

ContentDirector™ 2.0

Release Notes

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089-1125
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Information email: info@netapp.com
Information Web: <http://www.netapp.com>

Part number 210-00075
November 2001

Copyright and trademark information

Copyright information

Copyright © 1994–2001 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

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 European Union and a trademark of Network Appliance, Inc. in the United States 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, ContentDirector, ContentReporter, SecureAdmin, Serving Data by Design, Smart SAN, SnapManager, SnapMirror, SnapRestore, 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 2.0 Release Notes

Release notes contents

These release notes provide information on the following topics:

- ◆ “[User Interface](#)” on page 2
- ◆ “[Disk space and file maintenance](#)” on page 6
- ◆ “[Network-related issues](#)” on page 8
- ◆ “[Installing a Network Appliance self-signed certificate for SecureAdmin](#)” on page 11
- ◆ “[Filer integration](#)” on page 14
- ◆ “[Operating systems and applications](#)” on page 17

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 2.0 Installation Guide*.
- ◆ For configuration and administration information, see the *ContentDirector 2.0 Administration Guide*.

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 manuals.

Section A: User Interface

Scope of this section

This section contains information on issues related to the ContentDirector 2.0 user interface, including known problems, feature changes, and usage recommendations.

Topics in this section

This section provides information about the following topics:

- ◆ [“Log file levels”](#) on page 2
- ◆ [“Restart CDA service after configuration changes”](#) on page 3
- ◆ [“Removed Enable Shadow Copies, Enable Rollback, and Checkpoint”](#) on page 3
- ◆ [“The installation utility and GUI require 256 color capability”](#) on page 3
- ◆ [“Avoid changing mime types in the Preferences dialog”](#) on page 4
- ◆ [“Change in URL for starting applet”](#) on page 4
- ◆ [“Ignoring drive access warnings results in invalid workspace”](#) on page 4
- ◆ [“Methods for updating network segments from the applet”](#) on page 4
- ◆ [“Avoid setting number of retries to 1 in policies”](#) on page 4
- ◆ [“Avoid logging in and out several times as different users”](#) on page 5
- ◆ [“Must revalidate header requires additional setting”](#) on page 5
- ◆ [“Core application hangs and GUI freezes”](#) on page 5
- ◆ [“Upgrades from beta versions X1 - CD2.0X5 preserve file:/ source”](#) on page 5

Log file levels

You can configure the amount of detail that is saved in the log files by editing the cm.properties file in the \CCM\config directory. The default log detail (level 5) causes a reduction in performance speed due to the magnitude of disk writes. This level of log detail is unnecessary under most circumstances. If the reduction of performance is a concern for you, change the following line in the cm.properties file:

```
log_level=5
```

The log levels are listed below from least verbose to most verbose:

- ◆ ERROR = 1

- ◆ WARNING = 2
- ◆ SPECIAL = 3
- ◆ INFO = 4
- ◆ DEBUG = 5

Restart CDA service after configuration changes

You must disable and reenable the CDA service for configuration changes to take effect. On the Setup > ContentDirector pages in the NetCache Manager Utility, complete the following steps:

Step	Action
1	On the General page, under ContentDirector Agent Enable, disable the ContentDirector service by deselecting the check box.
2	Click Commit Changes to disable the CDA.
3	Make the desired changes in the CDA configuration.
4	Click Commit Changes to save your configuration changes.
5	Reenable the ContentDirector service.
6	Click Commit Changes to reenable the CDA.

Removed Enable Shadow Copies, Enable Rollback, and Checkpoint

The Enable Shadow Copies and Enable Rollback check boxes have been removed from the Policies > Options tab. The Checkpoint option has been removed from the Tools menu.

The rollback and checkpoint functions have been removed from the program. A shadow copy is made automatically unless the source is optimized for the filer, and the root for the source is on the volume of the filer shown by the optimization settings. In that case, a snapshot is substituted for the shadow.

The installation utility and GUI require 256 color capability

The installation program and the user interface require that the video system be able to display at least 256 colors. If it cannot, the installation will not complete, and the user interface will not be displayed 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 may cause the ContentDirector application 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.

