



CHAPTER 13

Servicing ACNS Devices and Origin Servers

This chapter explains how you can minimize the impact upon content delivery services when you perform maintenance on your ACNS network devices, such as replacing failed hardware or adding or relocating origin servers, root Content Engines, Content Routers, or Content Distribution Managers.

This chapter contains the following sections:

- [Preventing Catastrophic Content Losses, page 13-1](#)
- [Relocating or Replacing the Origin Server, page 13-4](#)
- [Relocating or Replacing the Root Content Engine, page 13-6](#)
- [Relocating or Replacing the Content Distribution Manager, page 13-7](#)
- [Best Practices for Managing and Servicing Devices, page 13-8](#)
- [Troubleshooting, page 13-10](#)

Preventing Catastrophic Content Losses

Content Engines use an indexing mechanism to identify and track content that is to be acquired and distributed. Whenever content is modified, moved, deleted, added or in some other way changed in the origin server, indexing is affected. Any change that affects the indexing of content can cause the content to be reacquired and redistributed.

When new content is acquired and distributed, existing content is removed from all the Content Engines in the channel. When you make certain critical changes in your network, you can be at risk for catastrophic loss of content. The purpose of this section is to help you identify situations that could lead to loss of content, what you can do to mitigate the risk, and how you can prevent content losses.

Before Making Changes

Before you make any changes to the manifest file or to the location or IP address of a device in your network, read the following important information carefully.



Caution

Anything that changes the starting URL in the manifest file could trigger content to be reacquired and redistributed, causing the deletion of all previously distributed content for a crawl task. When changes are made to the starting URL, either by modifying the manifest file or by relocating an origin server or changing an IP address, the acquirer views the URL as a new starting URL. When the acquirer detects a new starting URL, it deletes the older content and starts a fresh crawl task.

The following types of changes can cause you to lose pre-positioned content:

- Moving the manifest file and changing the manifest URL in the Content Distribution Manager
- Upgrading application software used to dynamically generate and publish manifest files
- Changing anything in the crawl task entry at the end of the file
- Adding or removing a leading forward slash (/) from the starting URL
- Removing an item entry from the manifest file when the item is not fetched by the crawl task
- Changing an IP address that is part of a starting URL for a crawl task
- Changing the hostname of the origin server
- Relocating the origin server
- Changing the user ID or password when authentication is required
- Changing a match rule
- Changing the port number in the starting URL for a crawl task

The following changes do not cause content loss:

- Changing the content provider
- Changing the website origin server
- Changing the website FQDN

Upgrading Software Used to Publish Externally Hosted Manifest Files

If you are using an application that dynamically generates and publishes manifest files, you must take precautions before you upgrade this application software in your ACNS network. During the software upgrade of the manifest publishing software, the manifest file could become invalid, causing the distributed content to be inadvertently deleted.

To avoid losing content in this situation, we recommend that before you upgrade the manifest publishing software, you disable acquisition and distribution processes on the root Content Engine and on any potential temporary root Content Engines in the root location. Any Content Engine that is in the same channel and same location as the root Content Engine is a potential temporary root. After the application software upgrade is complete, you can restart the acquisition and distribution process on each Content Engine.

- To disable the acquisition and distribution process, use the **acquisition-distribution stop** EXEC command.
- To restart the acquisition and distribution process, use the **acquisition-distribution start** EXEC command.

Changing an IP Address—Effects on Acquisition and Distribution Services

When you change the IP address of a Content Engine, you must stop the acquisition and distribution services before you make the change. If you do not stop the acquisition and distribution services before you change the IP address, the multicast receiver will be listening for the previous IP address and will not recognize the new one.

