-remote-id
x-hiercode
rs(Content-Type) See “About logging HTTP headers received by the appliance” on page 20.

How data is displayed in the cs-username field

As the following table shows, the appliance preserves the case (capitalization) of domains and user names when it logs data in the cs-username field in the Web access log.

If the domain is...	If the user name is...	The cs-username field shows...
ntapnc	ADMINISTRATOR	"ntapnc\ADMINISTRATOR"
ncqa	admin	"ncqa\admin"
ntapnc	Joe Black	"ntapnc\Joe Black"
Empty	admin	"admin"
Empty	Empty	"" [invalid -- no user name]

The domain is separated from the user name by a backslash. Unlike W3C and IIS log field formats for the cs-username field, NetCache quotes this field's value so that log analyzers can accept cs-username values with embedded whitespace.

x-transaction header entries in the Web access log

Codes for the x-transaction field

The following table shows the possible HTTP transaction codes for the x-transaction field.

Transaction code	Explanation
TCP_HIT	Requested object was cached and returned to the client.
TCP_HIT_ACCESS_DENIED	The object was in the cache but the user was not allowed to access the content.
TCP_HIT_EJECT	The object was successfully ejected.
TCP_HIT_IMS_NOTMOD	Client requested an IMS check, and the object was found to be not modified (304 reply code).
TCP_HIT_PRECONDITION_FAILED	The object was in the cache, but the If-Match condition specified by the client failed (did not match).
TCP_HIT_PARTIAL	The client requested partial content (byte range request) and the requested content was served from the cache (NetCache returned 206 Partial Content).
TCP_HIT_VERIFY	The object was IMS checked and found to be not modified (304 reply code).
TCP_MISS	The object was not in the cache.
TCP_MISS_EJECT	An eject was requested but could not be executed because the object was not found in the cache.
TCP_MISS_CACHE_VERSION	The object was in the cache, but the cached object's file version did not match the requested version (because of software upgrades or reversions that were made without zeroing the disks).

Transaction code	Explanation
TCP_MISS_MIN_AGE	The object could not be served because the minimum age specified in the Cache Control header had not yet been reached.
TCP_MISS_NOFETCH	The object could not be delivered to the client because the Cache Control header specified only-if-cached and the object was not in the cache.
TCP_MISS_PRIVATE	The object is private and cannot be shared with other clients.
TCP_MISS_PRIVATE_AUTHORIZATION	The object is password-protected, so it is not cacheable.
TCP_MISS_PRIVATE_BAD_LEN	The actual object length does not match the reported length in the MIME header.
TCP_MISS_PRIVATE_CCTRL	The origin server has defined this object as noncacheable using the Cache-Control header, so the object cannot be shared with other clients. The request is proxied but not cached.
TCP_MISS_PRIVATE_COOKIE	Because the object contains cookie information, it is considered private and cannot be shared with other clients.
TCP_MISS_PRIVATE_DISK_BUSY	The object was not cached because NetCache was overloaded.
TCP_MISS_PRIVATE_DISK_FULL	The object was not cached because NetCache did not have the disk space.
TCP_MISS_PRIVATE_EXPECT	Information in the Expect header is private (something other than 100-continue).
TCP_MISS_PRIVATE_HEADER_OVERFLOW	The object could not be cached because the header entry was not defined and is longer than the default predefined length.
TCP_MISS_PRIVATE_METHOD	This request uses a noncacheable method, such as PUT, POST, or CONNECT.

Transaction code	Explanation
TCP_MISS_PRIVATE_NO_LAST_MOD	NetCache did not cache the object because the object does not have a last modification timestamp.
TCP_MISS_PRIVATE_ON_STOP_LIST	The requested object is proxied but not cached because of an entry in the Uncacheable Objects by URL Substring option on the HTTP - Caching Behavior page in the Appliance Manager (Setup tab > HTTP > Caching Behavior).
TCP_MISS_PRIVATE_STATUS_CODE	The transaction could not be completed because a 200 OK status was not received.
TCP_MISS_PRIVATE_VARY	NetCache did not cache the object because several representations of the object exist as specified in the Vary header.
TCP_MISS_RELOAD	The client refreshed the object, flushing the old one from the cache.
TCP_MISS_VERIFY	The object was found in the cache, but after an IMS check, a new object was returned (200 reply code).
TCP_UNKNOWN	NetCache did not cache the object because an error was encountered before NetCache could determine the transaction type.

About logging HTTP headers received by the appliance

Fields for logging HTTP headers

The Web access log provides two log file fields that enable you to log the HTTP headers received by the appliance. Any HTTP header can be logged. You log a different HTTP header by inserting the header name in the parentheses.

Use the following fields to log the HTTP response and request headers:

- ◆ `rs(http header name)`
The `rs()` header logs the HTTP response header that the appliance received from the origin server. To log a specific HTTP header, enter the HTTP header name within the parentheses.
- ◆ `cs(http header name)`
The `cs()` header logs the HTTP request header that the appliance received from the client. To log a specific HTTP header, enter the HTTP header name within the parentheses.

If you want to log multiple HTTP headers, enter a separate `rs()` or `cs()` header for each HTTP header you want to log. The HTTP header information will subsequently be logged within double quotation marks in the Web access log.

See RFC 2616 for descriptions of the HTTP headers that can be logged.

x-hiercode header entries

About entries in the x-hiercode field

The x-hiercode header field, which appears in several types of appliance logs, can have the values shown in the following table.

Transaction Code	Explanation
DIRECT	URL was fetched directly from the source.
FIRST_PARENT_MISS	Miss was resolved through the fastest parent.
NEIGHBOR_HIT	A neighbor holds the object.
NO_DIRECT_FAIL	The requested URL resides outside the firewall, and the URL maps to no parents or neighbors.
NO_FAILOVER	A forwarding rule match occurred. However, the parent could not be contacted and because rule failover is disabled for this rule the next hierarchy rule is not tried.
NO_PARENT_DIRECT	This object has no valid parents or neighbors.
PARENT_HIT	A parent holds the object.
SINGLE_PARENT	This object must be fetched from a specific parent.

WebWasher DynaBLocator codes

DynaBLocator codes

Entries in the x-wwfilter-categories header in the Web access log can have the values shown in the following table. See the Appliance Manager online Help for category descriptions.

Code	DynaBLocator category
ab	Abortion
ad	Self-Help and Addictions
al	Alcohol
an	Anonymous Proxies
ar	Art and Museums
au	Auctions and Classified Ads
ba	Banking and Home Banking
bb	Newsgroups and Bulletin Boards
bk	Literature and Specialized Books
bl	Building, Residence, Architecture, and Furnishings
cc	Computer Crime
ch	Chat
co	Cities, Regions, and Countries
dr	Illegal Drugs
dt	Dating and Relationships
ed	Education
en	Nature and Environment
ex	Extreme
fa	Fashion, Cosmetics, and Jewelry

Code	DynaBLocator category
gb	Gambling
gm	Computer Games
gv	Governmental Organizations
hl	Health, Recreation, and Nutrition
hm	Humor
ht	Hate and Discrimination
ia	Illegal Activities
in	Investment
is	Information Security
js	Job Search
mo	SMS and Mobile-related
mu	Music
ng	Non-governmental Organizations
nw	General News, Newspapers, and Magazines
os	Online Shopping
pc	Digital Postcards
pn	Pornography
po	Political Parties
pr	Private Homepages
rc	Recreational Facilities
re	Religion
rs	Restaurants and Bars
sc	Sects
sl	Swimwear, Lingerie, and Nudity

Code	DynaBLocator category
sp	Sports
sr	Search Engines, Web Catalogs, Portals
st	Shares and Stocks
sv	Software and Hardware Vendors and Distributors
sw	Illegal Software
sx	Erotica and Sex
tb	Tobacco
tp	Transportation
tr	Travel
ts	Translation
tv	Cinema and Television
ty	Toys
wh	Web Hosting and Bandwidth Services
wm	Web Mail
wp	Weapons

SmartFilter transaction codes

SmartFilter codes

Entries in the x-smartfilter-categories header in the Web access log can have the values shown in the following table. See the Appliance Manager online Help for category descriptions.

Transaction code	SmartFilter category
ac	Art and Culture
an	Anonymizer/Translator
ch	Chat
cs	Criminal Skills
dr	Drugs
et	Entertainment
ex	Extreme
ga	Games
gm	Gambling
hm	Humor
hs	Hate Speech
in	Investing
js	Job Search
lf	Lifestyle
mm	Dating
mp	MP3 Sites
mt	Mature
na	Usenet news
nd	Nudity

Transaction code	SmartFilter category
nw	General news
oc	Cults/Occult
os	Online Sales and Merchandising
po	Opinion, Politics, and Religion
pp	Personal Pages
ps	Portal Sites
sh	Self-Help
sp	Sports
sx	Sex
tr	Travel
wm	Webmail
wt	Worthless

About this chapter

This chapter contains information about the entries that can appear in the x-note header field of the Web access log. Many of these entries can also be seen by end users in a Web browser. When an end user contacts you, ask for the code that appears at the end of the message, for example, ACL_DENY, so that you can look up the message in this chapter quickly.

Topic in this chapter

This chapter contains the following topic:

- ◆ “x-note entries—explanation and actions” on page 28

x-note entries—explanation and actions

ACL_DENY

Message Text in Browser: Your request was denied by an access control list.

Explanation: An access control is blocking requests sent by the user or client.

Action: Evaluate whether you want to keep the control that is blocking the user's request. Check the current settings on the Access Control Settings page (Setup tab > Access Control > Access Control Lists).

AUTH_FAIL

Message Text in Browser: Authentication failed. Verify that you have a valid user name and password.

Explanation: The user who received this message is not authorized to view the requested URL.

Typically, you can expect to see single instances of this error in your log files as individual users are denied access to the protocol. However, in the case of NTLM over HTTP, you might see a grouping of AUTH_FAIL messages as the appliance records its communication with the domain controller. If authentication is successful, you will see two AUTH_FAIL messages followed by a response code from the origin server. If authentication is unsuccessful, you will see a group of three AUTH_FAIL messages.

Action: If you want the user to be authenticated for a particular protocol, you must ensure that the user is authorized for that protocol. Check the following:

- ◆ Is the user or client request blocked (denied) by an ACL?
- ◆ Select Setup tab > Access Control > Access Control Lists.
If the user is in the appliance local database, does the user belong to a group for which protocol authentication has been configured?
- ◆ Select Setup tab > Authentication > Users to check the groups to which the user belongs. Then select Setup tab > Authentication > Groups to determine the protocol authentication for the user's groups.
- ◆ If the user is in a remote database for which a group has been configured in the appliance local database, is protocol authentication configured for the group?
Select Setup tab > Access Control > Access Control Lists.

BAD_REQUEST_NO_HOST

Message Text in Browser: Your browser sent an HTTP 1.1 request that does not comply with the HTTP standard. Try another browser or contact your system administrator.

Explanation: The browser sent an HTTP 1.1 request to the appliance that did not contain a host header, which violates the HTTP/1.1 specification. This can result from a browser bug.

Action: To troubleshoot the problem:

- ◆ Find out the browser and browser version that was used to send the request.
- ◆ Run a packet trace to confirm that the request did not contain a host header.

In the Appliance Manager, select Utilities tab > Diagnostics > Packet Trace.

You might need to advise users to avoid using specific browsers.

BAD_URL

Message Text in Browser: An invalid URL was detected. The appliance cannot serve the request as entered.

Explanation: A typical cause of this message is that the URL does not contain a server name.

Action: If the problem cannot be attributed to a user error such as not including the server name in the URL, reissue the request and take a packet trace. Then contact NetApp Technical Support. To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.

BYPASSED_URL

Message Text in Browser: The client request was forwarded directly to the origin server. No action is required.

Explanation: If transparency and dynamic forwarding are enabled on the appliance and a client request results in a server response containing a status code listed in the HTTP Status Codes option, the appliance sends a 302 redirection message to the client. The client then requests the content again. Because of transparency, the request is sent to the appliance, but the appliance ignores the request and forwards it directly to the origin server (no origin server connection is opened). The returned content is not redirected to the appliance, and is delivered directly to the client.

Action: If you do not want the content delivered directly to the client, disable the Dynamic Forwarding option or change the HTTP status codes. In the Appliance Manager, the Dynamic Forwarding option and the HTTP Status Codes option are on the Transparency - Request Forwarding page (Setup tab > Transparency > Request Forwarding).

CACHE_FILL_READ

Message Text in Browser: Internal error or file corruption problem while attempting to read a cached file. Contact your system administrator.

Explanation: An error occurred when the appliance attempted to read a cached file. For example, the file might be corrupt or the appliance might have experienced an internal error.

The result of this error is a cache miss. However, the appliance does not fetch the object from the origin server for this request. The appliance will fetch the object from the origin server the next time the same object is requested.

Action: Try to manually eject the cached file. The URL for the problem file is included in the log entry. If ejecting the object does not solve the problem, contact NetApp Technical Support.

CACHE_FILL_OPEN_FILE

Message Text in Browser: An internal error prevented the object from being sent to the client and cached. Try again later.

Explanation: The appliance fetched the object from the origin server because it was not cached. However, an error occurred that prevented the object from being served to the client and cached. For example, an internal error occurred when the appliance tried to write to the cache or the appliance was extremely busy handling requests.

Action: If this problem occurs frequently, contact NetApp Technical Support.

CACHE_FILL_TRANSPORT

Message Text in Browser: An error occurred while transferring data to the client. Contact your system administrator.

Explanation: The client might have become available. Alternatively, an internal error could have occurred while the appliance was reading data from disk.

Action: Check the availability of the client. If the client is available, contact NetApp Technical Support for assistance.

**CACHE_FILL_
WRITE_FILE**

Message Text in Browser: An internal error occurred while writing the data to the cache. Contact your system administrator.

Explanation: An error occurred while the appliance was trying to send data to the client and cache the objects. The client did not receive the data, and the objects were not cached.

Action: Try sending the same request while performing a packet trace. Select Utilities > Diagnostics > Packet Trace in the Appliance Manager. Contact NetApp Technical Support for assistance.

**CACHE_HIT_FILE_
VERSION**

Message Text in Browser: A previously cached object was refetched after a software upgrade. No action is required.

Explanation: After some appliance releases, all cached objects must be refetched from origin servers. The reason is that some new software releases require additional meta data in the headers to support the new features. Therefore, the appliance does not recognize the objects that were cached before the software upgrade because the older software did not use this meta data.

When a client requests a previously cached object, the appliance refetches the object from the server and serves it to the client. The appliance hit rate will be low until the cache is populated with new objects.

Action: No administrative action is required.

**CACHE_HIT_
FORCED_EJECT**

Message Text in Browser: Your Reload request could not be completed. Try again.

Explanation: The user clicked Reload in the browser. As a result, the appliance ejected its cached copy of the object and attempted to fetch the new copy of the object from the origin server. This message appears if the appliance was not able to fetch the new copy of the object for some reason, for example, a network problem.

Action: No action is required.

**CACHE_HIT_
WRITE_SOCKET**

Message Text in Browser: The object you requested could not be delivered because your computer closed the connection. Contact your system administrator.

Explanation: The appliance was attempting to send a cached object to the client, but the client closed the connection. Most likely this occurred because of a networking problem.

Action: Verify the network connectivity.

CANT_CONNECT

Message Text in Browser: Could not connect because of networking problems. Contact your system administrator.

Explanation: This is a generic error. For some reason, the client or the server is experiencing network connectivity problems.

Action: Verify the network connectivity.

**CANT_CONNECT_
IPSPOOF**

Message Text in Browser: The client could not connect because of IP spoofing problems.

Explanation: The error occurs if both IP spoofing and SecureAdmin are enabled on the appliance and the client Web browser is set up to send secure administrative requests to the appliance admin port.

Action: Do not configure the Web browser to send secure requests to the admin port of the appliance that you want to administer. Instead, access the appliance that you want to administer by entering a URL in the Web browser that includes the appliance IP address and admin port.

**CANT_CONNECT_
LOOPBACK**

Message Text in Browser: Could not connect due to potential loopback problems.

Explanation: This message is issued to alert you that a client is attempting to find a security hole in the appliance where connections initiated through a loopback are accepted. The client might be attempting to connect through an appliance port (an HTTP proxy port, admin port, or a port configured to listen for requests such as HTTPS requests). Alternatively, someone might be issuing CONNECT http://cache:80/HTTP/1.0 repeatedly, which could result in a DOS attack.

The appliance does not accept connections initiated through a loopback.

Action: Look for the client IP address in the log file to find out which client is attempting to connect to the appliance.

CLIENT_CLOSE

Message Text in Browser: The client closed the connection. Reopen the browser and retry the request.

Explanation: The most likely cause of this error is a browser problem. Network connectivity problems can also cause the connection to close.

Action: If the problem cannot be attributed to a browser problem and if the problem persists, verify the network connectivity.

CLIENT_REQUEST_READ

Message Text in Browser: A network problem occurred. Retry your request.

Explanation: The appliance could not receive the request from the client browser because of a network error.

Action: Send the request again. If the problem persists, verify the network connectivity.

