

ContentDirector™ 2.1

Release Notes

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089
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 210-00198
March 2002

Copyright and trademark information

Copyright information

Copyright © 1994–2002 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.

This Software contains materials from third parties licensed to Network Appliance Inc. which is sublicensed, and not sold, and title to such material is not passed to the end user. All rights reserved by the licensors. You shall not sublicense or permit timesharing, rental, facility management or service bureau usage of the Software.

Portions developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 1999 The Apache Software Foundation.

Portions Copyright © 1995–1998, Jean-loup Gailly and Mark Adler

Portions Copyright © 2001, Sitraka Inc.

Portions Copyright © 2001, iAnywhere Solutions

Portions Copyright © 2001, i-net software GmbH

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. SnapManager is a registered 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 and SecureShare 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. ApplianceWatch, BareMetal, Center-to-Edge, ContentDirector, ContentReporter, DataFabric, MultiStore, NearStore, NetApp—the Network Appliance Company, SecureAdmin, Serving Data by Design, Smart SAN, SnapCache, SnapDrive, SnapMirror, SnapRestore, 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.

ContentDirector 2.1 Release Notes

Release notes contents

These release notes provide information about the following topics:

- ◆ “[New features and bug fixes in ContentDirector](#)” on page 3
- ◆ “[User Interface](#)” on page 13
- ◆ “[Disk space and file maintenance](#)” on page 16
- ◆ “[Network-related issues](#)” on page 18
- ◆ “[Installing a Network Appliance self-signed certificate for SecureAdmin](#)” on page 20
- ◆ “[Filer integration](#)” on page 23
- ◆ “[Operating systems and applications](#)” on page 26

Where you can obtain product information

Included with your ContentDirector™ software is a pair of guides that describe the deployment, installation, configuration, and administration of this product:

- ◆ For deployment and installation information, see the *ContentDirector Installation Guide*.
- ◆ For configuration and administration information, see the *ContentDirector Administration Guide*.

Note

The 2.1 versions of these guides are available only on the product CD-ROM in .pdf format. The 2.0 versions of these guides are available in printed format; they contain all but the very latest ContentDirector 2.1 information.

In addition, the *ContentDirector 2.0 API Guide* provides an overview and introduction to the API.

The following table describes where to find additional information about ContentDirector.

Location	Description
The NOW Web site (now.netapp.com)	This site provides information such as technical reports, answers to frequently asked questions, and descriptions of bugs. The Knowledge Center page, available from the main Technical Assistance and Documentation page, contains on-line versions of the ContentDirector guides.

Section A: New features and bug fixes in ContentDirector

Required version of NetCache	ContentDirector 2.1 requires NetCache™ 5.3 software or later. If you are upgrading to ContentDirector 2.1 from ContentDirector 2.0, you must upgrade all NetCache destinations to NetCache 5.3. The ContentDirector 2.1 core application is not compatible with ContentDirector 2.0 agents.
Required version of Java Virtual Machine	The applet for ContentDirector 2.1 requires the Java™ Virtual Machine (JVM) 1.3.1 plug-in. This plug-in is available from the ContentDirector installation CD-ROM. If you do not install it from the CD-ROM, the applet downloads the JVM automatically from a SUN® Systems Web site when you first load the applet from the browser.
Scale to 150 NetCache destinations	ContentDirector 2.1 scales to 150 NetCache destinations. The destinations can consist of any combination of group leaders and group members: from one group leader and 150 group members on a single transport group, to 150 combined group leaders and group members. The previous limit was 100 for ContentDirector 2.0.
Integration with Global Request Manager	ContentDirector 2.1 can be integrated with the Global Request Manager (GRM) feature of NetCache. The integration of GRM and ContentDirector offers a key combination of features to enable premium service: ◆ GRM uses DNS routing to direct content requests to the NetCache appliances that are closest to the clients. ◆ ContentDirector prepopulates content to specific NetCache appliances. Proximity combined with content awareness improves service to clients. It enables GRM to redirect client requests to the closest available NetCache appliance that contains the requested content. This redirection combines the speed of prepopulated content with the speed and higher data integrity of geographic proximity.