When you change the IP address of a Content Engine that is being used for acquisition and distribution, you must follow these steps:

-
- Step 1** Stop the acquisition and distribution services by using the **acquisition-distribution stop** EXEC command.
- ```
CE# acquisition-distribution stop
```
- Step 2** Change the IP address of the interfaces.
- Step 3** Restart the acquisition and distribution services by using the **acquisition-distribution start** EXEC command.
- ```
CE# acquisition-distribution start
```
-

Changing an IP Address—Effects on Caching Services

If you change the IP address of a Content Engine that is being used for content caching, the effects on the various applications are as follows:

- Rules—No issues are seen.
- WCCP—When the IP address is changed a WCCP error message appears. After you configure the new IP address, the cache farm is formed and no issues are seen.
- Authentication—No issues are seen (tested with LDAP only).
- SmartFilter—When an IP address is removed, the SmartFilter application is disabled. You must reassign the IP address and re-enable SmartFilter URL filtering.
- Websense—When an IP address is changed, Websense stops and the restarts. No issues are seen.
- Translog—Transactions continue to be logged after an IP address is changed.

Changing an IP Address—Effects on Streaming Services

If you change the IP address of a Content Engine that is being used for streaming content, the effect on the various applications are as follows:

- Broadcast alias—If a broadcast alias is configured on the Content Engine and you change the Content Engine's IP address, you must also change the broadcast alias URL because the Content Engine IP address is used in the broadcast alias URL, as shown in the following example:
http://<CEIP>/Broadcast-alias.
- Direct proxy live request to Windows Media Server—When you change the IP address of the Windows Media Server, you must change the publishing URL, as shown in the following example:
http://<WMSIP>/filename.
- Outgoing proxy—When you change the IP address in the network, you must reconfigure the outgoing proxy.
- Managed live—When you change the root Content Engine IP address, you must change the origin server setting for the channel and restart the program.
- Managed live multicast—If your root Content Engine fails, changes, or is replaced, you must change the multicast publishing URL to use the IP address of the new root Content Engine.

When the root Content Engine changes, the location leader in the root location or in the next location in the forwarding path will get the stream directly from the source and send the stream to its down-level location leader; however, the multicast and unicast publishing URLs remain unchanged and still contain the original root Content Engine IP address. When a unicast request is issued to a down-level Content Engine using the unicast publishing URL, the stream is delivered. But when a multicast request is issued to a down-level Content Engine using a multicast publishing URL, the stream fails because the Content Engine cannot find the missing root Content Engine to obtain the .nsc file that it needs.

Use one of the following workarounds to correct this problem:

- Use the IP address of the down-level location leader in the multicast URL instead of the root Content Engine IP address.
- Use Content Router redirection for the request, so that the client can be redirected to fetch the .nsc file from other Content Engines that are associated with that program based on the coverage zone file.
- Location leader election—Changing a Content Engine IP address can affect the location leader election because the Content Engine with the lowest value IP address is always elected as leader. Live splitting is not directly affected by this type of change.

Relocating or Replacing the Origin Server

When an origin server that is being used for pre-positioned content in the ACNS network fails, and you then replace it, in the worst case, all content from the failed origin server is removed from all receiver Content Engines. If this occurs, all content that is acquired from the new origin server is considered to be new content and must be replicated again to all receiver Content Engines. If you have a large number of items, replication can take a long time, which means a delay will occur for the content being served.

You can take steps to minimize the disruption of pre-positioned content services, assuming that you can restore all content from backup storage to the new origin server and that the content has not changed. These steps apply to all ACNS-supported content acquisition protocols.

When you replace an origin server, you can either assign the same host name and IP address to the new hardware, or you can assign a new hostname and IP address to the new hardware. The following sections explain what steps to take and which steps work the best in each case.

Using the Same Hostname and IP Address for the Origin Server

To replace an origin server and use the same hostname and IP address, follow these steps:

Step 1 Power off the old origin server hardware.

When the old origin server is powered off, if the manifest file specifies an item or crawl task recheck using the *ttl* attribute, the acquirer module in the root Content Engine rechecks the specified content at the old origin server. Because the old origin server is not operating, the root Content Engine will report errors, but it will not delete the old, previously acquired content. The powering off of the origin server will be transparent to the receiver Content Engines.

Step 2 Power on the new origin server using the same hostname and IP address as the old one. Use the same channels and the same manifest file for content pre-positioning.

