

ContentDirector™ 2.1 Read Me First

ContentDirector now supports Data ONTAP 6.2

For file integration, ContentDirector 2.1 supports Data ONTAP™ 6.2 software.

New method for handling port conflicts during installation

The port changer automatically detects port conflicts during installation on the default 3229 command port, 1099 RMI port, and 8080 data/applet port. The behavior of the port changer depends on the operating system of the core application machine:

- ◆ On Solaris®, the port changer silently selects another port. The new ports are written to /opt/NTAPccm/lib/cm.properties.
- ◆ On Windows®, the port changer displays the Port Conflict Resolver wizard, which offers the following options:
 - ❖ Type in a specific port number.
 - ❖ Request the Port Conflict Resolver to automatically find a free port.

Note

If the data/applet port changes from the default, be sure to specify the correct port when accessing ContentDirector through the browser applet. On Solaris, the new port is in cm.properties, on the line: `http_servlet_port=[new port]`. On Windows, the new port is displayed in the File > Configuration > Ports screen.

Configuring ContentDirector Agent General options on NetCache

Before configuring the ContentDirector Agent General options, note the changes in terminology in the current release.

Changes to group leader option names: The names for group leader options have changed, but the functionality is the same as in the previous release. The following table lists each old option name and the corresponding new option name.

Old name	New name
Assigned	Primary
Candidate	Backup

Configuring the ContentDirector Agent as group leader: To configure the ContentDirector Agent as a group leader, complete the following steps.

Step	Action	
1	From the NetCache™ Manager utility, choose Setup tab > ContentDirector > General.	
2	Select the ContentDirector Agent Enable check box.	
3	In the ContentDirector Agent Operating Mode option, select Group Leader and choose the group leader state. Group leaders can have two states: ◆ Primary (assigned) ◆ Backup (candidate)	
4	If...	Then...
	You selected primary group leader in the previous step	Enter the IP address of the core application in the Core Application IP Address option.
	You selected backup group leader	The Core Application IP Address option is read only. Skip to the next step.
5	Click Commit Changes at the bottom of the page.	
6	Configure any required group leader advanced settings. See “Configuring ContentDirector Agent Advanced options on NetCache” on page 3 for information about these advanced settings.	

Configuring the ContentDirector Agent as group member: To configure the ContentDirector Agent as a group member, complete the following steps.

Step	Action
1	From the NetCache Manager utility, choose Setup tab > ContentDirector > General.

Step	Action
2	If you have not already done so, select the ContentDirector Agent Enable check box.
3	In the ContentDirector Agent Operating Mode option, select Group Member.
4	Click Commit Changes at the bottom of the page.
5	Configure any required group member advanced settings. See “Configuring ContentDirector Agent Advanced options on NetCache” on page 3 for information about these advanced settings.

Configuring ContentDirector Agent Advanced options on NetCache

Use the following recommendations to determine whether you need to configure any of the ContentDirector Advanced options.

Note

For changes on the Advanced page to take effect, after committing your changes you must disable and then reenable ContentDirector as detailed at the top of the ContentDirector > Advanced page.

Situation	Recommendation	See...
Recommendation for all ContentDirector Agents		
If this NetCache appliance has multiple interfaces enabled and you want to use a specific interface for ContentDirector	Select an interface from the Interface Selection - Interface to Use option.	“Selecting a NetCache appliance interface” on page 4
Group member recommendations		
If the group member is behind a firewall and can’t communicate with the group leader	Configure the Firewall Configuration - External Address option.	“Identifying a ContentDirector Agent behind a NAT-based firewall” on page 5

Situation	Recommendation	See...
If the group member is not on a multicast-enabled network and can't communicate with the group leader	Configure the Transport Configuration - Group Leader IP Address option	“Specifying the group leader IP address” on page 5
Group leader recommendations		
If the group leader is behind a firewall and can't communicate with group members	Configure the Firewall Configuration - External Address option.	“Identifying a ContentDirector Agent behind a NAT-based firewall” on page 5
If the group leader uses a satellite or wireless network to distribute ContentDirector data to group members	Enable the Transport Configuration - Satellite Network option.	“Enabling the Satellite Network option” on page 6
If there is a restriction on the number of multicast IP address that the CDA can use	Enter a value in the Transport Configuration - Maximum number of Multicast IP Addresses to use option.	“Specifying the number of multicast IP addresses” on page 6

Selecting a NetCache appliance interface: If this NetCache appliance has multiple interfaces enabled, you can select which interface to use for the ContentDirector agent. To select an interface, complete the following steps.