CLIENT_TAKEOVER

Message Text in Browser: Protocol takeover occurred during the tunneling process. No action is required.

Explanation: This message is sent when the appliance is tunneling a request. Another protocol (such as FTP) was sent over HTTP and has taken over.

Action: No action is required.

CLIENT_WRITE

Message Text in Browser: The client was not available to receive data. Contact your system administrator.

Explanation: When the appliance attempted to send the requested data to the client, the client was not available so an error occurred. A typical cause of this error is a network problem that is causing very slow response times. As a result, by the time the appliance sends a response to the client, the user has already clicked Stop in the Web browser.

Action: If the problem cannot be attributed to the user's actions with the Web browser, look for DNS problems and networking problems.

CONTENT_NOT_PRESENT

Message Text in Browser: Content is temporarily not present. Contact your system administrator.

Explanation: If the appliance is configured as an accelerator for HTTP Web servers and monitoring of HTTP Web servers is enabled (the Enable Monitor option is selected), this message is issued if a server that the appliance is monitoring becomes unavailable.

Action: Check the connection between the appliance and the Web server identified in the message. The message will contain the URL with the server's host name. If you need the IP address associated with the server, check the Messages log for an entry such as the following:

Mon Apr 29 18:12:01 GMT [sthread_loop:notice]: accel_monitor: http server <ip address:80> unreachable.

If you expect that the Web server will be unavailable for an extended period of time, you can remove the server from the list of servers that this appliance is to accelerate. To remove the server from the accelerator rules, select Setup tab > HTTP > Web Server Acceleration > Rules tab in the Appliance Manager and delete the entry for the server.

DNS_HOST_NOT_FOUND

Message Text in Browser: The host name was not found during the DNS lookup. Contact your system administrator if the problem is not resolved by retrying the URL.

Explanation: The appliance has been able to communicate with the DNS server correctly. However, the host name could not be found in the DNS database. This could have occurred because the user mistyped the host name in the URL.

Actions: Try the following:

- ◆ Have the user retype the URL to rule out whether the user incorrectly entered the host name.
- ◆ If you can rule out a typing error, try running nslookup on the host from the user's computer.

If the request resolves from the user's computer, contact NetApp Technical Support. A problem might exist with the appliance that is preventing the host name from being resolved through the appliance.

DNS_MISC_ERROR

Message Text in Browser:

A DNS lookup error occurred.

Explanation: The most likely cause of this message is that the Hosts file was deleted or corrupted.

Actions: Check the following:

- ◆ Review the appliance DNS configuration to ensure that everything is correct. In the Appliance Manager, select Setup tab > DNS > General.
- ◆ Verify that the DNS nameserver is functioning.
- ◆ Verify that the routing to the DNS nameserver is configured correctly. You can check the routing configuration on the appliance by selecting Setup tab > Network > Routing > View All Routes tab in the Appliance Manager.
- ◆ Ping the nameserver to determine whether a route to it exists.

DNS_NO_DATA

Message Text in Browser: The IP address was not found during the DNS lookup. Contact your system administrator.

Explanation: The appliance has been able to communicate with the DNS server correctly. However, a DNS lookup error occurred because the host name was found in the DNS database but not the IP address.

Actions: Try running nslookup on the host from the user's computer. If the request resolves from the user's computer, contact NetApp Technical Support. A problem might exist with the appliance that is preventing the IP address from being resolved through the appliance.

DNS_TIMEOUT

Message Text in Browser: A DNS lookup error occurred because the request timed out during the lookup.

Explanation: The appliance did not receive a response from the DNS server within an allotted period of time and timed out.

Actions: Verify the network connectivity and attempt the request again. If the problem persists, try the following actions:

- ◆ Verify that the DNS nameserver configuration is correct. In the Appliance Manager, select Setup tab > DNS > General.
- ◆ Verify that the DNS nameserver is functioning.
- ◆ Verify that the routing to the DNS nameserver is configured correctly.

To check the routing setup on the appliance, select Setup tab > Network > Routing > View All Routes tab in the Appliance Manager.

- ◆ Ping the nameserver to determine whether a route to it exists.

FTP_BAD_RESPONSE

Message Text in Browser: Bad response from the FTP server

Explanation: The most common cause of this message is that the FTP server does not send back a well-formed response for some reason. This message will also be generated if the user did not include the server name in the request when the appliance is configured for encapsulated FTP (that is, you have selected FTP Proxy Enable on the FTP - General page.

Action: If you have FTP Proxy Enable selected on the FTP - General page, remind the user to include the server name in the request. The user must ftp to the appliance IP address and then enter the user name in the following form: userabc@ftp.site.com.

FTP_LOGIN

Message Text in Browser: This FTP user name or password is invalid.

Explanation: The appliance did not recognize the user name or password you used to issue an FTP connection.

Action: Verify the user name and password on the FTP server.

FTP_NOFILE

Message Text in Browser: No such file or directory on the FTP server.

Explanation: The file requested by the user does not exist on the origin server.

Action: Verify that the file exists and try to establish an FTP connection to the server again.

FTP_NOPERM

Message Text in Browser: The FTP server has denied permission to the file.

Explanation: The FTP server administrator has not granted the user permission to access the file on the FTP server. This message is not associated with appliance permissions.

Action: No action is required.

FTP_NULL_ USERNAME

Message Text in Browser: Login failed. Check the user name setting in your browser.

Explanation: Although the user name in the request was empty, the FTP server accepted it. The typical cause of this error is a server bug.

The FTP protocol does not allow FTP servers to accept an FTP request without a user name. However, if the server does not follow the protocol and accepts the request, the appliance (which follows the protocol) cannot handle the request.

Action: Have the user check the Web browser to ensure that the browser is configured with a user name for FTP requests.

GATEWAY_ TIMEOUT

Message Text in Browser: A gateway timeout occurred. The server is unreachable. Retry the request.

Explanation: The appliance or the server acting as a gateway or proxy to fulfill the client request did not receive a timely response to serve the HTTP request. This is usually caused by slow IP communications from the origin server.

Action: Try to connect again. If the problem persists, there might be a problem with the network or the Web server.

HTTP_MIME_TOO_ LONG

Message Text in Browser: The server response MIME header is too long. No action is required.

Explanation: The proxy-cache server cannot process a MIME header of more than about 4,096 characters.

HTTP_REQUEST_ TOO_LONG

Message Text in Browser: The HTTP request is too long. Contact your system administrator.

Explanation: The appliance has an internal limit for the length of an HTTP request. This limit is generous enough that only extraordinarily long requests will exceed it.

Action: Run a packet trace, then contact NetApp Technical Support. A packet trace can help you determine what line of the request is too long. To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.

ICAP_OPTIONS_ MISMATCH

Message Text in Browser: The ICAP OPTIONS response from the service does not match the server. Contact your ICAP system administrator.

Explanation: The OPTIONS response obtained from an ICAP service does not match the current set of OPTIONS used by all active ICAP services within the ICAP service farm. This problem can occur because the ICAP versions in two or more ICAP servers in the same service farm are not the same.

Action: Try the following:

- ◆ Check the ICAP software versions on the ICAP servers in the service farm to determine if they are the same.
- ◆ If the ICAP software versions are not the same, the ICAP server administrator must ensure that the software versions match.
- ◆ If the ICAP software versions are the same, contact NetApp Technical Support.

ICAP_OPTIONS PARSE_FAIL

Message Text in Browser: ICAP OPTIONS response could not be parsed. Contact your system administrator.

Explanation: The appliance did not recognize the OPTIONS response obtained from an ICAP service.

Action: Possible actions:

- ◆ The ICAP server administrator should check the OPTIONS response returned by the ICAP server for problems with protocol semantics.
- ◆ If the ICAP administrator cannot find problems with protocol semantics, the appliance administrator should take a packet trace and send it to NetApp Technical Support or the ICAP server vendor for review.

To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.

ICAP_REQMOD_ CLIENT_READ_ FAIL

Message Text in Browser: The client request could not be read. Contact your system administrator.

Explanation: An error occurred while the appliance to read the request from the client during the ICAP request modification. This error can occur when the client receives an incorrect or incomplete set of message headers from the appliance. Alternatively, a browser bug might be causing a problem with the message headers.

Action: Retry the request and take a packet trace. Then contact NetApp Technical Support. To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.

ICAP_REQMOD_ CLIENT_WRITE_ FAIL

Message Text in Browser: The response could not be sent to the client. Contact your system administrator.

Explanation: An error occurred while the appliance was attempting to write the response to the client during the ICAP request modification phase.

This error can occur in the following circumstances:

- ◆ A user closes the Web browser before receiving the response.
- ◆ The ICAP server sends an incorrect response.
- ◆ The appliance experiences an internal error.

Action: Contact your ICAP system administrator or contact NetApp Technical Support and provide a packet trace. To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.

ICAP_REQMOD_ SVC_DISABLED

Message Text in Browser: A required ICAP request modification service is down. Contact your system administrator.

Explanation: A non-bypassable ICAP request modification service that is needed for this ICAP request is disabled in the appliance configuration.

Action: Check the list of configured service farms in the appliance configuration. The list will show which service farms are disabled. If you want a service to be active, you must enable it.

If the problem persists, contact NetApp Technical Support.

ICAP_REQMOD_ SVC_INVALID_ RESPONSE

Message Text in Browser: A malformed ICAP request modification response was received. Contact your system administrator.

Explanation: The ICAP service sent a malformed request modification response. The most likely reason is that a protocol semantics violation occurred because of the way that the ICAP server responded. For example, the response might be missing fields or it might include incorrect status codes.

Action: Reissue the same request. Contact your ICAP system administrator or contact NetApp Technical Support and provide a packet trace. To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.

**ICAP_REQMOD_
SVC_READ_BODY_
FAIL**

Message Text in Browser: Could not read the response body from the ICAP service. Contact your system administrator.

Explanation: An error occurred while the appliance was receiving the ICAP request modification response from the ICAP service. This error could occur during the POST phase of an HTTP transaction. The ICAP server could have sent the wrong body or experienced some type of problem.

Action: Contact either NetApp Technical Support or your ICAP system administrator.

**ICAP_REQMOD_
SVC_READ_FAIL**

Message Text in Browser: Could not read the response from the ICAP service. Contact your system administrator.

Explanation: An error occurred while the appliance was receiving the ICAP request modification response from the ICAP service. The error could have been caused by problems with headers, or the ICAP server could have experienced some type of problem.

Action: Contact your ICAP system administrator.

**ICAP_REQMOD_
SVC_WRITE_FAIL**

Message Text in Browser: Could not write the request to the ICAP service. Retry the request.

Explanation: An error occurred while the appliance was attempting to send the ICAP request modification request to the ICAP service. The appliance was tried unsuccessfully to write a request. The ICAP server could have closed the connection for some reason. If the ICAP server becomes unavailable, this is the first message you will see in a set of messages regarding ICAP service problems.

Action: If the problem reoccurs, reissue the same request and take a packet trace. Then contact NetApp Technical Support. To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager. If NetApp Technical Support cannot determine the cause of the problem, contact the ICAP system administrator.

**ICAP_RESPMOD_
EXIT_FAIL**

Message Text in Browser: Could not successfully exit for response modification. Contact your system administrator.

Explanation: An internal error occurred while the appliance was attempting to complete the ICAP response modification transaction.

Action: Contact NetApp Technical Support and provide a packet trace. To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.

**ICAP_RESPMOD_
GEN_HDR_FAIL**

Message Text in Browser: Could not generate headers for response modification. Contact your system administrator.

Explanation: An error occurred while the appliance was attempting to generate a protocol request or response headers, or ICAP's request headers for the ICAP response modification transaction. This problem could be caused by an appliance internal error, or the origin server could be experiencing a problem.

Action: Contact NetApp Technical Support and provide a packet trace. To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.

**ICAP_RESPMOD_
IO_BODY_FAIL**

Message Text in Browser: An IO failure occurred during the response modification of the body. Contact your system administrator.

Explanation: An error occurred while the appliance was reading the response from the origin server and sending it to the ICAP server. The problem could be caused by an internal appliance error or by a problem with the origin server.

Action: Contact NetApp Technical Support.

**ICAP_RESPMOD_
IO_PREVIEW_FAIL**

Message Text in Browser: An IO failure occurred during response modification preview. Contact your system administrator.

Explanation: An IO failure occurred during the preview phase of the ICAP response modification transaction. This could have been caused by an internal appliance error or by a problem with the ICAP server.

Action: Reissue the request and take a packet trace. Then Contact NetApp Technical Support. To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.

ICAP_RESPMOD_ RCV_STATUS_FAIL

Message Text in Browser: Could not receive the status for a response modification. Contact your server administrator.

Explanation: An error occurred while the appliance was receiving the ICAP response modification response from the ICAP service. This problem could be caused by an input/output error or a protocol semantics error.

Action: Try the following:

- ◆ Ensure that the ICAP server is functional by checking the status at the appliance.
- ◆ If the problem persists, take a packet trace. Then contact NetApp Technical Support or the ICAP server vendor.
- ◆ To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.
- ◆ Contact your ICAP system administrator.

ICAP_RESPMOD_ SEND_BODY_FAIL

Message Text in Browser: Could not send body for a response modification. Contact your system administrator.

Explanation: An error occurred while the appliance was sending the ICAP response modification request body to the ICAP service. The appliance failed to send part of the request to the ICAP server.

Action: Try the following:

- ◆ Ensure that the ICAP server is functional by checking the status at the appliance.
- ◆ If the problem persists, take a packet trace. Then contact NetApp Technical Support or the ICAP server vendor.
- ◆ To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.
- ◆ Contact your ICAP system administrator.

ICAP_RESPMOD_ SEND_HDR_FAIL

Message Text in Browser: Could not send headers for response modification. Contact your system administrator.

Explanation: An error occurred while the appliance was attempting to send the ICAP response modification headers to the ICAP service.

Action: Try the following:

- ◆ Ensure that the ICAP server is functional by checking the status at the appliance.
- ◆ If the problem persists, take a packet trace. Then contact NetApp Technical Support or the ICAP server vendor.
To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.
- ◆ Contact your ICAP system administrator.

ICAP_RESPMOD_ SEND_PREVIEW_ FAIL

Message Text in Browser: Could not send the body during the response modification preview. Contact your system administrator.

Explanation: An error occurred while the appliance was attempting to send the ICAP response modification preview request to the ICAP service. This error is most likely due to an ICAP server problem.

Action: Try the following:

- ◆ Ensure that the ICAP server is functional by checking the status at the appliance.
- ◆ If the problem persists, take a packet trace. Then contact NetApp Technical Support or the ICAP server vendor.
To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.
- ◆ Contact your ICAP system administrator.

ICAP_RESPMOD_ SERVICE_ DISABLED

Message Text in Browser: The required ICAP response modification service is down. Contact your system administrator.

Explanation: A non-bypassable ICAP response modification service that is needed for this ICAP request is disabled in the appliance configuration.

Action: Check the list of configured service farms in the appliance configuration. The list will show which service farms are disabled. If you want a service to be active, you must enable it.

If the problem persists, contact NetApp Technical Support.

ICAP_SF_BYPASS

Message Text in Browser: Bypassing ICAP service. Contact your system administrator.

Explanation: A service is configured as bypassable and an error occurred. The appliance will attempt to invoke the next service in the ICAP pipeline if one exists and continue. No ICAP transformations were applied at the service that failed.

Action: Reissue the request and take a packet trace. Then Contact NetApp Technical Support. To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.

ICAP_SF_FARM_DISABLED

Message Text in Browser: Attempted to connect to a disabled ICAP server farm. Contact your system administrator.

Explanation: An attempt was made to connect to a disabled service farm.

Action: Check the list of configured service farms in the appliance configuration. The list will show which service farms are disabled. If you want a service to be active, you must enable it.

If the problem persists, contact NetApp Technical Support.

ICAP_SF_NOFARM_AVL

Message Text in Browser: The specified ICAP server farm is not available. Contact your system administrator.

Explanation: An attempt was made to connect to an ICAP service farm that is in the process of being disabled or no longer exists. This error can occur if a client attempts to use the service farm while the appliance administrator is disabling the service farm.

Action: Verify the specified ICAP service farm is valid. If the service farm is valid and the problem occurs when the service farm configuration is not being changed, contact NetApp Technical Support.

ICAP_SF_NOSERVICE_AVL

Message Text in Browser: There is no functional ICAP service in the ICAP service farm. Contact your system administrator.

Explanation: A connection could not be opened to any ICAP service that is contained in the appliance configuration for the specified ICAP service farm.

An attempt was made to connect to an ICAP service farm for which no services are configured, or the service is being disabled or no longer exists. This error can occur if a client attempts to use the service farm while the appliance administrator is disabling the service farm.

Action: Verify that the ICAP service farm contains a service. If the ICAP service farm contains a service and the problem occurs when the service configuration is not being changed, contact NetApp Technical Support.

INVALID_HIT_ VERIFY

Message Text in Browser: The data was fetched from the server instead of from the appliance. No action is required.

Explanation: An error occurred while the appliance was attempting to verify whether a cached object had been modified since the last request. The request was processed as a miss, and the object was fetched from the origin server.

Action: No action is required.