When the new origin server is powered on, the root Content Engine acquirer, triggered by either the *failRetryInterval* attribute or by *ttl* attribute in the manifest file, checks the content at the new origin server. The root Content Engine will detect that the timestamp has changed, and it will refetch the content from the new origin server. Because the relative URL and the MD5 checksum have not changed, only the content metadata will be redistributed. The content files will not need to be replicated.

**Note**

The *ttl* attribute is optional and designates a time interval, in minutes, for revalidation of the content. If a time value is omitted, the content is fetched only once and its freshness is never checked again.

- Step 3** If the manifest file does not specify the *ttl* attribute for rechecking items or crawl tasks, you can trigger the root Content Engine to recheck the content from the new origin server by clicking the **Fetch Manifest Now** button in the Content Distribution Manager GUI Channel Content window (**Services > Web > Channels > Channel Content**).

When you click the **Fetch Manifest Now** button, the ACNS software checks to see if the manifest file has been updated, and the updated manifest file is downloaded and reparsed. Also, regardless of whether the manifest file has been updated, all content in the channel is rechecked and the updated content is downloaded.

Alternatively, use the **acquirer start-channel EXEC** command in the root Content Engine CLI.

The root Content Engine continues to serve content while it is downloading the newer version. After the content has been downloaded to the root Content Engine, the software removes the older content files and replaces them with the new version.

Using a New Hostname and IP Address for the Origin Server

If your manifest file contains single content items only and does not define any crawl tasks, replacing the origin server with a new hostname and IP address is not complicated. To replace an origin server and use a new hostname and IP address, follow these steps:

- Step 1** If your manifest file contains single content items only and does not define any crawl tasks, modify the manifest file by replacing the old hostname and IP address with the new hostname and IP address in all the URLs.
- Step 2** To trigger the root Content Engine to fetch and parse the new manifest file, click the **Fetch Manifest Now** button in the Content Distribution Manager GUI Channel Content window (**Services > Web > Channels > Channel Content**), or use the **acquirer start-channel EXEC** command in the root Content Engine CLI.

After the new manifest file is parsed, the root Content Engine acquires new items from the new origin server. The metadata for these content items is redistributed to the receiver Content Engines. The content files themselves do not need to be replicated.

If your manifest file contains crawl tasks, replacing the origin server and changing the hostname or IP address is a more complicated procedure.

**Caution**

When you change the origin server hostname and IP address, you are changing the starting URL for the crawl task. The root Content Engine regards the new starting URL as a new crawl task, and before it acquires new content from this new URL, it deletes all the content acquired from the old starting URL.

You must use the following workaround to prevent the root Content Engine from deleting all of your pre-positioned content:

-
- Step 1** Locate a spare Content Engine with enough disk space in the pre-positioned file system (cdnfs) to hold the pre-positioned content.
 - Step 2** Register the spare Content Engine to the Content Distribution Manager, and configure the same location as the old root Content Engine.
 - Step 3** Log in to the old root Content Engine, and use the **acquirer stop-channel EXEC** command to disable each affected channel.
 - Step 4** Modify the manifest file to use the new hostname and IP address by replacing the old hostname and IP address with the new hostname and IP address in all the URLs.
 - Step 5** Assign the spare Content Engine to the channels, and elect it as the new root Content Engine for the channels.

The new root Content Engine crawls the new origin server to fetch the new content, but it does not propagate content deletion events to all other Content Engines. The new root Content Engine marks the content as updated because the timestamps have changed. The metadata for the crawl task content is redistributed to the receiver Content Engines. The content files themselves do not need to be replicated.

- Step 6** After the crawl task content has finished replicating to all the receiver Content Engines, you can switch back to your old root Content Engine and remove the spare Content Engine.

For information about registering Content Engines to Content Distribution Managers, configuring locations, assigning and unassigning Content Engines to channels, and electing root Content Engines, see the *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments*.

Relocating or Replacing the Root Content Engine

When taking steps to prevent the loss of acquired content and minimize delays in content delivery, it is useful to understand the following information regarding the root Content Engine and receiver Content Engines:

- When content is acquired, the root Content Engine checks the full URL, the file size, and the file time stamp to determine the file version. If the URL or the file time stamp has changed, the root Content Engine must acquire the content again.
- When content is distributed, the receiver Content Engine checks the relative URL and the MD5 checksum of each file. The MD5 checksum produces a fingerprint of the file that identifies whether or not the content of the file has changed. If the relative URL and the file content have not changed, the ACNS software does not need to redistribute the files; it needs to redistribute the content metadata only.

