



CHAPTER 10

Creating and Managing a Content Server Cluster

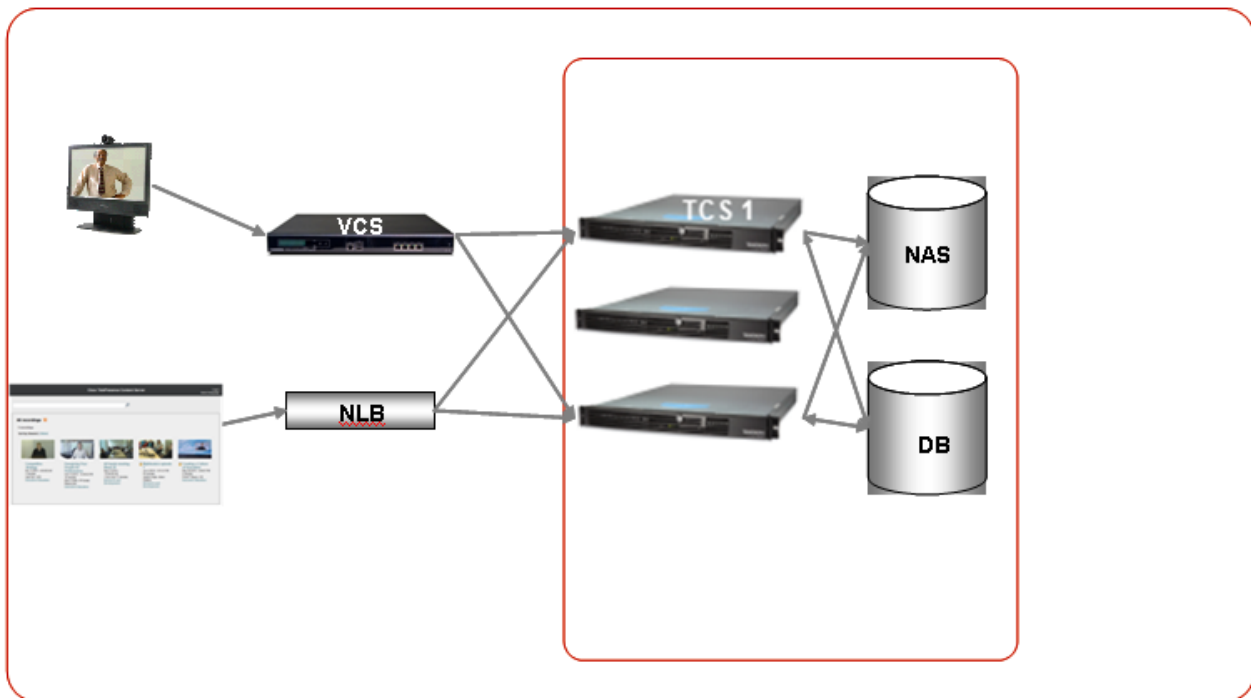
This chapter describes the main features, system requirements, setup, and management of a Cisco TelePresence Content Server (TCS) cluster. To a user, a Content Server Cluster behaves exactly as a single Content Server does, but a cluster has a much greater capacity for recording, streaming, and serving the web interface.

- [Main Features, page 10-2](#)
- [System Requirements, page 10-4](#)
- [Important Guidelines, page 10-5](#)
- [Setting up a Content Server Cluster, page 10-6](#)
- [Managing a Content Server Cluster, page 10-20](#)
- [Removing a Content Server from the Cluster, page 10-28](#)
- [Using TMS to Schedule Calls on a Content Server Cluster, page 10-29](#)
- [Upgrading the Cluster to a New Software Version, page 10-30](#)
- [Upgrading the External Microsoft SQL Server from SQL Server 2005 to SQL Server 2008, page 10-30](#)
- [Backing Up and Restoring the Content Server Cluster, page 10-31](#)

Main Features

General Reliability

Multiple Content Servers can be clustered together to increase total recording and playback capacity. In this cluster architecture, there is no controller; each Content Server performs exactly the same tasks. If a Content Server is taken out of the cluster, the only effect on the cluster is a decrease in the total capacity of recording and playback.



Interface Redundancy

The user can manage a cluster from any Content Server in the cluster. The Cluster Overview page provides information about the number of calls and transcoding jobs in progress on the whole cluster, as well as the calls, transcoding jobs, and the status of essential services on each Content Server in the cluster.

HTTP Load Balancing

The use of a network load balancing solution (NLB) ensures that incoming user HTTP requests are spread across the cluster. While multiple solutions are available to handle NLB, the final recommendation in this document includes a hardware solution, Loadbalancer.org.

Inbound H.323 Call Routing

Inbound call load balancing is managed by the VCS (Video Communications Server) that the cluster is registered to. Each Content Server is only capable of two transcoded live streaming outputs out of a total call capacity of five calls. Using a live streaming alias means that others can watch recording while it is in progress and then also view the recording on demand later. Using a non-live streaming alias means that the call is recorded, but it cannot be watched until recording has finished and the offline transcoder has processed the outputs for on-demand viewing.

While standalone Content Servers have a mixture of live and non-live aliases, they only require one gateway prefix for both. However, a Content Server Cluster needs two gateway registrations with separate prefixes—one for live transcoded calls and another for non-live (offline transcoded) calls—to ensure good load balancing of both types of calls across the cluster. Resource Allocation Indication messages are used to signal the VCS when a Content Server in the cluster is out of resources for a particular call type. These messages allow the gatekeeper to route calls appropriately. A Content Server that signals that it is out of resources for a live call type prefix will not be allocated any more calls that come in on that prefix until it signals that resources are available.

Additionally, for registrations with the VCS, each Content Server needs four system aliases: live and non-live H.323 ID and E.164 system aliases. It is important that each of these aliases is unique on each Content Server and in the cluster. There must be no duplicate aliases.

System aliases should not be used for calling the cluster, as they are routed to a particular Content Server. If this Content Server is busy, calls to its system alias will be rejected even if other Content Servers are not busy at that time. Calls are appropriately load balanced across the cluster only when recording aliases are used for dialing a cluster.

Outbound H.323 Calls Load Balancing

Outbound calls can be made using the web interface or the ClusterDial API command. Load balancing is based on current call load; the Content Server with the smallest call load is chosen to handle the call. Because there is no controller in the cluster architecture, the API commands can be sent to any of the Content Servers in the cluster. For added redundancy of the API functionality and to ensure that the external implementation does not artificially create a controller, it is up to the integrator to build the logic around distributing the API commands among all Content Servers in the cluster to deal with situations such as Content Server unavailability.

Scalable Storage

One Network Attached Storage (NAS) is used for the whole cluster, and all media files are hosted on the NAS. Using NAS ensures that storage can grow as the cluster grows and is not constrained by the Content Server hardware capacity. Because transcoded media files are stored on the NAS, on-demand streaming of any recording is possible from any Content Server.

External Microsoft SQL Server Database

All Content Servers in the cluster connect to one external Microsoft SQL Server 2005 or 2008 database. Using one SQL server ensures that cluster configurations and recording information are global across the cluster. If a Content Server is taken out of the cluster, the recordings that were created by that Content Server are accessible from the interface of any of the other Content Servers remaining in the cluster.

It is the responsibility of the cluster implementer to provide the external Microsoft SQL Server 2005 or 2008 instance. It should be noted that the SQL server instance on a Content Server cannot be used to configure an external database for other Content Servers in the cluster. While there are multiple ways to configure external databases, configurations that are required for the correct functioning of a cluster are described in more detail later in this document.

API support

The cluster is supported by the API, which provides a special command for dialing out of the cluster as well as cluster status documents to report status and configuration across all nodes. The cluster API commands are fully documented in the Cisco TelePresence Content Server API Guide.

System Requirements

Cisco TelePresence Content Server

- Version 3.3 or higher.
- Each Content Server in the cluster and the NAS must be added to the same Windows Active Directory domain.
- A Cluster Enabled option key is required for each Content Server that is going to be added to a cluster. The option key must be installed before running the TCS wizard so that the clustering option is accessible in the wizard.
- A valid HTTPS security certificate should be obtained from a trusted source, such as a Certificate Authority (COMODO, VeriSign, etc.). This certificate should then be installed on each Content Server in the cluster.

External SQL Server database

- Microsoft SQL Server 2005 (Service Pack 2 or higher) or Microsoft SQL Server 2008 Standard or Enterprise supported by S4.x. The cluster requires an external database instance to be configured on a separate machine (not a Content Server).
- The database server requires dual 3 GHz processors and a minimum of 4 GB RAM.
- Microsoft .NET Framework 2 or higher must be installed on the server where the Microsoft SQL Server is installed.