Step	Action
1	From the NetCache Manager utility, choose Setup tab > ContentDirector > Advanced.
2	In the Interface Selection - Interface to Use option, select an interface from the drop-down list box.
3	Commit changes.
4	Disable and then reenable ContentDirector from the ContentDirector > General page.

Identifying a ContentDirector Agent behind a NAT-based firewall: If this ContentDirector Agent is behind a firewall that uses Network Address Translation (NAT) to obscure internal IP addresses, you must specify the IP address of the ContentDirector Agent so that it can communicate with the external ContentDirector devices.

Note

Firewalls configured for dynamic NAT addressing are not supported. The ContentDirector Agent communicating with group members or a group leader outside the firewall must have a static NAT address.

To specify the static NAT IP address of the ContentDirector Agent, complete the following steps.

Step	Action
1	From the NetCache Manager utility, choose Setup tab > ContentDirector > Advanced.
2	Under Firewall Configuration, enter the IP address in the External Address option.
3	Commit changes.
4	Disable and then reenable ContentDirector from the ContentDirector > General page.

Specifying the group leader IP address: If the group member is not on a multicast-enabled network and can't communicate with the group leader, configure the group leader IP address option.

To configure this option, complete the following steps.

Step	Action
1	From the NetCache Manager utility, choose Setup tab > ContentDirector > Advanced.
2	Under Transport Configuration, enter the group leader IP address in the Group Leader Address option.
3	Commit changes.

Step	Action
4	Disable and then reenable ContentDirector from the ContentDirector > General page.

Enabling the Satellite Network option: For group leaders that communicate with group members through a satellite or wireless network, enable the Satellite Network option.

To enable this option, complete the following steps.

Step	Action
1	From the NetCache Manager utility, choose Setup tab > ContentDirector > Advanced.
2	Under Transport Configuration - Satellite Network, select the Satellite Communication Enabled check box.
3	Commit changes.
4	Disable and then reenable ContentDirector from the ContentDirector > General page.

Specifying the number of multicast IP addresses: If your organization limits the number of multicast addresses you can use on the network, set the number of multicast IP addresses.

To specify this option, complete the following steps.

Step	Action
1	From the NetCache Manager utility, choose Setup tab > ContentDirector > Advanced.
2	Under Transport Configuration, enter a value in the Maximum Number of Multicast IP Addresses to Use option.
3	Commit changes.
4	Disable and then reenable ContentDirector from the ContentDirector > General page.

Upgrading from ContentDirector 2.0

You can upgrade ContentDirector 2.0 to ContentDirector 2.1. The Upgrade/Repair option in the installation utility contains automatic file merger and backup routines that conserve your existing database and settings from ContentDirector 2.0.

Before you start: The installation utility attempts to back up critical files before upgrading. In case the utility cannot perform the automatic backup, it is recommended that you back up the following ContentDirector database and settings files to a separate location before upgrading:

- ◆ cmdata.db
- ◆ cmdata.log
- ◆ cm.properties
- ◆ jssecacerts
- ◆ cacerts
- ◆ vsites.properties
- ◆ server.xml

The paths to these files are listed in the following tables.

File name	Windows path <i>\install directory\CCM...</i>
cmdata.db, cmdata.log	.\Sybase\SybaseData
server.xml	.\jakarta-tomcat\conf
cm.properties, jssecacerts, cacerts, vsites.properties	.\config

File name	Solaris path <i>/opt/NTAPccm...</i>
cmdata.db, cmdata.log	./sybase/SYBSsa7/ContentDirector
server.xml	./jakarta-tomcat/conf
cm.properties	./lib
cacerts	./JRE/lib/security

File name	Solaris path /opt/NTAPccm...
jssecacerts, vsites.prop	/etc/opt/NTAPccm

Cm.properties merge: ContentDirector 2.1 requires a new version of the cm.properties settings file. The installation utility creates a copy of your existing cm.properties file, called cm.properties.old. It then attempts to merge this copy with the new version, saving any customized settings you have in this file. After the two files are merged, the installation utility either displays or records a record of any differences, depending on the operating system of the core application machine:

- ◆ On Windows, the differences are presented on screen.
- ◆ On Solaris, the differences are written to the /opt/NTAPccm/lib/cm.properties.log file.

Note

The log file contains only differences between properties that exist in both the old and new versions. If you added a property, it is preserved in the new version of cm.properties but its existence is not recorded in the log file.

Settings file backup: The installation utility automatically backs up the existing versions of the vsites.properties, server.xml, jssecacerts, and cacerts settings files. The backup files have the same names as the originals, but add a .old extension.