Note

If you press the F5 key to update network segments from the applet, ensure that the focus is on the "All Network Segments" of the Network Segment View. Otherwise, you are returned to the Login window. To avoid this behavior in the applet, click the Refresh button to request a network segment, instead of using the F5 key.

Avoid setting number of retries to 1 in policies

On the Policy > Quorum tab, to enable retries, always set the Number field to 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, log in becomes very slow and log out becomes impossible. The workaround is to close the GUI and reopen it.

Must revalidate header requires additional setting

On the Policy > Cache tab, when you enable the Must revalidate header feature, the header will not be 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 GUI freezes

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

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

where <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.

Upgrades from beta versions X1 - CD2.0X5 preserve file:/ source

The upgrade from beta version X1, X2, X3, X4, or X5D3 leaves visible the option to use file:/ as a source in the source view, new source dialogue, and new job (source) dialogue. This feature is no longer supported. The workaround is to uninstall the previous version and start with a clean install of ContentDirector.

Section B: Disk space and file maintenance

Scope of this section	This section contains information on maintenance issues for ContentDirector 2.0, including disk space, backup, and file deletion.
Topics in this section	This section provides information about the following topics: ◆ “Database backup” on page 6 ◆ “Insufficient disk space” on page 6 ◆ “Deleting assignment files in tomcat directory” on page 6 ◆ “Insufficient disk space on cache” on page 7
Database backup	It is advisable to back up the database file cmdata.db once ContentDirector is up and running and configured as you wish. On Windows systems, this file is found in the \CCM\Sybase\SybaseData directory. On Solaris systems, it is located 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 <i>ContentDirector 2.0 Administration Guide</i> 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 is unable to delete the assignment files in this directory after job assignments have 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 GUI.

Section C: Network-related issues

Scope of this section

This section contains information on network issues for ContentDirector 2.0, 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 8
- ◆ [“Moving transport group constituents”](#) on page 8
- ◆ [“Single and multiple multicast IP addresses”](#) on page 9
- ◆ [“Synchronize time zone and time for Min Age feature”](#) on page 9
- ◆ [“Group leader limitation for NAT-based firewalls with single external address”](#) on page 9
- ◆ [“Unicast member of transport group not recognized as GL”](#) on page 10
- ◆ [“NetCache limit on number of multicast IP addresses”](#) on page 10
- ◆ [“Avoid multiple group leaders behind the same firewall”](#) on page 10

Exchanging network interface cards

Once ContentDirector is installed and running, do not exchange network interface cards between ContentDirector destinations. This will cause 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 CDA from one transport group to another, and this CDA 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 CDA is a potential group leader.

Single and multiple multicast IP addresses

Within a transport group, multicast transport is used for communication between the transport group leader and group members if possible. This requires multicast IP addresses. In the NetCache Manager utility, on the Setup > ContentDirector > Advanced page, you can choose between two methods of assigning IP addresses within multicast transport groups:

- ◆ Use Single Multicast IP address
- ◆ Use Multiple Multicast IP addresses for better performance

If you are using the cache for streaming content outside of ContentDirector, or if multicast IP address constraints are a concern for you, you should select "Use Single Multicast IP address" in the Advanced setup page for ContentDirector. In this case, two IP addresses are used, 239.100.1.1 and 239.100.1.2. This method is somewhat slower than the alternative.

"Use Multiple Multicast IP addresses for better performance" uses up to eight IP addresses, 239.100.1.1 to 239.100.1.8.

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 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.

Group leader limitation for NAT-based firewalls with single external address

If the core application and group leaders (GLs) are behind separate NAT-based firewalls that support only a single external address, the core application can recognize only one group leader behind each firewall. The single external address limitation means that additional GLs must be mapped to separate inbound administrative ports. The core application recognizes only one outbound administrative port. A fix is planned for a future release that will allow the core application to recognize additional outbound administrative ports.

