Release Notes for Cisco ACNS Software, Release 5.4.1

January 20, 2006

ACNS Build 5.4.1b9

Note The most current Cisco documentation for released products is available at Cisco.com at http://www.cisco.com. The online documents may contain updates and modifications made after the hardcopy documents were printed.

Contents

These release notes contain information about the Cisco Application and Content Networking System (ACNS) 5.4.1 software. These release notes describe the following topics:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

The ACNS software combines the technologies of demand-pull caching and pre-positioning for accelerated delivery of web applications, objects, files, and streaming media; the ACNS software runs on Cisco Content Engines, Content Distribution Manager, and Content Router hardware platforms.

These release notes are intended for administrators who will be configuring, monitoring, and managing devices that are running the ACNS 5.4.1 software. These release notes describe the new product features, the supported hardware, and the open and resolved caveats regarding the ACNS 5.4.1 software release.

New and Changed Information

This section describes new and changed features in the ACNS 5.4.1 software release. It also lists the supported hardware.

New Features in the ACNS 5.4.1 Software

- The ACNS 5.4.1 software release includes the following video-related enhancements:
  - Windows Media Technologies (WMT) server side playlists (SSPL) support (limited support was added in the ACNS 5.4.1 software release)
  - Third Generation Partnership Project (3GGP) support by the Cisco Streaming Engine. The Cisco Streaming Engine has been upgraded with a new streaming component that supports 3GPP streaming files (files with the .3gp and .3g2 file extension). This streaming service upgrade in the ACNS 5.4 software release provides for the uniform delivery of rich multimedia content over broadband mobile networks to multimedia-enabled cellular phones.

    3GPP and 3GPP2 are comprehensive standards for the creation, delivery, and playback of multimedia content over third generation wireless networks. While the scope of 3GPP spans everything from encoding to delivery, the ACNS 5.4 software supports the delivery of 3GPP-encoded files using RTSP or RTP-over-UDP transport through the Cisco Streaming Engine only.

Note Although 3GPP files can be transported as RTP-over-RTSP interleaved streams, the Cisco Streaming Engine supports RTP-over-UDP only. The Cisco Streaming Engine does not support HTTP progressive downloading.

Note Programs created using the Content Distribution Manager can be restarted from the Content Distribution Manager GUI. Programs created by using the CLI cannot be restarted if the program fails.

This feature has been tested with the following clients: PacketVideo 3GPP client (PC-based simulator version 3.4.1), RealPlayer 3GPP client (version 10 and above), QuickTime Player (version 6.0.5 and 7.0.2), and the Nokia EDGE-integrated video player (model 6230i).

This feature has been tested with the following origin servers and encoders: AXIS 210 Network Camera, Helix Mobile Producer version 10, and Darwin Broadcaster Version 5.0.3.1.

This feature has been tested with the H.263 video codec.

This feature has been tested with the following bit rates for both VoD and live streams: 28 Kbps, 56 Kbps, 100 Kbps, 128 Kbps, 256 Kbps, and 512 Kbps.

  - H.264 support (MPEG-4 part 10), which provides AVC streaming support

- The ACNS 5.4.1 software release includes the following Content Distribution Manager GUI enhancements:
  - Service-based GUI enhancements that streamline management tasks
  - The ability to configure LDAP through the GUI
  - The ability to deactivate a root Content Engine through the Content Distribution Manager GUI. You can deactivate a Content Engine from the Device Activation window even if the device is the root Content Engine for a channel.
- The ACNS 5.4.1 software release includes the following authentication enhancements:
  - Support of NTLM version 2 for the Windows environment
  - Support of FTP proxy authentication (support for proxy authentication of nontransparent FTP requests) and access control of proxy-mode requests based on IP access control lists (ACLs)
  - Support of cookie authentication for content acquisition (user admin). An authentication option with origin servers for content acquisition up to the root device was added. Ability to specify in the manifest file that cookies are to be used for acquisition crawl tasks.
- The ACNS 5.4.1 software release includes service provider load level optimization that includes the following changes:
  - The memory management and the reclaimer were adjusted to avoid low-load based memory starvation.
  - The error message logging frequency was modified to avoid the logs from being flooded with excessive low-memory messages.
  - The buffer threshold settings were modified to improve the memory management and reclamation transitions.
  - The amount of buffer memory allocation on a model CE-7325 or model CE-7326 was increased to improve the Content Engine's ability to handle the high server loads of service providers.
  - The network read ahead was adjusted to reduce outstanding buffer allocations, which will conserve memory for long-haul, long-term network transfers.