INVALID_ OUTBOUND_PORT

Message Text in Browser: This port is not available because the administrator has restricted its use.

Explanation: If a port listed in the HTTP Proxy Ports option is also listed in the Outbound Ports option and someone tries to send a request to the port, this message appears.

Action: In the Appliance Manager, check the ports listed in the HTTP Proxy Ports option (Setup tab > HTTP > General) and the Outbound Ports option (Setup tab > Network > General). Remove any ports from the Outbound Ports option that are listed in the HTTP Proxy Ports option.

INVALID_TUNNEL_ PORT

Message Text in Browser: Tunneling is not allowed on this port. Contact your system administrator.

Explanation: The administrator has blocked the use of this port from requesting secure requests from clients.

Action: In the Appliance Manager, check both the Outbound Ports option (Setup tab > Network > General) and the HTTP-Based Tunneling ACL option (Setup tab > HTTP > Tunneling) to verify that the options are configured to block only the ports that you want blocked.

OBJECT_OPEN

Message Text in Browser: The requested object was refetched from the server because of an error. No action is required.

Explanation: An error occurred when the appliance tried to verify the object in the cache, for example, because the file was corrupted. The appliance refetched the object from the origin server and cached it.

Action: No action is required.

PARENT_NEEDED

Message Text in Browser: Unable to service this URL without a parent cache. Contact your system administrator.

Explanation: The HTTPS URL can be serviced only through a parent but no parent that can service HTTPS over HTTP has been configured in the hierarchy configuration on this appliance.

Action: Typically, nonappliance computers service HTTPS requests. To direct HTTPS requests to a computer that can service HTTPS requests, you configure a hierarchy with a computer that can service HTTPS as a parent. You must then create a hierarchy rule that enables the appliance to send HTTPS requests to the parent. When you configure the hierarchy rule, include the following in your rule specifications:

Protocol: HTTP

Phrase: Beginning of URL equals https

Distribution method: Single host <select parent name>

To access the hierarchy configuration pages, select Setup tab > Hierarchies in the Appliance Manager.

PRECONDITION_FAILED

Message Text in Browser: Precondition failed.

Explanation: The HTTP request sent by the browser included a precondition specification, which the Web server detected as not met. This error indicates a serious problem with the Web server.

Action: Contact the Web server system administrator.

RESOURCE_ RECLAIMED

Message Text in Browser: Internal error. Try again.

Explanation: The most common cause of this error is that the appliance has too much load.

Action: If this error occurs frequently, consider purchasing an additional appliance.

RESP_AFTER_100_ CONTINUE_ MISSING

Message Text in Browser: The server response does not comply with HTTP 1.1 specifications. The final status code following a 100-continue response is missing. Contact your system administrator.

Explanation: The server sent the HTTP 1.1 100-Continue response but failed to send the final status code, such as 200 OK or 500 Server Error. HTTP 1.1 specifications require a final status code.

Action: Contact the Web server administrator to determine why the server is not responding according to HTTP 1.1 specifications.

SERVER_CLOSE

Message Text in Browser: The server closed the connection. Contact your system administrator.

Explanation: For some reason, the origin server closed the connection to the appliance.

Action: Verify the network connectivity.

SERVER_REQUEST_ _WRITE_REQUEST

Message Text in Browser: Request could not be sent to the server. Contact your system administrator.

Explanation: Typically, this problem is caused by a networking problem that prevents the appliance from successfully sending an HTTP request to a Web server. Rarely, this problem is caused by the server closing the connection immediately after it accepts the HTTP request from the appliance.

Action: Try the following:

- ◆ Check the network connections.
- ◆ Contact the server administrator.

SERVER_RESP_ERROR

Message Text in Browser: The server response could not be recognized or accepted. Contact your system administrator.

Explanation: A common cause of this message is that the appliance received a response from the origin server that it could not recognize because the response does not follow standard HTTP format. The most likely cause is a problem on the server.

Action: Reissue the request and take a packet trace. Then Contact NetApp Technical Support. To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.

SERVER_RESPONSE_CLOSE

Message Text in Browser: The server closed the connection while reading the response. Contact your system administrator.

Explanation: An error occurred and the origin server closed the connection to the appliance. This error could have been caused by a networking problem, or the server could have become unavailable.

Action: Try the following:

- ◆ Verify the network connectivity.
- ◆ Contact the server administrator to determine if the server is available.

SERVER_RESPONSE_RESET

Message Text in Browser: The server response could not be read because of an error. Contact your system administrator.

Explanation: An error occurred while the appliance was reading a response from the origin server. This error could have been caused by a networking problem, or the server could have become unavailable.

Action: Try the following:

- ◆ Verify the network connectivity.
- ◆ Contact the server administrator to determine if the server is available.

**SERVER_
TRANSPORT**

Message Text in Browser: A server transport error occurred. Contact your system administrator.

Explanation: An error occurred while the origin server was either reading or writing data.

Action: Verify the network connectivity.

SERVER_WRITE

Message Text in Browser: Data could not be sent to the server because of a network or server problem. Contact your system administrator.

Explanation: The appliance encountered an error while attempting to write to the origin server.

Action: Try the following:

- ◆ Verify the network connectivity.
- ◆ Contact the server administrator to determine if the server is available.

**TUNNEL_DESTIP_
SELF**

Message Text in Browser: Attempt to establish tunnel from appliance to itself

Explanation: An error in the HTTP protocol tunneling feature configuration is causing looping problem with the appliance. For example, assume that the Mapping for Protocol Tunneling option was configured as * 81 * 80. With this configuration, all traffic destined for port 81 on the appliance would be transparently picked up and redirected to port 80. The appliance connects back to itself at port 80 and the connection is dropped by port 80.

Action: Try the following:

- ◆ Check the Mapping for Protocol Tunneling option setting (Setup tab > Network > Protocol Tunneling in the Appliance Manager) to ensure that you have not misconfigured the option.
- ◆ If changing the value of the Mapping for Protocol Tunneling option does not solve the problem, take a packet trace and contact NetApp Technical Support.

**UNRECOGNIZED_
REQUEST**

Message Text in Browser: The browser is sending an invalid request. Contact your system administrator.

Explanation: The appliance could not recognize the request because it does not conform to HTTP format. This problem is most likely due to a browser bug.

Action: Reissue the request and take a packet trace. A packet trace can help you verify the type of request. Then Contact NetApp Technical Support. To take a packet trace, select Utilities tab > Diagnostics > Packet Trace in the Appliance Manager.

About this chapter This chapter provides information about optional Web accelerator logs.

Topic in this chapter This chapter contains the following topic:
◆ “About Web server acceleration logs” on page 52

About Web server acceleration logs

Description of Web server acceleration logs

By default, Web server acceleration transactions are logged in the Web access log. However, you can log Web server acceleration transactions separately in one or more Web server acceleration logs. A Web server acceleration log reports transactions between the appliance configured as an accelerator and one or more Web servers that it accelerates, depending on how you have configured your Web (HTTP) accelerator rules.

When to use a Web server acceleration log

Use Web server acceleration logs when you want to log Web server transactions separately. You can log transactions in the same log for all customers for which you provide acceleration services or for each customer separately.

Log headers

The headers in the Web server acceleration logs are the same as the headers in the Web access log. The settings for the headers to be used in the Web access log are also used for Web server acceleration logs. See “Web access log headers” on page 4 for details.

About this chapter

This chapter describes the FTP transfer access log. The FTP transfer access log records the details of FTP proxy transactions on the appliance.

Topic in this chapter

This chapter contains the following topic:

- ◆ “FTP transfer access log headers” on page 54

FTP transfer access log headers

Description of headers

The following table lists the log file headers that are specific to the FTP transfer access log. These log file headers are preset and cannot be modified.

Log Header	Description
access-mode	The method by which the user is logged in. a — Indicates an anonymous guest user. r — Indicates a “real” user with a regular account on the FTP server. NetCache assumes that a non-anonymous user is a regular account user.
authenticated-user-id	The user ID returned by the authentication method. NetCache always logs a * character (indicating not available) for the authenticated user ID field.
authentication-method	The authentication method used. NetCache always logs a 0 (none) for the authentication method field.
completion-status	A single character indicating the status of the transfer. c — Indicates a complete transfer. i — Indicates an incomplete transfer. Any transmission error during the FTP session causes NetCache to log an “i” for this field.

Log Header	Description
current-time	The current local time in the form: DDD MMM dd hh:mm:ss YYYY Where: DDD is the day of the week. MMM is the month. dd is the day of the month. hh is the hour. mm is the minutes. ss is the seconds. YYYY is the year.
direction	The direction of the transfer. o — Indicates outgoing. i — Indicates incoming.
file-size	The size of the transferred file in bytes.
filename	The name of the transferred file.
remote-host	The name of the remote host.
service-name	The name of the service being invoked, usually FTP.
special-action-flag	Special actions taken. NetCache always log an underscore character (_) for this field, indicating that no special action was taken.
transfer-time	The total time in seconds for the transfer.
transfer-type	A single character indicating the type of transfer. a — Indicates an ASCII transfer. b — Indicates a binary transfer.
username	The name of the local user, or if a guest, the ID string provided.

About this chapter

This chapter describes the Streaming access log and the Streaming details log and provides details about the data that can appear in the header fields of the logs. See also Chapter 6, “x-status Header Entries (Streaming Access Log),” on page 83, which provides a reference to each error message that can appear in the x-status header field of the Streaming access log.

Topics in this chapter

This chapter contains the following topics:

- ◆ Section A, “Streaming access log,” on page 58
- ◆ Section B, “Streaming details log,” on page 66
- ◆ Section C, “Information applicable to both streaming logs,” on page 75

Section A: Streaming access log

About this section

This section describes the Streaming access log and provides details about the data that can appear in the header fields in the Streaming access log. See also, Section C, “Information applicable to both streaming logs,” on page 75 and Chapter 6, “x-status Header Entries (Streaming Access Log),” on page 83.

Topics in this section

This section contains the following topics:

- ◆ “About the Streaming access log” on page 59
- ◆ “Streaming access log headers” on page 61
- ◆ “sc-status header codes in the Streaming access log” on page 65

About the Streaming access log

Description of the Streaming access log

The Streaming access log records client and server information for streaming media connections. Each log entry contains specific connection information you can use to diagnose and solve problems, optimize performance, and track usage patterns.

When client information is logged

No client information is reported in the streaming access log until the client has closed the connection. Therefore, no Streaming access log entries appear for clients that are still connected.

RTSP connections close whenever the client clicks Stop on the media player, whereas MMS connections close only when the client closes the media player or selects a new stream.

Note

The Streaming details log provides statistics for clients with active streaming connections.

Use the Streaming access log if you want to do any of the following:

- ◆ Diagnose connection problems
- ◆ Determine the identity of clients
- ◆ Determine the frequency of client connections
- ◆ Track content served
- ◆ Identify error messages sent by the client and server
- ◆ Track bandwidth per connection
- ◆ Determine peak load times
- ◆ Determine which streaming protocols are used most often
- ◆ Determine which streaming products (WMT, RealNetworks G2, and QuickTime) are used most often

**Excerpt from a
Streaming access
log**

The following is an excerpt from a Streaming access log (custom format):

```
10.34.26.6 2000-09-06 18:27:21 205.188.237.217
rtsp://205.188.237.217:7071/demand/nearkiss176.rm 200 - CACHE 1 0 0
0 0 5 0 RTSP UDP REAL-G2 1

10.34.26.6 2000-09-06 18:27:22 205.188.238.57
rtsp://205.188.238.57:7071/demand/nearkiss176.rm 461
CLIENT_UDP_CONNECT_FAILED(203015.2) CACHE 2 0 0 0 0 1 0 RTSP TCP
REAL-G2 2

10.34.26.6 2000-09-06 18:28:21 205.188.238.57
rtsp://205.188.238.57:7071/demand/nearkiss176.rm 200 - CACHE 3
343142 704 0 0 34 33 RTSP UDP REAL-G2 3

10.34.26.6 2000-09-06 18:28:46 205.188.237.185
rtsp://205.188.237.185:7071 200 - CONNECTING 4 0 0 0 0 0 - RTSP TCP
REAL-G2 4

10.34.26.6 2000-09-06 18:29:07 205.188.237.185
rtsp://205.188.237.185:7071/adtag/general/live/bblive3_player.smi
200 - CACHE 5 629 2 0 0 21 18 RTSP UDP REAL-G2 5

10.34.26.6 2000-09-06 18:29:07 205.188.238.25
rtsp://bb1.stream.aol.com:7071/farm/*/encoder/bblive3.rm 200 -
SPLIT 6 86685 210 0 0 17 15 RTSP UDP REAL-G2 6

...
```

Streaming access log headers

Description of headers

The following table shows the headers that can appear in the Streaming access log. The default log format includes a specific set of headers that appear in a specific order. If you want headers in addition to those provided by the default format, or if you want the headers to appear in an order different than the order provided by the default format, you can configure your log headers using the custom log format.

Header	Description	Default format	Custom format
avgbandwidth	Average bandwidth in bytes per second	—	X
bytes	Total number of bytes NetCache delivered to the client	X	X
c-cpu	Client CPU type, for example, Pentium II	—	X
c-dns	Client's fully qualified domain name (FQDN) Reporting the FQDN can result in a performance penalty because of the latency associated with the DNS lookup.	—	X
c-ip	Client IP address	X	X
c-os	Client operating system, for example, Windows	—	X
c-osversion	Client operating system version, for example, 98	—	X
c-playerversion	Client media player version, for example, RealPlayer	—	X
cs-uri	Streaming URL, for example: rtsp://abc/hello.rm?"there"	X	X
cs-uri-query	Query portion of URL (the portion after the "?" in the URL), for example: rtsp://abc/hello.rm?"there"	—	X

Header	Description	Default format	Custom format
cs-uri-stem	Stem portion of URL, for example: rtsp://abc/hello.rm	—	X
cs(User-Agent)	Logs the information contained in the request header field that the client delivered to the appliance. This header functions as a wildcard. You can replace the header in parentheses, User-Agent in this case, with any header.	—	X
date	GMT date when the transaction ended, in YYYY-MMM-DD format	X	X
filelength	Length of the stream, in seconds	—	X
r-dns	Origin server's fully qualified domain name	—	X
r-ip	Origin server IP address	X	X
sc-status	HTTP-like status code for connection, for example: 200 or 404 (means success) See “sc-status header codes in the Streaming access log” on page 65 for details about specific MMS and RTSP sc-status codes	X	X
time	GMT time when the client connection ended, in HH:MM:SS format. Indicates the client disconnection time	X	X
x-action	The action performed by NetCache, for example: SPLIT, PROXY, CACHE, CONNECTING See “x-action header codes (Streaming logs)” on page 76 and “x-action header values for pushed content” on page 80 for more details.	X	X

Header	Description	Default format	Custom format
x-assignment	An unsigned 64-bit number for the content push transaction. If multiple SM_PUSH and SM_EJECT log entries with the same assignment appear in the log and they are committed, an SM_COMMIT with the same assignment appears. x-assignment is analogous to an SM_ABORT.	—	X
x-client-id	Unique client-side stream identifier used to correlate the Streaming access log and Streaming details log entries pertaining to that client stream	X	X
x-client-port	Client-side port number of the client connection	X	X
x-connect-time	Total time the client was connected (in seconds)	X	X
x-dropped-bytes	Total number of bytes dropped because the client was slow	X	X
x-dropped-packets	Total number of packets dropped because the client was slow	X	X
x-hiercode	NetCache hierarchy code/peer IP address. See “x-hiercode header entries” on page 21.	—	X
x-localtime	NetCache local time, in DD/MMM/YYYY:HH:MM:SS GGGG format (where GGGG is the time differential from GMT)	—	X
x-packets	Total number of packets NetCache delivered to the client	X	X
x-play-time	Total duration of time the client received content (in seconds)	X	X

Header	Description	Default format	Custom format
x-product	Streaming product used to create and stream content	X	X
x-protocol	Protocol used during the connection	X	X
x-requested-packets	Total number of packets the client requested for retransmission	—	X
x-resent-packets	Total number of packets NetCache resent to the client	—	X
x-status	NetCache-specific error code for sc-status code, for example: DNS_HOST_NOT_FOUND See Chapter 6, “x-status Header Entries (Streaming Access Log),” on page 83.	X	X
x-stream-id	Unique server-side stream identifier used to correlate the Streaming access log and Streaming details log entries pertaining to that server stream	X	X
x-timestamp	Number of seconds since the UNIX epoch—January 1, 1970; for example: 963873698.73 Indicates the client disconnection time	—	X
x-transport	Data transport protocol used during the connection	X	X
x-username	User name given for proxy authenticated requests	—	X

sc-status header codes in the Streaming access log

About the additional codes for RTSP

The Streaming access log reports status codes for both MMS and RTSP protocols. Both MMS and RTSP use the same status codes as those used in HTTP 1.1. However, RTSP has additional status codes specific to RTSP connections.

RTSP-specific status codes

The following table shows the RTSP-specific status codes for the sc-status field. The RTSP-specific status codes start at X50 (where X is an integer).