In addition to improving service quality, integrating GRM and ContentDirector means that you do not need to duplicate content on data centers that are geographically close to each other.

To permit integration of GRM and ContentDirector, ContentDirector sends a report in XML format to GRM. This report contains information required by GRM on network segments and destinations. It also flags unicast group members and network segments that contain satellite links.

To successfully integrate GRM with ContentDirector, observe the following guidelines:

- ◆ Each NetCache appliance that participates in the GRM and ContentDirector integration must have both the GRM agent and the ContentDirector agent enabled. If both agents are not enabled, GRM sees the NetCache appliance as unavailable and not eligible for redirection.
- ◆ All NetCache appliances that are destinations on a single ContentDirector transport group must be co-located. Do not group NetCache appliances that are on different networks into a single transport group.
- ◆ Ensure that each destination group comprises one or more complete transport groups. This is necessary because GRM groups are the same as ContentDirector transport groups. GRM currently assumes that all members in a group have identical content.
- ◆ Each transport group must be in a destination group to receive GRM traffic. If a transport group is not included in a destination group, it is included in the report from ContentDirector to GRM, but receives no traffic.
- ◆ To obtain global settings from ContentDirector, in the NetCache Manager utility, select Setup > System > Automatic Configuration. In the Automatic Configuration Files option, enter the following URL:
`<http://cdipaddress:data/applet port/ContentDirector/servlet/dbrequest>`
The default data/applet port is 8080. This changes automatically if port 8080 is already bound at the time of installation. It can also be changed manually after installation. You can check the current data/applet port from ContentDirector in the File > Configuration > Ports screen.
- ◆ The administrator must enable the GRM server and the GRM log in the NetCache Manager utility. However, the administrator should not configure domains, center groups, or center caches . Configuring these settings locally overrides the global settings obtained from ContentDirector.
- ◆ When using ContentDirector to obtain GRM settings, GRM should be authoritative in the DNS hierarchy for the Fully Qualified Domain Names (FQDNs) pushed by ContentDirector. GRM then provides redirection only for those FQDNs handled by ContentDirector.

Note

In each transport group receiving GRM traffic, only the group members (or group leaders that are also group members) receive GRM traffic. NetCache appliances that are only group leaders do not serve content to clients.

Note

ContentDirector does not use edge groups. All NetCache appliances that are reported from ContentDirector are configured in GRM as center caches.

For more information about GRM, see the *Guide to Global Request Manager*. It is available from the NetCache 5.3 documentation pages on the NOW site at <http://now.netapp.com>.

Multiple language OS support

ContentDirector 2.1 supports the Chinese and Japanese versions of Solaris® and Windows®, with the following limitations:

- ◆ All GUI strings and log files are in English only.
- ◆ File names for pushed content must use 8-bit characters.

8-bit languages other than English should not pose a problem, but have not been tested.

UNC support for source locations

In the New Source and Modify Source screens, you can now type in the path to source locations instead of browsing. The path requires Universal Naming Convention (UNC) format: `\\server-name\\shared-resource-pathname`. ContentDirector checks connectivity when you click OK, and does not accept a nonexistent path.

Filer-optimized jobs use a single rsh connection

ContentDirector uses only one rsh connection for filer-optimized jobs. All requests are queued on that one connection. The number of concurrent filer-optimized jobs is no longer limited by the number of rsh connections available on the filer, as it was in ContentDirector 2.0.

Cross platform file sharing must be configured for case-sensitivity

Samba, or any similar system for sharing files across platforms, must be configured to be case-sensitive when used in conjunction with ContentDirector. Case-sensitivity allows it to differentiate duplicate file names that differ only in

case. Without case-sensitivity, it can cause jobs on a Windows-based core application to fail, because Windows cannot detect duplicate file names that differ only in case.