- The ACNS 5.4.1 software release also includes the other following enhancements:
  - The **feedback** command option was added to the **show statistics distribution mcast-date-sender** EXEC command. This new option allows you to display NACK statistics from the feedback files about the receivers:

```
ContentEngine# show statistics distribution mcast-data-sender feedback ?
 duration  Feedback statistics for the particular duration
ContentEngine# show statistics distribution mcast-data-sender feedback duration ?
 days     Number of Days <1-365>
 hours    Number of Hours <1-24>
 minutes  Number of minutes <1-60>
ContentEngine# show statistics distribution mcast-data-sender feedback
duration days 20 ?
 detail  Detailed statistics
```

  - Load-based content request routing
  - NTLM proxy authentication support for preloading content
  - The type of content that can be forwarded to external third-party ICAP-compliant servers was extended to include ICAP processing of FTP-over-HTTP traffic.
  - Support of the Websense Version 5.5 software and the SmartFilter Version 4.1 software for URL filtering

Hardware Supported

The ACNS 5.4.1 software supports the following hardware platforms:

Note All of the listed platforms also support the ACNS 5.3.1 software and the ACNS 5.2.x software releases except for the following three new Wide-Area Application (WAE) platforms that are only supported in the ACNS 5.3.3 software and later releases: the WAE-511, the WAE-611, and the WAE-7326.

- NM-CE-BP-SCSI
- NM-CE-BP-80G
- NM-CE-BP-40G
- NM-CE-BP
- CDM-4630
- CDM-4650
- CE-507
- CE-507AV
- CE-510-K9
- CE-510A-80GB-K9
- CE-565-K9
- CE-565A-72GB-K9
- CE-565A-144GB-K9
- CE-590
- CE-590-DC
- CE-7320
- CE-7305-K9
- CE-7305A-K9
- CE-7325-K9
- CE-560

- CE-510A-160GB-K9
- CE-511
- CE-566-K9
- WAE-511
- WAE-611
- CE-560AV
- CE-7325A-K9
- CE-7326
- WAE-7326
- CR-4430

Important Notes

This section emphasizes important information regarding the ACNS 5.4.x software. It includes the following sections:

RAM Requirements for ACNS 5.4 Software and Websense 5.5 Software

The integrated Websense Enterprise software Version 5.5 in the ACNS 5.4 software requires a minimum of 512 MB of RAM. We recommend that you upgrade the RAM on your device to 512 MB or greater, or move your integrated Websense server to another device that has at least 512 MB of RAM.

Websense Issues When Downgrading to the ACNS 5.0 Software or ACNS 5.1 Software

If the local (internal) Websense server is enabled on the Content Engine and you downgrade from the ACNS 5.2.x software to either ACNS 5.0 software or ACNS 5.1 software, the WebsenseEnterprise directory is removed from the Content Engine and the local Websense server stops working. The ACNS 5.2.x software does not generate an error message indicating that the WebsenseEnterprise directory has been removed. However, in the ACNS 5.3.1 software and later releases, the following error message is displayed to notify you about this Websense downgrade issue:

```
WARNING:
Websense does not support downgrade
Hence removing /local/local1/WebsenseEnterprise
Websense will stop working after copy ftp install
```

To avoid this problem when downgrading from the ACNS 5.3.x or ACNS 5.2.x software to either ACNS 5.1.x software or ACNS 5.0.x software, follow these steps:

Step 1 Disable the local (internal) Websense server on the Content Engine.

Step 2 Deactivate the Websense services on the Content Engine.

Step 3 Install the ACNS 5.1 software or ACNS 5.0 software downgrade image on the Content Engine.

Media File System Issues When Downgrading to ACNS 5.0 Software

If you have configured the media file system (mediafs) with the ACNS 5.1 software and later releases, and then downgrade to the ACNS 5.0 software, the mediafs disk space assignment is lost and reverts to the ACNS network file system (cdnfs) disk space. (The mediafs is used for on-demand content that is fetched through the two streaming protocols [RTSP and WMT]. The cdnfs is used for pre-positioned content in the ACNS network.)