Unicast member of transport group not recognized as GL

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

Even if you configure the unicast GM as a GL candidate or an assigned GL, the ContentDirector Agent ignores the GL designation. It remains a GM 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 GL designation because recognizing a separate unicast GL would break the transport group.

NetCache limit on number of multicast IP addresses

NetCache 5.2 has a limitation on the number of multicast IP addresses (eight is the maximum). ContentDirector has no limitation associated with this number. However, if both CDA and NetCache streaming (MMS or RTSP in multicast mode) are used at the same time, then one of these features of NetCache can be impacted if all multicast IP addresses are taken by another feature. The workaround is to check "Use Single Multicast IP address" on the group leader's Advanced page in the NetCache Manager utility. In this mode the group leader CDA instructs all group members in its transport group to use (to join) only one multicast IP address. The remaining seven multicast IP addresses could be used by NetCache streaming. Group members that are also configured to be a potential group leader (candidates and assigned) use one more IP address for the election process. Therefore the maximum number of IP addresses used by potential group leader CDAs in single IP mode would be 2. That leaves six multicast IP addresses for NetCache streaming.

Avoid multiple group leaders behind the same firewall

Avoid setting up multiple group leaders behind the same firewall. This can cause problems with duplicate IP addresses in the core application.

Section D: 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 11
- ◆ [“Before you start”](#) on page 11
- ◆ [“Loading the certificate from NetCache into the browser database”](#) on page 12
- ◆ [“Creating a copy of the certificate”](#) on page 12
- ◆ [“Importing the certificate into the keystore”](#) on page 12

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, <http://now.netapp.com>) to upload and install SecureAdmin on the NetCache appliance, and generate a self-signed certificate.

Caution

Once you enable SecureAdmin on NetCache, the network segment to which the group leader belongs appears in the management console as offline 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 on 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 CDA on NetCache to ensure that they recognize the new certificate. This is not an issue for NetCache appliances that are group members only.

Section E: 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 2.0 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 14
- ◆ [“Configuring ContentDirector to use a source on a filer”](#) on page 14
- ◆ [“Setting up the source on the filer”](#) on page 14
- ◆ [“Configuring ContentDirector to use the filer source”](#) on page 15
- ◆ [“Setting up a job to use the filer source”](#) on page 15
- ◆ [“Limit on number of concurrent jobs optimized for filer”](#) on page 16

Supported filer versions

For filer integration, ContentDirector 2.0 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 .

Step	Action
2	Click Filer View and log in.
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.
2	For the source, select the new source that you have just created on the filer.
3	Fill out the rest of the requirements for the job.

Note

For information on setting up permissions to use a filer as a source, see the *ContentDirector 2.0 Administration Guide*, Appendix E, "Mapped Drive Permissions."

Limit on number of concurrent jobs optimized for filer

The number of rsh connections supported by your filer limits the number of filer-optimized jobs you can run concurrently in ContentDirector. For each job that is optimized for the filer, ContentDirector uses a single rsh connection on the filer. There is an absolute limit on the number of rsh connections available for the filer. This limit is specific to the version of Data ONTAP running on the filer. The following table lists this limit for supported versions of Data ONTAP.

Data ONTAP version	Maximum number of rsh connections
6.0x	8
6.1x	12

Caution

Do not run more filer-optimized jobs concurrently than your version of Data ONTAP can support. Exceeding this limit can cause jobs to fail.

Other operations not related to ContentDirector can also use rsh connections. If you plan to run multiple jobs concurrently that are optimized for the filer, you need to be aware of the total number of rsh connections being used on the filer, both by ContentDirector and other operations.

Section F: Operating systems and applications

Scope of this section	This section contains late-breaking information on issues related to operating systems and other applications.
Topics in this section	This section provides information about the following topics: ◆ “Operating system language” on page 17 ◆ “Windows Terminal Server” on page 17 ◆ “Solaris pkgadd limitation” on page 17 ◆ “RealServer requirement” on page 17 ◆ “Clear NetCache registry entry for pre-existing master key” on page 18
Operating system language	ContentDirector supports only US English operating systems.
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. Press 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 in order 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 the master key is not referenced in the autoconfig file.