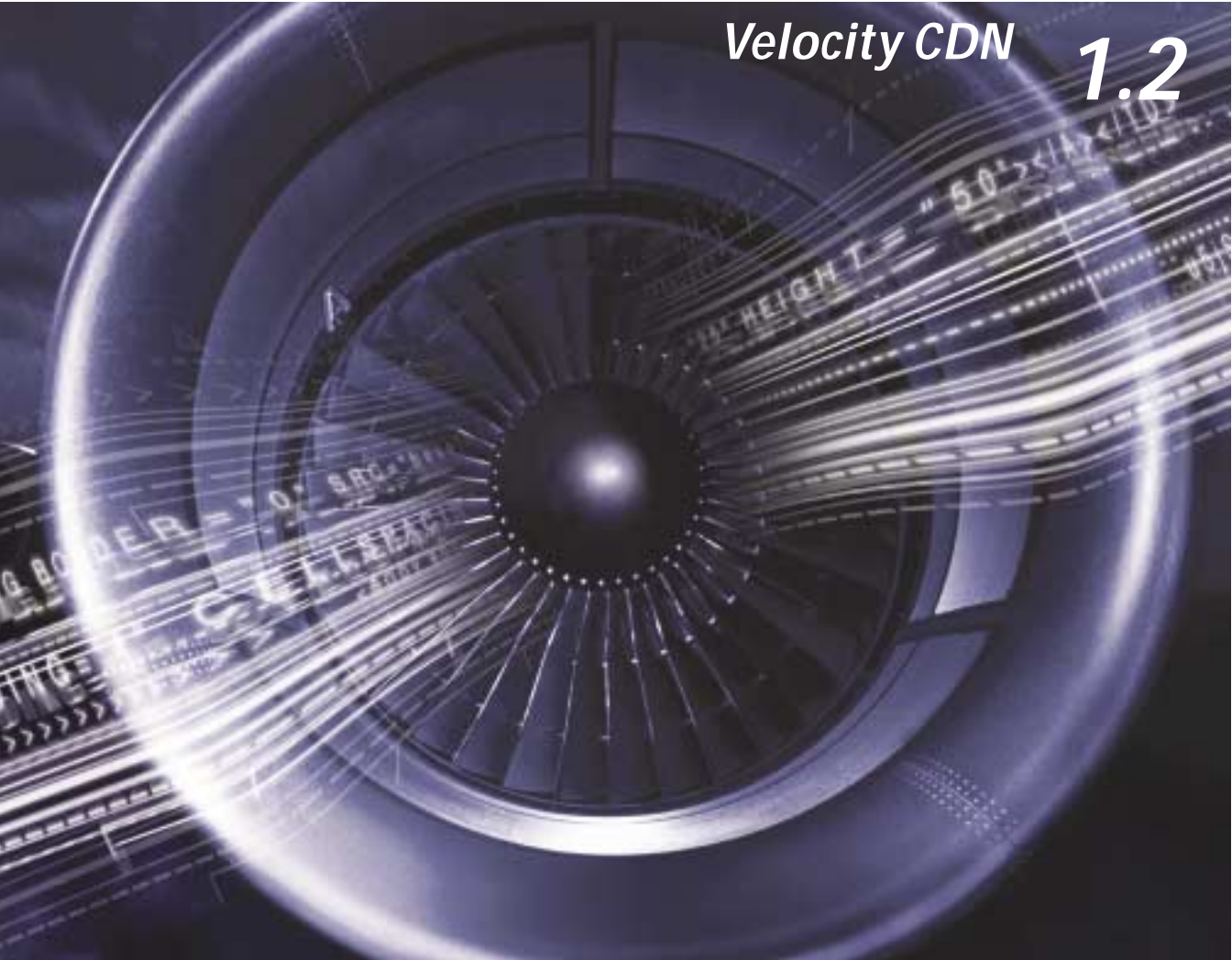




Velocity CDN **1.2**



***System Controller
Deployment Guide***

Legal Notices

Volera, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Volera, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Volera, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Volera, Inc. reserves the right to make changes to any and all parts of Volera software, at any time, without any obligation to notify any person or entity of such changes.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

Copyright © 1997-2002 Volera, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

U.S. Patent Nos. 5,870,739; 5,873,079; 5,884,304; 6,330,605. U.S. and Foreign Patents Pending.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

Volera, Inc.
2211 North First Street
San Jose, CA 95131-2021
U.S.A.

www.volera.com

System Controller Deployment Guide
June 2002

Online Documentation: To access the online documentation for this and other Volera products, and to get updates, see www.volera.com.

Volera Trademarks

Volera is a trademark of Volera, Inc. in the United States and other countries.

Third-Party Trademarks

Third-party trademarks (indicated by asterisks[*]) are the property of their respective owners.

Contents

About This Guide	9
Part I Preparing Your Content Network for Management	
1 Preparing Velocity Management Servers	13
Installing the First Velocity Management Server	13
Installing Velocity License Files	14
Installing Additional Velocity Management Servers	14
Providing for Communication Between Content Network Components	15
2 Using the Browser-Based Management Tool	17
Starting the Browser-Based Management Tool	17
Using the Management Suite List Filters.	17
3 How the Velocity Management Suite Scheduler Works	19
Only Administrators with Full Access Can Schedule and Modify Configuration Changes	19
Scheduling Configuration Changes	19
Scheduling Group Configuration Changes.	20
How the Scheduler Reschedules Failed Events	21
4 Creating Private CDNs	23
5 Creating and Managing Content Network Administrators	25
A Preview to Granting Administrative Access Rights	25
Creating Administrators	31
Additional Steps for System Controller Administrators	32
Additional Steps for Content Controller Administrators.	33
Modifying Administrator Information and Access Rights	34
Deactivating Administrator Accounts.	34
Removing Administrators	35
6 Preparing Cache Devices for Management	37
Initial Setup.	37
Configuring New Cache Devices	37
Setting a vcdn Management Address on Each Cache Device	37
Device Passwords Must Not Contain Spaces	38
Adding New Cache Devices in System Controller	38

7	Managing and Configuring Cache Devices	39
	Working with Cache Device Management Addresses.	39
	Managing Cache Device Configurations	39
	Automatic Recovery After a Failed Configuration Attempt	40
8	Managing and Configuring Cache Device Groups	41
	The Purposes of Cache Device Groups.	41
	How Group Configuration Works	42
	Understanding Group Configuration Settings	42
	Group Configuration Settings Are Stored in Configuration Data Objects	43
	Group Configuration Settings Are Initially Empty	44
	Cautions for Applying Configuration Settings at a Group Level	45
	A Tip for Grouping Cache Devices	46
	How Group-Level Configuration Affects Grouped Cache Devices.	46
	Creating Cache Device Groups	55
	Removing Cache Device Groups	56
	Adding a Cache Device to a Group	57
	Removing Cache Devices from Groups.	58
 Part II Creating Caches on Your Content Network		
9	Creating HTTP Caches	61
10	Creating Streaming Media Caches	63
	Excelsior Cache Devices Support Apple QuickTime by Default	63
	Using Media Excelsior for Apple QuickTime	63
	Using Media Excelsior for Windows Media	64
	Using Media Excelsior for Real Media	64
 Part III Providing Access to Caches		
11	Configuring Browsers and Players to Use Network Caches	67
12	Web Proxy Auto-Discovery (WPAD) Setup	69
13	Limiting Access to Caches	71
	Implications for Using Authentication on Your Content Network	71
 Part IV Monitoring and Maintaining Your Content Network		
14	Monitoring Device and Group Health	75
15	Monitoring Cache Devices and Content	77
	General Overview	77
	System Performance Monitoring	78
	Additional Requirements for System Monitoring.	78
	How System Monitoring Works	79

Troubleshooting System Monitoring Problems	79
Content Monitoring	80
16 Uninstalling Velocity Management Suite Components	81
Uninstalling Content Accountant	81
From a GUI Interface	81
At the Server's Command Line	81
Uninstalling Content Controller	82
From a GUI Interface	82
At the Server's Command Line	82
Uninstalling System Controller	82
From a GUI Interface	82
At the Server's Command Line	82
17 Upgrading the Velocity Management Suite	83
Versions 1.0 and 1.2 Cannot Be Used Together	83
Migrating an Existing 1.0 Datastore	83
Upgrading to Version 1.2	83
Synchronizing Exceleator 2.1 Devices	84
Upgrading a Multiserver Installation	84
18 Synchronizing Devices and Datastores	85
Device-Level Synchronization	85
Group-Level Synchronization	86
System-Level Synchronization	87
19 Changing the Management Server's IP Address	89
20 Shutting Down and Restarting	91
Shutting Down Cache Devices	91
Shutting Down Velocity Management Servers	91
21 Synchronizing Time on Your Content Network	93
Server Time Must Be Set Prior to Installation	93
22 Backing Up and Restoring the Datastore	95
23 Securing the Content Network	97
Securing the Connections Between Browsers and Management Servers	97
Managing HTTP CONNECT Method Support	98
24 Keeping Content Network Data Secure	99
SSL and Exceleator Cache Devices	99
Exceleator's Internal CA	99
Generating Certificate Signing Requests (CSRs)	100
Using Secure Exceleator on Your Content Network	100

About This Guide

This manual contains an overview of content distribution and delivery networks (CDNs) and explains how the Velocity™ management suite helps you create and manage them.

To	See
Prepare your content distribution and delivery network (CDN) for management	“Preparing Your Content Network for Management” on page 11.
Create content caches on your CDN	“Creating Caches on Your Content Network” on page 59.
Provide access to CDN caches	“Providing Access to Caches” on page 65.
Monitor and maintain the CDN after it is installed and delivering content	“Monitoring and Maintaining Your Content Network” on page 73.

Preparing Your Content Network for Management

The following table summarizes the tasks discussed in this section.

To	See
Prepare one or more Velocity management servers to manage your content distribution and delivery network (CDN)	Chapter 1, "Preparing Velocity Management Servers," on page 13.
Use the browser-based management tool	Chapter 2, "Using the Browser-Based Management Tool," on page 17
Understand how the Velocity management suite event scheduler works	Chapter 3, "How the Velocity Management Suite Scheduler Works," on page 19
Create private CDNs	Chapter 4, "Creating Private CDNs," on page 23
Create content network administrators and restrict administrative access to Velocity management suite components	Chapter 5, "Creating and Managing Content Network Administrators," on page 25
Prepare cache devices for management	Chapter 6, "Preparing Cache Devices for Management," on page 37
Manage cache devices	Chapter 7, "Managing and Configuring Cache Devices," on page 39
Manage cache device groups	Chapter 8, "Managing and Configuring Cache Device Groups," on page 41

1

Preparing Velocity Management Servers

Getting Started with System Controller describes basic Velocity management server setup. This chapter provides additional setup information, including the topics summarized in the following table:

To	See
Set up the first Velocity management server	“Installing the First Velocity Management Server” on page 13
Set up additional Velocity management servers	“Installing Additional Velocity Management Servers” on page 14

Installing the First Velocity Management Server

When installing the first Velocity management server, you are asked to specify a name for the Velocity management suite datastore. This same datastore name must be specified for each additional Velocity management server that will share and jointly manage the objects in the datastore.

If you plan to have multiple, independent Velocity management suite implementations for evaluation or testing purposes, you must ensure that you give each management suite datastore a unique name.