See the [“Configure the External SQL Server Database” section on page 10-7](#) for information about database configuration.

Gatekeeper

- VCS X2.1 or higher.

Network Load Balancer (NLB) solution

There are a number of options for load balancing HTTP page requests.

The recommended solution for a Content Server Cluster includes hardware-based NLB. This document describes the setup for a Loadbalancer.org hardware load balancer.

For installations where optimized load balancing of page requests is not important, DNS round robin can also be used.

Network Attached Storage (NAS)

- Compatible systems include any NAS device built on the Windows Storage server and which is Windows Hardware Quality Lab certified. The file sharing protocol used by the Content Server to the NAS is Microsoft SMB.
- The NAS device must be added to the same Windows Domain as the Content Servers.
- The NAS should be dedicated to media storage. Installing your Domain Controller on the NAS device is not supported and might cause the Content Server cluster to stop functioning.

See [“Configure the NAS” section on page 10-10](#) for information about the required NAS share configuration.

Important Guidelines

- The current solution supports up to 10 Content Servers in a cluster.
- A cluster supports Content Servers with mixed 5-and-10-port capacity.
- All Content Servers in a cluster must be at the same physical site, within a network round-trip time (RTT) to the NAS and SQL servers not exceeding 10 ms.
- The solution supports H.323 protocol only. SIP registration and SIP calling is not supported.
- Dialing into the cluster using the load balanced frontend address or IP addresses of Content Servers in the cluster is not supported. The cluster design relies on call balancing done by the gatekeeper, and this call balancing can occur only when recording aliases (or playback addresses in a Premium Resolution cluster) are dialed.
- The ConfigRestore command (**Main Menu > Commands > Restore Defaults > ConfigRestore**), which is available through a serial port connection, is not available when a Content Server is in a cluster.
- The FullRestore command (**Main Menu > Commands > Restore Defaults > FullRestore**), which is available through a serial port connection, restores the Content Server to its original settings, but the command also causes it to lose its cluster settings, while cluster database continues as if the Content Server were still in the cluster. Adding the TCS back to the cluster after running FullRestore is recommended. The Content Server can then be removed from the cluster, if required, using the TCS wizard.
- Adding or removing the live output from a template results in a change of the gateway prefix of recording aliases that use that template.

Example:

The live gateway prefix on your cluster is `tcscluster.live` and the non-live gateway prefix is `tcscluster.nonlive`.

A recording alias with an H.323 ID of `tcscluster.nonlive.myalias@company.com` uses a Windows Media switching template with no live streaming output. If a live streaming output is added to the template, the H.323 ID of the recording alias changes from `tcscluster.nonlive.myalias@company.com` to `tcscluster.live.myalias@company.com`. Calls to the original alias fail.

- A Premium Resolution Content Server that you add to a non-Premium Resolution cluster behaves like a non-Premium Resolution Content Server until Premium Resolution keys are added to all Content Servers in the cluster. Each Content Engine checks the database at startup and once per hour to see if other Content Servers in the cluster are Premium Resolution or not. If all Content Servers are restarted after Premium Resolution keys have been added to each, the cluster begins to behave

as Premium Resolution cluster immediately. If the Content Servers with newly installed Premium Resolution keys are not restarted, the cluster behaves as a Premium Resolution cluster approximately one hour after the keys are installed.

If you add a non-Premium Resolution Content Server to a Premium Resolution cluster, the cluster becomes a non-Premium Resolution cluster. If the Content Servers are restarted after the non-Premium Resolution Content Server is added, the cluster behaves as a non-Premium Resolution cluster immediately. If they are not restarted, the cluster behaves as a non-Premium Resolution cluster approximately one hour later. See [Chapter 9, “Premium Resolution”](#) for more information about Premium Resolution.

See the release notes for a list of other known issues for this release.

Setting up a Content Server Cluster

Setting up a Content Server Cluster consists of eight steps. To set up a cluster successfully, follow the steps in the order that is given below.

We recommend that you familiarize yourself with the [“Important Guidelines”](#) section on page 10-5 before setting up a cluster.

Overview of the Process

-
- | | |
|---------------|---|
| Step 1 | Understand Content Server Prerequisites, page 10-6 |
| Step 2 | Configure the External SQL Server Database, page 10-7 |
| Step 3 | Configure the NAS, page 10-10 |
| Step 4 | Create a Content Server Cluster, page 10-11 |
| Step 5 | Add a Content Server to an Existing Cluster, page 10-16 |
| Step 6 | Configure Gatekeeper Registration, page 10-17 |
| Step 7 | Configure Domain Authentication, page 10-18 |
| Step 8 | Configure Network Load Balancing (NLB), page 10-18 |
-

Understand Content Server Prerequisites

- Ensure that all the Content Servers that you want to cluster are at version S3.3 or higher. If they are not, upgrade them to at least version S3.3, and check that they have the same build number.
- Add all Content Servers that you want to cluster to a Windows Active Directory domain. The general requirements for adding a Content Server to a Windows domain must be adhered to.
- Add the cluster option key. A cluster option key should be installed on each Content Server. To install the key, go to the **Management** tab. Then go to **Diagnostics > Server overview**, and locate the **Software option** section. The option key must be installed before running the TCS wizard so that the clustering option is accessible in the wizard.

- Install security certificates from a trusted source, such as a Certificate Authority (COMODO, VeriSign, etc.). This certificate should then be installed on each Content Server in the cluster. Using a common certificate on all the Content Servers ensures that users do not have to obtain unique certificates for each Content Server in the cluster when they access the cluster through the network load balanced address.

For more information on installing security certificates, please see the Security Certificate Management section in the TCS Getting Started Guide.

- Ensure that the time zone, time, and date settings are identical on all Content Servers to be clustered.

Configure the External SQL Server Database

Ensure that your existing Microsoft SQL server is compatible with the Content Server Cluster system requirements (see [“System Requirements” section on page 10-4](#)).

The process of configuring the external SQL server consists of the following steps. Each step is described in a separate section:

-
- Step 1** [Add an SQL Server Instance, page 10-7](#)
 - Step 2** [Configure the SQL Server Instance, page 10-8](#)
 - Step 3** [Create a Special User on the SQL Server, page 10-9](#)
-

Add an SQL Server Instance

One SQL server database is used by all Content Servers in a cluster. This database must not be hosted on any of the Content Servers used in the cluster.

The Content Server Cluster requires its own instance of the SQL server. If Microsoft SQL Server is already installed, you have to add a new instance to your existing SQL server installation. If Microsoft SQL Server is not already installed, you must install Microsoft SQL Server in order to create the new instance. In both cases, in order to create the instance, you need the Microsoft SQL Server installer available from Microsoft on the installation media (CD or DVD). See the [“System Requirements” section on page 10-4](#) to ensure that you use the correct version of the SQL server installer to create the new instance.



Note

Only installation wizard steps that are required for a Content Server Cluster are included in this document.

Using the Microsoft SQL Server 2005 or 2008 installation media to add a new instance:

-
- Step 1** Insert the Microsoft SQL Server installation media into the disk drive of the machine that will host your SQL server. Start the Microsoft SQL Server Installation Wizard.
 - Step 2** In Components to Install, check the **SQL Server Database Services** box.
 - Step 3** In Instance Name, click the **Named instance** radio button, and enter the instance name.
 - Step 4** In Service Account, choose Use the built-in System account (Local system, or Network service).

- Step 5** In Authentication Mode, click the **Mixed Mode (Windows Authentication and SQL Server Authentication)** radio button. Enter and confirm the SA (system administrator) password.
- Step 6** SQL server collation should be set to **Latin1_General_CI_AS, 'Dictionary, case insensitive, 1252 character set'**.