Status code	Explanation
451	Parameter not understood
452	Conference not found
453	Not enough bandwidth
454	Session not found
455	Method not valid in this state
456	Header field not valid for resource
457	Invalid range
458	Parameter is read-only
459	Aggregate operation not allowed
460	Only aggregate operation allowed
461	Unsupported transport
462	Destination unreachable
551	Option not supported

Section B: Streaming details log

About this section

This section describes the Streaming details log and provides details about the data that can appear in the header fields in the Streaming access log. See also, Section C, “Information applicable to both streaming logs,” on page 75.

Topics in this section

This section contains the following topics:

- ◆ “About the Streaming details log” on page 67
- ◆ “Streaming details log headers” on page 68
- ◆ “x-transaction codes in the Streaming details log” on page 72

About the Streaming details log

Description of the Streaming details log

The Streaming details log provides statistics for clients with active streaming connections. It records the internal transactions initiated by NetCache and the client during a streaming connection. Internal transactions reported by the Streaming details log can include statistics for partial object hits and misses, prefetched objects, proxied objects, and objects served from disk.

When to use the Streaming details log

Use the Streaming details log to gather information about how clients are accessing the cache and how NetCache is storing and retrieving objects, and to determine which portions of streams are most frequently accessed.

Excerpt from a Streaming details log

The following is an excerpt from a Streaming details log (default format):

```
rtsp://205.188.237.217:7071/demand/nearkiss176.rm 1 1 2000-09-06
18:27:21 CLIENT_DATA 0 0 0 0

rtsp://205.188.238.57:7071/demand/nearkiss176.rm 3 3 2000-09-06
18:28:21 SERVER_DATA_CACHE_MISS 10000 35508 286538 587

rtsp://205.188.238.57:7071/demand/nearkiss176.rm 3 3 2000-09-06
18:28:21 CLIENT_DATA 0 35508 343142 704

rtsp://205.188.237.185:7071/adtag/general/live/bblive3_player.smi
5 5 2000-09-06 18:29:07 CLIENT_DATA 0 0 629 2

rtsp://bb1.stream.aol.com:7071/farm/*/encoder/bblive3.rm 6 6 2000-
09-06 18:29:07 CLIENT_DATA 2922 17953 86685 210

rtsp://bb1.stream.aol.com:7071/farm/*/encoder/bblive3.rm 6 6 2000-
09-06 18:29:08 SERVER_DATA_PRIVATE_LIVE 3093 18337 90086 215

...
```

Streaming details log headers

Description of Streaming details log headers

The following table shows the headers that can appear in the Streaming details log. The default log format includes a specific set of headers that appear in a specific order. If you want headers in addition to those provided by the default format, or if you want the headers to appear in an order different than the order provided by the default format, you can configure your log headers using the custom log format. The order of the headers for the default log format is shown on the Streaming - Logging page in the Appliance Manager (Setup tab > Streaming > Logging).

Header	Description	Default format	Custom format
avgbandwidth	Average bandwidth in bytes per second	—	X
bytes	Total number of bytes NetCache delivered to the client	X	X
c-cpu	Client CPU type, for example, Pentium II	—	X
c-dns	Client's fully qualified domain name (FQDN) Reporting the FQDN can result in a performance penalty because of the latency associated with the DNS lookup.	—	X
c-ip	Client IP address	—	X
c-os	Client operating system, for example, Windows	—	X
c-osversion	Client operating system version, for example, 98	—	X
c-playerversion	Client media player version, for example, RealPlayer	—	X
cs-uri	Streaming URL accessed, for example, rtsp://abc/hello.rm?"there"	X	X

Header	Description	Default format	Custom format
cs-uri-query	Query portion of URL (the portion after the “?” in the URL), for example, rtsp://abc/hello.rm?"there"	—	X
cs-uri-stem	Stem portion of URL, for example: rtsp://abc/hello.rm	—	X
cs(User-Agent)	Logs the information contained in the request header field that the client delivered to the appliance. This header functions as a wildcard. You can replace the header in parentheses, User-Agent in this case, with any header.	—	X
date	GMT date when the transaction ended, in YYYY-MMM-DD format	X	X
filelength	Length of the stream, in seconds	—	X
r-dns	Origin server’s fully qualified domain name	—	X
r-ip	Origin server’s IP address	—	X
sc-status	HTTP response code that NetCache returned to the client, for example, 401 Details of sc-status header codes	—	X
time	GMT time when the transaction ended, in HH:MM:SS format	X	X
x-action	Action performed by NetCache: SPLIT, PROXY, CACHE, CONNECTING See “x-action header codes (Streaming logs)” on page 76 and “x-action header values for pushed content” on page 80 for details.	—	X
x-client-id	Unique client-side stream identifier used to correlate all of the log entries pertaining to that client stream	X	X
x-client-port	Client-side port number of the client connection	—	X

Header	Description	Default format	Custom format
x-clip-end	Number of milliseconds into the stream (relative to the beginning of the media file, which is millisecond 0) where the client stopped receiving the stream	X	X
x-clip-start	Number of milliseconds into the stream (relative to the beginning of the media file, which is millisecond 0) where the client started receiving the stream	X	X
x-connect-time	Total time the client was connected	—	X
x-dropped-bytes	Total number of bytes dropped between NetCache and the client	—	X
x-dropped-packets	Total number of packets dropped between NetCache and the client	—	X
x-hiercode	NetCache hierarchy code/peer IP address See “x-hiercode header entries” on page 21.	—	X
x-localtime	NetCache local time DD/MMM/YYYY:HH:MM:SS GGGG format (where GGGG is the time differential from GMT)	—	X
x-packets	Total number of packets NetCache delivered to the client	X	X
x-play-time	Total duration of time the client received content	—	X
x-product	Streaming product used to create and stream content	—	X
x-protocol	Protocol used during the connection	—	X
x-requested-packets	Total number of packets the client requested	—	X
x-resent-packets	Total number of packets NetCache resent to the client	—	X

Header	Description	Default format	Custom format
x-status	NetCache-specific error code for sc-status code, for example, DNS_TIMEOUT	—	X
x-stream-id	Unique server-side stream identifier used to correlate the Streaming access log and Streaming details log entries pertaining to that server stream	X	X
x-timestamp	Number of seconds since the UNIX epoch—January 1, 1970, for example, 963873698.73 This field indicates when the transaction ended.	—	X
x-transaction	Streaming transaction code, for example, CLIENT_DATA_FROM_DISK See “x-transaction codes in the Streaming details log” on page 72 for details.	X	X
x-transport	Transport protocol used during the connection. The possible values for x-transport are HTTP, TCP, UDP, MCAST (multicast). These values are applicable to both client-side and server-side cases of x-transport.	—	X
x-username	User name given for proxy authenticated requests In the Streaming details log, the x-username field logs the user name of the client on whose behalf NetCache initiated the origin server connection. For clients receiving content from split connections, the x-username field logs the user name of the client who initiated the origin server connection that NetCache split from.	—	X

x-transaction codes in the Streaming details log

Possible values in the x-transaction codes field

The following table shows the possible values for the x-transaction field in the Streaming details log. If transaction codes other than those in the following table are displayed in the x-transaction field, contact Network Appliance Technical Support.

Note _____
Bit-rate numbers, in kilobits per second, might be appended to the transaction codes listed in the following table (for example SERVER_DATA_CREATE_FAILED_256k). These numbers indicate the bit rate at which the streaming data was configured to download to the client.

Transaction code	Explanation
CLIENT_DATA	Streaming data was sent to the client from an active server connection.
CLIENT_DATA_FROM_DISK	Streaming data was sent to the client from disk; the object was either a HIT or a prefetched MISS.
SERVER_DATA_ The SERVER_DATA_ prefix indicates that streaming data was fetched from the origin server and cached in response to a client streaming request. The following transaction code combinations are associated with this prefix.	
SERVER_DATA_CACHE_MISS	Streaming data was fetched from the origin server in response to a cache miss on the appliance.
SERVER_DATA_CREATE_FAILED	Streaming data might have been fetched before but had to be refetched because a cache object could not be created.
SERVER_DATA_DISK_READ_FAILED	Streaming data might have been fetched before but had to be refetched because of I/O failure on the cache disks.
SERVER_DATA_DISK_WRITE_FAILED	Streaming data might have been fetched before but had to be refetched because of I/O failure on the cache disks.
SERVER_DATA_OPEN_FAILED	Streaming data was refetched because its cache object could not be opened.

Transaction code	Explanation
SERVER_DATA_ LOW_MEMORY	Streaming data was fetched or refetched but not cached because of low available memory.
SERVER_DATA_ PRIVATE_CLIP_FRAG	Denotes data that could not be saved to disk because the client began playing in the middle of an object.
SERVER_DATA_ PRIVATE_FETCHING	Streaming data is already being downloaded to the cache in response to a request from another client. Because the data is already being fetched and cached by another client request, data is not cached twice.
SERVER_DATA_PRIVATE_HTTP	This code applies to QuickTime content only. The stream could not be cached because the appliance used RTSP over HTTP to reach the origin server. The QuickTime HTTP server will drop large amounts of packets without informing the client. Therefore, the appliance cannot depend on the validity of the data for caching.
SERVER_DATA_ PRIVATE_LIVE	Live content fetched from the origin server. The content was not cached because it is live.
SERVER_DATA_ PRIVATE_ON_STOP_LIST	The stream was proxied to the client because an ACL rule required it, or because it was blocked from being cached by the following streaming cacheability substring option: (config.streaming.cacheability.substring)
SERVER_DATA_ PRIVATE_OUTOFSEQ	The content was uncacheable due to packet loss that occurred between the appliance and the streaming server.
SERVER_DATA_ PRIVATE_PREROLL	The appliance requested a specific portion of a stream from the origin server, but the origin server sent extra data that the appliance and the client did not need.
SERVER_DATA_ PRIVATE_PROXY	Specifies content that must be proxied (such as QuickTime on-demand streams).
SERVER_DATA_ PRIVATE_SWITCHING	The client switched bit rates before that portion of the object could be cached, causing a false MISS.
SERVER_DATA_ PROXY_MODE	The appliance was in startup mode. No fetch was executed.

Transaction code	Explanation
SERVER_DATA_PREFETCH_ The SERVER_DATA_PREFETCH prefix indicates that streaming data was fetched from the origin server and cached in anticipation of a client request. (The streaming object initially requested was in the cache, but subsequent parts of the object had to be fetched.) The following transaction code combinations are associated with this prefix.	
SERVER_DATA_PREFETCH_ BAD_DATA	Prefetch operation encountered bad data, so streaming data was refetched from the origin server.
SERVER_DATA_PREFETCH_ CACHE_MISS	Streaming data was prefetched from the origin server because it was not yet cached.
SERVER_DATA_PREFETCH_ CREATE_FAILED	Streaming data might have been prefetched before but had to be refetched because a cache object could not be created.
SERVER_DATA_PREFETCH_ DISK_READ_FAILED	Streaming data might have been prefetched before but had to be refetched because of I/O failure on the cache disks.
SERVER_DATA_PREFETCH_ DISK_WRITE_FAILED	Streaming data might have been prefetched before but had to be refetched because of I/O failure on the cache disks.
SERVER_DATA_PREFETCH_ OPEN_FAILED	Streaming data might have been prefetched before but had to be refetched because its cache object could not be opened.
SERVER_DATA_PREFETCH_ LOW_MEMORY	Streaming data might have been prefetched before but had to be refetched because low memory will not allow caching of this data.
SERVER_DATA_PREFETCH_ PRIVATE_FETCHING	Streaming data is already being downloaded to the cache in response to a request from another client. Because the data is already being fetched and cached by another client request, a second cache will not be maintained after the client is finished with it.
SERVER_DATA_PREFETCH_ PROXY_MODE	The appliance was in startup mode. No prefetch was executed.
SERVER_VERIFY	The appliance contacted the origin server to check the freshness of the stream.

Section C: Information applicable to both streaming logs

About this section

Information in this section applies to both the Streaming access and Streaming details logs.

Topics in this section

This section contains the following topics:

- ◆ “x-action header codes (Streaming logs)” on page 76
- ◆ “x-action header values for pushed content” on page 80

x-action header codes (Streaming logs)

About the x-action header field

The x-action log field shows what action NetCache performed on the streaming media content. Valid entries for this field are CACHE, CONNECTING, PROXY, and SPLIT.

CACHE

NetCache recognized the streaming media URL as on-demand content and cached its contents to disk for playback to future clients.

CONNECTING

NetCache is connecting upstream to retrieve this streaming media URL. Log entries with a CONNECTING x-action value typically mean that the client disconnected before any streaming began.

PROXY

NetCache will usually try to split live streams and cache on-demand streams. For streams where splitting or caching is not possible, NetCache will simply proxy the stream without splitting or caching the content. In the Streaming access log, "PROXY(<reason>.<internal_code>)" will be logged in the "x-action" field, where <reason> is a code describing why NetCache chose to proxy the stream.

- ◆ ACL

The streaming media URL matched an ACL rule (for example, config.streaming.acl) containing a "proxy" action. In the "x-action" field of the streaming access log, NetCache will include the text of the matched ACL rule instead of simply logging "ACL"; for example: PROXY(proxy rtsp).

- ◆ AUTHENTICATED

The streaming media origin server required authentication; NetCache does not split or cache certain authenticated streams.

- ◆ CACHE_HOST

The streaming media URL matched a hierarchy rule (use the "hier_config" command to set config.hierarchy.rulelist) specifying that the content be proxied.

- ◆ CLIENT_PROTOCOL_ERROR

The streaming media client software violated the RTSP protocol in some way.

- ◆ **MIN_AGE_NOT_ELAPSED**
The streaming media URL represents content locked in the cache whose Min-Age value has not yet elapsed.
- ◆ **MULTICAST**
The streaming media player requested multicast transport. However, NetCache is not configured for client-side multicast (config.streaming.multicast.output.enable) or NetCache is receiving the stream through multicast from an origin server but is not configured for multicast tunneling (config.streaming.multicast.tunnel.enable).
- ◆ **NOT_LICENSED**
NetCache does not have the appropriate license to support splitting or caching the stream. Contact Network Appliance to receive the appropriate license.
- ◆ **NO_ASM_RULES**
The Real stream does not contain any rules in its ASMRuleBook. This is a problem with the content on the streaming media origin server.
- ◆ **NO_CONTENT_BASE**
The RTSP DESCRIBE response from the streaming media server did not contain a "Content-Base" header. This is a problem with the streaming media origin server.
- ◆ **NO_RTP_BASE_TIME**
The RTP-Info header in the RTSP PLAY response did not contain an "rtpptime" value. This is a problem with the streaming media origin server.
- ◆ **NO_RTP_CLOCK_RATE**
The session description provided by the streaming media origin server did not contain an RTP clock rate in its rtpmap attribute.
- ◆ **NO_SDP_AVERAGE_BITRATE**
The session description provided by the streaming media origin server did not contain an AvgBitrate attribute.
- ◆ **NO_SDP_MEDIA**
The session description provided by the streaming media origin server did not contain the expected number of media descriptions.
- ◆ **NO_SDP_STREAM_COUNT**
The session description provided by the streaming media origin server did not contain a StreamCount attribute.
- ◆ **ON_STOP_LIST**
The streaming media URL contained one of the substrings in config.streaming.cacheability.substring.

- ◆ **SERVER_NOCACHE**
The streaming media origin server was configured to mark the streaming media URL as uncacheable. The streaming media origin server must be configured appropriately to allow NetCache to split or cache its content.
- ◆ **SERVER_NOCACHE_NOMEI**
The streaming media origin server was configured to mark the streaming media URL as uncacheable. The streaming media origin server must be configured appropriately to allow NetCache to split or cache its content.
- ◆ **SERVER_PROTOCOL_ERROR**
The streaming media origin server software violated the RTSP protocol in some way.
- ◆ **TOO_MANY_ASM_RULES**
The ASMRuleBook in the session description provided by the streaming media origin server specified a number of rules greater than the NetCache limit (63 ASM Rules).
- ◆ **TOO_MANY_TRACKS**
The session description provided by the streaming media origin server specified a number of media tracks greater than the NetCache limit for that media type.
- ◆ **UNKNOWN_SDP**
The session description provided by the streaming media origin server was unrecognized by NetCache.
- ◆ **UNSUPPORTED_ASM_RULEBOOK**
The ASMRuleBook in the session description provided by the streaming media origin server was unrecognized by NetCache.
- ◆ **UNSUPPORTED_CONTENT**
The streaming media URL contains a data type unrecognized by NetCache.
- ◆ **UNSUPPORTED_MEDIA_FORMAT**
The session description provided by the streaming media origin server contained a media description unrecognized by NetCache.
- ◆ **UNSUPPORTED_MEDIA_TYPE**
The session description provided by the streaming media origin server contained a media type unrecognized by NetCache.
- ◆ **UNSUPPORTED_PRODUCT**
The streaming media client software supplied an unrecognized User-Agent header.

- ◆ **UNSUPPORTED_TRANSPORT**
The streaming media client or server requested transports unrecognized by NetCache.
- ◆ **VALIDATE_FAILED**
NetCache was unable to validate whether or not the streaming media URL required authentication.