For example, if you install two content networks with two management servers for independent testing of HTML and multimedia functionality, you might name the datastore on the first server *TestHTML*, and the datastore on the second server *TestMM*. If you added more servers to either network, you would then name the datastores either *TestHTML* or *TestMM*, depending on which network the new Velocity management server will help manage.

WARNING: This is especially critical if the networks are independent and not initially connected but might be connected in the future. Failure to follow this rule will cause corruption and data loss if and when the networks can communicate with each other.

Installing Velocity License Files

Each Velocity license file contains two critical authorization numbers for each management suite component it licenses:

- ◆ The number of management servers on the network that can run the management suite components (System Controller, Content Controller, or Content Accountant) for which the license was issued
- ◆ The total number of Excelerator cache devices that the management servers running on the network can manage

All of the license files for all Velocity products can and should be installed on each management server.

The reason for this is that each server requires a locally installed license for each Velocity product it communicates with, including the Excelerator cache devices it manages on the network. A given management server will not recognize more Velocity product instances than it has licenses for.

Install all of your Velocity license files on each management server on the network by completing the following steps:

- 1 Use any method to copy all purchased license files to the `/opt/volera/roma/licenses` directory on each management server.
- 2 Restart each server after copying the license files.

Installing Additional Velocity Management Servers

The Velocity management suite provides for automatic datastore synchronization between the datastores on all Velocity management servers managing the same content distribution and delivery network. There are three requirements for datastore synchronization:

- ◆ The management servers must be able to communicate with each other on the same network.
- ◆ During System Controller installation of each additional management server, you must specify that each is a secondary server that shares an existing datastore.
- ◆ You must enter the same datastore name when installing each additional management server.

- ♦ All management servers using the same datastore must have time synchronized using NTP or some other time synchronization tool.

For help enabling the standard RedHat 7.2 Date and Time mechanisms, refer to the following URL: <http://www.redhat.com/docs/manuals/linux/rhl-7.2-Manual/custom-guide/dateconfig.html>.

Providing for Communication Between Content Network Components

You must ensure that the following communication is possible on your network:

- ♦ **Velocity management servers:** All Velocity management servers containing System Controller must be able to communicate with each other to keep their datastores synchronized.
- ♦ **Velocity management servers and cache devices:** The management servers must be able to communicate with the cache devices on the port configured (default port is 443). You must provide communication through any firewalls that are between the servers and the cache devices. Additionally, no other services can be running on the same IP address/port combination. For example, if you are using Secure Excelsator on managed devices, you must move Velocity management to another IP address/port combination.
- ♦ **Velocity management servers and Managing Browsers:** If browsers and Velocity management servers are on the same network, they can communicate using the standard HTTP or HTTPS protocols. To use HTTPS, the management server must be configured to do so. For more information, see [“Securing the Connections Between Browsers and Management Servers” on page 97](#).

If they are separated by one or more firewalls, you will need to ensure that the appropriate HTTP or HTTPS ports are enabled for this communication.

2

Using the Browser-Based Management Tool

You manage your content network using a browser to access one or more of the Velocity management servers you have installed.

This chapter provides information regarding the following topics:

Starting the Browser-Based Management Tool

To start the browser-based management tool, complete the following steps:

- 1 On your management workstation, start a browser.
You must use Internet Explorer 5.5 or higher.
- 2 Direct the browser to the IP address, hostname, DNS name, or URL of the Velocity management server.
- 3 Log in using the Administrator name and password you specified when installing System Controller.

Using the Management Suite List Filters

If you need to find multiple groups, cache devices, collections or jobs, you can use the list filter. If partial names are used, you must include an asterisk for the characters that follow. Only the names matching the filter field value are displayed. Use the Clear button to redisplay the entire list.

Also, when selecting named objects for applying some action, keep in mind that selected objects are cleared each time the filter feature is used. For example, if you select an object at the beginning of the list and then apply a filter to find another object, the first object is no longer selected.

Boolean searching is not supported. To select multiple objects that cannot be easily returned by a single search operation, you might need to check each object from within the complete listing.

3

How the Velocity Management Suite Scheduler Works

Understanding the process the Velocity management server follows when applying configuration changes to managed cache devices and Exceleator groups will prevent your thinking that a configuration operation has failed when in fact the change is merely in the process of being applied.

NOTE: There is no upper limit to the number of operations (configuration changes, synchronization requests, etc.) you can schedule for your network.

The management server executes 20 operations at once. Therefore, if you schedule more than 20 operations, the first 20 will begin executing when the scheduled time arrives, and the 21st operation will begin when any one of the initial 20 operations completes and a slot opens up.

Only Administrators with Full Access Can Schedule and Modify Configuration Changes

Administrators with access to System Controller and full access rights to devices and group can create and modify all scheduled change events for their managed groups and devices, including those changes that were previously scheduled by other administrators. This includes changing the time at which scheduled changes will be applied.

The datastore keeps only the last-scheduled configuration settings for any given service or parameter. All scheduled changes are applied when the scheduled time arrives.

Scheduling Configuration Changes

All configuration changes that are not immediately applied have a scheduled time at which the changes will be sent to the affected cache device and put into effect at the cache device level.

Status messages for individual cache devices are as follows:

- ◆ **Pending:** This means that changes have been registered in the datastore and will be applied when the scheduled date and time arrive. Click the View link for more detail.

- ♦ **Executing:** This means that the scheduled date and time has arrived and the changes have been sent to the cache device. Click the View link for more detail.
- ♦ **Succeeded:** This means that the cache device received the changes and the changes have been applied. Click the View link for more detail.
- ♦ **Failed:** This means that the change failed at some level. If there is a View link, you can click it for more detail. If there is no View link, this indicates that the change could not be scheduled for the cache device.
- ♦ **Incomplete:** Not all changes have been applied. Click the View link to access an Alert page listing the failed configuration changes.

NOTE: If the Failed Configuration Changes alert has been deleted, the View link might not be active.

Scheduling Group Configuration Changes

All configuration changes to groups have an associated scheduled time at which the changes will be sent to the group's cache devices and put into effect at the cache device level.

After you have applied (scheduled) a configuration change to the group, you can see the status of the event on the Schedule screen. However, you cannot see the status of devices within the group from this screen. You must click the event name to see the status of individual devices.

Status messages for groups are as follows:

- ♦ **Pending:** This means that changes have been registered in the datastore and will be applied when the scheduled date and time arrive.
- ♦ **Executing:** This means that the changes have been sent to the cache devices. Click the View link for more detail.
- ♦ **Failed:** This means that changes failed at some level. Click the View link for details.
- ♦ **Finished:** This means that the changes were created for each cache device.

IMPORTANT: This does not indicate that changes were applied successfully to each cache device. You should always verify at the cache device level that changes have actually been applied. To do this, access the schedule for each cache device.

To see the status of individual devices, click the event name.

Scheduled group changes are applied to the cache devices that are members of the group when the scheduled event occurs. For example, if you add a cache device to a group after scheduling a configuration event and before the scheduled time arrives, the changes will be applied to the entire group, including the cache device you have added to the group. The same logic applies to cache device resources, such as IP addresses bound to network cards, etc. Configuration changes are applied to the resources that are current when the changes actually occur.

Also, if configuration changes are made to an individual cache device during the execution of a group scheduled change, there is no guarantee that the group changes will be made.

How the Scheduler Reschedules Failed Events

Various conditions might prevent a scheduled event from completing the first time it is attempted. For example, a cache device might be restarting as part of a maintenance cycle when the scheduled date and time arrives.

All group configuration changes are scheduled. Configuration changes to individual cache devices that are immediately applied are not scheduled. However, if the configuration change fails, it will be automatically rescheduled. The same applies to group configuration changes that fail when the first scheduled date and time arrives.

Velocity management servers reschedule failed events according to the following table

Table 1 **Event Rescheduling**

Retry Attempt Number	Interval From Last Failed Attempt
1	15 minutes
2	15 minutes (30 minutes from initial attempt)
3	15 minutes (45 minutes from initial attempt)
4	15 minutes (one hour from initial attempt)
5	One Hour (two hours from initial attempt)
6	One Hour (three hours from initial attempt)
7	One Hour (four hours from initial attempt)

Retry Attempt Number	Interval From Last Failed Attempt
8	One Hour (five hours from initial attempt)
9	One Hour (six hours from initial attempt)
10	One Hour (seven hours from initial attempt)
11	One Hour (eight hours from initial attempt)
12	One Hour (nine hours from initial attempt)
13	One Hour (ten hours from initial attempt)
14	One Hour (11 hours from initial attempt)
15	One Hour (12 hours from initial attempt)
16	Twelve hours (24 hours from initial attempt)

NOTE: If this attempt fails, the event fails and is not rescheduled.

4

Creating Private CDNs

The instructions in this chapter apply only if your content network requires private CDNs. The process for determining this is explained in [Planning Your Content Network](#) in the *Planning Guide*.

If you need to create one or more private CDNs, complete the following steps:

- 1 Locate the Private CDN Planning Worksheets you created in [Planning Private CDNs](#) in the *Planning Guide*.

- 2 Access the browser-based management tool and log in as the Velocity super administrator.

For more information on using the management tool, see [“Using the Browser-Based Management Tool”](#) on page 17.

- 3 In Available Tools > Administration, click Create New CDN.

- 4 Type the private CDN name you wrote on the first planning worksheet.

- 5 If desired, type a description of the private CDN.

- 6 Click the Continue to Step 2 button.

- 7 If you have already created additional administrators, you can assign them access rights to the private CDN. If not, continue with [Step 8](#).

NOTE: For more information about private CDN access rights and their implications, see [Understanding Access Rights Assignments](#) and [Understanding How Administrators Use Private CDNs](#) in the *Planning Guide*.

- 8 Click the Continue to Step 3 button.

- 9 If you have already created device groups, you can assign them to the private CDN. If not, continue with [Step 10](#).

Only the device groups you assign to a private CDN are available to administrators when they assign content jobs to the private CDN. In other words, you must assign a device group to a private CDN before any of the CDNs content can be cached and managed on the group’s devices.

For more information on the role device groups play in private CDNs, see [Understanding How Administrators Use Private CDNs](#) in the *Planning Guide*.

- 10 Click the Continue to Step 4 button.

- 11** Review the private CDN configuration > click the appropriate Edit button to change any incorrect information.
- 12** Click Create Private CDN Now.
- 13** Repeat the process for each additional private CDN you need to create.

5

Creating and Managing Content Network Administrators

The super administrator who is created during System Controller installation has rights to manage all objects on the system. This administrator can create additional administrator accounts in the datastore.

This chapter explains the tasks summarized in the following table.

To	See
Understand the details of granting various administrative access rights	“A Preview to Granting Administrative Access Rights” on page 25
Create administrator	“Creating Administrators” on page 31
Modify administrator information	“Modifying Administrator Information and Access Rights” on page 34
Effectively deactivate an administrator account	“Deactivating Administrator Accounts” on page 34
Remove administrators	“Removing Administrators” on page 35

A Preview to Granting Administrative Access Rights

Acting as the super administrator, you can create other administrators to help administer your content network.

The Velocity management suite lets you assign administrators access rights specific to the content networking tasks they are to perform. Prior to creating these administrators, you should understand how access rights work as explained in [Understanding Access Rights Assignments](#) in the *Planning Guide*.

Table 2 summarizes the steps for assigning access rights to various content network components.