**Note**

For SQL Server 2005 installations, Service Pack 2 or later must be applied to the newly created instance. If you apply an earlier service pack, the TCS wizard database connection test fails, and you cannot create a Content Server Cluster with this instance

For more information on installing SQL Server 2005, see Microsoft article in the SQL Server 2005 Books Online:

Preparing to Install SQL Server 2005: <http://msdn.microsoft.com/en-us/library/ms143719.aspx>

Security Considerations for a SQL Server Installation:

<http://msdn.microsoft.com/en-us/library/ms144228.aspx>

Check Parameters for the System Configuration Checker:

<http://msdn.microsoft.com/en-us/library/ms143753.aspx>

Configure the SQL Server Instance

To configure the SQL server instance for a Content Server Cluster, follow these steps:

- Step 1** Open the SQL Server Configuration Manager (usually located from the **Start** menu under **All Programs > Microsoft SQL Server 2005 (or 2008) > Configuration Tools**).
- Step 2** In **SQL Server 2005 (or 2008) Network Configuration**, select Protocols for *instance_name*. The *instance_name* is the name you specified when creating an SQL Server instance (see the “[Add an SQL Server Instance](#)” section on page 10-7).
- Step 3** Ensure that these parameters are configured as follows:
- Shared Memory is enabled.
 - Named Pipes are disabled.
 - TCP/IP is enabled.
 - VIA is disabled.
- Step 4** Right click **TCP/IP** and click properties. Click the **IP Addresses** tab:
- For each IP address, set **Enabled** to **No**.
 - Clear all **TCP Dynamic Ports** fields. Delete any zeros that appear in those fields.
 - Clear all **TCP Ports** fields from all IP Addresses.

- d. Under **IP All**, enter the TCP port that the Content Server will use to connect to this instance:

An example for TCP Port is 2090.

You can use any port in the range of between 1000 and 64000 that is open on the firewall and is not used by other software on TCS or on the server that is hosting the SQL server. The port that you specify here also must not conflict with ports set up for other instances on the server.

- Step 5** Click **SQL Server 2005 (or 2008) Services**, select the instance you just created, right-click, and then click **Restart Service**.

Create a Special User on the SQL Server

The user that you create in the following steps are used by the Content Servers to connect to the SQL server external database. For security reasons, we recommend that you do not use the existing system administrator (SA) user account. Instead, create a new user account

Before You Begin

This user requires administrative privileges and CREATE TABLE and ALTER TABLE authorization. Choose any username that you want for this user.

- Step 1** Using the sqlcmd utility, open a command prompt on the machine on which the SQL server is running.

- Step 2** To connect to the SQL Server, enter one of the following commands:

- To use a trusted connection, enter `sqlcmd -S (local)\instance_name -E`
- To connect with SQL authentication, enter `sqlcmd -S (local)\instance_name -U login_id -P password`

The instance_name is the name you specified when creating an SQL Server instance (see the [“Add an SQL Server Instance”](#) section on page 10-7).

- Step 3** At the Command Utility prompt 1>, enter the following command to create a user:

```
CREATE LOGIN user_name WITH PASSWORD='strong_password'
```

Then press **Enter**.

- Step 4** At the prompt, enter **GO** and press **Enter**.

- Step 5** Enter **EXIT** and press **Enter** to exit sqlcmd.

This example shows how to create user TCS_DB_USER on the SQL server:

```
C:\Documents and Settings\Administrator>sqlcmd -S (local)\my_instance -E
1> CREATE LOGIN TCS_DB_USER WITH PASSWORD='xxxxxxxxxxxxxxxxxx'
2> GO
1>EXIT
```

For more information on using the sqlcmd utility, see the Microsoft article in the SQL Server Books Online: “sqlcmd Utility.”

For more information on creating a user using CREATE LOGIN, see the Microsoft article in the SQL Server Books Online: “CREATE LOGIN (Transact-SQL).”

Configure the NAS

The Content Server cluster uses a share on the NAS as its media storage location. See [“System Requirements” section on page 10-4](#) first to ensure that your NAS is compatible with Content Server Cluster system requirements.

The process of configuring the NAS consists of the following steps. Each step is described in a separate section:

-
- Step 1** [Manage the Windows Active Directory Domain, page 10-10](#)
 - Step 2** [Choose or Create a Domain Account to Access the NAS Share, page 10-10](#)
 - Step 3** [Set up a Share on the NAS, page 10-10](#)
 - Step 4** [Set Permissions and Security Settings on the Share, page 10-11](#)
-

Manage the Windows Active Directory Domain

All Content Servers in cluster and the NAS must be added to the same Windows Active Directory domain.

Choose or Create a Domain Account to Access the NAS Share

Choose or create a domain user. You may choose any username you want for this user. In this document, we refer to this user as MYDOMAIN\TCS_NAS_USER. MYDOMAIN\TCS_NAS_USER is used by the Content Server Cluster to access the NAS share.



Note

You must enter the username and password for MYDOMAIN\TCS_NAS_USER when you run the TCS wizard.

Set up a Share on the NAS

-
- Step 1** Log on to the NAS using Windows Remote Desktop Connection.
 - Step 2** Create a folder on the NAS.
 - Step 3** Make this folder a shared folder.
-



Note

You must enter the path to this share when you run the TCS wizard.

Set Permissions and Security Settings on the Share

All Content Servers and the domain account that the Content Server Cluster uses to access the share on the NAS must be given full control over the share. You must set up the NAS share correctly to use the TCS wizard successfully.

-
- Step 1** Right-click the share, and click **Sharing and Security**.
- Click **Permissions**.
 - Click **Add**.
 - Click **Object Types**.
 - Check the box for Type—**Computers**.
 - Enter all the DNS names of Content Servers that you want to cluster. You used these DNS names when you registered the Content Servers in the domain.
 - Click **Check Names**. Click **OK**.
 - Enter the name of the MYDOMAIN\TCS_NAS_USER account.
 - Click **Check Names**. Click **OK**.
 - Give each of the Content Servers and MYDOMAIN\TCS_NAS_USER full control over the share.
- Step 2** Click the **Security** tab.
- Click **Add**.
 - Click **Object Types**.
 - Check the box for Type—**Computers**.
 - Enter all the DNS names of Content Servers that you want to cluster. You used these DNS names when you registered the Content Servers in the domain.
 - Click **Check Names**. Click **OK**.
 - Enter the name of the MYDOMAIN\TCS_NAS_USER account.
 - Click **Check Names**. Click **OK**.
 - Give each of the Content Servers and MYDOMAIN\TCS_NAS_USER full control over the share in the Security Settings tab.
-

Create a Content Server Cluster

In order to create a cluster of Content Servers, you must run the TCS wizard from Remote Desktop on one of the Content Servers. Then you must run the TCS wizard on all the remaining Content Servers to add them to the cluster.

The Order of Content Servers Added to the Cluster



Caution

If you cluster Content Servers that have existing recorded content and configurations that you want to keep, the order in which you add Content Servers to the cluster is important.

- **The first Content Server in the cluster.** Existing content and configurations (recording aliases, templates, call configurations, media servers) from the first Content Server that you use to create a new cluster are added and available to other Content Servers in the cluster.

Only the first Content Server preserves its playback addresses to play back recordings on endpoints. The playback addresses of all subsequently added Content Servers are modified to avoid duplicates.

For example, take these playback addresses of three standalone content servers:

Playback addresses for standalone Content Server 1:

- 13115 Recording 1
- 14117 Recording 2
- 21416 Recording 3

Playback addresses for standalone Content Server 2:

- 1521 Recording A
- 1635 Recording B

Playback addresses for standalone Content Server 3:

- 1521 Recording X
- 2142 Recording Y
- 21413 Recording Z

Notice that standalone Content Servers 2 and 3 have a playback address that is the same (1521). If all three of these Content Servers are added in order to the same cluster, playback aliases are modified for all Content Servers that are added to the cluster after the first server to avoid duplicate aliases. The playback aliases for these servers in the same cluster would look like this:

All three Content Servers in the same cluster

- 13115 Recording 1 (Content Server 1—playback aliases are retained)
- 14117 Recording 2
- 21416 Recording 3
- 101 Recording A (Content Server 2—playback aliases are modified)
- 102 Recording B
- 103 Recording X (Content Server 3—playback aliases are modified)
- 104 Recording Y
- 105 Recording Z

- **The second and any additional Content Servers.** All content from the second and any other Content Servers that you add to the cluster is imported into the cluster. The following configurations are not imported:
 - Configurations that are added include media servers associated with recordings and categories associated with recordings.
 - Configurations that are not added include recording aliases; templates; call configurations; media servers not associated with recordings; categories not associated with recordings; and LDAP servers and users.

For all Content Servers that are added to the cluster, the wizard does not move any media files that are not associated with the Content Server's database. Media files that are not moved include orphaned temporary files not used in any recordings; .tcb import or export files; or files placed in the data folder by the user. These files are not moved to the NAS from the local TCS disk drive and are deleted. If you move media between NAS locations or from the NAS to a local TCS disk drive, the wizard does not move these files, but the wizard does not delete them.