This situation occurs because of a design change that was implemented in the ACNS 5.1 software. Because the ACNS 5.0 software is not compatible with this change, the disk space becomes assigned to cdnfs instead of mediafs. To work around this problem, follow these steps:

1. After you downgrade to the ACNS 5.0 software, use the CLI (**disk config** EXEC command) or the GUI to assign the mediafs disk space.

   Use the Content Distribution Manager GUI for Content Engines that are registered with a Content Distribution Manager. Use the Content Engine GUI for standalone Content Engines (Content Engines that are not registered with a Content Distribution Manager and are being managed through the Content Engine GUI or CLI).

2. Reboot the Content Engine for the disk configuration changes to take effect.

SmartFilter Issues When Upgrading or Downgrading to Another ACNS Software Release

When you upgrade or downgrade the Content Engine to a different release of the ACNS software, if there is a difference in the SmartFilter plug-in version, the SmartFilter database and configuration files are deleted and default configurations are loaded. This change occurs because the configuration details might be changed with each new version of SmartFilter software. After each upgrade or downgrade of the SmartFilter plug-in, a fresh database has to be downloaded from the SmartFilter Administration Console to the Content Engine.

Interoperability with ICAP Vendors

The Internet Content Adaptation Protocol (ICAP) is an open standards protocol for content adaptation, typically at the network edge. Content adaptation includes virus scanning, content translation, content filtering, content insertion, and other ways of improving the value of content to end users. ICAP specifies how a Content Engine, acting as an HTTP proxy server, can communicate with an external device that is acting as an ICAP server, which filters and adapts the requested content.

ICAP provides two content-processing modes for HTTP services. These modes define the transactions that can occur between a Content Engine acting as an ICAP client and an ICAP server. The two modes are as follows:

- Request modification (reqmod**)**—Allows modification of requests as they are sent from the Content Engine to the ICAP server on their way to the origin server. The ICAP server can modify these requests depending on the services requested.
- Response modification (respmod)—Allows modification of requests after they return from the origin server. The ICAP server only acts on requested objects after they return from the origin server.

The following is a complete list of the ICAP vendors that have been certified to interoperate with the Content Engine:

- TrendMicro for reqmod and respmod
- Symantec for respmod
- Finjan for reqmod and respmod
- SurfContol for reqmod

ICAP Performance

With the respmod vectoring point, which is used by virus-scanning Internet Content Adaptation Protocol (ICAP) vendors, the performance of the Content Engine model CE-7305 will be 300 transactions per second.

With the reqmod-precache vectoring point, which is used by URL filtering ICAP vendors, the performance of the Content Engine model CE-7305 will drop 20 percent from the rated performance.

Note The performance of the Content Engine will be limited by the performance of the ICAP server.

Matrix of Supported Caching, Filtering, and Authentication Methods

Table 1 lists the caching, filtering, and authentication methods supported by Content Engines that are running the ACNS 5.4.x software. An asterisk (*) indicates that a feature is supported for that particular protocol.

Table 1 Caching, Filtering, and Authentication Methods and Related Protocol Support

	Filtering				Proxy Authentication			
Protocol	**Caching**	**N2H2**	**Websense**	**SmartFilter**	**RADIUS**	**LDAP**	**NTLM**	**TACACS+**
HTTP	*	*	*	*	*	*	*	*
FTP-over-HTTP	*	*	*	*	*	*	*	*
HTTPS-over-HTTP	*	*	*	*	*	*	*	*
RTSPG	*							
MMSU	*							
MMST	*							
MMS-over-HTTP	*				*	*		
HTTP-WCCP	*		*	*	*	*	*	*
FTP-WCCP (native FTP)	*							
HTTPS-WCCP	*		*	*				
RTSPG-WCCP	*							
MMSU-WCCP	*							
MMST-WCCP	*							
MMS-over-HTTP -WCCP	*				*	*		

Caveats

This section lists and describes the open and resolved Severity 1, 2, and 3 caveats in the ACNS 5.4.1 software. Caveats describe unexpected behavior in the ACNS 5.4.1 software. Severity 1 caveats are the most serious; Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

Open Caveats - ACNS 5.4.1 Software

This section lists caveats that have not been resolved in the ACNS 5.4.1 software release.