Table 2

Content Network Component	Access Level	Requirement for Assigning this Access	What the Administrator Can Then Do
System Controller	n/a	1. You must assign the user access to System Controller. See Step 5 on page 31 .	<ul style="list-style-type: none">◆ Access System Controller◆ View or manage all configuration settings for the devices and device groups to which they are assigned access.
Content Controller	n/a	1. You must assign the user access to Content Controller. See Step 5 on page 31 .	<ul style="list-style-type: none">◆ Access Content Controller◆ View or manage all collections and jobs within the CDNs to which they are assigned access.

Content Network Component	Access Level	Requirement for Assigning this Access	What the Administrator Can Then Do
Device Group	Read	<ol style="list-style-type: none"> 1. You must assign the user access to System Controller. See Step 5 on page 31. 2. You must assign the user read access to the device group. See Step 1 on page 32. 	<ul style="list-style-type: none"> ♦ View all configuration settings for all devices assigned to the group.
	Full	<ol style="list-style-type: none"> 1. You must grant the user access to System Controller. See Step 5 on page 31. 2. You must grant the user full access to the device group. See Step 1 on page 32. 	<ul style="list-style-type: none"> ♦ View and change all configuration settings for all devices assigned to the group. <p>NOTE: When you assign full access to a device group, the device-level rights are automatically set to full as well.</p> <p>In other words, you cannot restrict access to devices in a group to which full access is granted by changing the access to read at the device level.</p>

Content Network Component	Access Level	Requirement for Assigning this Access	What the Administrator Can Then Do
Device	Read	<ol style="list-style-type: none"> 1. You must assign the user access to System Controller. See Step 5 on page 31. 2. You must grant the user read access to the device (see Step 3 on page 32). 	<ul style="list-style-type: none"> ◆ View all configuration settings for the device.
	Full	<ol style="list-style-type: none"> 1. You must assign the user access to System Controller. See Step 5 on page 31. 2. You must grant the user full access to the device. See Step 3 on page 32. 	<ul style="list-style-type: none"> ◆ View and change all configuration settings for the device. <p>NOTE: Full access to a device overrides read access to a device group that includes the device.</p> <p>If you assign read access to a group that includes a device and you also grant full access to the device, the user will have full access to the device.</p>

Content Network Component	Access Level	Requirement for Assigning this Access	What the Administrator Can Then Do
Master_CDN	Read	<ol style="list-style-type: none"> 1. You must assign the user access to Content Controller. See Step 5 on page 31. 2. You must assign the user read access to the master CDN. See Step 1 on page 33. 	<ul style="list-style-type: none"> ♦ View existing content collections and jobs assigned to the master CDN.
	Full	<ol style="list-style-type: none"> 1. You must assign the user access to Content Controller. See Step 5 on page 31. 2. You must assign the user full access to the master CDN. See Step 1 on page 33. 3. You must assign the user full access to one or more device groups. See Step 1 on page 32. 	<ul style="list-style-type: none"> ♦ Create and modify content collections and jobs. ♦ Assign the content collections and jobs to the master CDN. ♦ Assign jobs to use any device groups to which the user has full access rights. <p>IMPORTANT: Unlike private CDNs, you cannot assign device groups to the master CDN. Instead, users with rights to the master CDN can assign jobs to any device groups to which they have full access rights in System Controller.</p> <p>Therefore, if you assign full Master_CDN access to a user, you should also assign full rights to at least one device group as well. Otherwise the user will not be able to create collections and jobs for the master CDN.</p>

Content Network Component	Access Level	Requirement for Assigning this Access	What the Administrator Can Then Do
Private CDN	Read	<ol style="list-style-type: none"> 1. You must assign the user access to Content Controller. See Step 5 on page 31. 2. You must assign the user read access to the Private CDN. See Step 1 on page 33. 	<ul style="list-style-type: none"> ♦ View existing content collections and jobs assigned to the CDN.
	Full	<ol style="list-style-type: none"> 1. You must assign the user access to Content Controller. See Step 5 on page 31. 2. You must assign the user full access to the CDN. See Step 1 on page 33. 3. If you want users to troubleshoot problems with device configurations in connection with their content management responsibilities, you will want to also grant them access to System Controller. See Step 5 on page 31. 	<ul style="list-style-type: none"> ♦ Create and modify content collections and jobs. ♦ Assign the content collections and jobs to the CDN. ♦ Assign jobs to use any device groups assigned to the CDN. <p>NOTE: If users also have rights to both System Controller and Content Controller, they can view the configuration settings in System Controller for any devices belonging to a device group assigned to the private CDN.</p> <p>Users can view these devices even when they were not originally assigned read access to the devices. This feature is designed to facilitate troubleshooting.</p>
Content Collections	Inherited from CDN rights assignment	You grant rights indirectly when you assign an access level to the CDN to which the collection belongs.	<ul style="list-style-type: none"> ♦ Depends on the access level assigned for the CDN to which the collection belongs.

Content Network Component	Access Level	Requirement for Assigning this Access	What the Administrator Can Then Do
Content Jobs	Inherited from CDN rights assignment	You grant rights indirectly when you assign an access level to the CDN to which the job belongs.	Depends on the access level assigned for the CDN to which the job belongs.

Creating Administrators

To create an administrator, complete the following steps:

- 1 Locate the Administrator Planning Worksheets you created in **Planning Content Network Administrators** in the *Planning Guide*.
- 2 Access the browser-based management tool and log in as the Velocity super administrator.

For more information on using the management tool, see “**Using the Browser-Based Management Tool**” on page 17.

- 3 In the browser-based tool, click Administration > Admin List > Create New Admin.
- 4 Type the admin profile information for the administrator.

Refer to the Administrator Planning Worksheet if applicable.

- 5 Select a Type radio button for the management suite component access this administrator will have:

NOTE: Checking these different options causes the step list at the top of the panel to reflect only the steps appropriate to the currently checked option.

- ◆ **System Controller:** Gives the user access to only the System Controller component. Users with System Controller access can manage the devices and device groups to which you assign them access, but they cannot access Content Controller and the content collections and jobs managed therein.
- ◆ **Content Controller:** Gives the user access to only the Content Controller component. Users with Content Controller access can view and/or manage the content collections and jobs covered by the private CDNs to which you grant them read or full access. However, they cannot access System Controller and the devices and device groups managed therein.

- ♦ **Both:** Gives the user access to both System Controller and Content Controller.

IMPORTANT: If you are creating private CDNs, you might want to consider assigning access to both System Controller and Content Controller. Otherwise, users with access to only Content Controller access won't be able to view and troubleshoot the devices assigned to the content jobs they are managing.

- 6 Type the company information for the administrator if applicable.
- 7 Click the Continue with Step 2 button.

IMPORTANT: The steps that follow depend on the type of access you are assigning the administrator

Additional Steps for System Controller Administrators

If you are creating an administrator with System Controller access, complete the following steps. Otherwise, skip to [“Additional Steps for Content Controller Administrators” on page 33](#).

- 1 Assign access to any previously created device groups by checking the appropriate option next to each group name.
 - ♦ **Full:** This option lets the administrator view and change the configuration settings on any devices assigned to the device group.

Full access always overrides read access. Therefore, if you grant an administrator full access to a device group, you will not be able to restrict access to any devices within the group.
 - ♦ **Read:** This option only lets the administrator view the configuration settings on any devices assigned to the device group.

NOTE: Administrators with access to both System Controller and Content Controller will not be able to see the device groups for which neither of the above options is checked unless the unchecked group is included in a private CDN to which they are granted access rights.

In the latter case, users will have automatic read rights to the CDN's devices, and will be able to view their configuration settings in System Controller.

- 2 Click the Continue button.
- 3 Assign rights to a device.

NOTE: Although not reflected in the interface during the creation process, the access rights you assigned to device groups in [Step 1](#) will be automatically applied to the individual devices in those groups when you finish creating this administrator.

3a If you assigned only read access to a device group and you want to change the access level to full for any devices within the group, you can do so in this screen. You cannot, however, reduce the access level from full to read access.

Checking the Read access option for a device whose group was assigned full access will have no effect since full access always overrides read access, and when you finish creating the administrator, the device's access settings will change to full.

3b If you want to grant rights to any device that is not covered by a group assignment made in **Step 1**, you can do that here as well.

4 Click the Continue button.

5 If the administrator does not have access to Content Controller, skip to **Step 3 on page 33**.

Additional Steps for Content Controller Administrators

If you selected either Content Controller or both in **Step 5 on page 31**, complete the following steps:

1 Grant either full or read access to any of the listed CDNs.

- ♦ **Full:** This option lets the administrator create new content collections and jobs and assign these to any devices and device groups included in the CDN.
- ♦ **Read:** This option only lets the administrator view the existing content collections and jobs assigned to the CDN's devices and device groups.

All administrators are restricted from accessing or viewing any content data that is not managed within one of their assigned CDNs.

2 Click the Continue button.

3 Review the information on the Admin Summary screen.

To change any of the information, do one of the following:

3a Click the appropriate link in the step list at the top of the panel > modify the information > click Admin Summary in the step list at the top of the panel.

Or

3b Click the Edit button for the section you want to modify > modify the information > Click Admin Summary in the step list at the top of the panel.

4 Click Create Admin Now.

Modifying Administrator Information and Access Rights

To modify an existing administrator, complete the following steps:

- 1** In the browser-based tool, click Administration > Admin List > the Admin Name of the account you want to modify.
- 2** Click the Edit button for the section you want to modify
- 3** Modify the information.

If you need help understanding any information, see the explanations in [“Creating Administrators” on page 31](#).

- 4** If you want to save your changes, click Save Changes.

If you want to return to the summary screen without saving your changes, click the Detail link in the Admin Detail bar at the top of the screen.

If you want to return to the list of administrators without saving your changes, click either Return to Admin List or the Admin List link in the Admin Detail bar at the top of the screen.

Deactivating Administrator Accounts

You can effectively deactivate an administrator account by removing all rights assignments to devices, device groups, and CDNs. To do this, complete the following steps:

- 1** In the browser-based tool, click Administration > Admin List > the Admin Name of the account you want to deactivate.
- 2** If applicable, edit the Assigned Device Groups section > uncheck (blank out) all rights assignments to device groups listed in the section > click Save Changes.
- 3** If applicable, edit the Assigned Devices section > uncheck (blank out) all rights assignments to devices listed in the section > click Save Changes.
- 4** If applicable, edit the Assigned CDNs section > uncheck (blank out) all rights assignments to CDNs listed in the section > click Save Changes.

Removing Administrators

To remove an administrator account, complete the following steps:

- 1 In the browser-based tool, click Administration > Admin List > the Admin Name of the account you want to deactivate.
- 2 Click Remove Admin > Yes.

6

Preparing Cache Devices for Management

This section contains instructions for preparing your cache devices for management using the Velocity management suite.

Initial Setup

Each Exceleator cache device has the following default setting:

```
vcdn managementaddress=10.1.1.1
```

For System Controller to recognize the cache device on the network, you must set the `vcdn managementaddress` value to an IP address that is bound to a network card on the cache device.

Configuring New Cache Devices

Initial configuration of cache devices for communication on the network is documented in [Getting Started with System Controller](#) and involves using an attached keyboard and monitor to access the cache device's command line.

Setting a vcdn Management Address on Each Cache Device

After you have configured the cache device for communication on your network, you must complete the following steps:

- 1 Access the cache device's command line using a Telnet connection or an attached keyboard and monitor as described in the Exceleator 2.2 documentation.