TCS Wizard Options

The TCS wizard that is available as a shortcut from the Remote Desktop of version S3.3 or later Content Servers has the following options:

- Alternate Storage (NAS) Wizard for a standalone Content Server.
- Cluster Management Wizard.

If you select the Cluster Management Wizard on a standalone TCS, you see these options:

- Create a new cluster.
- Add to an existing Cluster.

If you select the Cluster Management Wizard on a clustered TCS, you see these options:

- Generate Cluster Settings File.
- Configure Load Balancer Configuration.
- Update Cluster Settings.
- Remove from Cluster.

User Accounts for the TCS Wizard

The TCS wizard can run under the following user accounts:

- A domain administrator account.
- The special domain account you set up in the [“Configure the NAS”](#) section on page 10-10.
- The local default administrator account.



Note

Unless explicitly stated otherwise, this document assumes that the TCS wizard is run under a domain administrator account.

Before Running the TCS Wizard

Before you run the TCS wizard to create a new cluster, ensure you have the following information available:

- External SQL server IP address or name.
- Name of the SQL database instance.
- The TCP/IP port you have chosen for your instance. The TCS Wizard uses this TCP/IP port to connect to your instance. The wizard does not verify that this port is the correct one for your instance; the wizard connects to whatever database instance is available from that port. Ensure that this port is the port that you specified for your instance and that no other instance is using it.

- The password for system administrator (SA) user or the username and password of an SQL user with create and alter privileges (not TCS_DB_USER).
- The username and password of TCS_DB_USER.
- Path to the NAS share in the format of \\servername\sharefolder. IP addresses cannot be used for the NAS path.
- The username and password of MYDOMAIN\TCS_NAS_USER domain account.

Create a New Cluster

-
- Step 1** Using Windows Remote Desktop Connection as a domain administrator, log in to the first Content Server that you want to cluster.
- Step 2** Go to **Computer Management > System Tools > Local Users and Groups > Groups > Administrators**. Add the domain account MYDOMAIN\TCS_NAS_USER to the Administrators group on the Content Server.
- Step 3** Double click the TCS Wizard icon on the desktop, or open **All Programs > Cisco > Content Server > TCS Wizard**.
- Step 4** Click **Next** from the Welcome screen.
- Step 5** The wizard displays an overview screen and then runs through its initialization phase. If recordings are in progress on this Content Server, the wizard cannot continue. You can either end the recordings or cancel the wizard. If possible, end the recordings and continue running the wizard.
- Step 6** After the wizard finishes its initialization stage, it puts the Content Server in Idle mode. No calls can be made, and no transcoded outputs are processed. The Content Server returns to Online mode after the wizard process is completed or is cancelled.
- Step 7** Click the **Cluster Management Wizard** radio button. Click **Next**.
- Step 8** The wizard then verifies cluster prerequisites. Click **Next**.
- Step 9** Click the **Create a new cluster** radio button. Click **Next**.
- Step 10** Read the informational screen. Click **Next**.
- Step 11** At the **Connect to an external SQL Server Database** screen, enter the information for the database instance you have set up:
- SQL server IP address or name.
 - Name of the database instance.
 - TCS/IP port that was chosen for the instance.
 - Assign a database (catalog) prefix to your instance at this stage. It can be any string that you want. The wizard appends “3” to the end of the string that you have specify. The wizard uses this prefix to distinguish this database instance from other versions that might be added to the instance at a later time.
 - The username and password of the SA user, or the username and password of another SQL user with create and alter privileges (not TCS_DB_USER). The credentials of the SA user are used to create and configure the cluster database when this wizard is run. The TCS does not store the credentials of the SA user.
- Step 12** Click **Next** in the database configuration informational screen.
- Step 13** Enter the username and password of the database user that you created. The TCS uses these user credentials to connect to the database.

- Step 14** Click **Next** in the next informational screen.
- Step 15** Enter the path for the NAS share that you set up. The path is in this format: `\\server\share`. Ensure that you enter the NAS server computer name, not the IP address of the NAS.
- Step 16** Click **Next** in the next informational screen.
- Step 17** In the IIS Anonymous User Account screen, enter the username and password of the domain account that you created. The TCS uses these credentials to access the share on the NAS. An example of a username: `MYDOMAIN\TCS_NAS_USER`.
- Step 18** Click **Next** in the next informational screen.
- Step 19** In the Content Server System Configuration screen, you can change the **System name** and default **Non-Live** and **Live** system aliases for this Content Server. The defaults that are suggested by the wizard are based on the current settings of the standalone TCS. For factory new Content Servers, it is the serial number for the non-live H.323ID and the serial number with “.live” appended (*serial number.live*) for the live H.323 ID. You can change the system name and aliases for this Content Server from the Server Overview page after you successfully set up the cluster.
- Step 20** In the Content Server Checks screen, confirm that the Content Server is backed up and that antivirus software is stopped (if it is installed). If the TCS is not backed up and antivirus software is not stopped, cancel the wizard and complete those actions. Then run the wizard again. Your system will not have changed if you click **Cancel**.
- Step 21** The Cluster: Test Result screen displays information about your intended setup. If all tests are successful, click **Configure** to configure the cluster.
- You can also click **Finish** to exit the wizard without creating the cluster or making any changes. If any of the tests failed, you cannot continue to run the wizard.



Note Media files that are not associated with the Content Server's database include orphaned temporary files not used in any recordings, .tcb import file, and .tcb export files. These files are not moved to the NAS and are deleted from the local disk.

If you click **Configure**, the wizard configures your system and moves the media files to the NAS share. This process might take some time, depending on the amount of media to be moved to the NAS.

- Step 22** After the configuration process is complete, in the Cluster: Save Cluster Settings File screen, save the cluster settings file. Browse to the location where you want to save the file. Then click **Save**.
- You can also generate the cluster settings file by running this TCS wizard again after you finish creating the cluster (see [“Generate a Cluster Settings File” section on page 10-24](#)). You need the cluster settings file if you want to add other Content Servers to this cluster.
- Step 23** Click **Finish** to exit the wizard. The log location for the wizard is displayed on this screen.

You successfully set up a new cluster with one Content Server. You can now add other Content Servers to this existing cluster.



Note Your cluster cannot make calls until you have registered it to a gatekeeper. See the [“Configure Gatekeeper Registration” section on page 10-17](#).

Add a Content Server to an Existing Cluster

To add a Content Server to an existing cluster, you must meet the following prerequisites:

- Additional Content Servers must meet the criteria that are described in the [“Understand Content Server Prerequisites”](#) section on page 10-6.
- Additional Content Servers must be given full control over the NAS share that you created. If they are not given full control, you cannot successfully add these Content Servers to an existing cluster.
- You must copy the cluster settings file to the desktop of the Content Server that you want to add. You can generate a cluster settings file at any time by running a TCS wizard on any of the Content Servers that are already in the cluster. See the [“Generate a Cluster Settings File”](#) section on page 10-24.

**Note**

To understand which configurations and media content from additional Content Servers are added to the cluster, see [“The Order of Content Servers Added to the Cluster”](#) section on page 10-12.

After ensuring that additional Content Servers meet the prerequisites, run the TCS wizard on the Content Server that you want to add to the cluster.

-
- Step 1** Using Windows Remote Desktop Connection as a domain administrator, log in to the Content Server that you want to add to the cluster.
- Step 2** Go to **Computer Management > System Tools > Local Users and Groups > Groups > Administrators**. Add the domain account MYDOMAIN\TCS_NAS_USER to the Administrators group on the Content Server.
- Step 3** Double-click the TCS Wizard icon on the desktop, or open **All Programs > Cisco > Content Server > TCS Wizard**.
- Step 4** Click **Next** in the Welcome screen. The wizard displays an overview screen and then runs through its initialization phase. If recordings are in progress on this Content Server, the wizard cannot continue. You can either end the recordings or cancel the wizard. If possible, end the recordings and continue running the wizard.
- Step 5** After the wizard finishes its initialization stage, it puts the Content Server in Idle mode. No calls can be made, and no transcoded outputs are processed. The Content Server returns to Online mode after the wizard process is completed or is cancelled.
- Step 6** Click the **Cluster Management Wizard** radio button. Click **Next**.
- Step 7** The wizard then verifies cluster prerequisites. Click **Next**.
- Step 8** Click the **Add to an existing cluster** radio button.
- Step 9** In the Cluster: Load Cluster Settings File window, browse to the cluster settings file that you copied to the desktop.
- Step 10** In the Content Server System Configuration screen, you can change the **System name** and default **Non-Live** and **Live** system aliases for this Content Server. The defaults that are suggested by the wizard are based on the current settings of the standalone TCS. For factory new Content Servers, it is the serial number for the non-live H.323ID and the serial number with “.live” appended (*serial number.live*) for the live H.323 ID. You can change the system name and aliases for this Content Server from the Server Overview page after you add the Content Server to the cluster.
- Step 11** In the Content Server Checks screen, confirm that the Content Server is backed up and that antivirus software is stopped (if it is installed). If the TCS is not backed up and antivirus software is not stopped, cancel the wizard and complete those actions. Then run the wizard again.