Support for multiple group leaders behind the same firewall

ContentDirector now supports multiple group leaders behind the same firewall. This was a limitation in ContentDirector 2.0.

Changes in port usage

The ports used by ContentDirector have changed. The two ports it now uses are the command port 3229 (IANA assigned), and the data port 8080.

Port requirements for firewalls

Port requirements for firewalls have changed. The requirements for opening these ports depend on the location of the firewall:

- ◆ For firewalls in front of a group leader
 - ❖ There is no need to open inbound ports.
 - ❖ Ports 3229 and 8080 must be open for outbound traffic.
- ◆ For firewalls in front of a core application machine
 - ❖ Ports 3229 and 8080 must be open for inbound traffic.
 - ❖ Port 3229 must be open for outbound traffic.

Changing ports

You can change the ports used by ContentDirector to resolve port conflicts. For detailed instructions, see “[Ports](#)” on page 7.

New configuration options for system administrators

The new Configuration screen contains global settings for logging, communications ports, and location of the assignment file, a temporary file used during content distribution. The Configuration screen is accessible to system administrators only.

Logging: To set global logging, complete the following steps.

Step	Action
1	Log into ContentDirector as a system administrator.

Step	Action
2	On the main menu bar, click File.
3	Click Configuration.
4	Click the Logging tab.
5	Select the Debug Logging check box to enable debug logging and to show more detailed logging information in the status window.
6	In the Max Log Files field, enter the maximum number of log files you want to store before the log files roll over. The default number is five.
7	In the Max Log File Size field, enter the maximum size of each log file in bytes. The default number is 20000.
8	Under Log file location, click Browse to select another location for log files. If you enabled a large number of log files and a high maximum size, consider relocating log files to save space on the local drive of the core application machine.
9	Click OK.

Ports: To set global port assignments, complete the following steps.

Caution

If you change the command port on the core application, you must also change it on every group leader. In the NetCache CLI, use the command: `set config.cd.remote_command_port <portnumber>`. If you change the data port, the change is communicated to group leaders automatically.

Step	Action
1	Log into ContentDirector as a system administrator.
2	On the main menu bar, click File.
3	Click Configuration.
4	Click the Ports tab.

Step	Action	
5	If...	Then...
	You want to use a specific Data/Applet or Command port	Under the appropriate port, enter the port number into the Value field.
	You can use any free Data/Applet or Command port	Under the appropriate port, click Find Free Port.
6	Click OK.	

Assignment file: Moving the assignment file saves disk space on the local drive of the core application machine.

To set the global assignment file location, complete the following steps.

Step	Action
1	Log into ContentDirector as a system administrator.
2	At the main menu bar, click File.
3	Click Configuration.
4	Click the Assignment tab.
5	Click Browse and select the new location for the assignment file.
6	Click OK.

New multicast error correction settings

The Policy screen contains new multicast error correction settings.

To set error correction in a policy, complete the following steps:

Step	Action
1	Create a new policy, or edit an existing one.
2	Click the Network tab.

Step	Action
3	Under Multicast Error Correction, there are two options: ◆ Light Error Correction This option retransmits data with error correction when an error is detected. ◆ Forward Error Correction This option sends additional data for error checking, and retransmits data when an error is detected. Use the default setting of Light Error Correction unless your ContentDirector network has both satellite connectivity and a large number of group members. Consult your Network Appliance System or Support Engineer for more information about error correction.
4	Fill in other policy settings as necessary.
5	Click OK.

Changes to logging

ContentDirector now creates two types of logs, both stored in *<\\core application machine\core application\ccm\logs>*:

- ◆ User log files, that have the name CDLog.N.txt where N is a number from 0 to 9
User logs contain user-friendly messages about the content distribution process. They display in the status window of the management console.
- ◆ Debugging logs, that have the name CDFESDbgLog.N.txt where N is a number from 0 to 9
Debugging logs contain detailed technical information about ContentDirector functions. Debugging logs are optional. They are designed to be used by Network Appliance support engineers to help you answer questions and resolve problems.
- ◆ Initialization error log files, that have the name CDiniterr.N.txt
Initialization error logs contain information about error states that occur during startup, before the logging service becomes available.