SPLIT

NetCache recognized the streaming media URL as live content and split the upstream connection's streaming media data to one or more downstream clients viewing the same URL.

x-action header values for pushed content

About the x-action values for pushed content

The x-action header values in the Streaming logs for pushed content (particularly for content pushed with the ContentDirector(TM) software involve transmission and verification of the push transaction. The term "two-phase commit" is used in the following table to describe this process.

A two-phase commit is a content push consisting of the following necessary actions:

- ◆ The content is pushed to (or ejected from) NetCache in one or more messages. Each message corresponds to a PUSH_TWO_PHASE (pushed content) or EJECT_TWO_PHASE (ejected content) x-action log value.
- ◆ The pushing agent sends a termination message indicating the status of the transaction. The termination message either directs NetCache to make the previously pushed content available (COMMIT) or indicates that NetCache should delete the files (ABORT).

For pushed content, the x-action header reports the following actions in the Streaming access log.

x-action	Explanation
ABORT	The transaction was aborted and the previously pushed content was deleted.
COMMIT	The previous TWO_PHASE transactions have been committed. Pushed content is now available in the cache. Ejected content is no longer available.
EJECT	Content was ejected from the cache. The content is no longer available.
EJECT_TWO_PHASE	The content was ejected from the cache as part of a larger transaction. The actual content is not ejected from the cache until the transaction is completed.

x-action	Explanation
PUSH	Content was pushed into the cache. That content is now available.
PUSH_TWO_PHASE	The content was pushed to the cache as part of a larger transaction. The actual content is not pushed to the cache until the transaction is completed.

About this chapter This chapter contains information about the entries that can appear in the x-status header field of the Streaming access log.

Topic in this chapter This chapter contains the following topic:

- ◆ “About MMS and RTSP errors in the x-status header” on page 84

About MMS and RTSP errors in the x-status header

Purpose of the x-status log field

The x-status header log field describes the termination state of a client's streaming session.

ALERT

Explanation: The RTSP server sent a server alert message.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance Technical Support.

AUTH_DUPLICATE_GUID

Explanation: Two streaming clients using the same GUID attempted to view a stream with config.streaming.auth.one_guid_per_user enabled on NetCache.

AUTH_USER_CONNECTION_LIMIT

Explanation: The number of users logged in with the same credentials has exceeded the limit set in the config.streaming.auth.max_connections_per_user configuration option.

BADCACHEFILEFOR MAT

Explanation: NetCache detected corrupted VOD data on disk and will re-fetch the data from the origin server.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

BAD_FLAGS_ON_DATA

Explanation: NetCache received streaming data that it didn't understand.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

BAD_FUNNEL_IP	Explanation: NetCache received a malformed request from a streaming client. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
BAD_FUNNEL_NAME	Explanation: NetCache received a malformed request from a streaming client. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
BAD_FUNNEL_PORT	Explanation: NetCache received a malformed request from a streaming client. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
BAD_MSG_FMT	Explanation: NetCache received a malformed packet from a streaming client or streaming server. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
BAD_PLAY_RANGE	Explanation: NetCache did not understand the PLAY request sent by the RTSP client. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
BAD_PLAY_RTP_INFO	Explanation: The RTSP server's response to a PLAY request was malformed. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

BAD_READBLOCK	Explanation: NetCache detected a malformed packet during stream setup. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
BAD_REAL_CHALLENGE1	Explanation: The RealServer streaming server sent an unexpected value in the RealChallenge1 header. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
BAD_REAL_CHALLENGE2	Explanation: RealPlayer sent an unexpected value in the RealChallenge2 header. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
BAD_REAL_CHALLENGE3	Explanation: RealPlayer sent an unexpected value in the RealChallenge3 header. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
BAD_RTSP_VERSION	Explanation: An RTSP client or server send a request or response containing an unsupported RTSP version. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

BAD_SDP_CONTENT	Explanation: NetCache did not understand the session description sent by the RTSP server. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
BAD_SDP_CONTENT_LENGTH	Explanation: The RTSP server sent a negative Content-Length value. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
BAD_STREAM_SELECT	Explanation: An error occurred in the stream subscription list sent by the RealPlayer. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
BAD_URL_PORT	Explanation: The RTSP URL contained a connection request to a port outside the range 1-65535. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
BAD_URL_SCHEME	Explanation: The streaming client sent an unsupported URL scheme. Action: Configure the streaming client to send a valid URL.
CACHE_READ	Explanation: An error occurred while reading a streaming object from disk. Action: Attempt to run the stream through NetCache again and see if the problem repeats itself.

CACHE_WRITE

Explanation: An error occurred while writing a streaming object to disk.

Action: Attempt to run the stream through NetCache again and see if the problem repeats itself.

CANT_CONNECT

Explanation: NetCache failed to open a TCP connection to the streaming media server.

Action: Verify that the NetCache appliance network settings are functioning properly and try to run the stream again. If the problem persists, contact the streaming media server administrator.

**CAPACITY_
REACHED**

Explanation: NetCache refused the client connection because a bandwidth, licensing, or configuration limit was reached.

Action: Verify that the appropriate streaming licenses are installed, that bandwidth limitation rules and connection limits (config.mms.max_connections, config.rtsp.*.max_connection) are configured appropriately.

**CLIENT_
DISCONNECTED**

Explanation: The connection between NetCache and the streaming client was terminated.

Action: Verify end-user behavior and network connectivity.

**CLIENT_
EXPECTED_OPEN**

Explanation: NetCache received an unexpected response from a streaming server during stream setup.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**CLIENT_HTTP_
PNA**

Explanation: NetCache proxied a Real client using the legacy PNA protocol.

**CLIENT_MCAST_
CONNECT_FAILED**

Explanation: NetCache failed to set up a multicast channel for streaming to clients.

Action: Double-check the network configuration and try again.

CLIENT_READ

Explanation: An error occurred while performing a network read from the client.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**CLIENT_RTCP_
CONNECT_FAILED**

Explanation: A transient error occurred while NetCache accepted a client connection.

Action: Wait a few minutes and have the client try to connect again.

**CLIENT_RTCP_
SOCKET_FAILED**

Explanation: A transient error occurred while NetCache accepted a client connection.

Action: Wait a few minutes and try to connect again.

**CLIENT_
TIMEDOUT**

Explanation: A client connection timeout error occurred.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**CLIENT_UDP_
CONNECT_FAILED**

Explanation: A transient error occurred while NetCache accepted a client connection.

Action: Wait a few minutes and have the client try to connect again.

CLIENT_WRITE

Explanation: An error occurred while writing to the client.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**CONNECT_
ACCESS_DENIED**

Explanation: A NetCache access control list denied access to the RTSP client.

Action: Verify that the user has a valid user name and password. If the user is authorized, the user must be assigned to the group that has access to the streaming protocol. In the NetCache CLI, use the group command. In the Appliance Manager, select Setup tab > Authentication > NetCache Users.

DESCRIBE_FAILED

Explanation: The RTSP server did not respond to the DESCRIBE request.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**DNS_LOOKUP_
FAILED**

Explanation: NetCache failed to resolve the streaming server host name.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**EXPECTED_DATA_
MSG**

Explanation: NetCache received malformed data packets from a streaming server during stream setup.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**FILE_HEADER_
TOO_LARGE**

Explanation: NetCache received a malformed file header from a streaming server.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

FILE_NOT_FOUND	Explanation: NetCache failed to set up a stream with the streaming server. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
GRM_L7_REDIRECT	Explanation: This is an informational message that occurs as a result of normal operation of the GRM L7 server. A client was redirected to a GRM agent cache closer to the client. Action: None.
LOCK_ERROR	Explanation: NetCache system resources required to service a client were unavailable for an extended amount of time. Action: Have the client try again.
LOG_OPEN_ERROR	Explanation: NetCache encountered an error on the streaming server when it attempted to forward client logging information. Action: Verify the path name and file name on the streaming server.
MCAST_OUT_NO_MATCHING_STREAM	Explanation: NetCache received a stream which does not match any of the stream formats in the multicast metadata file. Action: Verify the failover unicast stream described in the multicast metadata file matches with one of the stream formats in the multicast metadata file.
MSG_TOO_LARGE	Explanation: NetCache received a malformed data packet from a streaming server. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**NO_CACHED_
STREAM**

Explanation: The streaming client switched to a stream that does not exist in the cache.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

NO_MEDIAINFO

Explanation: NetCache received an unexpected request from a streaming client.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**NO_RTSP_
VERSION**

Explanation: An RTSP request or response did not contain an RTSP version string.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

NO_STREAM

Explanation: NetCache was in an unexpected state while posting logging information to a streaming media logging server.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**NO_SUPPORTED_
TRANSPORTS**

Explanation: The streaming client selected a transport that is not supported by NetCache.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

NO_UDP

Explanation: NetCache ran out of system resources necessary to support UDP or multicast streaming to clients. This is most likely due to system load.

Action: Have the client try again later when the cache is under less load.

NO_URL

Explanation: The streaming client failed to supply a URL in its request.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

NSC_FILE_INIT_FAILED

Explanation: NetCache failed to set up a multicast Windows Media stream.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

OPEN_FAILED

Explanation: NetCache failed to set up a stream with the streaming server.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

PAUSE_FAILED

Explanation: A PAUSE request sent to the RTSP server caused an error.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

PLAY_ACCESS_DENIED

Explanation: The NetCache settings in the cacheability or the bandwidth management rule list denied access to this client.

Action: Verify that the streaming cacheability rules and bandwidth management rules are accurate. If necessary, change the rules to allow the client access.

- ◆ In the NetCache CLI: Use the [show | set] config.streaming.rulelist.cacheability command and the [show | set] config.ipfw.rules command.

- ◆ In the Appliance Manager: Select Setup tab > Streaming > Caching Behavior > Streaming Cacheability Rules option and Select Setup tab > Network > Bandwidth Allocation > Rules tab.

PLAY_BEFORE_SETUP

Explanation: The RTSP client issued a PLAY request before setting up a streaming session.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

PLAY_FAILED

Explanation: A PLAY request sent to the RTSP server caused an error.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

PORT_DENIED

Explanation: The NetCache outbound port settings prevented access to the port specified in the streaming URL.

Action: Verify the NetCache destination ports. If necessary, add the port. In the NetCache CLI, use the [show | set] config.system.outbound_ports command. In the Appliance Manager, select Setup tab > Network > General > Destination Ports option.

PROTOCOL_ERROR

Explanation: The RTSP client issued a bad RTSP request.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

READBLOCK_TIMEDOUT

Explanation: The origin server did not respond to NetCache requests for content in a timely manner.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

READ_MISMATCH	Explanation: NetCache received an unexpected RTSP request or RTSP response from a client or server. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
REDIRECT	Explanation: The client disconnected because of a server REDIRECT request. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
REQ_TOO_BIG	Explanation: An RTSP request or response was too large. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
RESTART	Explanation: While posting logging data, Net Cache failed to receive data from a Windows Media logging server. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
SDP_MEDIA_NO_URL	Explanation: An error occurred in the RTSP SDP response. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
SDP_NO_MEDIA	Explanation: An error occurred in the RTSP SDP response. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**SDP_
UNSUPPORTED_
MEDIA**

Explanation: The Session Description contained an unsupported media attribute.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**SDP_
UNSUPPORTED_
TRANSPORT**

Explanation: A Session Description media attribute named an unsupported transport.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**SERVER_BAD_
MCAST_ADDR**

Explanation: An origin server provided a bad multicast address.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**SERVER_BAD_
MCAST_PORT**

Explanation: An origin server provided a bad multicast port.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**SERVER_BAD_
MCAST_SRC_PORT**

Explanation: An origin server provided a bad multicast source port.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**SERVER_
CONNECTED_
FUNNEL_ERR**

Explanation: NetCache received a malformed packet from a streaming server during stream setup.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**SERVER_DATA_
TIMEDOUT**

Explanation: An origin server stopped sending streaming media data.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

SERVER_DIED

Explanation: The streaming media server is not responding to network requests.

Action: Contact the streaming media server administrator.

SERVER_EXITED

Explanation: For some reason, the connection to the origin server terminated.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**SERVER_
FUNNELINFO_ERR**

Explanation: NetCache received a malformed packet from a streaming server during stream setup.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**SERVER_HOST_
REWRITE_ERR**

Explanation: NetCache received a malformed request from a streaming client.

Action: Double-check any ASX rewrite settings on any other caches in the deployment and try again.

**SERVER_MCAST_
JOIN_FAILED**

Explanation: NetCache failed to join a multicast group for receiving multicast input from an origin server.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

SERVER_MISSING_MCAST_HEADER	Explanation: A streaming media server did not sent a complete set of Multicast headers: MulticastIP, MulticastSourcePort, MulticastPort. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
SERVER_READ	Explanation: An error occurred while performing a network read from the server. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
SERVER_TIMEDOUT	Explanation: The connection to the streaming server exceeded a timeout limit and NetCache aborted the connection. Action: Try streaming from the streaming server again. If the problem persists, the streaming server could be experiencing difficulties.
SERVER_WRITE	Explanation: An error occurred while performing a network write to the server. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
SESSION_READ	Explanation: A disk I/O error occurred. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
SESSION_WRITE	Explanation: A disk I/O error occurred. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

SETSTREAM_OPEN_ERROR	Explanation: NetCache received a malformed packet from a streaming server during stream setup. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
SETUP_BAD_SERVER_TRANSPORT	Explanation: The RTSP server selected a transport that is not supported by NetCache. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
SETUP_BEFORE_DESCRIBE	Explanation: An RTSP protocol error occurred. Attempt to run the stream without NetCache. Action: If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
SETUP_FAILED	Explanation: A SETUP request sent to the RTSP server caused an error. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
SETUP_INCOMPLETE	Explanation: An client issued a PLAY request before issuing a SETUP request for each track in the stream. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**SETUP_NO_
SUPPORTED_
TRANSPORTS**

Explanation: The streaming client selected a transport that is not supported by NetCache.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**SETUP_NO_
TRANSPORT**

Explanation: The SETUP request did not contain a transport header.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**SETUP_NO_
TRANSPORTS**

Explanation: The SETUP request did not contain any supported transports.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**SETUP_STREAM_
NOT_FOUND**

Explanation: An RTSP protocol error occurred.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**SETUP_TOO_MANY_
TRANSPORTS**

Explanation: The transport header in the SETUP request contains too many parameters.

Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

**STARTPLAY_OPEN_
ERROR**

Explanation: NetCache encountered an error on the streaming server when it attempted to open the file.

Action: Verify path and file name on the origin server.

STREAM_SWITCH_FAILED	Explanation: A stream switch request failed. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
TOO_MANY_MEDIA_TRACKS	Explanation: The RTSP stream contained too many media tracks for NetCache to handle. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
TOO_MANY_SESSIONS	Explanation: A single RTSP client tried to open more than 128 concurrent streams. This is not allowed and might indicate a denial of service attack.
UNAUTHORIZED	Explanation: Client NTLM authentication failed. Action: Double-check the client's credentials.
UNEXPECTED_DATA_MSG	Explanation: NetCache received a data packet when it was expecting a control message. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
UNEXPECTED_OPCODE	Explanation: NetCache received an unexpected control packet during stream setup. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.

UNKCACHEFILEFORMAT	Explanation: NetCache detected corrupted VOD data on disk and will re-fetch the data from the origin server. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
UNKNOWN	Explanation: An internal error occurred. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
UNKNOWN_PACKET_FORMAT	Explanation: NetCache received a malformed data packet from a streaming server. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
UNKNOWN_REQ_METHOD	Explanation: An RTSP protocol error occurred. Action: Attempt to run the stream without NetCache. If streaming succeeds without NetCache but fails with NetCache, contact Network Appliance customer support.
UNMATCHED_POST	Explanation: A streaming client using HTTP encapsulation sent an unexpected request. Action: Make sure that any load-balancing network devices are configured to send all requests from the same client to the same cache.
URL_BYPASS_REDIRECT	Explanation: The client-specified URL matched a pattern in the configured URL Forwarding list (config.transparency.bypass_urls.urls) and was redirected and transparently proxied to the origin server. Action: If you do not want the client URL to be transparently proxied, you must edit your URL Forwarding list.

About this chapter

This chapter describes the NNTP access log and provides details about the data that can appear in the header fields in the NNTP access log.