Step 12 The Cluster: Test Result screen displays information about your intended setup and the amount of media to be moved from this Content Server to the media location for the cluster (NAS). If all tests are successful, click **Configure** to configure the Content Server and add it to the cluster.

You can also click **Finish** to exit the wizard without adding the Content Server to the cluster or making any changes. If any of the tests failed, you cannot continue to run the wizard.

If you click Configure, the wizard configures your system and adds the Content Server to the cluster. This process might take some time, depending on the amount of media to be moved to the NAS.

Step 13 Click **Finish** to exit the wizard. The log location for the wizard is displayed on this screen.

You have successfully added another TCS to a cluster. Repeat this process for each new Content Server that you want to add to the cluster.

Configure Gatekeeper Registration

After you add Content Servers to the cluster, you must configure your gatekeeper registration before you can start making calls to record. The gatekeeper is permanently enabled for a Content Server Cluster; it is not possible to disable the gatekeeper functionality.

Step 1 Log in to the web interface of any of the Content Servers in the cluster as an administrator. From the **Management** tab, go to **Configuration > Site settings**.

Step 2 In the Gatekeeper settings section, enter a gatekeeper address.

Step 3 Enter Live and Non-Live H.323 and E.164 gateway prefixes. In Premium Resolution clusters, you also have the option of entering playback gateway prefixes to enable playing recordings back from endpoints. The prefixes that you enter cannot be subsets of one another. Ensure that they are unique and that they follow the dialing plan set up on your VCS.

A Content Server cluster needs two gateway registrations with separate prefixes: a live gateway prefix for live transcoded calls and a non-live gateway prefix for offline transcoded calls. Having two gateway registrations with separate prefixes ensure good load balancing of both types of call across the cluster by the gatekeeper.

Step 4 Check the Q.931 and Ras ports—the H.323 call setup and registration ports. By default, a Content Server Cluster uses the range of 1719 to 1722 so that it can independently register OOR (out of resources) for live calls (recordings that are transcoded live) and non-live calls (recordings that are transcoded after recording finishes). The ports are editable because you can instruct the cluster to listen on different ports (for example, non-standard ports). Ensure that the ports you enter do not conflict with each other or with ports that are used by other services on the TCS. Conflicts with other ports will prevent users from making recordings.

Step 5 Click **Save**. Wait until Registration Status displays that registration is successful.

If you are experiencing problems registering to the gatekeeper, verify that you do not have duplicate gateway prefixes or system H.323 ID or E.164 alias. Duplications might cause the gatekeeper to reject registration.

If you want to change system H.323 ID and E.164 alias for a Content Server, do the following:

Step 1 From the **Management** tab, go to **Diagnostics > Cluster overview**.

- Step 2** Locate the Content Server whose H.323 ID or E.164 alias you want to change. Click the **Server overview** link for that Content Server.
 - Step 3** Update the H.323 ID or the E.164 alias, and click **Save**.
 - Step 4** Repeat this procedure for any other Content Server whose H.323 ID or E.164 alias you want to change.
-

Live and Non-Live Prefixes for the Cluster

A Content Server Cluster needs two gateway registrations with separate prefixes: a live gateway prefix for live transcoded calls and a non-live gateway prefix for offline transcoded calls. Having two gateway registrations with separate prefixes ensures good load balancing of both types of calls across the cluster by the gatekeeper. In Premium Resolution clusters, you also have the option of entering playback gateway prefixes to enable playing recordings back from endpoints.

To register the cluster with the VCS, each Content Server also needs four system IDs/aliases: live and non-live H.323 IDs and live and non-live E.164 system aliases. It is important that each is unique on that Content Server and on the Content Server Cluster.

See the [“Inbound H.323 Call Routing” section on page 10-3](#) for more information.

Configure Domain Authentication

The recommended authentication mode for the Content Server Cluster is domain authentication. Domain authentication ensures that Active Directory users can log in to the cluster's network load balanced frontend address.

To use domain authentication, click the **Management** tab and go **Configure > Site settings**. In the Authentication section, click the **Domain** radio button. Add details for your domain LDAP servers. Refer to the TCS Online Help for more information on how to configure domain authentication.

The use of local authentication is not recommended in a Content Server Cluster because local users would have to be added to every Content Server to view pages that served from the network load balanced interface.

Configure Network Load Balancing (NLB)

To ensure that web page requests are spread across all Content Servers in a cluster rather than going to one specific Content Server interface, Cisco recommends that you set up a NLB solution. With an NLB solution, users access the cluster with the Virtual IP address (VIP) that you set up for the cluster on the load balancer. Users would not access the cluster with individual Content Server IP addresses.

The VIP address of the cluster is also referred to as the network load balanced frontend address of the cluster.

The load balancer as configured in this chapter works in direct routing mode. With direct routing, the load balancer changes the MAC address of a packet to the MAC address of the server that it sends the packet on to. In order for the Content Server to respond to this routing request it must assume the position of the VIP specified in the request and yet not advertise this address to the rest of the network. The Content Server cannot advertise this address because all Content Servers in the cluster assume the same VIP position. To ensure that this process works, you must install a loopback adapter and set its IP to the VIP.

In order to set up network load balancing for a Content Server Cluster, follow these steps:

-
- Step 1** [Configure a Load Balancer, page 10-19.](#)
 - Step 2** [Set up a Loopback Adapter on Each TCS in Cluster, page 10-20.](#)
 - Step 3** [Enter the Virtual IP Address of the Cluster \(VIP\) as the Frontend Address on the TCS, page 10-20.](#)
-

Configure a Load Balancer

The following procedure is based on Loadbalancer.org Enterprise version and should be applicable to any Loadbalancer.org product.

The steps below outline the process for configuring a load balanced cluster of three Content Servers. The IP addresses in the steps are examples.

-
- Step 1** Go to the web interface for the load balancing device.
 - Step 2** Set up a virtual server.

The virtual server represents the entire cluster. The virtual server IP address (VIP) will be accessed by Content Server users. When set up successfully, the load balancer receives a request on the VIP and forwards the request to one of the Content Servers in the cluster.

The VIP in this example setup is 10.10.2.111. In the example, we set up four virtual servers for the cluster, one for each port needed for a TCS to operate. The four ports are 80 (HTTP), 443 (HTTPS), 8080 (Windows Media HTTP streaming) and 554 (RTSP). If you want to load balance MMS streams, you also need a virtual server for port 1755.


 - a. To set up the virtual server, go to **Edit Configuration > Virtual Servers**. Click **Add a new Virtual Server**. For the label, give the server an appropriate name (you might want to include the protocol name here). Then enter the VIP that you want to use, followed by the port for this virtual server.

In this example, 10.10.2.111:80 is for the HTTP virtual server, with the persistent option set to **Yes**.
 - b. Create one of these virtual servers for each of the ports that you want to load balance. Use different labels each time but the same VIP.
 - Step 3** Configure the Virtual Server.
 - a. Click **Modify** for each server.
 - b. Change the **Check Type** to **connect**. Ensure that **Service to check** is set to none.
 - c. The **Check Port** should be set to 80 for HTTP, 8080 for Windows Media HTTP streaming, 554 for RTSP, 443 for HTTPS, and 1755 for MMS.
 - d. Leave the other options at their default values.
 - Step 4** Add each of the Content Servers in the cluster into each of the virtual servers you just set up.
 - a. Go to **Edit Configuration > Real Servers**.
 - b. For the first virtual server in the list, click **Add a new Real Server**. Enter a label for this TCS, as well as the server IP address, followed by the same port as the one that is used for the virtual server (for example, 80 for the HTTP virtual server).

- c. Ensure the weight is 1. A weight of 0 disables the server so that it receives no traffic. Also ensure that the forwarding method is set to DR.
- d. Repeating this procedure, add each additional server in the cluster to each of the virtual servers.