Sometimes, however, the root Content Engine erroneously propagates a content deletion event to all receiver Content Engines to remove the content even though the relative URL and the file content have not changed. When the content is acquired again, it must then be replicated again to all receiver Content Engines.

- If you replace a root Content Engine with a Content Engine that was not previously assigned to the channel, content is reacquired and old content is deleted.
- To prevent the reacquisition of content when replacing a root Content Engine, make one of the receiver Content Engines in the same channel the replacement root Content Engine. Wait until replication is complete for the receiver Content Engine, and then designate it as the root Content Engine. (For procedural information, see the *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments* publication.)

When you replace a root Content Engine in this manner, the Content Engines in the channel will synchronize with the new root Content Engine through the metadata poll. Content is not redistributed to the other Content Engines in the channel unless the content has changed since the last metadata poll.

Relocating or Replacing the Content Distribution Manager

When you change the IP address of a Content Distribution Manager, all managed devices need to learn of this change so they can poll it for configuration changes.

When you change the IP address of the standby Content Distribution Manager using the CLI or the GUI, the primary Content Distribution Manager sends the new IP address of the standby Content Distribution Manager to all the devices that are registered to it. As long as all of the devices are online, they will learn the new standby Content Distribution Manager IP address within two datafeed polling periods with no further action on your part.

Changing the IP address of the primary Content Distribution Manager is more difficult, since devices learn of configuration changes from the primary Content Distribution Manager. When the IP address of the primary Content Distribution Manager changes, registered devices can no longer poll the primary Content Distribution Manager.

These devices must learn the new IP address in one of the following three ways:

- The **cdm ip** global configuration command allows you to specify an IP address or a hostname. If you specified a hostname rather than an IP address for the primary Content Distribution Manager, managed devices can discover the Content Distribution Manager IP address through DNS. If you leave the Content Distribution Manager hostname unchanged, you can simply change the ip address of the Content Distribution Manager on your DNS server to reflect its new setting. The amount of time it takes for devices to learn of the new IP address depends on the TTL value that you configured in DNS for the Content Distribution Manager's name record.
- If you specified an IP address using the **cdm ip** global configuration command, you can log into each managed device, and enter the **cdm ip** command with the new IP address.
- If you have a standby Content Distribution Manager, you can switch your primary Content Distribution Manager to standby, and vice versa. The new primary (former standby) will send the former primary Content Distribution Manager's new IP address to all managed devices. All online devices will receive the new IP address within 2-4 datafeed polling periods. At that point, you can choose to leave the Content Distribution Managers as they are, or switch roles again.

Best Practices for Managing and Servicing Devices

When you are relocating Content Engines, Content Routers, and Content Distribution Managers to new locations within your ACNS network, you can minimize configuration changes by following these guidelines:

- During initial setup for centrally managed Content Engines and Content Routers, enter the Content Distribution Manager host name instead of the IP address, so that if you need to assign a new IP address to the Content Distribution Manager, you will not need to make configuration changes in each device that is registered to it.

Set the host name of the Content Distribution Manager with which the device is to be associated by using the **cdm ip** global configuration command, as shown in the following example:

```
CE-507# config
CE-507(config)# cdm ip hostname
```

This command associates the device with the Content Distribution Manager so that the device can be approved as a part of the network.

After the device is configured with the Content Distribution Manager host name, it presents a self-signed security certificate as well as other essential information, such as its IP address or host name, disk space allocation, and so forth, to the Content Distribution Manager.