Topics in this chapter

This chapter contains the following topics:

- ◆ “About the NNTP access log” on page 104
- ◆ “NNTP access log headers” on page 105
- ◆ “NNTP transaction codes” on page 108
- ◆ “x-error-msg header entries in the NNTP access log” on page 109

About the NNTP access log

Description of the NNTP access log	The NNTP access log records information about client transactions conducted through the appliance for news services.
When to use the NNTP access log	Use the NNTP access log if you want to view any of the following: ◆ Errors during transactions (NNTP codes) ◆ Groups and articles that a client accessed ◆ Time, in seconds and milliseconds, between a client connection and disconnection ◆ Number of bytes received from the client ◆ Number of bytes sent to the client ◆ Errors that the appliance or NNTP generated ◆ Errors that the server generated ◆ Timestamp (in seconds and milliseconds) ◆ Client IP address and port
Excerpt from an NNTP access log	The following is an excerpt from an NNTP access log (default format): <pre>968263470.50 10.34.26.6 0 6 173 276 - - - 0.074 968263470.50 10.34.26.6 0 7 193 308 - - - 0.074 968263470.50 10.34.26.6 0 8 218 345 - - - 0.074 968263470.50 10.34.26.6 0 9 233 370 - - - 0.074 968263470.50 10.34.26.6 0 10 255 398 - - - 0.074 968263470.50 10.34.26.6 0 11 279 426 - - - 0.074 968263470.50 10.34.26.6 0 12 300 455 - - - 0.074 968263470.50 10.34.26.6 0 13 319 482 - - - 0.074 968263470.50 10.34.26.6 0 14 334 505 - - - 0.074 968263470.51 10.34.26.6 0 15 358 533 - - - 0.084 968263470.51 10.34.26.6 0 16 377 561 - - - 0.084 968263470.51 10.34.26.6 0 17 389 586 - - - 0.084 ...</pre>

NNTP access log headers

Description of NNTP access log headers

The following table shows the headers for the NNTP access log. The headers in the default log format appear in a specific order. If you want the headers to appear in an order different than the order provided by the default format, you can configure your log headers using the custom log format. The order of the headers for the default log format is shown on the NNTP - Logging page in the Appliance Manager (Setup tab > NNTP > Logging).

Header	Description	Default format	Custom format
c-ip	Client IP address	X	X
time_taken	Time for a transaction, expressed as <seconds>.<milliseconds>	X	X
x-article-accessed	Article number or message ID of the request. This field applies only to ARTICLE/HEAD/BODY requests.	X	X
x-bytes-received	Total bytes, including carriage return and line feed, that NetCache received from the client for the request identified in the x-command field.	X	X
x-bytes-sent	Total bytes, including carriage return and line feed, that NetCache sent to the client for the request identified in the x-command field.	X	X
x-command	Commands and arguments that NetCache received from clients. If, for example, a client issues a command "group alt.binaries," that command is recorded in this field as "group_alt.binaries."	X	X

Header	Description	Default format	Custom format
x-error-msg	NNTP transaction code, NetCache error, or an error reported from the authentication domain, as follows: ◆ NNTP transaction codes Authentication domain reported error: Describes why an authentication request failed. ◆ NetCache errors: See “x-error-msg header entries in the NNTP access log” on page 109.	X	X
x-group-accessed	Newsgroup accessed by the client, if it is known.	X	X
x-status	Status of the request or command. This field includes one of the following entries: OK/HIT: The requested object was served from the cache. CANCEL/HIT: The requested object was found in the cache. However, NetCache determined when checking the NNTP server for cancellations that a user had canceled the object. The object in the cache is invalidated and is not served. EXPIRE/HIT: The requested object was in the cache but the TTL was expired. As a result, NetCache refetched the object from the server. ERR/HIT: The requested object was in the cache but an error condition was encountered while NetCache was trying to serve the request (for example, the client disconnected prematurely). xxx/MISS: The requested object was not in the cache, so NetCache fetched it from the NNTP server. An NNTP transaction code was returned from the server with the object. See “NNTP transaction codes” on page 108.		

Header	Description	Default format	Custom format
x-timestamp	Number of seconds since the UNIX epoch— January 1, 1970, for example: 963873698.73. Indicates the client disconnection time.	X	X

NNTP transaction codes

About NNTP transaction codes

The NNTP transaction codes are status reports from the origin server that indicate the response to the last command received from the client. NNTP transaction codes are seen in the x-status field, x-error-msg field, or both.

The text of the NNTP status codes that can appear can vary. However, the general format of the NNTP status codes is defined in RFC977 Network News Transfer Protocol. As documented in RFC977, the NNTP transaction codes begin with a three-digit numeric code. The first digit of the response broadly indicates the success, failure, or progress of the previous command. These three-digit codes are described in the following table.

Numeric code	Explanation
1xx	Informative message.
2xx	Command ok.
3xx	Command ok so far, send the rest.
4xx	Command was correct but could not be performed.
5xx	Command could not be implemented or was incorrect, or a serious program error occurred.
6xx	Appliance internal error, for example, an error reporting a failure of a disk I/O operation failure.

x-error-msg header entries in the NNTP access log

About this section

This section provides information about the error messages that can appear in the x-error-message header field of the NNTP access log.

CACHE_FILL_WRITE_FILE

Message Text in Browser: An internal error occurred while writing the data to the cache. Contact your system administrator.

Explanation: An error occurred while the appliance was trying to send data to the client and cache the objects. The client did not receive the data, and the objects were not cached.

Action: Try sending the same request while performing a packet trace. Select Utilities > Diagnostics > Packet Trace in the Appliance Manager. Contact NetApp Technical Support for assistance.

CACHE_HIT_READ_FILE

Message Text in Browser: A file that is cached could not be read. No action is required.

Explanation: The request is processed like a cache miss, and the object is fetched from the origin server.

Action: No action is required.

NNTP_AUTH_ERROR

Message Text in Browser: NNTP authentication error.

Explanation: The appliance cannot authenticate this user with the user name and password that the user supplied. The user likely entered the user name or password incorrectly.

Action: The user should retry entering the user name and password. If you do not intend for the user to enter a user name and password, check the following:

- ◆ If the user is in the appliance local database, does the user belong to a group for which protocol authentication has been configured?

In the Appliance Manager, select Setup tab > Authentication > Users to check the groups to which the user belongs. Then Select Setup tab >

Authentication > Groups to determine the protocol authentication for the user's groups.

- ◆ If the user is in a remote database for which a group has been configured in the appliance local database, is protocol authentication configured for the group?

NNTP_AUTH_PERM_ _DENIED

Message Text in Browser: NNTP permission was denied. Contact your system administrator.

Explanation: The authentication server returned a message to the appliance to deny the user.

Action: Check the permissions that are set for the user on the LDAP or RADIUS server.

NNTP_AUTH_ REQUIRED

Message Text in Browser: NNTP authentication was required (informational message).

Explanation: This informational message records the fact that the appliance is requesting that the user supply a user name and password. The appliance logs a set of messages related to a single NNTP request. Messages that appear in the log after this message indicate whether the client request was successfully fulfilled.

Action: No action is required.

NNTP_CLIENT_ DISCONNECT

Message Text in Browser: The NNTP client disconnected. Contact your system administrator.

Explanation: For an unknown reason, the client closed the connection while the appliance was attempting to read requests from the client.

Action: You might want to contact the user whose client disconnected to troubleshoot the problem. The system error code included in this log entry might provide some clues to the problem. The NNTP access log file will contain the IP address of the client that disconnected.

NNTP_COMMAND_ STATUS_ERROR

Message Text in Browser: Problem communicating with the news server. Contact your system administrator.

Explanation: The appliance could not communicate with the news server for some reason. Therefore, the appliance could not connect to the news server, send data to it, or receive data from it. The server might be unavailable or too busy, or a networking problem might exist.

Action: Contact the NNTP server administrator. Check for networking problems.

NNTP_COMMAND_ END_STATUS_ ERROR

Message Text in Browser: Your request could not be resolved. Contact your system administrator.

Explanation: The appliance could not resolve the user's request for some reason. For example, the user might have requested an article that is not on the server.

The NNTP transaction code in the log entry can provide a clue about the reason. For example, transaction code 423 means that the article is not there. Transaction code 430 means that the newsgroup does not exist.

The appliance issues this message after it receives a response from the server. In contrast, the appliance issues the NNTP_COMMAND_USER_ERROR message when the appliance tries to contact the NNTP server.

Action: After looking at the transaction code, provide feedback to the user as to the possible cause of the problem.

NNTP_COMMAND_ FATAL_ERROR

Message Text in Browser: Internal error. Contact your system administrator.

Explanation: The appliance is experiencing a resource problem that is preventing the appliance from resolving requests.

Action: Look at the information on the Data > System Status > General page in the Appliance Manager and the relationship between the data you see. A high resource load with little traffic being processed by the appliance indicates a problem. Conversely, if your appliance is processing a considerable amount of traffic without a high resource load, your appliance is functioning efficiently.

NNTP_COMMAND_ TIMEOUT_ERROR

Message Text in Browser: The client connection was dropped.

Explanation: The client connection was dropped while the appliance was communicating with the client. The user might have done something to cause the connection to be dropped. For example, the user might have shut down the news reader application. Alternatively, network problems might have caused the connection to be dropped.

Action: If you cannot determine that a user action might have caused the connection to be dropped, check for networking problems.

NNTP_COMMAND_ UNKNOWN_ERROR

Message Text in Browser: The command or request was entered incorrectly. Try again.

Explanation: The command or request that the user entered was not recognized by the NNTP server. A user using Telnet might have mistyped the command, for example. Alternatively, a non-newsreader application might be trying to connect to the appliance on port 119.

This type of error will include a transaction code 5xx, which might help you determine the cause.

Action: Possible actions are as follows:

- ◆ The user should try typing the request again.
- ◆ Ensure that the appliance is configured to accept NNTP request on port 119.

NNTP_COMMAND_ USER_ERROR

Message Text in Browser: The NNTP request was issued incorrectly. Try again.

Explanation: The user is issuing an NNTP request incorrectly. For example, the user might be trying to access overview information without selecting a newsgroup. The NNTP transaction code included with the message can help you determine the cause.

Action: Help the user determine how to correctly issue the NNTP request.

NNTP_CONNECT_ ERROR

Message Text in Browser: A networking problem is preventing the server from sending data. Contact your system administrator.

Explanation: The appliance was able to connect to the NNTP server but some problem is preventing the appliance from reading the data from the server.

Action: Check for network connectivity problems.

NNTP_POST_ ERROR

Message Text in Browser: An error occurred during the POST cycle. Contact your system administrator.

Explanation: The user might have done something to cause the error, for example, tried to post an article to a newsgroup that does not exist or killed the connection during the POST cycle. Alternatively, networking problems might have interrupted the POST cycle.

Action: Possible actions include the following:

- ◆ Check the NNTP server to determine if POSTing is allowed to the newsgroup
- ◆ In the Appliance Manager, ensure that article posting is enabled. Select Setup tab > NNTP > General and check the Article Posting Enable option.

NNTP_SERVER_ DISCONNECT

Message Text in Browser: The server connection was dropped. Contact your system administrator.

Explanation: The connection between the appliance and the NNTP server was dropped while the appliance was reading data from the server. The data transfer was not completed. This problem could have been caused by a networking failure or the server might have become unavailable.

Action: Determine if the NNTP server is available. Check for networking problems.

About this chapter This chapter describes the Messages log.

Topics in this chapter This chapter contains the following topics:

- ◆ “About the Messages log” on page 116
- ◆ “Subsystem (facility) information in the Messages log” on page 118
- ◆ “Severity levels in the Messages log” on page 120

About the Messages log

Purpose of the Messages log

The Messages log records status messages about NetCache appliance operation. It logs an entry each time the NetCache appliance is started, is shut down, or encounters an unusual operational state. You cannot customize or disable the Messages log. All system messages, except for those of severity level “debug,” are automatically written to the console and to the Messages log.

Note

The syslog daemon automatically sends messages to the Messages log and the system console. Optionally, you can configure the Send the Appliance Messages to a Remote Server option on the System - Logging page in the Appliance Manager to immediately send syslog messages to a remote server's syslog daemon that is listening on port 514.

When to use the Messages log

Use this log when you are looking for NetCache configuration or runtime errors.

Components of a Messages log entry

Each entry in the Messages log contains a date and timestamp, followed by the component generating the message (the facility), the severity level of the messages, and a brief message. For example

```
Mon Jul 15 21:00:00 GMT [kern.uptime.nc:info]: 9:00pm up 41 mins,
101 URLs, 0 NNTP client requests, 0 NNTP server requests, 0 streams
```

Excerpt from a Messages log

The following is an excerpt from a Messages log:

```
Mon Jul 15 20:18:59 GMT [CIFSAdmin:info]: Lookup of
APPS.hq.netapp.com failed with DNS server 10.10.20.42: Name server
failure.
```

```
Mon Jul 15 20:19:01 GMT [console_login_mgr:info]: root logged in
from console
```

```
Mon Jul 15 20:19:02 GMT [CIFSAdmin:warning]: CIFS - Could not find
a domain controller.
```

```
Mon Jul 15 20:19:03 GMT [telnet_0:info]: root logged in from host:
jam2.corp.netapp.com
```

Mon Jul 15 20:20:02 GMT [CIFSAuthen:info]: CIFS - password change failed. Will retry in 1 hour

Mon Jul 15 20:20:15 GMT [nbns_timer:info]: All CIFS name registrations complete for local server

Mon Jul 15 20:38:26 GMT [wafl_lopri:info]: Type bit scan done on vol vol0.

Mon Jul 15 20:44:44 GMT [sthread_loop:info]: Log management scheduled by host 10.41.18.30, user admin

Mon Jul 15 20:46:01 GMT [sthread_loop:info]: Log management scheduled by host 10.41.18.30, user admin

Mon Jul 15 21:00:00 GMT [kern.uptime.nc:info]: 9:00pm up 41 mins, 101 URLs, 0 NNTP client requests, 0 NNTP server requests, 0 streams

Mon Jul 15 21:20:03 GMT [CIFSAuthen:info]: Lookup of APPS.hq.netapp.com failed with DNS server 10.10.20.42: Name server failure.

Mon Jul 15 21:20:06 GMT [CIFSAuthen:info]: CIFS - password change failed. Will retry in 1 hour

Subsystem (facility) information in the Messages log

About subsystem components

Messages log entries include the application or component (facility) that generated the message. Knowing the subsystem that generated the message is useful during troubleshooting to isolate the cause of the problem.

The facility that generated the message appears in brackets following the time stamp, along and the severity of the message. For example, in [kern.uptime.nc:info], kern is the facility and info is the severity level of the message.

Subsystems that can generate messages

The following table describes the subsystems that can generate messages for NetCache.

Subsystem	Description
auth	Messages from the authentication system, such as login
authpriv	Privilege authorization system.
cmdsaudit	Command auditlog system
cron	Messages from the internal cron facility
daemon	Messages from the system daemons
ems	Messages from the Event Management System (EMS). Autosupport pulls information from the EMS and the EMS produces the XML scripting format for messages.
kern	Messages from the system kernal
mark	Mark message list manipulation facility
mail	Mail system
netcache	NetCache informational messages.
news	USENET network news system

Subsystem	Description
syslog	Syslog messaging system. For syslog, the Messages log might show lower-level internal functions, for example, telnet_0 and sthread_loop. These lower-level functions help NetApp Technical Support to debug problems.
user	Messages resulting from actions performed.

Severity levels in the Messages log

Description of severity levels

Following the time stamp, messages in the Messages log include in brackets the *facility* that generated the message and the severity of the message. For example, in [kern.uptime.nc:info], kern is the facility and info is the severity level of the message. The following table describes the severity levels that can appear in messages.

Level	Description
emerg	Panic conditions that cause a disruption of normal service.
alert	Conditions that you should correct immediately, such as a failed disk. Example: "Time server 10.10.20.241 is not responding to time synchronization requests."
crit	Critical conditions, such as a disk error.
err	Errors, such as those caused by a bad configuration file. Example: "Initialization failed on Fibre Channel adapter 7."
warning	Conditions that might become errors if not corrected. Examples: "Failed login from <security.anywhere.com>." "Protocol tunnel connection dropped because of a potential routing loop. sr_ip:

Level	Description
notice	Conditions that are not errors, but might require special handling. Examples: "The system was down for 88 seconds" "System shut down because : "halt"." "Rebuilding cache entries..."
info	Information, such as an hourly uptime message. Examples: "10:00pm up 18:44 0 URLs, 263 NNTP client requests, 123 NNTP server requests, 0 streams" "Firmware is up-to-date on all disk drives"
debug	Messages used for diagnostic purposes.

About this chapter

This chapter describes the ICAP 1.0 log and provides details about the data that can appear in the header fields in the ICAP 1.0 log.

Topics in this chapter

This chapter contains the following topics:

- ◆ “About the ICAP 1.0 log” on page 124
- ◆ “ICAP 1.0 log headers” on page 125

About the ICAP 1.0 log

Description of the ICAP log

The ICAP log records information about ICAP server transactions. You can specify one of two ICAP log file formats: default or custom. The default ICAP log file format captures common errors, such as unavailable services or ACL configuration problems. You can configure custom ICAP log files to record selected services, object size, and result codes for each ICAP transaction.

When to use the ICAP 1.0 log

Use the ICAP 1.0 log to determine any of the following:

- ◆ The time details of each ICAP transaction
- ◆ The client IP address and requested URL
- ◆ The pipeline of ICAP service farm names
- ◆ The authenticated user name for a request

Example

```
984170515.26 0.332 173.20.100.116 23134 http://www.cnn.com/sports
pornblocker | (virusblocker) | adinsertion .100|0|.232 paul
```

A pipe "|" demarcates server farm names. Parentheses () that enclose server farm names designate bypass for requests in the event of unavailable services, and angle brackets <> designate no bypass. Square brackets [] indicate that the vectored request, REQMOD or RESPMOD, resulted in a cache hit. Pipeline entries are followed by a record of the time taken by a service farm to perform a service.