Restart button for management console

The management console has a Restart button to restart the core application. You might want use the restart button in the following situations:

- ◆ You set the service login to ensure correct permissions for mapped drives and need to restart the core application with the new service login.
- ◆ You set up a certificate for SecureAdmin™ software on a group leader and need to restart the core application for ContentDirector to recognize the certificate.
- ◆ The core application ceased responding to user inputs.

To use the Restart button, complete the following steps.

Caution

Restarting the core application suspends all jobs in progress. It also suspends the management console and all applets that are connected to the core application.

Step	Action
1	On the menu bar at the top of the ContentDirector main screen, click Tools > Restart Core Application.
2	At the Restart warning screen, click Yes. Result: The Restarting Core Application screen appears, instructing you to wait. The core application restarts after a brief waiting period.

F5 refresh in applet no longer requires re-login

Refreshing the screen in the applet with the F5 keyboard shortcut no longer requires re-login. This was a bug in ContentDirector 2.0.

Changes in controls for Status window

The following changes were made to Status window controls:

- ◆ The Preferences > Status tab no longer contains logging level options for the Status window. On the Status tab, the Buffer size setting is now named Capacity.
- ◆ You can display a higher level of detail in the Status window by enabling debug logging. For detailed instructions, see “[Logging](#)” on page 6.
- ◆ The Status window is hidden by default. A new menu item in View > Status window enables display of the Status window.

Option to fail job if source unavailable

There is a new option available in policies to fail jobs if any source files are not available.

To set this option, complete the following steps.

Step	Action
1	Create a new policy, or edit an existing one.
2	Click the Options tab.
3	Next to Fail Assignment If Any Source File Is Unavailable, select the check box to automatically fail the job if ContentDirector cannot access one of the source files for any reason. If you want the job to continue and ignore files that are not available, leave the check box unselected (default). If a job fails because a source file is unavailable, ContentDirector attempts to retry and repush according to the settings in the policy for that job. Because retry and repush require additional time, your choice for this feature must take into account your priorities: the need to push content quickly versus the need to ensure that the content reaches its destination. The importance of content reaching its destination is determined in part by the content type: ◆ If you are distributing streaming media files, you probably want to ensure that the whole assignment reaches its destination. Client requests that result in a miss can require time-consuming, bandwidth-intensive downloads from the origin server. ◆ If you are distributing http files, file sizes are smaller so client requests that are redirected to the origin server create less load. It is less important to ensure that the whole assignment reaches its destination.
4	Fill in other policy settings as necessary.
5	Click OK.

Default user group and default domain cannot be deleted

The default user group and default domain cannot be deleted. This resolves a bug in ContentDirector 2.0 that allowed system administrators to delete the default user group and domain.

**Scheme in Source >
Modify now writable**

Source schemes are now writable in the Modify Source window. This enables you to modify the source to reflect changes in content type.

**Requirement for
user name in
Source > Filer**

The user name in Source > Filer must be identical to the one set up on the filer for rsh permissions. See your filer documentation for more information about rsh permissions.

**Include files
functionality in jobs
has changed**

In Job > Filters, under From Source Location, the Include function has been modified. The Include function no longer offers a Browse button, and cannot be based on file names or directories. It must be based on file types.

**Cross-filesystem
limitation for
include function**

In Job > Filters, if you want to use the Include Only Files That Have Changed logic, avoid the combination of sources on NTFS and the shadow on FAT. NTFS and FAT handle creation and last access time differently, so that file attributes do not always translate accurately from one filesystem to the other. The resulting inconsistent metadata can cause the appearance of failure in Include Only Files That Have Changed.

Note

This is not an issue for filer-optimized jobs because filer snapshots take the place of the shadow.

Section B: User Interface

Scope of this section

This section contains information about issues related to the ContentDirector 2.1 user interface, including known problems, feature changes, and usage recommendations.