- CSCdy82311

  Symptom: Content cannot be acquired using strong authentication from secure origin servers that use certificates from nonstandard certificate authorities (CAs). If strong authentication was chosen for content acquisitions from such a site, the acquirer error statistics will contain a 401 (Unauthorized) error code, and the acquirer error log contains the following error message:

  `Strong Cert Authentication rejects certificate due to error: ssl error code`

  Condition: This problem occurs if the origin server uses a certificate that is not known as a standard certificate to the ACNS software acquirer. For content acquisition from secure sites over HTTPS using strong authentication, only sites with certificates from standard certificate authorities are supported.

  Note With strong authentication, if any errors occur during certificate verification by the ACNS acquirer, then content from that site will not be acquired. With weak authentication, certain errors (for example, a certificate has expired, certificate is not yet valid, and a subject issuer mismatch has occurred) are allowed during certificate verification.

  Workaround: Use one of these workarounds:

  – Use weak authentication.

  – On the secure server, use a certificate that was generated by one of the standard certificate authorities. ACNS network administrators should refer to the following information to determine which CA certificate to install on their origin servers. Note that the certificate list differs based on the version of the ACNS software. For the ACNS 5.1.x software release or later, refer to the certificate list in the *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x*.

- CSCea51815

  Symptom: When a Content Engine model CE-565 is attached to a Storage Array SA-7 device, if too large a cache file system (cfs) partition is configured, and a combined streaming and caching workload is used, then a lower HTTP performance is observed.

  Condition: This problem occurs when the CE-565 has Windows Media Technologies (WMT) enabled, a combined streaming and caching workload is used, and the Content Engine is attached to an SA-7 device.

  Note The Storage Array device is used for the cache file system (cfs).

  Workaround: Allocate less space to the cfs if a Storage Array is attached to the Content Engine.

- CSCec52221

  Symptom: Windows Media Technologies (WMT) is enabled with no media file system (mediafs) after you downgrade from the ACNS 5.1b300 software to the ACNS 5.0.7b8 software.

  Condition: This problem occurs if you upgrade from the ACNS 5.0.7b8 to the ACNS 5.1bx software, configure the disk, and then downgrade to the ACNS 5.0.7b4 software.

  Workaround: Reconfigure the disk with a mediafs partition and reload the software.

- CSCed68727

  Symptom: The Content Distribution Manager only checks if coverage zone files refer to invalid Content Engines after there is a fresh import. When there is a configuration change that can cause already imported coverage zone files to refer to invalid Content Engines, the Content Distribution Manager does not check or display the correct error message until the next fresh import.

  Condition: This problem occurs if there is a coverage zone configuration change that causes already-imported coverage zone files to refer to invalid Content Engines.

  Workaround: There is no known workaround.

- CSCed77655

  Symptom: The Content Engine stops spoofing the client IP address and uses its own IP address to fetch content from the origin server.

  Condition: The **http l4-switch spoof-client-ip enable** global configuration command turns on IP spoofing on a Content Engine that is functioning as a caching engine. When a **rule action use-server** global configuration command is used, the Content Engine stops spoofing the client IP address and instead uses its own IP address to fetch the content.

  Workaround: Remove the rule configurations.

- CSCed84227

  Symptom: The network management system (NMS) host does not know where SNMP traps are coming from.

  Condition: This problem occurs if there are two interfaces and you configure interface redundancy using both interfaces. You must use a dummy address for the physical addresses. You then configure a real address that floats between the two interfaces. If you then configure SNMP traps, the traps are being sourced from the dummy address and not the routable address. Therefore, the NMS host does not know where the trap is coming from.

  Workaround: Configure the Content Engine to generate SNMP version 2c type trap messages. Because the SNMP version 2c trap message does not contain the IP address of the SNMP agent, the NMS software will use the source IP address of the UDP message to identify the address of the SNMP agent.

- CSCee25042

  Symptom: Even though you entered the **url-filter wmt bad-sites-deny** global configuration command on the Content Engine, the Content Engine is not filtering requests for content that is pre-positioned in its wmt_vod directory.