NOTE: Setting the `vcdn managementaddress` is not supported in either the management suite or the Exceleator browser-based management tools.

- 2 Enter the following command:

```
set vcdn managementaddress=iii.iii.iii.iii
```

where *i* is the IP address through which System Controller will manage the cache device.

Device Passwords Must Not Contain Spaces

Although it is possible to create a password that contains spaces for the Config and View users on a cache device, spaces are not allowed in Velocity passwords, and the device import will fail.

If this occurs, you must change the password on the device to one that doesn't contain spaces. Then you can import the device into System Controller.

Adding New Cache Devices in System Controller

To add a cache device in System Controller, complete the following steps:

- 1 Locate the Device Planning Worksheets you created in [Planning Cache Device Objects](#) in the *Planning Guide*.
- 2 Start the Velocity management suite browser-based management tool.
For more information on using the management tool, see [Chapter 2, "Using the Browser-Based Management Tool,"](#) on page 17.
- 3 Click System > Device List > Add New Device
- 4 Type a Device Name for the cache device.
This is the name System Controller displays in various lists.
- 5 Type the management address for the cache device you set in ["Setting a vcdn Management Address on Each Cache Device"](#) on page 37.
- 6 If you have set a password for the Config user on the cache device, type the password in the Management Password field.
- 7 Click the Continue to Step 2 button.
- 8 If you have created administrators, you can assign one or more of them read or full access rights.
For more information regarding access rights, see [Understanding Access Rights Assignments](#) in the *Planning Guide*.
- 9 When all the target administrators are checked, click the Continue to Step 3 button.
- 10 Review the Device Summary > click Edit to make changes > click Add Device Now.

IMPORTANT: If the device import fails, check the network connection to the device, and check to ensure the device password for the Config user doesn't contain spaces. See ["Device Passwords Must Not Contain Spaces"](#) on page 38.

7

Managing and Configuring Cache Devices

This chapter contains information and tips on managing cache devices using Velocity management servers.

Working with Cache Device Management Addresses

To ensure Velocity management server management access, each Excelerator cache device requires that its *vcdn managementaddress* system parameter always have a currently bound IP address as its assigned value. Since 10.1.1.1 is the only address initially bound to a cache device, this address is assigned as the cache device's *vcdn managementaddress* setting.

You can set the *vcdn managementaddress* parameter to another bound IP address, but the system doesn't let you clear the parameter (assign it a null value). This prevents Excelerators from becoming inaccessible.

By the same token, the system prevents any changes to the IP address that is set as the managementaddress. This includes removing the address or reassigning it to another network card. To remove or reassign the address, you must first assign another bound IP address as the *vcdn managementaddress*.

NOTE: The *vcdn managementport*, *vcdn managementid*, and *vcdn monitoringfrequency* system parameters also require appropriate non-null values and cannot be cleared. However, the *vcdn loggingurl*, *vcdn healthurl*, and *vcdn monitoringurl* have null values initially and can be set and cleared as desired.

Managing Cache Device Configurations

IMPORTANT: After adding cache devices to the Velocity datastore, we recommend you avoid using the Excelerator management tools to make configuration changes to any services except those currently not supported by the Velocity management suite (see [How the Velocity Management Suite Affects Excelerator Management](#) in *Planning Guide*).

The management suite provides tools to keep devices and datastore settings synchronized as explained in ["Synchronizing Devices and Datastores" on page 85](#). It is usually simpler to track configuration changes if you approach device configuration from the management suite side and employ system synchronization to keep the settings on the devices and in the datastore synchronized.

To manage a cache device using System Controller, you must first add the cache device to the Velocity datastore. For more information, see [Chapter 6, “Preparing Cache Devices for Management,” on page 37](#).

To access a cache device’s configuration settings in the Velocity management suite, complete the following steps:

- 1 Start the Velocity browser-based management tool.

For more information on using the Velocity management suite management tool, see [Chapter 2, “Using the Browser-Based Management Tool,” on page 17](#).

- 2 Click System > Device List > a device name.

- 3 Click Configuration.

- 4 The Device Configuration panel provides links to all settings and services available for configuration on the device.

NOTE: Services requiring separate licenses, such as Media Excelerator for Windows Media and Media Excelerator for Real Media, only appear on this page when the device has valid service licenses installed.

For more information on managing cache device licenses, see [“Installing Velocity License Files” on page 14](#).

- 5 For more information regarding the configuration settings accessible through the Device Configuration panel, see the Help associated with this panel and all of the configuration panels accessible through its links.

Automatic Recovery After a Failed Configuration Attempt

After System Controller sends configuration changes to a cache device, it waits for confirmation that the configuration changes succeeded.

If it receives an alert indicating that some of the configuration changes did not complete successfully, System Controller will verify that the device’s current configuration is accurately represented in the Velocity datastore by requesting the device’s current configuration and reconciling the datastore with the device’s actual configuration. It will then pass the alert to the Alert list so that the administrator is aware of what configuration settings failed to apply.

8

Managing and Configuring Cache Device Groups

The Velocity™ management suite lets you group cache devices to meet your device management needs. For example, you might want to group cache devices in different groups according to some or all of the following criteria:

- ◆ The geographical structure of your content network
- ◆ The administrators who manage the device group
- ◆ The services hosted on group devices
- ◆ The customers that the group provides services to
- ◆ The types of content you store on group devices

There is no limit to the number of groups you can create, and no limit to the number of groups that a cache device can belong to.

However, before you begin creating and managing cache device groups, it is vital that you understand how group configuration changes affect individual cache devices as explained in this chapter.

The following table summarizes the various cache device group topics discussed in this chapter.

To	See
Learn about cache device groups	“The Purposes of Cache Device Groups” on page 41
Create cache device groups for management	“Creating Cache Device Groups” on page 55
Make configuration changes to cache device groups	“How Group Configuration Works” on page 42

The Purposes of Cache Device Groups

Cache device groups are a powerful device management tool. To use them effectively, however, you must fully understand their purposes and how the Velocity management suite interacts with them.

Cache device groups are required for the following Activities:

- ♦ **Job-Related Actions:** Only device groups can be the target of content management tasks (prepopulating, pinning, purging, bypassing).

Monitoring: Using the Velocity management suite to monitor cache devices requires that the devices are members of at least one group.

- ♦ **Global Configuration Changes:** Applying configuration changes to multiple cache devices simultaneously requires that they are members of a group.

IMPORTANT: Be sure to read [How Group Configuration Works](#) before attempting to use the global configuration feature.

Additionally, rather than assigning administrators access rights to individual cache devices, you can assign access to device groups and the administrators will automatically have the same access rights to each device in the group.

How Group Configuration Works

To avoid causing problems with the configuration of cache devices in a group operation, it is vital that you understand how group configuration works in the Velocity management suite.

Understanding Group Configuration Settings

Since cache devices are grouped together for different purposes, System Controller expects that each cache device in a group will have initial configuration differences.

The most obvious example of configuration differences is that each cache device must have one or more IP addresses to communicate on the network. And since IP addresses cannot be shared by multiple cache devices, they are not configurable at the group level.

Another obvious example of settings that might not be shared is the cache device gateway configuration. On the other hand, cache devices on the same network subnet could very easily require the same exact gateway configuration. Therefore, the gateway settings are configurable at the group level.

Other configuration differences are more subtle. For example, you might have a group of cache devices from different geographical areas that have identical forward proxy configurations except that they send their log files to different locations.

System Controller is designed to both accommodate cache device differences and/or to enforce configuration conformity between the devices and the datastore. The mechanism for achieving this is the synchronization feature.

For example, if a Velocity administrator configures forward proxy services on a group of devices and an local cache device administrator makes a log file push change on one of the devices (not using the management suite), the Velocity administrator could choose to either accept the change to the device configuration by overwriting the datastore with the device's settings, or to reinstate the original log push settings by overwriting the device's settings with the configuration in the datastore.

Device and datastore synchronization options are explained in [“Synchronizing Devices and Datastores” on page 85](#).

Group Configuration Settings Are Stored in Configuration Data Objects

Cache device group configurations are stored in the datastore in 26 different configuration data objects (starting with Forward Proxy settings) that appear as links in the left hand column of Group Configuration tab as shown in [Figure 1](#).

Figure 1

The screenshot shows the 'Group Configuration Manager: lab65g' interface. The 'Configuration' tab is selected, displaying a list of settings. Each setting is shown in a table with a description and an 'Enabled' status. The settings are grouped into sections: HTTP Settings, FTP Settings, Streaming Settings, Cache Settings, System/Network Settings, Content Settings, and Content Filtering. Each section header is highlighted in yellow. The 'Enabled' status is shown in a column on the right.

Group Configuration Manager: lab65g	
[Activity View]	
HTTP Settings	Enabled
Forward Proxy	
Transparent Forward Proxy	
Reverse Proxy	
FTP Settings	Enabled
Mini FTP Server	
FTP Forward Proxy	
FTP Reverse Proxy	
Streaming Settings	Enabled
Global Settings	
Apple QuickTime™	
Real Media™	
Windows Media™	
Cache Settings	Enabled
Authentication	
Tuning	
Cache Freshness	
System/Network Settings	Enabled
DNS	
Gateway/Firewall	
TCP/CEM	
Date & Time	
SNMP	
IPQoS	
IP Access Control	
Content Settings	Enabled
Dynamic Bypass	
Content Filtering	Enabled
Filter Services	
Filter Override List	
Filter Bypass List	
Filter Logging	
Websense	

Group Configuration Settings Are Initially Empty

As explained in “[Understanding Group Configuration Settings](#)” on page 42, System Controller expects and accommodates the configuration differences in individual cache device configurations by not attempting to set them when the cache device is initially created.

System Controller therefore stores empty values for all fields in the group configuration data objects shown in [Figure 1 on page 44](#).

These empty configuration values are reflected by the fact that the Enabled column in the Group Configuration tab is mostly blank. This can be misinterpreted by administrators to mean that services are not enabled. However, all it really indicates is that the services have never been set *at the group level*. After they are set for the first time, the group settings will reflect the state of their respective configuration data object in the datastore. Subsequent changes to individual group members are not reflected in the Enabled column.

For example, the Enabled column is initially blank for Forward Proxy because a single value does not logically reflect the initial Forward Proxy status of individual cache devices in the group.

In other words, services that are individually configured cannot be reflected in a group configuration object that has not been activated or applied to the group as a whole.

Cautions for Applying Configuration Settings at a Group Level

There are three points to consider before applying a group configuration data object to a group of cache devices:

Point 1: All Configuration Settings Are Applied to All Group Members

When you apply one of the group configuration data objects to a group, all cache devices in that group will have identical settings for all the fields defined in the group configuration data object.

For example, if you define and apply forward proxy settings to a group, every member of the group will have identical settings. This is explained further in [“How Group-Level Configuration Affects Grouped Cache Devices” on page 46](#).

Point 2: Null Values Will Be Applied to Any Fields Left Empty

When applying settings to a group of cache devices, all fields in the configuration section you are changing are applied to all devices in the group.

For example, when configuring a Forward Proxy service on a group of cache devices, all values listed in the Forward Proxy configuration panel are sent to all devices in the group, including the empty values.