ICAP 1.0 log headers

Description of the ICAP log headers

The following table shows the headers that can appear in the ICAP 1.0 log. The default log format includes a specific set of headers that appear in a specific order. If you want headers in addition to those provided by the default format, or if you want the headers to appear in an order different from the order provided by the default format, you can configure your log headers using the custom log format.

The order of the headers for the default log format is shown on the ICAP 1.0 page in the Appliance Manager (Setup tab > ICAP > ICAP 1.0).

Log header	Description	Default format	Custom format
bytes	Number of bytes that NetCache delivered to the client	X	X
c-ip	Client IP address	X	X
cs-uri	URL of the incoming client request	X	X
time-taken	Time required to handle the request (in seconds)	X	X
x_icap_categories	Content filter categories, such as sports or news	—	X
x-icap-pipenames	Names of responding ICAP service farms	X	X
x-icap-pipeservs	Pipeline service URLs	—	X
x-icap-pipetimes	Time spent for each ICAP service farm	X	X
x-timestamp	Time when the DNS query was initiated	X	X
x-username	User name provided for proxy-authenticated requests	X	X

About this chapter

This chapter describes the GRM access log and the GRM details log and provides details about the data that can appear in the header fields of the logs.

Topics in this chapter

This chapter contains the following topics:

- ◆ “About the GRM server access log” on page 128
- ◆ “GRM server access log headers” on page 130
- ◆ “About the GRM server details log” on page 132
- ◆ “GRM server details log headers” on page 133

About the GRM server access log

Description of the GRM server access log

If the GRM server is configured as a DNS server, the GRM server access log provides DNS query information from interactions between DNS nameservers and the GRM server. If the GRM server is configured as an L7 server, the log reports the URL redirection information between the client and the GRM server (client IP address, the requested URL, and the agents to be returned).

The GRM server access log adheres to the Extended Log File Format, which enables you to add or delete log file headers so that you can create customized log files that can be read by generic log analyzers.

Note

The GRM server access log is intended for use on the GRM server only. Do not enable the GRM server access log if the appliance is acting only as a GRM agent.

When to use the GRM server access log

Use the GRM server access log to find out information that includes the following:

- ◆ The time when a DNS query was initiated
- ◆ The IP address of the local DNS nameserver (for a GRM DNS server) or client (for a GRM L7 server)
- ◆ For the GRM L7 server, the URL accessed and the domain queried
- ◆ The method used to return the cache address

Excerpt from a GRM server access log

The following is an excerpt from a GRM access server log:

```
995615695.394 0.001 10.10.20.241
phlegm.service.cdn.nc.grmsource.com 10.53.44.23,10.53.44.22 60 top-
center 2001-07-20 07:54:55

995615877.004 0.001 10.10.20.241
phlegm.service.cdn.nc.grmsource.com 10.53.44.22,10.53.44.23 60 top-
center 2001-07-20 07:57:57

995654116.430 0.001 10.10.21.6 vip1.service.cdn.nc.grmsource.com
10.53.44.23,10.53.44.22 60 top-center 2001-07-20 18:35:16

995681500.640 0.001 10.34.18.74 phlegm.service.cdn.nc.grmsource.com
10.53.44.23,10.53.44.22 60 top-center 2001-07-21 02:11:40
```

```
995681508.660 0.001 10.34.18.74 tears.service.cdn.nc.grmsource.com
10.53.44.22,10.53.44.23 60 top-center 2001-07-21 02:11:48
995871510.990 0.010 10.10.20.241
phlegm.service.cdn.nc.grmsource.com 10.53.44.22,10.53.44.23 60 top-
center 2001-07-23 06:58:30
...
```

GRM server access log headers

Description of the GRM server access log headers

The following table shows the headers that can appear in the GRM server access log. The default log format includes a specific set of headers that appear in a specific order. If you want headers in addition to those provided by the default format, or if you want the headers to appear in an order different from the order provided by the default format, you can configure your log headers using the custom log format.

The order of the headers for the default log format is shown on the GRM Server - Logging page in the Appliance Manager (Setup tab > GRM Server > Logging).

Header	Description	Default format	Custom format
c-ip	If the GRM server is configured as a GRM DNS server, this is the IP address of the local DNS server. If the GRM server is configured as an L7 server, this is the IP address of the client.	X	X
cs-uri	URL accessed, for example: http://abc/hello?there. Data appears in this header only if the GRM server is configured as an L7 server.	X	X
date	GMT date when the transaction ended, in YYYY-MMM-DD format.	—	X
time	GMT time when the transaction ended, in HH:MM:SS format.	—	X
time-taken	Time for a transaction, expressed as <seconds>.<milliseconds>	—	X
x-grm-answer	IP addresses of returning edge and center caches.	X	X
x-grm-method	Method used by the GRM server to return the cache address. The method can be closest-center, random-center, and edge.	X	X

Header	Description	Default format	Custom format
x-grm-dnsquery	Domain that was queried. Data appears in this header only if the GRM server is configured as an L7 server.	X	X
x-grm-ttl	TTL for DNS lookup results provided to local DNS servers. Data appears in this header only if the GRM server is configured as a GRM DNS server. (A dash (--) is shown if the GRM server is configured as an L7 server.)	X	X
x-timestamp	Time the when the query was initiated.	X	X

About the GRM server details log

Description of the GRM server details log

The GRM server details log records information about agents and IP addresses and the proximity data they send to the GRM server.

The GRM server details log adheres to the Extended Log File Format, which enables you to add or delete log file headers so that you can create customized log files that can be read by generic log analyzers.

Note

The GRM server details log is intended for use on the GRM server only. Do not enable the GRM server access log if the appliance is acting only as a GRM agent.

When to use the GRM server details log

Use the GRM server details log to determine how the proximity data for agents and IP addresses changes over time.

How to use the GRM server details log

The GRM server details log records a large amount of information. Therefore, it might be difficult for you to interpret specific types of information by viewing the log through the Appliance Manager. Network Appliance recommends that you use the `nclog` command from the command line to be able to specify the type of information you are interested in viewing. See the CLI online Help for information about how to use the `nclog` command.

GRM server details log headers

Description of GRM server details log headers

The following table shows the headers that can appear in the GRM server details log. The default log format includes a specific set of headers that appear in a specific order. If you want headers in addition to those provided by the default format, or if you want the headers to appear in an order different from the order provided by the default format, you can configure your log headers using the custom log format.

The order of the headers for the default log format is shown on the GRM Server - Logging page in the Appliance Manager (Setup tab > GRM Server > Logging).

Header	Description	Default format	Custom format
c-ip	If the GRM server is configured as a GRM DNS server, this is the IP address of the local DNS server. If the GRM server is configured as an L7 server, this is the IP address of the client.	X	X
date	GMT date when the transaction ended, in YYYY-MMM-DD format.	—	X
localtime	NetCache local time, in DD/MMM/YYYY:HH:MM:SS GGGG format (where GGGG is the time differential from GMT).	—	X
time	GMT time when the transaction ended, in HH:MM:SS format.	—	X
x-agent-ip	IP address of the GRM agent cache that is reporting to the GRM server.	X	X

Header	Description	Default format	Custom format
x-grm-reason	Possible codes for this field are as follows: New: The GRM server received information about this IP address for the first time. Update: Something about the proximity or probe method changed for the IP address that was probed. Delete: The GRM server deleted the entry from its tables. Merge: The GRM agent recognized that multiple IP addresses had the same proximity measurements, so it compacted the entries in the proximity table to save space. Merging of IP addresses can occur only on CIDR /26 masks. Split: For compactness, the GRM agent merged IP address entries in the proximity table for IP addresses with the same proximity measurements. The GRM agent split the merged entries, for example, because the proximity measurements for the IP addresses are no longer the same or one of the IP addresses became unreachable. Splitting of IP addresses can occur only on CIDR /26 masks.	X	X

Header	Description	Default format	Custom format
x-probe-method	The method that the GRM server used to determine proximity. The GRM server uses a number of mechanisms to determine proximity, changing from one to another if one does not produce results. This field can show any of the following entries: ◆ ping ◆ dns_lookup ◆ traceroute ◆ none ◆ gone If gone is shown, the reason code in the x-grm-reason field will be Delete.	X	X
x-proximity	The round-trip time as measured by the GRM agent cache for the method shown in the x-probe-method field.	X	X
x-timestamp	Time when the query was initiated.	X	X

About this chapter

This chapter describes the DNS log and provides details about the data that can appear in the header fields in the DNS log.

Topics in this chapter

This chapter contains the following topics:

- ◆ “About the DNS log” on page 138
- ◆ “DNS log headers” on page 139

About the DNS log

Purpose of the DNS log

The DNS log records information from the DNS lookups performed by the appliance DNS resolvers and the results of errors that it received.

The following information is recorded: the time the request was completed (or terminated), the time taken to complete (or terminate), the resolver that initiated the query, the DNS resource record that was requested, the host name that was queried, the answer or error in the DNS response if one was received, and the number of resource records in the answer section of the DNS response.

When to use the DNS log

Enable the DNS log if you want to know the following:

- ◆ The requests that resulted in the appliance querying other DNS servers
- ◆ How long a request took to complete or terminate for some reason

Excerpt from a DNS log

The following is an excerpt from a DNS log:

```
1021594419.50 2.264 full A a.gtld-servers.net NOERROR 1
1021594419.56 2.331 full A arrowroot.arin.net NOERROR 1
1021594462.88 0.785 stub PTR 110.64.16.144.in-addr.arpa NXDOMAIN 0
1021594520.60 0.155 full PTR 6.71.218.66.in-addr.arpa NOERROR 1
1021594593.53 0.001 stub A WWW.NETAPP.COM NOERROR 1
1021594651.62 0.067 full A wordsmith.org NOERROR 1
```

DNS log headers

The following table lists the log file headers that are specific to the DNS log. These log file headers are preset and cannot be modified.

Log Header	Description
time-taken	Time in seconds that the DNS lookup took, for example, 0.180.
x-dns-resolver	The resolver that initiated the DNS query. Possible entries are stub: Stub resolver. The appliance uses the stub resolver to contact the nameservers that are listed in the Nameservers option on the Setup tab > DNS - General page in the Appliance Manager. full: Full-service resolver. The appliance full-service resolver is “turned on” when you enable the DNS Iterative Resolution option on the DNS - General page. This field is primarily for use by NetApp Technical support for debugging. However, some customers who have enabled the full-service resolver like to use the information in this field to confirm that the full-service resolver serviced the request.
x-request-question	The question sent by the resolver, for example, ns0.corpex.de.
x-request-rr	The type of resource record that was requested. Possible entries are A: Address record (forward lookup) PTR: Pointer record (reverse lookup)
x-response-amount	The number of records in the answer section. This field is for use by NetApp Technical Support for debugging.

Log Header	Description
x-response-rcode	The return code that the resolver received in the response to the DNS query. Possible entries are NOERROR: No error occurred. SERVFAIL: An upstream server failed. This error indicates a configuration problem on a DNS nameserver. Such errors commonly occur in the DNS nameserver network. Do not contact NetApp Technical Support for these errors. TIMEOUT: The resolver did not receive a response within the expected time, so the request timed out. FORMERR: Format error. A format error is typically caused by a problem with how a user entered the IP address or host name in the URL. NXDOMAIN: No such host or domain.
x-timestamp	Completion time of the request, for example, 1021509281.86. The time shown is UNIX epoch time, which is the number of seconds since January 1, 1970.

About this chapter This chapter provides a brief description of the ContentDirector log. See the ContentDirector documentation for more information.

Topic in this chapter This chapter contains the following topic:

- ◆ “About the ContentDirector log” on page 142

About the ContentDirector log

Description of the ContentDirector log

The ContentDirector log provides diagnostic information about the ContentDirector agent software. This log is enabled by default. You cannot configure the headers that appear in it.

For more information about the ContentDirector log, contact your Network Appliance technical support representative.

When to use the ContentDirector log

Use the ContentDirector log to determine fatal errors.

Excerpt from a ContentDirector server log

The following is an excerpt from a ContentDirector server log:

```
L:807349: 8:18:D:[CtrlCh-Monitor]:Agent Storage returns Changed info
L:807349: 8:18:D:[CtrlCh-Monitor]:33,thing,1,25,0,1,unknownPartnName,146425221120,1,hme0,1,10.96.68.103,0,1250803,3132
L:807349: 8:9:I:[CtrlCh-Monitor]:Sending config request
L:807350: 8:3:D:[CtrlCh-Monitor]:setting TransactionEntry (retries: 3 interval: 5000
L:807369: 8:7:I:[GroupLeaderAnnouncementThread]:Group Leader sending announcement number: 1 to Global Channel
L:814619: 8:8:D:[Election timeout]:TMO
L:814619: 8:8:D:[Election timeout]:StateMachine Election: old state = 4 input = 1
...
```

About this chapter This chapter describes CONFILL error messages.

Topics in this chapter This chapter contains the following topics:

- ◆ “About CONFILL messages” on page 144
- ◆ “CONFILL messages—explanations and actions” on page 145

About CONFILL messages

What are CONFILL messages?

Some CONFILL messages describe situations over which you have control. Other CONFILL messages provide details about errors in the appliance internal processes that you can provide to Network Appliance(TM) Technical Support. The message explanations in this guide inform you when to contact Technical Support.

CONFILL error codes are present in the X-Netcache-Error header of the HTTP response that the appliance returns from the PUSH request. A description, which is highlighted in this chapter as Message Text, is available in the HTML that makes up the HTTP response body. The message explanations in this chapter provide more details than are available in the Message Text.

CONFILL messages—explanations and actions

About this section

This section provides explanations of CONFILL messages and describes the action to take if you receive a particular message.

CONFILL_PUSH_ CANT_GENERATE_ FQDN

Message Text: Could not generate a fully qualified domain name.

Explanation: To process a PUSH request for streaming media, the appliance must be able to generate a fully qualified domain name for the host name of the URL. The appliance could not do this for some reason. For example, the URL in the request could have been mistyped or a DNS server problem might have occurred.

Action: Check the following:

- ◆ Ensure that the URL in the PUSH request is valid.
- ◆ Check the DNS configuration on the appliance and the DNS server.

CONFILL_PUSH_ COMMIT_FAILED

Message Text: Commit failed. Could not rename content.

Explanation: An internal problem occurred while the appliance was committing HTTP pushed content into the cache.

Action: Contact Technical Support. Provide this error message and information about the content that you were pushing.

CONFILL_PUSH_ HTTP_CHUNKED_ UNSUPPORTED

Message Text: Pushing chunked encoding content is not supported.

Explanation: The appliance received a PUSH request to fill the cache with HTTP content that uses chunked encoding. The appliance does not currently support chunked encoding for PUSH requests.

Action: Rewrite your PUSH request so that it does not include the transfer encoding chunked header.

**CONFILL_PUSH_
HTTP_OBJ_
UNCACHEABLE**

Message Text: Headers indicate that the pushed object is uncacheable.

Explanation: The PUSH request was rejected. Either of two circumstances could result in this message. The PUSH request that the appliance received contains a no-cache header. Alternatively, caching rules on the appliance are set to prevent caching of the type of object referenced in the PUSH request.

Action: If you wrote the PUSH request:

- ◆ Check whether you included a no-cache header in the PUSH request. If you did, rewrite your PUSH request without the no-cache header.
- ◆ If your request does not include a no-cache header, check the caching rules on the appliance to determine whether a caching rule is set to prevent caching of the object type in the request. (Select Setup tab > HTTP > Heading and Caching Behavior.)

If the PUSH request was sent by ContentDirector:

- ◆ Check the caching rules on the appliance to determine whether a caching rule is set to prevent caching of the object type in the request. (Select Setup tab > HTTP > Heading and Caching Behavior.)

**CONFILL_PUSH_
LOG_IO_ERR**

Message Text: I/O error occurred on transaction log file.

Explanation: The appliance received a PUSH request to commit, abort, or publish a transaction. If the PUSH request was to commit or abort a transaction, the appliance could not locate the transaction file. A probable reason is that the transaction number in the PUSH request is incorrect.

Action: If you wrote the PUSH request to commit or abort the transaction, verify the transaction number to ensure that you did not make a typographical error. Then try to send the PUSH request again. If the error is repeated, contact Technical Support.

If the PUSH request was sent by ContentDirector or the PUSH request was to publish a transaction, contact NetApp Technical Support.

**CONFILL_PUSH_
LOW_MEM**

Message Text: Insufficient memory during fill.

Explanation: Not enough system memory was available for the appliance to process the PUSH request.

Action: Insufficient memory can be caused by different factors. Some things you can check are as follows:

- ◆ If you are sending PUSH requests at peak time, try sending them when the network is less busy.
- ◆ Consider how many other processes your appliance is handling at the same time. For example, if you are running a low-end appliance model, content filtering might be using up available memory.

If memory load on your appliance is consistently high, contact your Network Appliance sales engineer to discuss purchasing additional appliances.

CONFILL_PUSH_ MEDIA_IO_ERR

Message Text: An error occurred while the appliance was creating or reading an intermediate file.

Explanation: An internal problem occurred while the appliance was placing pushed content into the cache.

Action: Contact NetApp Technical Support. Provide this error message and information about the content that you were pushing.