- Topics in this section**
- This section provides information about the following topics:
- ◆ [“Restart ContentDirector agent service after configuration changes”](#) on page 13
 - ◆ [“The installation utility and UI require 256 color capability”](#) on page 14
 - ◆ [“Avoid changing mime types in the Preferences dialog”](#) on page 14
 - ◆ [“Change in URL for starting applet”](#) on page 14
 - ◆ [“Ignoring drive access warnings results in invalid workspace”](#) on page 14
 - ◆ [“Methods for updating network segments from the applet”](#) on page 14
 - ◆ [“Avoid setting number of retries to 1 in policies”](#) on page 15
 - ◆ [“Avoid logging in and out several times as different users”](#) on page 15
 - ◆ [“Must revalidate header requires additional setting”](#) on page 15
 - ◆ [“Core application hangs and UI freezes”](#) on page 15

Restart ContentDirector agent service after configuration changes

You must disable and reenable the ContentDirector agent service for configuration changes in the ContentDirector > Advanced page of the NetCache Manager utility to take effect. On the Setup > ContentDirector pages in the NetCache Manager Utility, complete the following steps.

Note

It is not necessary to disable and reenable the service after configuration changes in the ContentDirector > General page.

Step	Action
1	On the General page, under ContentDirector Agent Enable, disable the service by deselecting the check box.
2	Click Commit Changes to disable the service.

Step	Action
3	Make the desired changes in the service configuration.
4	Click Commit Changes to save your configuration changes.
5	Reenable the service.
6	Click Commit Changes to reenoble the service.

The installation utility and UI require 256 color capability

The installation utility and user interface require that the video system be able to display at least 256 colors. If it cannot, the installation is not completed, and the user interface does not display properly.

Avoid changing mime types in the Preferences dialog

Changing mime types using the Cache tab in the preferences dialog is not supported in this release. Doing so might cause ContentDirector to hang.

Change in URL for starting applet

The URL for starting the applet has changed from version 1.0. To start the applet, use the following URL:

`http://<core_application_ip>:8080/ContentDirector`

Ignoring drive access warnings results in invalid workspace

When selecting a workspace, ContentDirector warns you if you do not have administrative access to the selected drive. If this warning appears, resolve the access issue before selecting the drive as workspace. Otherwise, you might have an invalid workspace and jobs will fail.

Methods for updating network segments from the applet

There are two methods for updating network segments:

- ◆ Clicking the Network button on the View toolbar at the left side of the main screen. This sends a request to the database to update the user interface with the latest information in the database.
- ◆ Pressing the F5 key or clicking the Refresh button. This sends a request to every group leader to report the status of destinations on its network segment. This method provides the most up-to-date information, but it can

take more time than the Network button refresh, because the group leaders must gather data and report back over the network.

Avoid setting number of retries to 1 in policies

On the Policy > Quorum tab, to enable retries, always set the Number field to a minimum of 2. The number of retries ContentDirector attempts is one less than the number of retries specified in this screen. Setting the number to 1 means that no retry is attempted. This occurs because the scheduler counts the current job run as a retry.

Avoid logging in and out several times as different users

In the User view, if you choose the Domain tab and log out and log in as a domain administrator, or if you choose the Domain tab or User Groups tab and log out and log in as a regular user, login becomes very slow and logout becomes impossible. The workaround is to close the UI and reopen it.

Must revalidate header requires additional setting

On the Policy > Cache tab, when you enable the Must revalidate header feature, the header is not revalidated. The workaround when you must revalidate is to also enable Max Age in the same screen and set it to zero.

Core application hangs and UI freezes

If the database hangs, the UI or applet can freeze or go to a gray screen. This occurs whether the UI or applet is being run directly on the core application machine or from a remote machine. In either case, the UI must be shut down and restarted. Under these circumstances, you might have difficulty reloading the UI. If this occurs, first try to kill the dbeng7 process. From the Windows command line, you can use the following:

```
my_prompt>drwtsn32 -p <pid> <cr>
```

<pid> is the process ID from the Task Manager Processes tab. This causes the core application to restart the database and usually resolves the issue. If not, restart the core application services. The worst case requires system reboot.