Applying empty fields to a device can result in one of two conditions:

- ◆ Fields are set to empty values on all grouped cache devices
- or
- ◆ Configuration errors are generated for values that cannot be empty

Implications of empty settings in each group configuration object are discussed in [“How Group-Level Configuration Affects Grouped Cache Devices” on page 46.](#)

Point 3: All Network Card IP Addresses Are Set

Some group configuration objects require that you select a network card (eth0, eth1, etc.) for the configuration. When the group configuration object is applied, all IP addresses that are bound to the card at the time the configuration change occurs are assigned to provide the service being configured.

For example, if you apply a Forward Proxy configuration to a group of cache devices with eth0 selected as the network card, all the IP addresses assigned to eth0 will be configured to provide forward proxy services.

A Tip for Grouping Cache Devices

We recommend you create separate groups for each type of configuration you want to manage at the group level.

For example, you might have a group for cache devices that share forward service settings but do not have the same DNS settings. In such a case, you would not attempt to use the forward service group to manage cache device DNS settings. Rather you would create other groups of cache devices that share DNS settings for the express purpose of managing only DNS settings.

How Group-Level Configuration Affects Grouped Cache Devices

The following table discusses each of the 26 group configuration data objects and the implications for configuring the settings at the group level.

Table 4

Group Configuration Area	Implications to Consider
Forward Proxy	<p data-bbox="427 204 1231 260">When you configure forward proxy settings for a group, the following settings are set for each cache device in the group:</p> <ul data-bbox="427 277 1231 677" style="list-style-type: none"><li data-bbox="427 277 1231 390">◆ IP Address Settings: The same settings for the network card (eth0, eth1, etc.), port, and WPAD are applied to each cache device in the group, including the activation of forward proxy services for each IP address bound to each selected network card.<li data-bbox="427 407 1231 468">◆ Logging: The Logging options are applied to each cache device in the group.<li data-bbox="427 486 1231 572">◆ Authentication: Each cache device in the group has the same authentication settings—authentication is either disabled or the same profile is specified for accessing all the devices.<li data-bbox="427 590 1231 677">◆ Cache Control: The same cache control settings (x-forward for, custom cache control header, and HTTP connect method) are applied to each cache device in the group. <p data-bbox="427 703 1231 841">Configuring forward proxy services for the group will overwrite all forward proxy services set on individual cache devices. You can then configure each device with individualized settings if desired. However, you must make sure that you change the individual cache device configurations after applying the group configuration change.</p> <p data-bbox="427 868 1231 954">Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual device settings will be overwritten with the group setting.</p>

Group Configuration Area Implications to Consider

Transparent Forward Proxy

When you configure transparent forward proxy services at the group level, the following settings are set for each cache device in the group:

- ◆ **Transparent Forward Proxy:** Each IP address bound to the selected network cards on each cache device in the group is activated for transparent forward proxy services.
- ◆ **Proxy Ports:** The same port settings are applied to the transparent service on each cache device in the group.
- ◆ **Exception IP Address:** The same settings for bypassing the transparent service for requests to listed Web servers are applied to all devices in the group.
- ◆ **Routing:** The same gateway settings are applied to all devices in the group.

WARNING: You must set this value and ensure that all cache devices in the group are on the same subnet, or this will result in some or all devices not being able to communicate on the network.

- ◆ **Logging:** The Logging options you specify are applied to each device in the group.
- ◆ **Authentication:** The same authentication settings are applied to each device in the group. Authentication will either be either disabled or the same profile will be used to access all devices.
- ◆ **Options:** The same cache control settings (error handling method, x-forward for, custom cache control header, and HTTP connect method) are applied to each device in the group.
- ◆ **WCCP:** The same WCCP version and options are applied to each device in the group.

Configuring transparent forward proxy services for the group will overwrite all transparent handling services set on individual cache devices. You can then configure each cache device with individualized settings if desired. However, you must make sure that you make the individual cache device configuration changes after changing the group configuration.

Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual cache device settings will again be overwritten.

Group Configuration Area	Implications to Consider
Reverse Proxy	<p>When you configure reverse proxy services for a group, the same reverse proxy services and load balancing options are applied to each group member.</p> <p>Configuring reverse proxy services for the group will overwrite all reverse services defined on individual cache devices. You can then configure each device with individualized settings if desired. However, you must make sure that the individual cache device configuration changes occur after the group configuration changes are completed.</p> <p>Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual cache device settings will again be overwritten.</p>
Mini FTP Server	<p>When you configure the Mini FTP Server settings for a group, each IP address bound to the selected network card on each cache device in the group is activated for mini FTP server services.</p> <p>Configuring this for the group will overwrite Mini FTP Server settings on individual cache devices. You can then configure each cache device with individualized settings if desired. However, you must make sure that the individual cache device configuration changes occur after the group configuration changes are completed.</p> <p>Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual settings are again overwritten.</p> <p>This option is also available through the FTP Forward Proxy service link.</p>
FTP Forward Proxy	<p>When you configure the FTP forward proxy services for a group, each IP address bound to the selected network card on each cache device in the group is activated for FTP forward proxy services.</p> <p>Configuring this for the group will overwrite FTP Forward Proxy settings on individual cache devices. You can then configure each cache device with individualized settings if desired. However, you must make sure that the individual cache device configuration changes occur after the group configuration changes are completed.</p> <p>Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual settings are again overwritten.</p> <p>This option is also available through the Mini FTP Server link.</p>

Group Configuration Area	Implications to Consider
FTP Reverse Proxy	<p>When you configure FTP Reverse Proxy services for a group, each IP address bound to the listed FTP servers is accelerated by each cache device in the group.</p> <p>Configuring this for the group will overwrite FTP Reverse Proxy services configured on individual cache devices. You can then configure each cache device with individualized settings if desired. However, you must make sure that the individual cache device configuration changes occur after the group configuration changes are completed.</p> <p>Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual settings are again overwritten.</p>
Global Settings (Streaming)	<p>Global streaming settings do not apply to Real Media services. They do apply to Apple QuickTime and Windows Media.</p> <p>The object settings apply to any QuickTime or Windows Media objects.</p> <p>The disk usage setting applies to the entire cache device.</p>
Apple QuickTime	<p>When you configure Apple QuickTime services for a group, the same service settings are applied to each cache device in the group. For example, for forward and reverse proxy services, each IP address bound to the selected network card on each cache device in the group is activated for the service on the specified port.</p> <p>Configuring a QuickTime service for the group will overwrite QuickTime services configured on individual cache devices. You can then configure each cache device with individualized settings if desired. However, you must make sure that the individual cache device configuration changes occur after the group configuration changes are completed.</p> <p>Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual settings are again overwritten.</p> <p>Bandwidth settings made at the group level should fit the profile for each device in the group, otherwise device resources such as the network card could become overloaded.</p> <p>Configuring reverse proxy services at the group level only makes sense if you have multiple cache devices serving one origin media server.</p> <p>If an upstream proxy is specified for the group, you must ensure that the target proxy is not also a member of the group. Otherwise requests will get caught in an endless loop.</p>

Group Configuration Area	Implications to Consider
Real Media	<p data-bbox="427 163 1224 274">Groups are not aware of whether the devices in the group each have the required licenses installed. It could appear from the group perspective that configuration of Real Media services to all devices was successful when, in fact, it was not.</p> <p data-bbox="427 302 1233 444">Configuring Real Media services for the group will overwrite Real Media services configured on individual cache devices. You can then configure each cache device with individualized settings if desired. However, you must make sure that the individual cache device configuration changes occur after the group configuration changes are completed.</p> <p data-bbox="427 472 1233 552">Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual settings are again overwritten.</p> <p data-bbox="427 579 1210 659">Bandwidth settings made at the group level should fit the profile for each device in the group, otherwise device resources such as the network card could become overloaded.</p> <p data-bbox="427 687 1233 743">Configuring reverse proxy services at the group level only makes sense if you have multiple cache devices serving one origin media server.</p> <p data-bbox="427 770 1220 826">Configuring Real Media multicasting at the group level only makes sense if the devices are all on different networks.</p> <p data-bbox="427 854 1233 933">If an upstream proxy is specified for the group, you must ensure that the target proxy is not also a member of the group. Otherwise requests will get caught in an endless loop.</p> <p data-bbox="427 961 1224 1104">When you configure Real Media services for a group, the same service settings are applied to each cache device in the group. For example, for forward and reverse proxy services, each IP address bound to the selected network card on each cache device in the group is activated for the service on the specified port.</p>

Group Configuration Area	Implications to Consider
Windows Media	<p>Groups are not aware of whether the devices in the group each have the required license installed. It could appear from the group perspective that configuration of Windows Media services to all devices was successful when, in fact, it was not.</p> <p>When you configure Windows Media services for a group, the same service settings are applied to each cache device in the group. For example, for forward and reverse proxy services, each IP address bound to the selected network card on each cache device in the group is activated for the service on the specified port.</p> <p>Configuring Windows Media services for the group will overwrite services configured on individual cache devices. You can then configure each cache device with individualized settings if desired. However, you must make sure that the individual cache device configuration changes occur after the group configuration changes are completed.</p> <p>Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual settings are again overwritten.</p> <p>Bandwidth settings made at the group level should fit the profile for each device in the group, otherwise device resources such as the network card could become overloaded.</p> <p>Configuring reverse proxy services at the group level only makes sense if you have multiple cache devices serving one origin media server.</p> <p>Configuring Windows Media multicasting at the group level only makes sense if the devices are all on different networks.</p> <p>If an upstream proxy is specified for the group, you must ensure that the target proxy is not also a member of the group. Otherwise requests will get caught in an endless loop.</p>
Authentication	<p>Authentication profiles are global. Any profiles you define using this option are available to all managed cache devices and groups.</p>
Tuning	<p>After applying tuning parameters to a cache device group, you can change the tuning parameters on each device if desired. Changes made in this manner remain in effect until the group's Tuning panel is accessed and settings are applied to the group.</p>

Group Configuration Area	Implications to Consider
Cache Freshness	<p>The cache freshness settings you specify apply to all cache devices in the group.</p> <p>After applying cache freshness settings to a cache device group, you can change the settings on each cache device if desired. Changes made in this manner remain in effect until the group's Cache Freshness panel is accessed and settings are applied, at which time individual settings are again overwritten.</p>
DNS	<p>Use caution when changing the DNS settings for a group. Keep in mind that the same settings will be applied to each cache device in the group. Unless all cache devices can function with the same DNS settings, applying the same settings to a group might make some devices unavailable on the network. If this happens, someone must manually restore the correct DNS settings on each device before it can communicate on the network again.</p>
Gateway/Firewall	<p>Use caution when changing the Gateway/Firewall settings for a group. Keep in mind that the same settings will be applied to each cache device in the group. Unless all cache devices can function with the same settings, applying them to a group might make some cache devices unavailable on the network. If this happens, someone must manually restore the correct gateway/firewall settings on each device before it can communicate on the network again.</p>
ICP/CERN	<p>If you choose to configure ICP peer relationships at the group level, you must ensure that the peers specified are not also members of the group being configured. Otherwise, the device peer requests will get caught in an endless loop.</p>
Date & Time	<p>You should only configure the Date & Time settings for a group if the same settings apply to each cache device in the group. Incorrect settings will cause log entries and accounting statistics to be incorrect and can disrupt other system functions, such as the importing of SSL certificates.</p>
SNMP	<p>The SNMP settings you specify will apply to each group member. While some SNMP settings might be the same for each cache device in a group, the node name for each cache device must be unique. Otherwise, the origin of SNMP messages can't be determined.</p> <p>The node name will be changed if these settings are applied to the group. For example, a null node name will set a null node name on each cache device.</p> <p>If you use this option to set SNMP parameters for grouped cache devices, you will then want to change the node name and possibly other settings for each cache device in the group. The changes you make will remain in effect until you access and apply the SNMP settings at the group level again, at which time each cache device will again be assigned the same SNMP settings.</p>