- Content Engines and Content Routers do not need to deregister and reregister with the Content Distribution Manager for a change in IP address when the change is made through the Content Distribution Manager GUI. Newly relocated devices should retain their Content Distribution Manager host name configuration between reboots, and the Content Distribution Manager should recognize the device and update any changed information, including a new IP address. Changing the IP address of a root Content Engine or any other Content Engine should not affect content distribution.
- We recommend that you change the IP address of an interface from the Content Distribution Manager GUI, after the Content Engine has been registered with the Content Distribution Manager. After a Content Engine is registered, any changes that you make to its configuration are communicated to the other devices that are registered with the Content Distribution Manager.
 - **Content Engine**—If you change the IP address of a Content Engine’s primary interface directly using the Content Engine CLI, the Content Distribution Manager does not recognize the change, the Content Engine appears as offline in the Content Distribution Manager GUI, and there is no further communication between the Content Engine and the Content Distribution Manager Central Management System (CMS).



Note The CMS database stores all the device configurations known to the Content Distribution Manager. CMS communications at periodic intervals (datafeed polling periods) synchronize information between the devices. Configuration changes made through the Content Distribution Manager GUI are propagated to all registered Content Engines in the network. Configuration changes to acquisition and distribution elements, such as channels, websites, and manifest files are also propagated to the Content Engines.

An “Offline” device status shown in the Content Distribution Manager GUI means that CMS communications between the Content Engine and the Content Distribution Manager have not been successful for more than two datafeed polling periods. Offline status does not necessarily mean that other services on the Content Engine are not functioning. If the Content Engine itself is not functioning, the Content Distribution Manager GUI shows that the device is “Inactive.”

When a Content Engine goes offline because of an IP address change, acquired content is not lost; however, as long as the Content Engine appears offline to the Content Distribution Manager, that Content Engine is unable to detect any changes or updates made to the channel and manifest files.

The offline Content Engine might continue distribution tasks for the content it has already acquired, but it cannot participate in any acquisition or distribution tasks for new content or new manifest files assigned to the channel.

If you change the IP address of a Content Engine’s primary interface using the Content Distribution Manager GUI (**Devices > [Content Engine] > General Settings > Network > Network Interfaces**) the Content Distribution Manager communicates the IP address change to all of the devices in the ACNS network and the Content Engine does not go offline.

- **Content Router**—If you change the IP address of a Content Router’s primary interface directly using the Content Router CLI, the Content Distribution Manager does not recognize the change, the Content Router appears as offline in the Content Distribution Manager GUI, and there is no further CMS communication between the Content Router and the Content Distribution Manager.

When a Content Router goes offline because of an IP address change, it cannot receive subsequent configuration updates from the Content Distribution Manager, such as channel configuration changes or coverage zone file changes. The coverage zone file remains with the Content Distribution Manager, but any further updates to it cannot reach the Content Router. Consequently, the Content Router might contain stale coverage zone file information and stale routing tables, affecting the router’s ability to redirect ACNS content requests.

Acquisition and distribution is not affected by changing the IP address of a Content Router.

If you change the IP address of a Content Router’s primary interface using the Content Distribution Manager GUI (**Devices > (Content Router) > General Settings > Network > Network Interfaces**) the Content Distribution Manager communicates the IP address change to all of the devices in the ACNS network without affecting the Content Router functionality.

- If your Content Engine is behind a firewall, and you configured the NAT address setting in the Content Distribution Manager GUI, Device Activation window, you might need to change the setting.

When a NAT address is configured, the Content Distribution Manager communicates with devices in the ACNS network that are behind the NAT firewall using that explicitly configured IP address. After you relocate a device that has a NAT address setting configured, verify that the IP address is still correct.

To view the NAT address setting from the Content Distribution Manager GUI, choose **Devices > Devices**. Click the **Edit** icon next to the name of the Content Engine that you want to modify. The Device Home window appears. In the Contents pane, choose **Device Activation**. The Device Activation window appears showing the NAT Address configuration field. You can modify the NAT address in this field.

Troubleshooting

After you make changes to your network, such as replacing or relocating devices, changing IP addresses, or modifying the manifest file, you can check your network to monitor the outcome of these changes.

Checking the File Replication Status

The replication status feature allows you to view the status of content replication using the Content Distribution Manager GUI, output from CLI commands, or an API file. In the Content Distribution Manager GUI, replication status is provided under the Content tab and the Devices tab. You can view the replication status by channel or by device. The Content Distribution Manager GUI also allows you to obtain a detailed view for a specific Content Engine or channel. You can also view detailed replication status for a particular content item in a channel.