  Condition: This problem occurs in the following situation:

  a. You pre-position a file (for example, file.asf) on the Content Engine in its wmt_vod directory.
  b. After pre-positioning the file, you configure the bad site list for URL filtering using mmst://*Content Engine IP address*/wmt_vod/file.asf.
  c. A user makes a content request for this URL (mmst://*Content Engine IP address*/wmt_vod/file.asf).

  Workaround: Configure the bad site list using mmst://127.0.0.1/wmt_vod/file.asf instead of mmst://*Content Engine IP address*/wmt_vod/file.asf.

- CSCee38190

  Symptom: A WMT live stream in a managed live event environment is accessible for a period longer than the scheduled duration.

  Condition: This problem occurs only with WMT live programs that have unicast access enabled. In this situation, streams can be accessible for up to 24 hours after the last playtime of the event if “Auto Delete” is set to true or can be accessible indefinitely if “Auto Delete” is set to false.

  Workaround: Control the live-stream source through the schedule for the event. Typically, this process involves starting and stopping the WMT encoder.

- CSCee49106

  Symptom: The content replication status can show an incorrect manifest item count.

  Condition: This problem can occur if too many channels share the same content (for example, if over 100 channels share the same 30 files in each channel). Even though all 100 channels should show the 30 files that were acquired and distributed, it takes an extended period (days) before the correct manifest item count is displayed.

  Workaround: Reduce the number of channels that share the same contents.

- CSCee56998

  Symptom: The CPU usage on the Content Engine hits a peak of 100 percent.

  Condition: This problem can occur if the internal (local) Websense server is enabled on the NM-CE-BP models.

  Workaround: There is no known workaround.

- CSCee67227

  Symptom: If you specify foo as a folder URL in the manifest file, and there is a single item redirection from foo to foo/ by the web server, the ACNS acquirer fails to process such redirections and generates a 716 error message. If you are using the quick crawl tool in the Channel Content window, some of the files also report 716 error messages.

  Condition: This problem occurs if you are using the quick crawl tool and there is a single item redirect from foo to foo/. However, if foo is a link from a crawl job, single item redirections from foo to foo/ are allowed.

  Workaround: Specify foo/ in the manifest file, or specify a crawl job instead of using the quick crawl tool.

- CSCee67330

  Symptom: Microsoft NT LAN Manager (NTLM) authentication fails and the pop-up window is displayed again.

  Condition: This problem occurs if NTLM authentication is being used and the specified domain name is longer than 50 characters.

  Workaround: For NTLM authentication, use a domain controller (DC) that has a domain name shorter than 35 characters.

- CSCee71157

  Symptom: Channel routing causes loops for several Content Engines.

  Condition: This problem can occur if there are Content Engines that are running the ACNS 5.1.x software or earlier, and these Content Engines are registered with a Content Distribution Manager that is running the ACNS 5.2.x software.

  Workaround: Upgrade the Content Engines to the ACNS 5.2.x software. Currently, a Content Distribution Manager that is running the ACNS 5.2.x software does not propagate some configuration changes to Content Engines that are running an ACNS software release earlier than the ACNS 5.2.x software. Therefore, Content Engines that are running the ACNS 5.1.x software or earlier, may not recognize that the root Content Engine was changed from one Content Engine to another. Consequently, routing loops can develop within the system.

- CSCee81376

  Symptom: The CMS service on the Content Distribution Manager cannot start and fails to create the CMS database backup file.

  Condition: This problem can occur if the ACNS network configuration is very large (for example, with 2000 configured Content Engines) and the sysfs partition is 2 GB or less.

  Workaround: Create a sysfs partition that is greater than 2 GB.

- CSCee90245

  Symptom: Microsoft NT LAN Manager (NTLM) authentication occurs even though you disabled it on the Content Engine.

  Condition: This problem occurs very rarely. In very rare situations, even though you entered the **no ntlm server enable** global configuration command to disable NTLM proxy authentication on the Content Engine, NTLM proxy authentication is still not turned off. In such cases, NTLM authentication can still occur, although the output of the **show running** EXEC command shows that the NTLM server is not enabled on the Content Engine.

  Workaround: Enter the **no ntlm server enable** global configuration command again on the Content Engine.