Section C: Disk space and file maintenance

Scope of this section

This section contains information about maintenance issues for ContentDirector 2.1, including disk space, backup, and file deletion.

Topics in this section

This section provides information about the following topics:

- ◆ [“Database backup”](#) on page 16
- ◆ [“Insufficient disk space”](#) on page 16
- ◆ [“Deleting assignment files in tomcat directory”](#) on page 16
- ◆ [“Insufficient disk space on cache”](#) on page 17

Database backup

It is advisable to back up the cmdata.db database file after ContentDirector is up and running and configured as you want. On Windows systems, this file is in the \CCM\Sybase\SybaseData directory. On Solaris systems, it is in the /opt/NTAPccm/sybase/SYBSsa7/ContentDirector/cmdata.db directory.

To restore the database, you need to delete the cmdata.log file before copying cmdata.db back to the original location.

Insufficient disk space

Running out of disk space on the core application server while ContentDirector is running can cause several problems. One problem concerns the servlet engine, Tomcat. If the core application machine runs out of disk space while an assignment is being written, the Tomcat engine might stop. See Chapter 5 of the *ContentDirector Administration Guide* for strategies for avoiding this problem.

Deleting assignment files in tomcat directory

When you run a job, the assignment file is stored temporarily in the \CCM\jakarta-tomcat\webapps\ContentDirector directory. Under some circumstances, ContentDirector cannot delete the assignment files in this directory after job assignments run. This can cause the disk to fill up and jobs to fail. If you are running large jobs repeatedly, you should check the \CCM\jakarta-tomcat\webapps\ContentDirector directory frequently. If there are assignments in the directory that are not those of currently running jobs, you should delete them. You must stop the ContentDirector service before you delete the files.

Insufficient disk space on cache

If a job pushes content to a cache with insufficient disk space, the assignment appears to proceed normally but fails in the commit phase. The error code 12510 with the message “Cache content fill error” indicates that there is insufficient disk space on the cache. This appears in the job history details screen in the UI.

Section D: Network-related issues

Scope of this section

This section contains information about network issues for ContentDirector 2.1, including recommendations for IP addressing, configuring destinations, moving destination appliances, limitations related to firewalls, and transport group dynamics.

Topics in this section

This section provides information about the following topics:

- ◆ [“Exchanging network interface cards”](#) on page 18
- ◆ [“Moving transport group constituents”](#) on page 18
- ◆ [“Synchronize time zone and time for Min Age feature”](#) on page 18
- ◆ [“Unicast member of transport group not recognized as a group leader”](#) on page 19

Exchanging network interface cards

After ContentDirector is installed and running, do not exchange network interface cards (NICs) between ContentDirector destinations. This causes addressing problems. It is acceptable to replace a malfunctioning NIC on a destination with a new NIC.

Moving transport group constituents

If you move a ContentDirector agent from one transport group to another and this agent is a potential group leader in the new transport group, run the following command in a Telnet session to the NetCache appliance:

```
set config.cd.net_segment_id -1
```

The preceding command is necessary only if the agent is a potential group leader.

Synchronize time zone and time for Min Age feature

To use the Min Age feature in policies, you need to synchronize the time zone and time. This means that the time zone and time must be exactly the same on the specified devices, even if they are separated geographically. The requirements vary, depending on how you are running ContentDirector.

If you are running ContentDirector at the core application server, you need to synchronize the core application and the NetCache destination.

If you are running ContentDirector remotely through the applet, you need to synchronize the machine running the applet, the core application server, and the NetCache destination, and restart the machine running the applet.

Unicast member of transport group not recognized as a group leader

This problem can occur when you have a transport group that consists of a group leader and group members on one subnet, and a single unicast group member on a separate subnet. A unicast group member cannot receive multicast communication from the group leader. One cause of this problem is that a non-multicast-enabled router is located between the group leader and the unicast group member.