Group Configuration Area	Implications to Consider
QoS	<p>IP QoS settings specify how cache devices set Quality of Service (QoS) parameters in requests to servers, replies to clients, and cache device error pages. The same IP QoS settings will be applied to all group members.</p> <p>Having the same IPQoS settings is a likely requirement for many content networks.</p>
IP Access Control	<p>IP Access Control lets you allow or block browser access to cache devices using the Source IP list. It also lets you allow or block IP addresses from which cache devices will fill cache using the Destination IP list.</p> <p>It is very likely that the same lists might apply to multiple cache devices on a content network.</p>
Dynamic Bypass	<p>The Dynamic Bypass feature lets you configure cache devices so that specific errors from Web sites are explicitly not cached and subsequent requests to the Web sites are simply passed through for a specific time period.</p> <p>It is likely that administrators would want cache devices on a content network to have the same dynamic bypass settings.</p>
Filter Services	<p>n2h2: Initial setup of n2h2 filtering services is not supported at the group level. However, after you have an n2h2 filtering service on each device in a group you can then configure the category settings for all the devices in the group by changing them at the group level.</p> <p>8e6 (XStop): Initial setup of 8e6 filtering service and configuring categories for the services are supported at the group level.</p> <p>After creating a service and configuring the categories, you might want to consider also changing the download times at the device level so that the cache devices request downloads at different times. Otherwise multiple download requests could have a negative impact on network bandwidth.</p>
Filter Override List	<p>Be aware that each time you send filter override URLs to devices in a group, the overrides currently on the devices are overwritten with the group override list.</p> <p>Therefore, if you have configured different overrides on each device in a group, and you want to retain them, you must either include all overrides in the group configuration and accept all devices having all overrides once the configuration is pushed to the devices, or you must maintain the overrides only at the device level.</p>
Filter Logging	<p>If you configure filter logging at the group level, each device in the group will have the same logging configuration.</p>

Group Configuration Area	Implications to Consider
Websense	Configuring Websense at the group level only makes sense if you want all devices in the group to clear requests through the same Websense server. Because of the high performance of Excelerator cache devices, most Websense implementations match one Websense server to one cache device.
Purging	This option removes all cached objects from all grouped cache devices. Since filling cache is often a time-consuming and costly process, many administrators will rarely use this option.

Creating Cache Device Groups

NOTE: Cache devices must first be added as devices in the Velocity management suite datastore before they can be made members of a group.

If you used the worksheets mentioned in [Planning for Content Network Administration](#) in *Planning Guide*, you can refer to them in the following procedure.

To create a group of cache devices, complete the following steps:

- 1 Start the Velocity management suite browser-based management tool.
For more information, see [“Starting the Browser-Based Management Tool”](#) on page 17.
- 2 Click System > Group List > Create New Group.
- 3 Type a group name.
The name might indicate the purpose for which the group is being created. It can contain up to 16 alphanumeric characters.
- 4 Type the IP address or DNS name of the Velocity management server that will receive all alerts and monitoring data from group members.
Administrators of large installations with multiple management servers might want to designate only a few management servers for collecting alerts and monitoring data from all cache device groups on the content network.
- 5 If desired, type a brief description of the group for management reference.
- 6 After typing the description, click the Continue to Step 2 button.

- 7 In the Available Devices list, check the cache devices you are adding to the group.
For information about using the search feature to filter the list of available cache devices, see [“Using the Management Suite List Filters” on page 17](#).
- 8 After checking all cache devices to be added, click the Continue to Step 3 button.
- 9 If you have created administrators to help manage this group and its cache devices, check the appropriate access level next to each administrator’s name in the Available Admins list.
- 10 Click the Continue to Step 4 button.
- 11 If you have created private CDNs, check each CDN that will have content stored on the devices in this group.
- 12 Click the Continue to Step 5 button.
- 13 Review the group definition.
- 14 If you need to change the configuration, click the appropriate Edit button or click the appropriate step link beneath the top banner to go directly to a section of the group definition.
- 15 When the group definition is correct, click Create Group Now.

Removing Cache Device Groups

NOTE: Cache device objects are not deleted with this function, only the logical grouping of the devices is removed from the datastore.

To remove a group of cache devices, complete the following steps:

- 1 Start the Velocity management suite browser-based management tool.
For more information, see [“Starting the Browser-Based Management Tool” on page 17](#).
- 2 Click System > Group List.
- 3 In the Available Groups list under Select, check the group or groups you want to remove.
- 4 Below the Available Groups list, click Remove Selected Group(s).

Removing a group causes the following to occur:

- ◆ The group name no longer appears in the Available Groups list.

- ◆ Administrators lose access to group cache devices unless they have access through another group or individual cache device assignment.
- ◆ The device group is removed from any CDNs to which it was assigned.
- ◆ Scheduled group actions that are still pending are removed from the list of scheduled events. Any actions currently in process are not affected since they are executed at the cache device level.
- ◆ Cache devices stop reporting monitoring data to the group's designated monitoring server unless membership in another group causes them to continue reporting.

Adding a Cache Device to a Group

To add a cache device to an existing group of cache devices, complete the following steps:

- 1 Start the Velocity management suite browser-based management tool.
For more information, see [“Starting the Browser-Based Management Tool” on page 17](#).
- 2 Click System > Group List > *the target Group name* > Device List.
- 3 Below the Device List, click Add Devices to this Group.
- 4 In Devices Not in This List, check the cache devices you want to add to the group.

The group is updated to show your additions

Adding cache devices to a group is a scheduled event and might take several minutes to complete. When it completes, it causes the following to occur:

- ◆ The cache device starts reporting monitoring data to the monitoring server.
- ◆ Scheduled group actions that are still pending will affect the newly added cache device along with all other group members.
- ◆ The Alert status for the group (enabled or disabled) is applied to the cache device.
- ◆ Admins with access rights to the group now have access rights to the cache device.

Removing Cache Devices from Groups

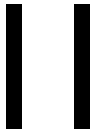
NOTE: Cache device objects are not deleted with this function, only their inclusion in the logical grouping of cache devices.

To remove a cache device from a group, complete the following steps:

- 1 Start the Velocity management suite browser-based management tool.
For more information, see [“Starting the Browser-Based Management Tool” on page 17](#).
- 2 Click System > Group List > the target Group name > Device List.
- 3 In the Devices in this Group list under Select, check the group or groups you want to remove.
- 4 Below the Available Groups list, click Remove Selected Device(s).

Removing a cache device from a group causes the following to occur:

- ◆ The cache device name no longer appears in the Group’s Device List.
- ◆ Administrators lose access to the cache device unless they have access through another group or cache device assignment.
- ◆ Scheduled group actions that are still pending will not affect the cache device. Any actions currently in process are not affected since they are executed at the cache device level.
- ◆ The cache device stops reporting monitoring data to the group’s designated monitoring server unless membership in another group causes it to continue reporting.



Creating Caches on Your Content Network

To	See
Create HTTP caches on your content distribution and delivery network (CDN)	Chapter 9, “Creating HTTP Caches,” on page 61
Create streaming caches on your CDN	Chapter 10, “Creating Streaming Media Caches,” on page 63

9

Creating HTTP Caches

You can create HTTP caches on your content network by configuring any of the caching service types described in the Excelerator 2.2 documentation. These services can be assigned to individual cache devices or to groups of cache devices as described in [Chapter 7, “Managing and Configuring Cache Devices,”](#) on page 39 and [Chapter 8, “Managing and Configuring Cache Device Groups,”](#) on page 41.

After you create the proxy services on your network, you can define collections and jobs for managing specific content objects. For more information, see [Planning Content Caching and Distribution](#) in *Planning Guide*.

To learn more about creating collections and jobs, see [Content Controller Deployment Guide](#).

To learn more about identifying content objects using URL masks, see [Ensuring Cache Freshness and Prepopulating, Retaining, and Removing Cached Objects](#) in *Content Controller Deployment Guide*.

10

Creating Streaming Media Caches

This chapter outlines the streaming support available in Excelerator 2.2 and later cache devices, including the streaming support available in the base product and in the Windows Media and Real Proxy 8 Media Excelerator add-ons.

Excelerator Cache Devices Support Apple QuickTime by Default

Excelerator 2.2 and later cache devices support the streaming formats listed below. For further information, see the Excelerator administration guide.

- ♦ HTTP streaming wherein a streaming file is delivered through HTTP and played in a browser plug-in
- ♦ Non-proprietary RTSP/RTP streaming media content (QuickTime only)
- ♦ Tunneling of an RTSP/RTP session inside an HTTP connection as implemented in the QuickTime* and Darwin* products from Apple Computer, Inc.

Using Media Excelerator for Apple QuickTime

The base Excelerator 2.2 product includes Media Excelerator for Apple QuickTime. No separate license is required for this service.

The management suite lets you create forward, transparent, and reverse accelerator services for all standard Apple QuickTime streams. It also lets you pin, prepopulate, and purge the streams.

For help configuring Apple QuickTime services, see [Apple QuickTime in Management Interface Help](#).

For help prepopulating Apple QuickTime content, see [Prepopulating Apple QuickTime Content in Content Controller Deployment Guide](#).

Using Media Excelerator for Windows Media

Each installation of Volera's Media Excelerator for Windows Media requires a valid license installed on the target cache device.

IMPORTANT: System Controller lets you specify the creation of Windows Media acceleration services for cache device groups without checking for valid Media Excelerator for Windows Media licenses on the target cache devices.

You must ensure that each target cache device in the group contains a valid Media Excelerator license. Otherwise, the service creation operation will fail on unlicensed cache devices, causing errors and alerts to be generated.

The management suite lets you create forward, transparent, and reverse accelerator services for all standard Windows Media streams. It also lets you pin, repopulate, and purge streams.

For help configuring Windows Media services, see [Windows Media in Management Interface Help](#).

For help repopulating Apple QuickTime content, see [Repopulating Windows Media Content in Content Controller Deployment Guide](#).

Using Media Excelerator for Real Media

Each installation of Volera's Media Excelerator for Real Media requires valid licenses (Media Excelerator and Real) installed on the target cache device.

IMPORTANT: System Controller lets you specify the creation of Real Media acceleration services for cache device groups without checking for valid licenses on the target cache devices.

You must ensure that each target cache device in the group contains valid licenses. Otherwise, the service creation operation will fail on unlicensed cache devices, causing errors and alerts to be generated.

The management suite lets you create forward, transparent services for all standard Real Media streams and reverse proxy services for RTSP streams. It also lets you pin, repopulate, and purge streams.

For help configuring Real Media services, see [Real Media in Management Interface Help](#).

For help repopulating Apple QuickTime content, see [Repopulating Real Media Content in Content Controller Deployment Guide](#).