Note

On Windows, all existing settings in the security cacerts and jssecacerts settings files are preserved, but the files are not copied to backups with .old extensions.

If there are any differences between the existing version and the new version, the installation utility uses your existing version, and the new version is saved with a .new extension.

Database backup: The installation utility automatically backs up the existing cmdata.db database file to an archive file with the same name and a .backup extension. The existing cmdata.db file is also copied to a temporary backup file with a .bak extension. The cmdata.db.bak file is copied to the new file, and the schema is updated to the new version.

Upgrading on Windows: To upgrade from ContentDirector 2.0 to ContentDirector 2.1 on Windows, complete the following steps.

Step	Action	
1	Insert the ContentDirector CD-ROM into the CD-ROM drive.	
2	If the CD-ROM does not run automatically, navigate to the Windows directory of the CD-ROM and double-click ContentDirector2_1.exe to begin the installation.	
3	At the InstallShield Wizard screen, click Next. Result: The installation utility extracts the necessary files.	
4	At the Welcome screen, select Repair/Upgrade and click Next.	
5	If...	Then...
	You did not back up the database and settings files	Click Yes at the Question screen. Result: The upgrade terminates.
	You did back up the database and settings file	Click No at the Question screen. Result: The upgrade continues.
6	At the Edit Data screen, enter your license key if you have one, or use the Evaluation license, and then click Next.	
7	At the first Information screen describing cm.properties file merger, click OK.	
8	At the second Information screen describing server.xml and vsites.properties backup, click OK. Result: The ContentDirector service starts.	
9	At the Maintenance Complete screen, click Finish to dismiss the InstallShield wizard.	

Upgrading on Solaris: To upgrade the core application on Solaris, complete the following steps.

Step	Action
1	From any prompt, enter the following command: <pre>pkgadd -d <cdrom mount point>/solaris/NTAPccm.</pre> Result: The available package information is displayed. You receive the following prompt. <pre>Select package(s) you wish to process (or 'all' to process all packages). (default: all)</pre>
2	Press Enter to select the default. Result: Processing begins and the following prompt is displayed: <pre>This appears to be an attempt to install the same architecture and version of a package which is already installed. This installation will attempt to overwrite this package.</pre> Processing begins and the license is displayed. The following prompt appears: <pre>Do you agree to this license (y/n)?</pre>
3	Enter Y to agree to the license and continue the installation. Result: The following prompt appears: <pre>Upgrade/Repair strongly suggests you back up the following files to a separate location. /opt/NTAPccm/sybase/SYBSsa7/ContentDirector/cmdata.db /opt/NTAPccm/sybase/SYBSsa7/ContentDirector/cmdata.log /opt/NTAPccm/lib/cm.properties /etc/opt/NTAPccm/jssecacerts /opt/NTAPccm/JRE/lib/security/cacerts /etc/opt/NTAPccm/vsites.prop /opt/NTAPccm/jakarta-tomcat/conf/server.xml Would you like to stop the Upgrade/Repair process so you can back up these files (y/n)? n</pre>

Step	Action	
4	Enter N to continue the installation, or Y to terminate the installation and back up the files.	
5	If...	Then...
	You entered N	The upgrade continues. Result: The following prompt appears: Enter product license key (press enter for evaluation):
	You entered Y	The upgrade stops.
6	Press Enter to accept the evaluation license or type in your license key. Result: The following prompt appears: Would you like the Install to start the ContentDirector Core Application daemon automatically when completed (y/n)?	
7	Enter Y. This package contains scripts which will be executed with super-user permission during the process of installing this package. Do you want to continue with the installation of <NTAPccm> [y,n,?]	

Step	Action
8	Enter Y. Result: the following text is displayed: <pre>Installing Core Application 2.1 as <NTAPccm> ## Installing part 1 of 1.</pre> The directories and files that are being copied scroll past, after which information about the final installation processes is displayed. If the installation is completed successfully, the last line of screen output is the following: <pre>Installation of <NTAPccm> was successful.</pre>

Use of host name when verifying filer settings

Use a known valid host name rather than an IP address when verifying filer settings. ContentDirector hangs in the Check Filer Settings window if the filer is not reachable due to any of the following causes:

- ◆ Invalid host name or IP address
- ◆ Valid IP address but filer lost connectivity or is down

Correct path to new master key

On page 129 of the *ContentDirector 2.0 Administration Guide*, in the section “Changing master keys to ensure data security - Generating a new master key,” the path to the newly created master key is incorrect. The correct path is as follows:

<path>/install directory/config/master_key_<digits>