Even if you configure the unicast group member as a primary group leader or a backup group leader, the ContentDirector agent ignores the group leader designation. It remains a group member only. To verify this situation and to view instructions for correcting it, view the ContentDirector agent log file on the Data > Log Files > ContentDirector page of the NetCache Manager utility. Search for the string “reconfig”.

The ContentDirector agent ignores the group leader designation because recognizing a separate unicast group leader would break the transport group.

Section E: Installing a Network Appliance self-signed certificate for SecureAdmin

Scope of this section This section contains instructions for setting up ContentDirector for use with the SecureAdmin™ software.

Topics in this section This section provides information about the following topics:

- ◆ “[About SecureAdmin](#)” on page 20
- ◆ “[Before you start](#)” on page 20
- ◆ “[Loading the certificate from NetCache into the browser database](#)” on page 21
- ◆ “[Creating a copy of the certificate](#)” on page 21
- ◆ “[Importing the certificate into the keystore](#)” on page 21

About SecureAdmin ContentDirector supports the SecureAdmin software for group leaders. The following instructions assume your browser is Internet Explorer and your core application is installed on a Windows NT® or Windows 2000 server.

Enabling support for SecureAdmin has three phases:

- ◆ Loading the certificate from NetCache into the browser database
- ◆ Creating a copy of the certificate
- ◆ Importing the certificate into the keystore

Before you start Before you start, follow the instructions in the SecureAdmin administration guide (available on the NOW site at <http://now.netapp.com>) to upload and install SecureAdmin on the NetCache appliance, and generate a self-signed certificate.

Caution

After you enable SecureAdmin on NetCache, the network segment to which the group leader belongs appears in the management console as off-line until you import the matching key file into ContentDirector and restart the service.

Loading the certificate from NetCache into the browser database

To load the certificate into the browser database, complete the following steps.

Step	Action
1	Connect to the NetCache appliance that has SSL enabled and has created a self-signed certificate, for example https://cache1.
2	Click Yes at the Security Alert screen regarding the certificate. This loads the certificate into the Internet Explorer database.

Creating a copy of the certificate

To create a copy of the certificate, complete the following steps.

Step	Action
1	In Internet Explorer, go to Tools > Internet Options > Content > Certificates > Intermediate Certification Authorities. The list should include a self-signed certificate issued to the NetCache appliance to which you connected, for example cache1.ourdept.ourcompany.com.
2	Click that certificate.
3	Click Export.
4	You enter a wizard to export a certificate. Choose the DER encoded binary X.509 format (default).
5	Export the file to any drive that can be accessed from the core application server.

Importing the certificate into the keystore

To import the certificate into the keystore, complete the following steps.

Step	Action
1	Change the current directory to the <Content Director Install Directory>/CCM/jre/lib/security.
2	Create a copy of the original cacerts file.

Step	Action
3	Using the keytool program installed in the jre, enter the following command: <pre>keytool -import -file netapp.cer -alias <unique key name> -keystore .\cacerts.</pre> You need the -alias option to assign a unique key to each group leader, assigned or candidate. Use an obvious name, such as the host name of the group leader. If you do not use the -alias option, you can import only one new key under the default name mykey. This is acceptable if the network segment has only one group leader.
4	Enter the password: changeit.
5	At the prompt, if you want to trust, press Y.
6	To view a list of the cacerts files and verify the presence of the new file, enter the following command: <pre>keytool -list -keystore .\cacerts</pre>
7	Restart the ContentDirector Service.

Note

If you generate a new certificate on a NetCache appliance configured as a group leader assigned or group leader candidate and import it into the ContentDirector core application, you need to restart the core application service and the ContentDirector agent on NetCache to ensure that they recognize the new certificate. This is not an issue for NetCache appliances that are group members only.