- CSCee92698

  Symptom: The ICAP service is enabled on the Content Engine, but the Content Engine is unable to retrieve the content.

  Condition: This problem can occur if the Content Engine is running the ACNS 5.x software, and you configure two or more ICAP services to subscribe to the same vectoring point (the response modification [RESPMOD] vectoring point).

  Workaround: There is no known workaround.

- CSCee92917

  Symptom: A cleanup of the sysfs partition removes all pre-positioned RealMedia contents from the /local1/real_vod/ directory on the Content Engine.

  Condition: This problem occurs if the sysfs partition is saturated because of the population of content in the real_vod directory.

  Workaround: There is no known workaround.

- CSCef11091

  Symptom: The WCCP cache farm (a cluster of Content Engines that are running WCCP) is formed using the assignment method even though you specified the **mask-assignment assign-method-strict** option when configuring the WCCP service.

  Condition: This problem occurs if the WCCP cache farm is associated with Cisco routers instead of switches.

  Workaround: There is no known workaround. Mask assignment was only designed for Catalyst 6500 series switches and is not supported by Cisco routers.

- CSCef16345

  Symptom: The stream scheduler in the edge Content Engine retrieves stale Session Description Protocol (SDP) information from its forwarder and stores it in its local1/cse_live/ucast folder if the encoding is modified through IP/TV Program Manager. All further RTSP requests are served with this stale SDP content.

  Condition: This problem occurs if the stream scheduler retrieves stale SDP information from its forwarder because the program has been edited and the encoding changed for a program. This situation occurs if the Content Distribution Manager notification at the edge Content Engine triggers the stream scheduler before the same occurs at the root Content Engine. Consequently, the edge Content Engine obtains the SDP content from its forwarder, which is valid content at that moment.

  Workaround: Reload the Content Engine.

- CSCef37606

  The Content Engine becomes unresponsive, and it takes a long time for commands to be executed.

  Condition: This problem occurs when the load that is running on the Content Engine is almost as high as the maximum permissible load for a Content Engine, and you then enable ICAP (especially with request modification [REQMOD] transactions). This situation causes the Content Engine to go into an overload state and not recover easily.

  Workaround: The load on the Content Engine with ICAP enabled (for the response modification [respmod] transactions) should be kept to 50 percent of the load that it can handle without ICAP.

- CSCef37947

  Symptom: A URL in the Synchronized Multimedia Integration Language (SMIL) file that has the “repeatCount” value set, may not be requested as many times as specified by the “repeatCount” setting.

  Condition: This problem occurs only when RealPlayer Version 10 is used. The player exhibits the same behavior whether or not there is a Content Engine between the client and the origin server.

  Workaround: Use RealOne player instead of RealPlayer Version 10, or request the SMIL file again. The URL will be played at least once in the player.

- CSCef44709

  Symptom: An HTTP 1.0 request that is received by the Content Engine from a client web browser is sent as an HTTP 1.1 request by the Content Engine to the origin server.

  Condition: This problem occurs only when the ICAP service is enabled on the Content Engine.

  Workaround: There is no known workaround.

- CSCef57641

  Symptom: The cache process on the Content Engine restarts.

  Condition: This problem occurs if a large volume of HTTPS and FTP traffic is being directed to the Content Engine, which is operating in transparent mode.

  Workaround: There is no known workaround.

- CSCef60282

  Symptom: Even though you entered a **write memory** command, after an immediate reload, a prompt appears that the configuration has been changed.

  Conditions: This problem occurs if the following conditions are met:

  – You have enabled Websense on the Content Engine.

  – The IP address of the Content Engine is removed or changed.

  – You enter a **write memory** command on the Content Engine.

  – You reload the Content Engine.

  Workaround: Note that ACNS functionality is not affected if this problem occurs. However, if a prompt appears stating that the configuration has been changed, enter **yes** to save the configuration.

- CSCef61845

  Symptom: Unicast access to a live program does not work.

  Condition: This problem occurs only when you use special characters (“?” and “#”) in the unicast reference URL.

  Workaround: To publish a live event, use URLs that do not contain special characters.

- CSCef62968

  Symptom: The Content Engine reboots suddenly when you are performing database maintenance.

  Condition: The problem can occur because of a platform issue in the power supply of the device.