You can check the replication status of a particular receiver Content Engine, for example, to make sure that all the content has been fully replicated to that device before you reassign it to the role of root Content Engine.

For more information about how to monitor content replication status from the Content Distribution Manager GUI, see the “Viewing Content Replication Status” chapter in the “*Cisco ACNS Software Configuration Guide for Centrally Managed Deployments*” publication.

Checking the Streaming Session Statistics

The Content Distribution Manager GUI provides monitoring tools to help you monitor the progress of streaming sessions and provide statistics, such as Windows Media program statistics for both video-on-demand and live programs. In the ACNS 5.5.1 GUI these monitoring tools can be found in the Devices tab: **Devices > Devices > Device Monitoring > Statistics > Streaming Sessions** or **Bytes Served**.

About Streaming Session Statistics

The streaming server workload is defined as the number of concurrent unicast and multicast sessions on a streaming server.

The Content Distribution Manager GUI displays the following streaming sessions using a line graph:

- The number of concurrent unicast streams being served by WMT, including live and on-demand content
- The number of concurrent multicast streams being served by WMT, including live and on-demand content
- The number of concurrent unicast streams being served by the Cisco Streaming Engine

The reports displayed in the Content Distribution Manager GUI include only those events that occur while the CMS service is enabled on the Content Engine. All activities (such as bandwidth usage, CPU utilization, and streaming sessions) that occur while the CMS is not running on the Content Engine are not included in the monitoring reports.

(For information about the device monitoring tools, see the context-sensitive online help in the Content Distribution Manager GUI.)

Displaying Streaming Session Statistics Using the CLI

To display statistics about WMT requests from the CLI, use the **show statistics wmt** EXEC commands.

```
ContentEngine# show statistics wmt ?
  all           Display all Windows Media statistics
  bytes        Display unicast bytes statistics
  errors       Display errors statistics
  multicast    Display multicast statistics
  requests     Display unicast request statistics
  rule         Display rule template statistics
  savings      Display unicast savings statistics
  streamstat   Display Windows Media streaming connections
  urlfilter    Display urlfiltering statistics for mms and rtsp requests
  usage        Display concurrent usage statistics
ContentEngine#
```

In the ACNS 5.3.1 software and later releases, the output of the **show statistics wmt** EXEC commands includes information about WMT RTSP requests. For example, the output from the **show statistics wmt** EXEC commands was changed as follows:

- RTSP-related information was added to the **show statistics wmt all** command output.
- Information about RTSPT and RTSPU were added in the transport protocol portion of the **show statistics wmt bytes** command output.
- RTSPT and RTSPU errors were added to the **show statistics wmt errors** command output.
- The **show statistics wmt requests** command output includes the RTSPT and RTSPU protocols as well as Fast Start and Fast Cache data.

In the ACNS 5.3.1 software and later releases, you can display aggregated live statistics by entering the **show statistics wmt streamstat live** EXEC command.

Checking the Syntax of the Coverage Zone File

Coverage zone files are manually imported or uploaded from the Content Distribution Manager GUI. (For procedural information, see the “Setting up Content Request Routing in the ACNS Network” chapter in the *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments* publication.)

The Content Distribution Manager has a built-in mechanism to validate coverage zone files as soon as they are imported or uploaded. If the coverage zone file contains any syntax errors, these errors are immediately reported in the Content Distribution Manager GUI. To correct syntax errors, you must manually correct the coverage zone file and re-import or upload the file.

If you change the IP address of a Content Router or Content Engine, the coverage zone file is not affected because coverage zone specifications refer to the Content Engine hostname and not to its IP address. The Content Router continues to redirect ACNS content requests to the Content Engine as long as the Content Router or the Content Engine remain online.

If a Content Router goes offline for any reason, updates to the coverage zone are not communicated to the Content Router, and the coverage zone information becomes stale. When the Content Router is restored and comes online in the Content Distribution Manager GUI, the Content Distribution Manager automatically sends updates to the Content Router. You do not need to refresh the coverage zone file manually.