Providing Access to Caches

To	See
Configure browsers and media players to use content network caches	Chapter 11, "Configuring Browsers and Players to Use Network Caches," on page 67
Use Web Proxy Auto-Discovery (WPAD) to configure network browsers to use content network caches	Chapter 12, "Web Proxy Auto-Discovery (WPAD) Setup," on page 69
Limit browser and player access to content network caches	Chapter 13, "Limiting Access to Caches," on page 71

11

Configuring Browsers and Players to Use Network Caches

The Excelerator 2.2 documentation contains instructions for configuring browsers and players to access caching services. The instructions also apply to the management suite.

12

Web Proxy Auto-Discovery (WPAD) Setup

When properly configured for the browsers used on your network, the Web Proxy Auto-Discovery (WPAD) feature lets network users automatically access the cache device's forward proxy services without having to individually configure their browsers.

Instructions for configuring the cache devices on your content network to work with Web Proxy Auto-Discovery are found in the [Excelsior 2.2 documentation](#).

13

Limiting Access to Caches

Version 2.2 Excelerators let you specify various ways of requiring that users authenticate before using the cache device's caching services. For help configuring authentication services, see [Authentication](#) in *Management Interface Help*.

You can also restrict access to caches based on the requesting IP address. For more information, see [IP Access Control](#) in *Management Interface Help*.

Detailed feature descriptions are provided in the Excelerator 2.2 documentation.

Implications for Using Authentication on Your Content Network

If you plan to use the same IP address for managing a cache device and delivering proxy or other services that have authentication enabled, you should be aware of a potential IP address/port conflict.

By default, the Velocity management server communicates with cache devices using a secure connection on the standard SSL port (443). Secure Excelerator also uses the standard SSL port for all authenticated connections by default (except for Basic Authentication, which uses an HTTP connection).

A cache device's Velocity management suite management port and each of its proxy service's SSL listening ports can be configured separately.

The conflict will arise if you attempt to use an IP address for both management of a cache device by the management suite and for a proxy service on the cache device that has authentication enabled. You must ensure that the management and the proxy services either use different IP addresses or use different SSL listening ports. No two services can share the same IP address/port combination.

IV

Monitoring and Maintaining Your Content Network

The chapters in this section contain information regarding the following tasks:

To	See
Learn about and use Velocity management suite's general health monitoring features	Chapter 14, "Monitoring Device and Group Health," on page 75
Learn about and use Velocity management suite's device and content monitoring features	Chapter 15, "Monitoring Cache Devices and Content," on page 77
Uninstall the Velocity management suite	Chapter 16, "Uninstalling Velocity Management Suite Components," on page 81
Install patches and upgrades to Velocity management suite components	Chapter 17, "Upgrading the Velocity Management Suite," on page 83
Ensure the Velocity datastore and managed cache devices are synchronized	Chapter 18, "Synchronizing Devices and Datastores," on page 85
Learn how to change the management server's IP address	Chapter 19, "Changing the Management Server's IP Address," on page 89
Shut down and restart cache devices and the management server	Chapter 20, "Shutting Down and Restarting," on page 91
Learn about time synchronization issues	Chapter 21, "Synchronizing Time on Your Content Network," on page 93
Learn about backing up and restoring the datastore	Chapter 22, "Backing Up and Restoring the Datastore," on page 95

To	See
Learn about securing the content network	Chapter 23, “Securing the Content Network,” on page 97
Learn about keeping content network data secure	Chapter 24, “Keeping Content Network Data Secure,” on page 99

14 Monitoring Device and Group Health

When you view either the Device list or the Device Group list, each entry in the list displays a Health icon.

From the Device list, you can view health details for each device service by clicking this icon.

From the Device Group list, the Health icons show general status for each group as follows:

- ♦ **Green:** All devices in the group are reporting a green health status.
- ♦ **Yellow:** One or more devices are reporting a yellow status and all other devices are reporting green.
- ♦ **Red:** One or more devices in the group are either reporting a red status or are not reporting any status.
- ♦ **Not Configured:** All devices in the group are not configured.

If a group shows a non-green status, you can quickly view the status of only the devices in the group by clicking the Devices link for the group. You can then troubleshoot device service health problems by clicking a device's icon.

15

Monitoring Cache Devices and Content

The Velocity management suite lets you monitor the following:

- ◆ Device system statistics
- ◆ Group statistics (summarizing all devices in the group)
- ◆ Object (URL mask) status for any objects defined in a collection
- ◆ Collection status (summarizing all objects within the collection)
- ◆ Job status (summarizing all collections within the job)

This chapter presents a general overview of how monitoring works. As you work with the management suite, you will discover the monitoring mechanisms that are most useful for your management purposes.

General Overview

Monitoring statistics are generated at two basic levels:

- ◆ **System and performance statistics:** These include such things as CPU utilization, cache hits, total current connection, etc.
- ◆ **Content-related statistics:** These include such things as bytes downloaded from origin servers, bytes served to browsers, cache hits, etc.

Velocity monitoring involves the interaction of four components:

- ◆ **Exceleator Cache Device:** All monitoring statistics are generated on individual Exceleator cache devices.
- ◆ **Monitoring Server:** The monitoring server receives data from cache devices through HTTP POSTS and collects them until they are requested

by System Controller. Monitoring servers are Velocity management servers with System Controller or Content Accountant running.

- ♦ **Velocity Management Server:** The management server (which might also be the monitoring server) collects statistics from the monitoring server and prepares them for delivery to administrators through the browser-based management tool.

To view system and performance statistics, the administrators must have access to System Controller and the devices and groups they need to monitor.

To view content statistics, the administrators must have access to Content Controller and the CDNs (private or master) to which the jobs and collections they are monitoring belong.

- ♦ **Browser-Based Management Tool:** The administrator uses a Web browser to access the management server and view monitoring statistics.

System Performance Monitoring

Additional Requirements for System Monitoring

Each cache device must meet the following requirements for system and performance monitoring to function.

- ♦ Each cache device must exist as a device on the management server and be assigned to a device group
- ♦ The following settings must be set on each device. (These settings can be viewed only from the device's System prompt.)

vcdn managementid=<name>: This name is assigned when the device is created in the management suite. The device's managementid must always match the name expected by the management server. If it doesn't match, monitoring will not work.

IMPORTANT: To avoid monitoring problems, you should never change the *vcdn managementid* at the Excelerator system prompt or by adding the device in the management suite under a different name.

vcdn monitoringurl=http://<IP/DNS_name>/ex: This value contains one or more IP addresses or DNS names and is set when you specify a monitoring servers for groups to which the device belongs. Each IP address or DNS name listed is a destination to which the device sends system monitoring information. If the device belongs to multiple

groups that have the same monitoring server, that server has only one entry in this field. The monitoring servers must each be valid Velocity management servers with System Controller and/or Content Accountant installed.

vcdn monitoringfrequency=<seconds>: This specifies how often the cache device sends system statistics to the monitoring server. It has a default value of 600 (10 minutes).

How System Monitoring Works

The following describes the system monitoring process.

1. The Excelerator cache device collects monitoring information.
2. At the interval specified by the *vcdn monitoringfrequency* setting, the device sends the information and its device name (*vcdn managementid*) to each of its monitoring servers (*vcdn monitoringurl*) using HTTP POST.
3. The monitoring servers receive the information, process it, and create a file with the same name as the device's *vcdn monitoringurl* parameter setting. The file is located in /opt/volera/roma/modules/monitoring/xml on each monitoring server.
4. Each time new monitoring information is received, the files on the monitoring servers are overwritten with the new data.
5. When an administrator requests monitoring information for a device, System Controller contacts the first monitoring server listed for the device and requests information for the device.
6. System Controller then displays the information returned.

IMPORTANT: The cache device sends the first batch of information to the monitoring server only after an initial time period as defined by *monitoringfrequency* has elapsed. The monitoring server has nothing to report for the device until this happens.

Troubleshooting System Monitoring Problems

If you experience monitoring problems, check the following:

- The *vcdn managementid* on the device matches the name used for the device by the management server.
- Check to ensure the device is operating and able to communicate with its monitoring server (*vcdn monitoringurl*).

- ❑ Check the file for the device on the monitoring server (`/opt/volera/roma/modules/monitoring/xml/managementid`). If the file is more than 45 minutes old, the monitoring server ignores it when System Controller requests information for the device.

Content Monitoring

Content monitoring is discussed in [Monitoring Content Delivery](#) in *Content Controller Deployment Guide*.

16

Uninstalling Velocity Management Suite Components

If you need to uninstall Velocity management suite components, you must uninstall them in reverse installation order—Content Accountant first, Content Controller second, and System Controller last.

IMPORTANT: Uninstalling System Controller also removes the datastore and all the information it contains. However, you can restore datastore information from the previous installation if you have created a datastore backup. For more information, see [Chapter 22, “Backing Up and Restoring the Datastore,”](#) on page 95.

Uninstalling Content Accountant

From a GUI Interface

To uninstall Content Accountant using a GUI interface on the Velocity management server, run the following executable:

```
/opt/volera/roma/ca_uninstall
```

At the Server’s Command Line

To uninstall Content Accountant from the command line on the Velocity management server, enter the following command:

```
./ca_uninstall -console
```

Uninstalling Content Controller

From a GUI Interface

To uninstall Content Controller using a GUI interface on the Velocity management server, run the following executable:

```
/opt/volera/roma/cc_uninstall
```

At the Server's Command Line

To uninstall Content Controller from the command line on the Velocity management server, enter the following command:

```
./cc_uninstall -console
```

Uninstalling System Controller

From a GUI Interface

To uninstall System Controller using a GUI interface on the Velocity management server, run the following executable:

```
/opt/volera/roma/sc_uninstall
```

You will need to provide the datastore name and administrator password specified during installation to uninstall System Controller.

At the Server's Command Line

To uninstall System Controller from the command line on the Velocity management server, enter the following command:

```
./sc_uninstall -console
```

WARNING: Uninstalling the last System Controller on your network from the command line also removes the Velocity datastore. You are not asked to supply the datastore name or administrator password, and the uninstall doesn't warn you that the last remaining copy of the datastore is being removed.

However, you can restore datastore information from the previous installation if you have created a datastore backup prior to uninstalling System Controller. For more information, see [Chapter 22, "Backing Up and Restoring the Datastore,"](#) on page 95

17

Upgrading the Velocity Management Suite

You can upgrade an existing Velocity management suite installation by running the installation for the newer version on the same server.

Versions 1.0 and 1.2 Cannot Be Used Together

Version 1.2 management servers cannot interoperate with version 1.0 servers. If you have multiple Velocity management servers operating on the same datastore, they must all be running at the same version.

Once one of the servers has been upgraded to version 1.2, all others must also be updated to version 1.2 before they will perform correctly. Otherwise, when you attempt to log into a server that has not been upgraded, you will receive the message *ERROR: Authentication error, check username and password and try again*. This is caused by the datastore format having been updated for version 1.2.

Migrating an Existing 1.0 Datastore

If you run the Velocity installation program on an existing management server, you are asked whether you want the datastore migrated. If you select this option, all of the information in your 1.0 datastore is migrated to your 1.2 installation.

Upgrading to Version 1.2

If you are upgrading a management suite installation, you must complete the following tasks:

- 1 Upgrade the server's operating system from RedHat Linux 7.0 to RedHat Linux 7.2.
- 2 Run the installation utility for each Velocity product that is installed on the server.
 - ♦ The installation warns that a Java Virtual Machine (JVM) is being overwritten and asks you to confirm that you want to proceed. You must answer Yes or the process aborts.
 - ♦ The installation creates new uninstall modules in /opt/volera/roma-one for each management suite component.