Set up a Loopback Adapter on Each TCS in Cluster

The TCS wizard is used to set up a loopback adapter for network load balancing. This operation must be repeated on each TCS in the cluster.

-
- Step 1** Log in to the Content Server using Windows Remote Desktop Connection. Run the TCS wizard. The wizard scans your system. If the Content Server is in a cluster, only the Cluster Management Wizard option is available.
- Step 2** Click **Configure Load Balancer Configuration**.
- Step 3** In the Frontend address field, enter the virtual IP (VIP) address of the cluster that you set up on the load balancer. In the Subnet mask field, enter the subnet mask of your network.
-  **Note** Ensure that you enter the correct VIP address. An incorrect VIP address results in unexpected behavior when users attempt to access the cluster interface.
-
- Step 4** Click **Next**.
- Step 5** Click **Configure** for the wizard to install the loopback adapter.
- Step 6** Click **Finish**.
- Step 7** Repeat this procedure for all the other Content Servers in the cluster.
-

See the “[Update Load Balancer Configuration](#)” section on page 10-25 for details about updating the load balancer configuration.

Enter the Virtual IP Address of the Cluster (VIP) as the Frontend Address on the TCS

The virtual IP address or DNS name of the cluster as set up on the load balancer must be entered in the Frontend address field in Site settings. To enter the VIP address or DNS name, click the **Management** tab. Then go to **Configure > Site settings**. Entering the frontend address ensures that all recording links that are generated by a Content Server and on TMS use the frontend address.

Managing a Content Server Cluster

This section describes cluster management functionalities that are different from the functionalities of a standalone TCS. This section supplements the Content Server online help.

- [Access Cluster Administrative Pages, page 10-21](#)
- [View Cluster Status, page 10-21](#)
- [Edit Information for Each Content Server in Cluster, page 10-22](#)

- [Edit Information Common to All Content Servers in Cluster, page 10-23](#)
- [Generate a Cluster Settings File, page 10-24](#)
- [Update Load Balancer Configuration, page 10-25](#)
- [Update Cluster Settings, page 10-25](#)

Access Cluster Administrative Pages

You can access the web interface of a Content Server Cluster by logging in to the IP address or DNS name of a specific Content Server in the cluster. If you set up load balancing, you log in with the network load balanced frontend address of the cluster. The items available in the Management tab vary depending on the address you log in to.

If you log in with the IP address or DNS name of a specific Content Server in the cluster, the Management tab includes these four menus and their sub-menus:

- Diagnostics—Cluster overview, Server overview, Server logs, Transcoding queue
- Recordings—Edit recordings, Import recordings, Create recording
- Recording Setup—Recording aliases, Categories, Templates, Media server configurations, Call configurations
- Configuration—Site settings, Groups and users, Window server

If you log in to the cluster with the network load balanced frontend address (the VIP address), the Management tab includes these four menus and their sub-menus:

- Diagnostics—Cluster overview, Transcoding queue
- Recordings—Edit recordings, Import recordings, Create recording
- Recording Setup—Recording aliases, Categories, Templates, Media server configurations, Call configurations
- Configuration—Site settings, Groups and users

When accessing the cluster through the network load balanced frontend address, you do not see Server logs, Server overview, and Windows server because these sub-menus are specific to each Content Server. To see these sub-menus for a specific Content Server, access that specific server from Cluster overview page.

View Cluster Status

Management: Diagnostics > Cluster overview

The Cluster overview page does the following:

- Lists the system names and IP addresses of all Content Servers in the cluster.
- Displays a link to the Server overview page for each Content Server.
- Reports the total number of current calls for the cluster and for each Content Server.
- Reports the total number of offline transcodes for the cluster and for each Content Server.
- Reports the server mode for each Content Server.

- Reports the status for each Content Server. If the Content Server mode is online, then the status displays a green check, which means that the Content Server is running correctly. If the server mode is not online, then the status displays a red exclamation mark. Go to the Server overview page for the specific Content Server to see more details. From the Server overview page, you can check which of the services is not running.
- Displays links to each Content Server's logs and Windows Server administration interface.
- Allows you to End all Calls on the whole cluster. You can end recording calls on a specific Content Server from the Server overview page for that Content Server.
- Allows you to put a Content Server in maintenance mode. When the Content Server is in maintenance mode, that server cannot accept new recording calls. Current calls and transcoding jobs continue until finished. The other Content Servers in the cluster continue working as usual.

Maintenance mode should be used to ensure that no new calls are made to a Content Server—for example, when you want to defragment the server drive, run a Windows security update installer, or update antivirus software on that Content Server. You should also put a Content Server in maintenance mode (after ending current recording calls on that server) if you need to shut it down and move it to another location.

To enter maintenance mode, click the **Enter maintenance mode** button. The button label changes to **Rejoin cluster**, and server mode shows that the server is in maintenance. After you finish maintenance on the server, click the **Rejoin cluster** button. The button label changes to **Enter maintenance mode** and Server mode is online. The Content Server is now ready to receive calls.

Server overview with log in to a specific Content Server—Management: Diagnostics > Server overview

Server overview with log in to the network load balanced frontend address— Management: Cluster overview > Server overview link

The Server overview page provides some additional information relevant to the cluster, such as:

- Total disk space and free disk space on the cluster media storage location (in addition to the disk space information for the C and E drives of this Content Server).



Caution

If remaining disk space on the NAS is below the critical 10% level, it will be displayed in red as a warning to the administrator. The administrator should free up space on the NAS. When free disk space on that share falls below 5%, the cluster stops receiving recording calls and processing offline transcoded jobs.

- Database data source—displays the address of the external database server, port, and instance name.
- Database name—displays the database (catalog) prefix that you entered when you created the cluster and a suffix added by the TCS wizard ('3').
- Cluster media storage location—displays the external NAS share name.

Edit Information for Each Content Server in Cluster

Go to the Server overview page to edit information specific to each Content Server in a cluster.

From the Server overview page, you can edit the following:

- System name
- Non-live and live H.323 IDs and non-live and live E.164 system aliases

Non-Live and Live system IDs/aliases are required for registering to the gatekeeper.



Note You should not use those system IDs/aliases for dialing the cluster because they will always (and only) be routed to a specific Content Server. Only calls made to recording aliases or playback addresses are balanced across the cluster by the gatekeeper.

Any changes made to the system name and to non-Live and live system IDs/aliases fields are applied to a Content Server that is not currently in a recording call. Changes cannot be applied to a Content Server in a call. Saving changes on this page automatically puts this server in Configuration reload mode.



Note In Configuration reload mode, incoming calls are not accepted and outgoing calls cannot be made from that Content Server.

When all current calls are finished, the new settings are applied, and the Content Server mode changes back to online.

The administrator might also choose to override Configuration reload mode and apply changes immediately by ending recording calls manually on the Content Server. Clicking on **End all calls** from the Server overview page stops all calls on the Content Server. When calls have ended, the new settings are applied to the Content Server. When the Content Server comes back online, it is ready to accept new calls.

Edit Information Common to All Content Servers in Cluster

Any changes made in these areas are applied to all Content Servers in the cluster through the shared database:

- Cluster overview
- Import recordings
- Recording aliases
- Categories
- Templates
- Media server configurations
- Call configurations
- Site settings
- Groups and users

This section highlights some exceptions and special considerations when managing the cluster.

Import recordings

When importing files smaller than 2 GB, log in to the IP address of one of the Content Servers. Do not use the network load balanced frontend address.

Click the **Management** tab, then go to **Recordings > Import recordings** to import recording files through the web interface.

When importing files larger than 2 GB in size, place the .tcb file in the Imports folder on a desktop of one of the clustered Content Servers. You then need to log in to the web interface of this Content Server (using its IP address or DNS name) to import the .tcb file. After it is imported, the recording is available to the whole cluster. However, the import file is only visible on the Import recordings page for the Content Server to which it was uploaded.

Site settings

The Site settings page (from the **Management** tab, **Configuration > Site settings**) is available for editing even if Content Servers are in recording calls.

Most settings from the Site settings page can be changed and applied while Content Servers are in recording calls. Settings that cannot be changed and applied when recording calls are in progress are the following:

- Cluster name
- Gatekeeper settings
- Advanced H.323 settings
- E-mail settings
- Default recording alias

Any changes that are made in those areas are applied only to Content Servers that are not currently in recording calls. Changes cannot be applied to Content Servers that are in calls, so saving Site settings automatically puts those servers in Configuration reload mode.