CONFILL_PUSH_ MEDIA_VERSION_ UNSUPPORTED

Message Text: This media file version is not supported.

Explanation: The appliance received a streaming media file with a version that the appliance does not support.

Action: Contact NetApp Technical Support. Provide this error message and information about the content that you were pushing.

CONFILL_PUSH_ MISSING_HEADER

Message Text: The required HTTP header is missing or invalid, or the URL is for unsupported content.

Explanation: The appliance could not process the PUSH request. This problem could occur because a header in the request is either absent or contains invalid content. Alternatively, the URL could be for content that the appliance does not support for PUSH requests, for example, gopher or HTTPS content.

Action: PUSH requests have specific requirements for the headers that must be included and the placement of headers. If you created the PUSH request, review any information you might have about creating PUSH requests. Otherwise, contact NetApp Technical Support.

**CONFILL_PUSH_
MUST_USE_ADMIN_
_PORT**

Message Text: PUSH requests must be received on the administration port.

Explanation: The PUSH request was not sent to the appliance admin port. The appliance must receive PUSH requests on its admin port.

If you are using ContentDirector, the most likely cause of this problem is that ContentDirector is not configured with the correct admin port for the appliance. If you are sending PUSH requests outside of ContentDirector, you did not include the correct appliance admin port when you connected to the appliance.

Action: Check the Admin Port setting in the Appliance Manager to determine the correct port to enter in the ContentDirector software or in PUSH requests when you connect to the appliance. To check the Admin Port setting in the Appliance Manager, select Setup tab > Administration > Administrative Access.

**CONFILL_PUSH_
NO_DISK_SPACE**

Message Text: Insufficient disk space during fill.

Explanation: Not enough disk space is available for the appliance to write the pushed objects to disk.

Locked content, log files, core files, and packet traces all compete for the space that can be used by ejectable content, that is, content fetched from origin servers. The amount of disk space used by core files and packet traces is typically negligible. However, if you fill a cache with locked content, log files, or both, you will severely limit or eliminate the ability of the appliance to cache objects fetched from an origin server because few objects would be eligible to be ejected if the disk becomes too full. As a result, the appliance might have to fetch content more frequently from origin servers, thereby reducing possible bandwidth savings.

Action: Start by looking at the disk usage information on the System Status - General page (Data tab) in the Appliance Manager to determine how your disk space is used.

If you are locking content, set your lock times according to how long you really need specific content in your caches.

If your disk usage chart shows a considerable amount of space being used by log files, consider taking the following actions:

- ◆ Reduce the size of your log files.
- ◆ Push log files to an HTTP or FTP server.

To configure log file management behavior, select Setup tab > System > Log Files.

**CONFILL_PUSH_
NO_LOCK_
TIMEOUT**

Message Text: Publish requests must specify a lock timeout.

Explanation: This request did not specify a lock timeout. The appliance requires publish requests (requests to prepublish the content to the cache but not commit until the appliance receives a commit message) to specify a lock timeout denoting the length of time the object will be locked on disk.

Action: If you are pushing content by using a two-phase commit process, ensure that the PUSH request includes a lock timeout.

**CONFILL_PUSH_
OBJ_IO_ERR**

Message Text: An error occurred while the appliance was creating or writing a cache object.

Explanation: An internal problem occurred while the appliance was placing pushed content into the cache.

Action: Contact NetApp Technical Support. Provide this error message and information about the content that you were pushing.

**CONFILL_PUSH_
OBJ_NOT_FOUND**

Message Text: Content is not present in the cache.

Explanation: The appliance received a PUSH request for content that was expected to be in the cache but it was not present. For example, the PUSH request specified specific content to eject, but the content was not in the cache.

Action: No action is required.

**CONFILL_PUSH_
PROXY_ONLY**

Message Text: Cache was in proxy-only mode during fill.

Explanation: The appliance is in the process of preparing to cache objects.

Action: No action is required.

**CONFILL_PUSH_
PUBLISHED_ITEM_
MISSING**

Message Text: Unable to find an object to commit.

Explanation: An internal problem occurred while the appliance was committing pushed content into the cache.

Action: Contact NetApp Technical Support. Provide this error message and information about the content that you were pushing.

**CONFILL_PUSH_
QT_MOV_NOT_
HINTED**

Message Text: QuickTime media is not hinted.

Explanation: The appliance supports only QuickTime media files that are hinted. The hint tracks tell the server exactly how to package the media data for the network.

Action: Try the following:

- ◆ Use a tool to add hints to a QuickTime media file. For more information, see <http://www.apple.com/quicktime/products/tutorials/hintracks.html>. Third-party tools are also available.
- ◆ Contact NetApp Technical Support. Provide this error message and information about the content that you were pushing.

**CONFILL_PUSH_
QT_VERSION_
UNSUPPORTED**

Message Text: QuickTime confill supports only audio and video tracks.

Explanation: The PUSH request had no problems, but the media file included tracks other than audio and video.

Action: No action is required.

**CONFILL_PUSH_
SUCC_ABORT**

Message Text: Aborting two-phase commit.

Explanation: This message is informative. The appliance received a PUSH request to abort the push transaction currently in progress, and the transaction was successfully aborted.

Action: No action is required.

**CONFILL_PUSH_
SUCC_COMMIT**

Message Text: Committing content to cache was successful.

Explanation: This message is informative. The appliance received a PUSH request to commit the push transaction currently in progress, and the transaction was successfully committed. The object is now available in the cache.

Action: No action is required.

**CONFILL_PUSH_
SUCC_
CONVERSION**

Message Text: Successfully converted media content.

Explanation: This is an informative message that is generated in either of the following circumstances:

- ◆ The appliance received a PUSH request to prepush streaming media content to the cache (that is, content is pushed to the cache but not committed), and the transaction was successful. This is the first phase of a two-phase transaction. At this point, the object is not available in the cache and will not be available until the object is committed.
- ◆ The appliance received a PUSH request for a single-phase transaction to fill the cache with streaming media content, and the operation was successful.

Action: No action is required.

CONFILL_PUSH_ SUCC_EJECT

Message Text: Content was successfully ejected from the cache.

Explanation: This message is informative. The appliance received a PUSH request to eject an object from the cache, and the operation was successful.

Action: No action is required.

CONFILL_PUSH_ SUCC_HTTP

Message Text: HTTP content was successfully pushed to the cache.

Explanation: This message is informative. The appliance received a PUSH request to fill the cache with HTTP content, and the operation was successful.

Action: No action is required.

CONFILL_PUSH_ SUCC_PUBLISH

Message Text: Publishing content to the cache was successful.

Explanation: The appliance received a PUSH request to prepush HTTP content to the cache (that is, content is pushed to the cache but not committed), and the transaction was successful. This is the first phase of a two-phase transaction. At this point, the object is not available in the cache and will not be available until the object is committed.

Action: This message is informative. No action is required.

CONFILL_PUSH_ UNABLE_TO_ CONVERT

Message Text: Unable to convert media file.

Explanation: The appliance does not understand a part of the streaming media file format. Therefore, the appliance could not convert the file. This problem might have occurred because the media file was corrupted or because of the subset of media file format that the appliance supports.

This error could occur in the first phase of a two-phase transaction or in a single-phase transaction.

Action: Verify that the media file is good by playing the media file. Contact NetApp Technical Support if you need more assistance. Provide this error message and information about the content that you were pushing.

CONFILL_PUSH_ URL_INVALID

Message Text: The target URL is invalid.

Explanation: A URL was sent to the cache without an error, but the cache could not cache the content because the URL is an invalid format for the PUSH content request.

Action: Verify that the PUSH request you are attempting to make contains a valid URL for the media format.

About this chapter

This chapter describes the Content Management System (CMS) log and provides details about the data that can appear in the header fields in the CMS log.

Topics in this chapter

This chapter contains the following topics:

- ◆ “About the CMS log” on page 154
- ◆ “CMS log headers” on page 155

About the CMS log

Description of the CMS log

The Content Management System (CMS) is one component of the DataFabric Manager product. The CMS is responsible for generating a table of contents (TOC) of URLs and some meta-data for each Web and streaming site being managed. If the appliance is acting as a CMS agent for DataFabric Manager (DFM), the CMS log is available on the appliance. The CMS agent is enabled through DFM or through a third-party product.

The CMS log provides details about the appliance's processing of the TOC file, including the results of examining the TOC file to determine which objects in the cache are present and up to date. The CMS log includes information about the status of entries in the TOC file, logs successful entries, and reports errors that the appliance encountered while updating objects in its cache.

CMS log headers

Description of CMS log headers

The following table shows the headers that can appear in the Content Management System (CMS) log. The headers appear in the following order in the log:

job-id revision last-runtime time-taken toc-uri schedule total-retries retry-schedule
retry-no total-entries errors prefills content-size tocgen-user tocgen-host

This log is not customizable.

Log Header	Description
content-size	“Raw” total size of the content that was downloaded from origin servers and committed to the appliance. With streaming, multiple bit rates can be stored in the appliance cache so the actual content size can be larger than the raw total size shown in this log.
errors	Errors that occurred when the appliance was processing the entries in TOC file.
job-id	Job ID set by DataFabric Manager
last-runtime	The last time that the appliance processed the table of contents (TOC) file.
prefills	Number of objects that were refreshed in the cache after the appliance checked the last-modified time of the objects.
retry-no	Number of times that the appliance retried processing the errors that it encountered during previous processing of the TOC file. The retry number shown in this field can never exceed the value that is configured for the total possible retries.

Log Header	Description
retry-schedule	Schedule at which the appliance will retry processing of the TOC file if it cannot process the TOC file according to the schedule set. The retry schedule is configurable through DataFabric Manager, the appliance CLI, or through the zephr API.
revision	A revision number to identify the TOC file.
schedule	Schedule at which the appliance processes the TOC file. The schedule is configurable through DataFabric Manager, the appliance CLI, and through the zephr API.
time-taken	Time taken to process the TOC file, in seconds.
toc-uri	The URI (URL) of the TOC file that the appliance pulled from a Web server and processed. The Web server from which the appliance pulls the TOC is configurable through DataFabric Manager, the appliance CLI, and through the zephr API.
tocgen-host	The DataFabric Manager host that was responsible for creating the TOC.
toc-gen-user	The DataFabric Manager user that created the job on the DFM computer that is represented by this TOC.
total-entries	Total number of entries in the TOC file.
total-retries	Total number of times that the appliance tries to reprocess the errors that occur during processing of the TOC file. The total retries that are allowed is configurable through DataFabric Manager, the appliance CLI, and through the zephr API.

Index

A

ACL_DENY 28
AUTH_FAIL 28

B

BAD_REQUEST_NO_HOST 29
BAD_URL 29
BYPASSED_URL 29

C

CACHE_FILE_READ 30
CACHE_FILL_OPEN_FILE 30
CACHE_FILL_TRANSPORT 30
CACHE_FILL_WRITE_FILE 31
CACHE_HIT_FILE_VERSION 31
CACHE_HIT_FORCED_EJECT 31
CACHE_HIT_WRITE_SOCKET 32
CANT_CONNECT 32
CANT_CONNECT_IPSPOOF 32
CANT_CONNECT_LOOPBACK 32
CLIENT_CLOSE 33
CLIENT_REQUEST_READ 33
CLIENT_TAKEOVER 33
CLIENT_WRITE 33
CMS log 153
CONFILL messages
 defined 145
 purpose of 144
CONFILL_PUSH_CANT_GENERATE_FQDN 145
CONFILL_PUSH_COMMIT_FAILED 145
CONFILL_PUSH_HTTP_CHUNKED_UNSUPPORTED 145
CONFILL_PUSH_HTTP_OBJ_UNCACHEABLE 146
CONFILL_PUSH_LOG_IO_ERR 146
CONFILL_PUSH_LOW_MEM 146
CONFILL_PUSH_MEDIA_IO_ERR 147
CONFILL_PUSH_MEDIA_VERSION_UNSUPPORTED 147

CONFILL_PUSH_MISSING_HEADER 147
CONFILL_PUSH_MUST_USE_ADMIN_PORT 148
CONFILL_PUSH_NO_DISK_SPACE 148
CONFILL_PUSH_NO_LOCK_TIMEOUT 149
CONFILL_PUSH_OBJ_IO_ERR 149
CONFILL_PUSH_OBJ_NOT_FOUND 149
CONFILL_PUSH_PROXY_ONLY 149
CONFILL_PUSH_PUBLISHED_ITEM_MISSING 149
CONFILL_PUSH_QT_MOV_NOT_HINTED 150
CONFILL_PUSH_QT_VERSION_UNSUPPORTED 150
CONFILL_PUSH_SUCC_ABORT 150
CONFILL_PUSH_SUCC_COMMIT 150
CONFILL_PUSH_SUCC_CONVERSION 150
CONFILL_PUSH_SUCC_EJECT 151
CONFILL_PUSH_SUCC_HTTP 151
CONFILL_PUSH_SUCC_PUBLISH 151
CONFILL_PUSH_UNABLE_TO_CONVERT 151
CONFILL_PUSH_URL_INVALID 152
Content Management System log 153
CONTENT_NOT_PRESENT 34
ContentDirector log
 description 142
 excerpt 142
 when to use 142

D

DNS log
 excerpt 138
 headers 139
 purpose 138
 when to use 138
DNS_HOST_NOT_FOUND 34
DNS_MISC_ERROR 35
DNS_NO_DATA 35
DNS_TIMEOUT 35
DynaBLocator codes 22

F

- FTP transfer access log 53
 - headers 54
- FTP_BAD_RESPONSE 36
- FTP_LOGIN 36
- FTP_NOFILE 36
- FTP_NOPERM 36
- FTP_NULL_USERNAME 37

G

- GATEWAY_TIMEOUT 37
- GRM server access log
 - description 128
 - excerpt 128
 - headers 130
 - when to use 128
- GRM server details log
 - description 132
 - headers 133
 - how to use 132
 - when to use 132

H

- HTTP_MIME_TOO_LONG 37
- HTTP_REQUEST_TOO_LONG 37

I

- ICAP log
 - description 124
 - headers 125
 - when to use 124
- ICAP_OPTIONS_MISMATCH 38
- ICAP_OPTIONS_PARSE_FAIL 38
- ICAP_REQMOD_CLIENT_READ_FAIL 38
- ICAP_REQMOD_CLIENT_WRITE_FAIL 39
- ICAP_REQMOD_SVC_DISABLED 39
- ICAP_REQMOD_SVC_INVALID_RESPONSE 39
- ICAP_REQMOD_SVC_READ_BODY_FAIL 40
- ICAP_REQMOD_SVC_READ_FAIL 40
- ICAP_REQMOD_SVC_WRITE_FAIL 40
- ICAP_RESPMOD_EXIT_FAIL 41

- ICAP_RESPMOD_GEN_HDR_FAIL 41
- ICAP_RESPMOD_IO_BODY_FAIL 41
- ICAP_RESPMOD_RCV_STATUS_FAIL 42
- ICAP_RESPMOD_SEND_BODY_FAIL 42
- ICAP_RESPMOD_SEND_HDR_FAIL 42
- ICAP_RESPMOD_SEND_PREVIEW_FAIL 43
- ICAP_SF_BYPASS 44
- ICAP_SF_FARM_DISABLED 44
- ICAP_SF_NOFARM_AVL 44
- ICAP_SF_NOSERVICE_AVL 44
- INVALID_HIT_VERIFY 45
- INVALID_OUTBOUND_PORT 45
- INVALID_TUNNEL_PORT 45

M

- Messages log
 - entry components 116
 - excerpt 116
 - purpose 116
 - severity levels in 120
 - subsystem data in 118
 - when to use 116

N

- NNTP access log 103
 - excerpt 104
 - headers 105
 - transaction codes 108
 - x-error-message entries 109

O

- OBJECT_OPEN 46

P

- PARENT_NEEDED 46
- PRECONDITION_FAILED 46

R

- RESP_AFTER_100_CONTINUE_MISSING 47

S

- SERVER_CLOSE 47
- SERVER_REQUEST_WRITE_REQUEST 47
- SERVER_RESP_ERROR 48
- SERVER_RESPONSE_CLOSE 48
- SERVER_RESPONSE_RESET 48
- SERVER_TRANSPORT 49
- SERVER_WRITE 49
- SmartFilter codes 25
- Streaming access log
 - description 59
 - excerpt 60
 - headers 61
 - sc-status codes 65
 - when data is logged 59
 - x-action field 76
- Streaming details log 67
 - excerpt 67
 - headers 68
 - when to use 67
 - x-action field 76
 - x-transaction codes 72

T

- TUNNEL_DESTIP_SELF 49

U

- UNRECOGNIZED_REQUEST 49

W

- Web accelerator logs 51
- Web access log 1
 - cs-username field 16
 - description 2
 - DynaBLocator codes 22
 - excerpt 2
 - headers 4
 - predefined formats 14
 - SmartFilter codes 25
 - when to use 2
 - x-hiercode field 21
 - x-note entries 27
 - x-transaction field 16, 17
- WebWasher DynaBLocator codes 22

X

- x-action log field 76
- x-error-message entries 109
- x-hiercode header 21
- x-note entries 27
- x-status header 83