IMPORTANT: After the upgrade process completes, System Controller automatically resynchronizes with all of its Exceleator cache devices to ensure data consistency. Cache devices are not available for configuration changes until they have been synchronized with System Controller.

Failure to upgrade all Velocity products on a management server will result in the management suite not starting. See [“Versions 1.0 and 1.2 Cannot Be Used Together” on page 83](#).

Synchronizing Exceleator 2.1 Devices

When Exceleator 2.1 devices that have Media Exceleator for Windows Media installed are automatically resynchronized, if the extended log method and extended log version are not configured on a device, the following configuration conflicts are reported:

```
set mmservice mmsfor extlogmethod=no
set mmservice mmsfor extlogversion=no
```

These errors are inconsequential and will not cause any problems with management or configuration of the devices.

Upgrading a Multiserver Installation

To upgrade an installation of multiple Velocity management servers, complete the following tasks:

- 1 Upgrade the first Velocity management server you installed originally.
- 2 Upgrade all other Velocity management servers that use the same datastore.

18

Synchronizing Devices and Datastores

As mentioned in “[Managing and Configuring Cache Devices](#)” on page 39, the management suite has a set of options to ensure that the configuration settings on cache devices match the settings stored in the datastore.

This synchronization can happen at either of two levels as explained in the following sections.

Device-Level Synchronization

Administrators with full access rights to a device can synchronize the device’s configuration settings with the datastore by doing the following:

- 1 In the browser-based management tool, click System > *Device Name* > Synchronize.
- 2 Select one of the options listed below.
 - ♦ **VCDN Datastore Overrides Device Settings:** The configuration settings on the device are overwritten by the settings in the datastore.
 - ♦ **Device Settings Override VCDN Datastore:** The configuration settings in the datastore are overwritten by the settings on the device.
 - ♦ **Generate Conflict Report Only:** System Controller notifies the administrator that the device settings and the datastore settings are not synchronized and lets the administrator either accept or reject the changes.
- 3 Specify when the synchronization will take place.
- 4 Click Synchronize.

If you selected to synchronize the settings immediately, the system reports whether there were conflicts and directs you to the Schedule page for details.

If you scheduled the synchronization for later, the system reports that the synchronization has been scheduled and directs you to the Schedule page for details.

Group-Level Synchronization

Administrators with full access rights to a device group can synchronize the configuration settings of the devices in the group with the datastore by doing the following:

- 1 In the browser-based management tool, click **System > Group Name > Synchronize**.
- 2 Select one of the options listed below.
 - ◆ **VCDN Datastore Overrides Device Settings:** The configuration settings on the devices are overwritten by the settings in the datastore.
 - ◆ **Device Settings Override VCDN Datastore:** The configuration settings in the datastore are overwritten by the settings on the devices.
 - ◆ **Generate Conflict Report Only:** System Controller notifies the administrator that the device settings and the datastore settings are not synchronized and lets the administrator either accept or reject the changes.
- 3 Specify when the synchronization will take place.
- 4 Click **Synchronize**.

The system reports that the synchronization has been scheduled and directs you to the Schedule page for details.

The Synchronization Details window displays a report of the synchronization event in two main sections, as follows:

- ◆ **Summary:** This includes when the event was started, who scheduled it, and whether it succeeded.
- ◆ **Configuration Settings:**

Configuration Settings Synchronization: Details regarding the status of settings.

VCDN Parameters: Status of Velocity management parameters on the device.

Device Parameters: Status of other configuration settings on the device.

System-Level Synchronization

You can schedule synchronization of all devices and datastores by doing the following:

- 1 In the browser-based management tool, click Administration > Synchronization.
- 2 Set the following System Synchronization options:
 - ◆ **Enable Recurring System Wide Synchronization:** Checking this option causes the system to synchronize repeatedly as scheduled. This works in connection with the Recurring Schedule option.
 - ◆ **Configuration Synchronization Policy:** This section contains the same options listed in [“Device-Level Synchronization” on page 85](#).
 - ◆ **Recurring Schedule:** This section lets you specify when recurring synchronization will occur. This works in connection with the Enable Recurring System Wide Synchronization option.
 - ◆ **Save Changes:** Selecting this option saves the configuration and enables the specified synchronizations.
 - ◆ **One Time Synchronization:** This opens a one-time system synchronization dialog.

19

Changing the Management Server's IP Address

If you need to change the IP address of the Velocity management server, you must complete the following steps to avoid failures and delays:

- 1 Shut down the Velocity management server using the **stop** command found in `/opt/volera/roma/bin`.

IMPORTANT: Failure to stop the Velocity management server at this point will prevent the licensing system from immediately detecting the IP address change when you reboot the server. This will result in a 30-minute startup delay after the reboot.

- 2 Change the IP address on the Red Hat Linux operating system using its network management configuration utilities.
- 3 Open the `vcdn.conf` file found in `/opt/volera/roma/conf` in a text editor.
- 4 Change all references to the old IP address to the new IP address and save the file.
- 5 Reboot the server.

20 Shutting Down and Restarting

As you manage content network components it is important to be able to shut down and restart Excelerator cache devices and Velocity management servers.

Shutting Down Cache Devices

Using Velocity management suite, you can schedule the shutdown and restart of cache devices in advance.

You can also shut down or restart an individual cache device.

If you need to shut down a cache device, be aware that cached objects stored in the device will be lost. The cache will have to be repopulated.

Shutting Down Velocity Management Servers

You might also need to shutdown Velocity management servers occasionally. If the server is shut down properly, all the data in the datastore is preserved. If your network has multiple management servers and datastores, the datastore on the server that has been shut down will be resynchronized automatically when the server is brought back online.

21

Synchronizing Time on Your Content Network

Server Time Must Be Set Prior to Installation

The Velocity management suite datastore requires that all system times are synchronized.

It is, therefore, critical that you configure management servers for network time protocol (NTP) support prior to installing System Controller.

For help enabling and configuring NTP support, refer to the following URL:
<http://www.redhat.com/docs/manuals/linux/RHL-7.2-Manual/custom-guide/dateconfig.html>.

22

Backing Up and Restoring the Datastore

Volera™ recommends that you back up the Velocity datastore regularly and has provided a utility named `ndsbackup` for this purpose on each management server containing System Controller.

To back up the datastore, complete the following steps:

- 1 Choose a location on the Velocity management server where you want the backup file created.

- 2 In the chosen directory, enter the following command:

```
ndsbackup cvf backupfile datastore_name
```

where *backupfile* is a filename you choose and *datastore_name* is the name of the datastore you specified when installing System Controller.

- 3 When prompted, enter the fully distinguished admin name as follows:

```
admin.is.vcdn
```

- 4 Enter the datastore administrator password you specified when installing System Controller.

A file of the name you have chosen is created in the directory from which you ran the backup utility.

- 5 Archive the backup file in a secure location.

To restore the datastore, complete the following steps:

- 1 Copy the archived copy of your datastore backup file to the management server in the directory where you originally created the file.

- 2 In the directory containing the file, enter the following command:

```
ndsbackup xvf backupfile
```

where *backupfile* is the name of the datastore backup file are using to restore the datastore.

- 3 When prompted, enter the fully distinguished admin name as follows:

admin.is.vcdn

- 4 Enter the datastore administrator password you specified when installing System Controller.

The datastore is restored with the information it contained when you backed it up.

For more information on the `ndsbackup` utility, enter the following command in the Linux command shell:

man ndsbackup

If the datastore stops communicating with System Controller or if objects disappear from the datastore, you will need to repair the datastore.

23 Securing the Content Network

This chapter discusses content network security issues.

Securing the Connections Between Browsers and Management Servers

The Velocity management server is configured by default for non-secure (port 80) communication with the management browser.

To configure the server for secure SSL communication with management browsers, complete the following steps:

- 1 Obtain SSL certificates and keys from a certificate authority (CA) that is recognized by your management browser.

- 2 Copy the certificates to a secure location on the management server.

We recommend you copy the certificate files to `/opt/volera/roma/apache/conf/ssl.crt`.

- 3 Copy the keys to a secure location on the management server.

We recommend you copy the key files to `/opt/volera/roma/apache/conf/ssl.key`.

- 4 Open the `/opt/volera/roma/apache/conf/httpd.conf` file for editing

- 5 Modify the `ssl.crt` line to point to the directory where you copied the certificate files.

- 6 Modify the `ssl.key` line to point to the directory where you copied the key files.

- 7 Open the `/opt/volera/roma/bin/start` file for editing.

- 8 Modify the following line:

```
/opt/volera/roma/apache/bin/apachectl start
```

to read

```
/opt/volera/roma/apache/bin/apachectl startssl
```

- 9 To attach to the Velocity management server, use the HTTPS protocol rather than HTTP.

Managing HTTP CONNECT Method Support

The HTTP protocol supports a number of different access methods such as GET, POST, and CONNECT.

The CONNECT method is normally used to establish a tunneled connection through which encrypted SSL traffic can be sent. However, it is not safe to assume that all CONNECT requests received by proxy servers are actually for SSL traffic. Outsiders frequently scan the Internet for proxies on port 8080 and other commonly used proxy ports to discover proxy servers that are accessible to them.

Exceleator cache devices include features to protect your network from such attacks. For more information, see the Exceleator documentation.

24 Keeping Content Network Data Secure

This chapter discusses the following topics:

To	See
Learn about built-in SSL support on cache devices	“SSL and Excelerator Cache Devices” on page 99
Learn about Volera’s Secure Excelerator add-on	“Using Secure Excelerator on Your Content Network” on page 100

SSL and Excelerator Cache Devices

Each Excelerator cache device has public key infrastructure mechanisms for generating, importing, using, and maintaining public key certificates. These include an internal CA which automatically generates certificates for each assigned IP address, and mechanisms for generating certificate signing requests (CSRs).

Excelerator’s Internal CA

Each Excelerator has an internal certificate authority (CA) which automatically generates certificates for each assigned IP address and certain other resources.

Excelerator uses these auto-generated certificates for securing certain system management communications, such as obtaining filtering lists and communicating with the Velocity management server.

These internally generated certificates can also be used for secure connections with browsers using appliance caching services. However, browsers won’t

recognize the appliance CA unless they are specifically configured to do so. Unconfigured browser will receive confirmation messages that can confuse users and cause them to not use the appliance's caching services.

To create appliance-specific certificates, see the instructions in the Excelerator documentation.

Generating Certificate Signing Requests (CSRs)

To prevent users from receiving unsettling SSL confirmation messages, you need to request a certificate from an external certificate authority (CA) that browsers will recognize. Generating a CSR is the first step to obtaining a certificate from an external CA.

After you obtain certificates from one or more external CAs, you can use Excelerator's certificate maintenance features to monitor certificate status, back up certificates in case the appliance fails, and replace certificates when they expire.

To generate a CSR and store the issued certificate, see the instructions in the Excelerator documentation.

Using Secure Excelerator on Your Content Network

If you have installed Secure Excelerator on any cache devices on your network, you should be aware of a potential IP address/port conflict.

The Velocity management server communicates with cache devices using SSL on the standard port (443). Secure Excelerator also uses the standard port for all SSL connections. Both of these ports can be configured.

The conflict will arise if you attempt to use a cache device's IP address for Velocity management that Secure Excelerator is also using. You must ensure that these services use different IP addresses or configure the SSL communication port for one of the services to another port number.