Note In Configuration reload mode, incoming calls are not accepted and outgoing calls cannot be made from that Content Server.

After all current calls are complete, the new settings are applied and the Content Server mode changes back to online.

The administrator might also choose to override Configuration reload mode and apply changes immediately by ending calls manually on all Content Servers. Clicking **End all calls** from the Cluster overview page stops all calls in the cluster. When recording calls end, new settings are applied to the Content Servers and all Content Servers are in online mode again, ready to accept new calls.

API

The clustering functionality requires that API be enabled. It is not possible to disable the API when Content Servers are clustered. It is important to ensure that the API password is changed from the default at the time of setup.

Generate a Cluster Settings File

You need a cluster settings file to add more Content Servers to an existing cluster (see the [“Add a Content Server to an Existing Cluster” section on page 10-16](#)). Cluster settings are in an XML file that contains details of the external database and the TCS_NAS_USER. If cluster settings change from the original cluster setup, you must generate a new cluster settings file to use when you want to add more Content Servers to the cluster.

To generate a cluster settings file, do the following:

Step 1 Log in to a Content Server using Windows Remote Desktop Connection. Run the TCS wizard.

The wizard scans your system. If the Content Server is in a cluster, only the Cluster Management Wizard option is available.

- Step 2** Click the **Generate Cluster Settings File** radio button.
- Step 3** Click **Browse** if you want to save the cluster settings file in a location other than on the TCS desktop. Click **Next**.
- Step 4** Click **Finish** to exit the wizard.
-

Update Load Balancer Configuration

If you have changed the virtual IP (VIP) address of the cluster on the load balancer, you need to update it on each Content Server using the TCS wizard.

-
- Step 1** Log in to the Content Server using Windows Remote Desktop Connection. Run the TCS wizard. The wizard scans your system. If the Content Server is in a cluster, only the Cluster Management Wizard option is available.
- Step 2** Click the **Configure Load Balancer Configuration**.
- Step 3** Click **Update Load Balancer Configuration**.
- Step 4** Enter the new virtual IP (VIP) address of the cluster that you set up on the load balancer and/or the subnet mask of your network.
- Step 5** Click **Next**.
- Step 6** Click **Configure** for the wizard to update the loopback adapter. This process might take some time.
- Step 7** Click **Finish**.
- Step 8** Repeat this procedure for each Content Server in the cluster.
- Step 9** In Site settings page, update the frontend address in Site Settings to the new VIP. See [“Enter the Virtual IP Address of the Cluster \(VIP\) as the Frontend Address on the TCS”](#) section on page 10-20 for details.
-



Note

The loopback adapter is automatically removed when you remove the Content Server from a cluster. You can also remove it using the TCS wizard. Run the wizard as described above and click the **Remove Load Balancer Configuration** option. Applying this option only uninstalls the loopback adapter on the specific Content Server. You will need to manually remove the Content Server from your load balancer configuration.

Update Cluster Settings

You can update alternate media location (NAS) settings for the cluster using the TCS wizard.

The TCS wizard allows you to:

- [Update the Password for MYDOMAIN\TCS_NAS_USER Account, page 10-26](#)
- [Change the MYDOMAIN\TCS_NAS_USER Account to Another Domain Account, page 10-26](#)

- [Change the Location of the Media Files to a Different NAS Share, page 10-27](#)

**Note**

As an alternative to the procedures described below, you could also remove all Content Servers from the cluster (see [“Removing a Content Server from the Cluster” section on page 10-28](#) for details) and use the TCS NAS wizard on the last Content Server that you removed from the cluster to update the password, change the account, or change the media location. Then create a new cluster and add the Content Servers to the cluster again.

Update the Password for MYDOMAIN\TCS_NAS_USER Account

If the password for the account that cluster uses to connect to the NAS—MYDOMAIN\TCS_NAS_USER—expires, the cluster cannot connect to the NAS, and media files cannot be moved to their media location. Users will not be able to view recordings.

The domain administrator needs to set a new password for the account on the domain, and then you must run the TCS wizard on each Content Server in the cluster to update the password:

-
- Step 1** Log in to the Content Server using Windows Remote Desktop Connection as a domain administrator. Run the TCS wizard.
- The wizard scans your system. If the Content Server is in a cluster, only the Cluster Management Wizard option is available.
- Step 2** Click the **Update Cluster Settings** radio buttons.
- Step 3** The wizard displays the username and password for the account that the cluster uses to connect to the NAS. Change the password, and click **Next**.
- Step 4** The wizard displays the current media location. Click **Next**.
- Step 5** The Cluster: Test Result screen displays information about your intended setup. If all tests are successful, click **Configure** to update the cluster settings.
- You can also click **Finish** to exit the wizard without updating the cluster settings.
- Step 6** If you click **Configure**, the wizard configures your system and updates settings. This process might take some time.
- Step 7** Click **Finish** to exit the wizard.
- Step 8** Repeat the procedure on the other Content Servers in the cluster.
-

Change the MYDOMAIN\TCS_NAS_USER Account to Another Domain Account

If the account that the cluster uses to connect to the NAS—MYDOMAIN\TCS_NAS_USER—needs to change, get the details of the new domain account from your domain administrator. Then do the following:

-
- Step 1** Add the new account (in this procedure, we refer to the new account as MYDOMAIN\TCS_NEW_NAS_USER) to the permissions on the NAS share. Give the account full control (see [“Set Permissions and Security Settings on the Share” section on page 10-11](#) for details).
- Step 2** Log in as a domain administrator to one of the Content Servers in the cluster using Windows Remote Desktop Connection.

- Step 3** Go to **Computer Management > System Tools > Local Users and Groups > Groups > Administrators**. Add MYDOMAIN\TCS_NEW_NAS_USER to the Administrators group.
- Step 4** Start the TCS Wizard.
- The wizard scans your system. If the Content Server is in a cluster, only the Cluster Management Wizard option is available.
- Step 5** Click the **Update Cluster Settings** radio button.
- Step 6** The wizard displays the username and password of the account that the cluster uses to connect to the NAS. Change the username and password to the new account, MYDOMAIN\TCS_NEW_NAS_USER. Click **Next**.
- Step 7** The wizard displays the current media location. Click **Next**.
- Step 8** The Cluster: Test Result screen displays information about your intended setup. If all tests are successful, click **Configure** to update the cluster settings.
- You can also click **Finish** to exit the wizard without updating the cluster settings.
- Step 9** If you click **Configure**, the wizard configures your system and updates settings. This process might take some time.
- Step 10** Click **Finish** to exit the wizard.
- Step 11** Repeat this procedure on the other Content Servers in the cluster.

Change the Location of the Media Files to a Different NAS Share

If you need to change the default media location for the cluster to a different NAS share, do the following steps:

- Step 1** Set up a new NAS share (see the [“Configure the NAS” section on page 10-10](#) for details). The permissions on this share must allow all Content Servers in the cluster and the MYDOMAIN\TCS_NAS_USER full control of the share. You can continue to use the same MYDOMAIN\TCS_NAS_USER, or create and use a different domain account.
- Step 2** Manually copy the data folder from the old NAS share to the new NAS share.



Note You cannot copy files that are in use—in other words, files that are being watched or downloaded by users. Cisco recommends that the cluster not be active during the copy process. Follow your usual file server migration procedures when copying the files. Putting the Content Servers in maintenance mode alone is not sufficient to guarantee a safe copy of media because maintenance mode still allows users to watch and download recordings.

- Step 3** After the copy process is complete, verify that the number of files and size of the data folder is identical on the new NAS share as on the old NAS share.
- Step 4** Log in to a Content Server in the cluster using Windows Remote Desktop Connection. Start the TCS wizard.
- The wizard scans your system. If the Content Server is in a cluster, only the Cluster Management Wizard option is available.
- Step 5** Click the **Update Cluster Settings** radio button.

- Step 6** The wizard displays the username and password of the account that the cluster uses to connect to the NAS. Change the username and password to a new account if required. Click **Next**.
 - Step 7** The wizard displays the current media location. Enter the location of the new NAS share in the format \\servername\share.
 - Step 8** The Cluster: Test Result screen displays information about your intended setup. If all tests are successful, click **Configure** to update the cluster settings.
At this stage you can also click **Finish** to exit the wizard without updating the cluster settings.
 - Step 9** If you click **Configure**, the wizard configures your system and updates settings. This process might take some time.
 - Step 10** Click **Finish** to exit the wizard.
 - Step 11** Repeat this procedure on the other Content Servers in the cluster to set the new media location details in IIS.
-

Removing a Content Server from the Cluster

You can remove one or more Content Servers from the cluster at any time and use them as standalone Content Servers. Run the TCS wizard if you want to remove a Content Server from a cluster.