Section F: Filer integration

Scope of this section

This section contains instructions for using ContentDirector content sources on a Network Appliance filer. This information is also available in the *ContentDirector 2.1 Administration Guide*. It is presented here for convenience.

Topics in this section

This section provides information about the following topics:

- ◆ [“Supported filer versions”](#) on page 23
- ◆ [“Configuring ContentDirector to use a source on a filer”](#) on page 23
- ◆ [“Setting up the source on the filer”](#) on page 23
- ◆ [“Configuring ContentDirector to use the filer source”](#) on page 24
- ◆ [“Setting up a job to use the filer source”](#) on page 24

Supported filer versions

For filer integration, ContentDirector 2.1 supports the following versions of the Data ONTAP™ software:

- ◆ 6.1.1R1
- ◆ 6.0.1
- ◆ 6.0.3

Configuring ContentDirector to use a source on a filer

Configuring ContentDirector to use a source on a filer has three phases:

- ◆ Setting up the source on the filer
- ◆ Configuring ContentDirector to use the filer source
- ◆ Setting up a job to use the filer source

Setting up the source on the filer

To set up the source on the filer, complete the following steps.

Step	Action
1	Go to the administration page for the filer: http://filename/na_admin .
2	Click FilerView and log in.

Step	Action
3	Click Security, manage rsh access.
4	Click Insert entry.
5	Enter the host name or IP address of your core application machine. For user, enter root .

Configuring ContentDirector to use the filer source

To configure ContentDirector to use the source on the filer, complete the following steps.

Step	Action
1	Log into ContentDirector as a system administrator.
2	Create a new source by clicking Sources > New.
3	Select the scheme.
4	Enter the host name.
5	For source location, browse and select a location on the filer you set up in the previous steps.
6	Click Filer.
7	Click Optimize for filer.
8	Enter the host name for the filer.
9	Enter the volume name that your source location is mounted to, for example vol1, vol2, and vol3.
10	For remote user name, enter root .

Setting up a job to use the filer source

To set up a job for the filer source, complete the following steps.

Step	Action
1	Create a job by clicking Jobs > New.

Step	Action
2	For the source, select the new source that you just created on the filer.
3	Fill out the rest of the requirements for the job.

Note

For information about setting up permissions to use a filer as a source, see the *ContentDirector Administration Guide*, Appendix E, “Mapped Drive Permissions.”

Section G: Operating systems and applications

Scope of this section	This section contains information about issues related to operating systems and other applications.
Topics in this section	This section provides information about the following topics: ◆ “Windows Terminal Server” on page 26 ◆ “Solaris pkgadd limitation” on page 26 ◆ “RealServer requirement” on page 26 ◆ “Clear NetCache registry entry for pre-existing master key” on page 26
Windows Terminal Server	ContentDirector does not support Windows Terminal Server as an operating environment.
Solaris pkgadd limitation	This item applies to users who plan to install ContentDirector on a Solaris machine. Solaris pkgadd recognizes free space only for the partition containing the /opt directory. If you have the /opt directory set up as a sym link, the installation utility might display a warning message about inadequate available space, even though there is adequate free space in /opt. Click Yes to continue and proceed with the installation. The installation then proceeds normally.
RealServer requirement	If you distribute RTSP files using rtsp:// as the protocol, RealServer must be installed and running on the machine associated with the host site referenced in the source dialog for RealServer authentication to take place. The source files must be accessible to RealServer.
Clear NetCache registry entry for pre-existing master key	On any NetCache appliance that used an earlier version of ContentDirector, you must clear the NetCache registry entry for the master key before running the ContentDirector Agent. To clear the registry entry, complete the following steps.

Step	Action
1	At the CLI, enter the following command to check for a master key: show config.cd.master_key
2	If a master key is present, run the following command to clear the master key: set config.cd.master_key
3	Check that the NetCache autoconfig file is not still set to automatically update the master key. In the NetCache Manager utility, go to Setup > System > Automatic Configuration. Make sure that the master key is not referenced in the autoconfig file.