Note

If you are removing Content Servers from a cluster, the order in which you remove them is important.

None of the media or configurations from the cluster are available on Content Servers after you remove them from the cluster. These removed Content Servers become standalone installations with no content or configurations, with the exception of the last Content Server you remove from the cluster. When you run the TCS wizard on the last Content Server remaining in a cluster and click **Remove from cluster**, the last Content Server become a standalone server with media on a NAS. This last Content Server retains all content recorded by the cluster and all cluster configurations. The external database instance is dropped, and all data are copied to the local database, while all media files remain on a NAS.

On this standalone Content Server, you can use the Alternate Storage (NAS) wizard option to move the media files to another NAS location or to move them back to the local drive on the Content Server (if the size of the recorded media allows it).

To remove a Content Server from the cluster:

- Step 1** Log in to the Content Server using Windows Remote Desktop Connection. Run the TCS wizard.
The wizard scans your system. If the Content Server is in a cluster, only the Cluster Management Wizard option is available.
- Step 2** Click the **Remove from Cluster** radio button.
- Step 3** In the Content Server Checks screen, confirm that the Content Server is backed up and that antivirus software is stopped (if it is installed). If the Content Server is backed up and antivirus software is not stopped, cancel the wizard and complete those actions. Then run the wizard again.
- Step 4** The Cluster: Test Result screen displays information about your intended setup. If all tests are successful, click **Configure** to remove the Content Server from the cluster.
You can also click **Finish** to exit the wizard without removing the Content Server from the cluster. If the external database set up test failed, you cannot remove this Content Server from the cluster.

If you click **Configure**, the wizard configures your system and removes the Content Server from the cluster. This process might take some time.

Step 5 Click **Finish** to exit the wizard. The log location for the wizard is displayed on this screen.

The Content Server can be added back to the same or a different cluster at any time.

**Caution**

Removing a Content Server from a cluster deletes the network load balanced loopback adapter from this Content Server, but this Content Server is not removed from the load balancer setup. You must remove this Content Server from your load balancer configuration manually. If you do not remove the Content Server from the load balancing configuration, the load balancer continues to try to direct traffic to a Content Server that no longer belongs to the cluster.

**Caution**

If the frontend address in a cluster was pointing to a load balanced address, you must delete the load balanced address manually from the Site settings page of the last Content Server that you removed from the cluster. Otherwise, you cannot save the site settings.

Using TMS to Schedule Calls on a Content Server Cluster

TMS 12.2 or higher can be used to schedule recording calls on a version 3.3 or higher cluster. Cisco recommends that clusters use either TMS to schedule calls or ad hoc dialing. A mixture of scheduled and ad hoc dialing is not recommended.

To use TMS to schedule recording calls on a cluster, do the following:

Step 1 Ensure that the cluster name in the Site settings page is a meaningful name. The TMS displays the name in the Recording drop-down menu on the Conference Booking page.

**Note**

When registering a cluster in TMS, ensure that the cluster name in the Site settings page is not blank. If you do not include a cluster name, cluster resource allocation in TMS might not be correct.

Step 2 Ensure that the frontend address in the Site settings page is entered and that it is the correct network load balanced address. This address is used to generate conference links in TMS.

Step 3 Add one or more Content Servers in the cluster to TMS. You only need to add one Content Server in the cluster to make calls to the whole cluster.

Step 4 Check that users can select at least one live and one non-live recording alias in the Recording drop-down menu on the TMS New Conference Booking page. Each recording alias type (live and non-live) can be used to schedule a number of calls to the maximum cluster capacity for this call type.

Upgrading the Cluster to a New Software Version

Before upgrading a Content Server Cluster to a new software version, do the following:

- Ensure that the Content Server Cluster is backed up (see the [“Backing Up and Restoring the Content Server Cluster” section on page 10-31](#)). If the upgrade installer fails, you can restore from the backup in order to downgrade to the previous version.
- Stop any antivirus software, if running.
- The cluster is not operational for the duration of the upgrade of the first Content Server in the cluster. The cluster operates at a reduced capacity until all the Content Servers are upgraded. Cisco recommends that you take a system outage into account when scheduling the upgrade.
- Ensure that you have release keys available if you are upgrading to a major version. Release keys need to be entered at the time that the installer is run.

To upgrade the Content Server Cluster, log in to each of the Content Servers using Windows Remote Desktop Connection and run the software upgrade installer on one TCS at a time.



Caution

Running upgrade installers simultaneously on two or more clustered Content Servers cause SQL server errors and might damage your cluster installation.

You do not need to put clustered Content Servers into maintenance mode before starting the upgrade. The installer ensures that they are not available for accepting recording calls during the upgrade. After the installation process is complete on the first Content Server, it automatically becomes available for making and accepting calls to its capacity.

During the upgrade, the web interface of the Content Servers that are not yet upgraded display this message: “Server under maintenance. This Content Server is being upgraded and is currently unavailable. For more information, please contact your local Administrator.” The Cluster overview page display their mode as “Upgrading” and their status as “Not OK.” Each server becomes available to the cluster after the installation is completed on each.

Upgrading the External Microsoft SQL Server from SQL Server 2005 to SQL Server 2008

Content Server cluster version 3.3 supported only one external Microsoft SQL server version: MSSQL Server 2005. Content Server cluster version 4.0 or later now supports MSSQL Server 2005 or MSSQL Server 2008. When you upgrade your Content Server Cluster from 3.3 to 4.0 or later, you have a choice to upgrade the external SQL server.

To upgrade the external Microsoft SQL server from MSSQL Server 2005 to MSSQL Server 2008, do the following:

- Step 1** Back up the cluster (see the [“Backing Up and Restoring the Content Server Cluster” section on page 10-31](#)).
- Step 2** Upgrade the cluster by running the S4.0 upgrade installer on each TCS in cluster (see [“Upgrading the Cluster to a New Software Version” section on page 10-30](#)).
- Step 3** Cisco recommends that you shut down all the Content Servers in a cluster to stop them from communicating with the database while your external SQL server is upgraded.

Shutting down the Content Servers prevents them from trying to access the database while your external SQL server is being upgraded. Putting the Content Servers in maintenance mode alone does not ensure that they stop communicating with the database.

- Step 4** Upgrade the instance the cluster uses on the external Microsoft SQL server from MSSQL Server 2005 to MSSQL Server 2008.
 - Step 5** Power on the Content Servers.
 - Step 6** Verify that the upgrade was successful by logging in to the web interface of the cluster. Click on the **Management** tab, and go to **Diagnostics > Cluster overview** to check that the server mode for all Content Servers is online and that the status is Ok (a green check). Cisco also recommends making a test call to the cluster.
-

Backing Up and Restoring the Content Server Cluster

Cisco recommends that you back up the cluster regularly and also before you upgrade it or install a security update.

It is very important to follow the procedure described here. If you do not follow this procedure, future upgrades might not work or you might lose your data.

There are three parts to backing up and restoring a Content Server Cluster from backup:

- [The Clustered Content Servers, page 10-31](#)
- [The external MS SQL database, page 10-31](#)
- [The Media on the NAS/External Streaming Server, page 10-31](#)

The Clustered Content Servers

To back up and restore the Content Servers in a cluster, follow the backup and restoring procedures as described in [Chapter 7, “Maintaining the Content Server.”](#)

The external MS SQL database

To back up and restore the external SQL server database, follow the administrative guidelines for your SQL server.

Ensure that you back up the database at the same time as the Content Server and the NAS. If you restore from backup, you must restore the database backup that was done at the same time as your Content Server and NAS backups; otherwise, you might not be able to view some recordings.

The Media on the NAS/External Streaming Server

To back up cluster media, follow the administrative guidelines for backing up your file servers. To ensure all media are backed up, back up all files in the share on the Network Attached Storage device (NAS) that is used by the cluster and also any media on external streaming servers.

To restore the media, copy the relevant backup back to the share on the NAS (and the correct location on the external streaming server).

Ensure that you back up your NAS or an external media server at the same time as the Content Server and the SQL server database. If you restore from backup, you must restore the NAS and external streaming server backup that was done at the same time as your Content Server and SQL server database backup; otherwise, you might not be able to view some recordings.