  Workaround: Properly trim the power supply of the Content Engine.

- CSCef67934

  Symptom: The proxy autoconfiguration file is missing from the Content Engine after you switch from group settings to device settings, and then switch back to group settings.

  Condition: This problem can occur in the following condition:

  a. You have specified values in the Client Proxy Autoconfig Device Group window of the Content Distribution Manager GUI.

  b. You override these values through the Client Proxy Autoconfig Device window of the Content Distribution Manager GUI.

  c. You revert the Content Engine back to the device group settings (you click the **Force device group settings** button in the device group window or you select the device group from the drop-down menu in the device window).

     The autoconfiguration file is not found but the proxy autoconfiguration feature is shown as enabled.

  Workaround: Return to the device window in the Content Distribution Manager GUI, delete the values from the proxy autoconfiguration fields in the device window, and then select **device group** from the drop-down menu.

- CSCef67938

  Symptom: When using the quick start tool in the Content Distribution Manager GUI, if you repeatedly click the **Add-Router to List** button before the window completely loads in your browser, the following message appears in your browser:

  ```
  The system had trouble processing your last request.
  ```

  This situation can occur under the following circumstances:

  – You click the **BACK** or **REFRESH** browser buttons.

  – Multiple browser windows from the same client machine are accessing the Content Distribution Manager GUI.

  – Another user deletes the item that you are working with in the Content Distribution Manager GUI.

  Condition: This problem occurs only when there is a slow connection between the Content Distribution Manager and your browser and you perform any of the unsupported actions described above.

  Workaround: Return to the Content Distribution Manager GUI and wait until the window is completely loaded in your browser before you click the **Add-Router to List** button.

- CSCeg04809

  Symptom: HTTP VoD file statistics are not being updated correctly.

  Condition: This problem can occur if you enter the **show statistics wmt requests** EXEC command while you are using the HTTP protocol to play a stream. The command output shows the total unicast requests field as 2 but shows the other types of requests (for example, the number of served streaming requests) as only 1.

  Workaround: Wait until the stream ends before you enter the **show statistics wmt requests** EXEC command.

- CSCeg22697

  Symptom: The Websense EIM server that is running on the Content Engine generates a core file.

  Condition: This problem can occur when the Websense server is enabled on the Content Engine.

  Workaround: No user intervention is required. If this problem occurs, the Websense server functionality is not affected. After generating a core file, the Websense server will be automatically restarted and the functionality is restored.

- CSCeg47793

  Symptom: If you modify a Content Engine GUI page and reload the page without first clicking the Update button, the new (unsaved) values are displayed on the page instead of the old (saved) values.

  Condition: This problem only occurs if you are using the latest versions of the Netscape browser (Version 7.0 or later) to access the Content Engine GUI.

  Workaround: Go to another Content Engine GUI page, and then return to the same Content Engine GUI page instead of reloading the page. The redisplayed Content Engine GUI page will display the old (saved) values instead of the new (unsaved) values.

- CSCeg56075

  Symptom: RealPlayer crashes when the streams are switched from the first stream to the second stream.

  Condition: This problem can occur if you have set the reconnect as automatic for broadcast redundancy.

  Workaround: Set the reconnect as manual instead as automatic.

- CSCeg60760

  Symptom: CPU usage on the Content Engine reaches 99 percent.

  Condition: This high CPU usage can occur if the Content Engine is serving numerous live-streaming requests and it is running the ACNS 5.1.11 software and later releases.

  Workaround: If you are not expecting a very high load on the Content Engine, you can turn off kernel optimization by entering the **no wmt accelerate live-split enable** global configuration command.

- CSCeg82405

  Symptom: The Internet Explorer client retrieves a partial (incomplete) customized error page and displays it along with some partial HTML code.

  Condition: This problem occurs if a customized error page is configured on the Content Engine and an Internet Explorer client requests a nonexistent HTTPS URL, which causes the customized error page to be returned.

  Workaround: There is no known workaround.

- CSCeg84004

  Symptom: NTLM authentication for a valid user may take a longer period than usual (approximately two minutes) if the client sends the request when the Content Engine has been idle for a long period of time.

  Condition: This problem can occur in the following condition:

  a. NTLM request authentication is enabled on the Content Engine.
  b. The request is sent after the Content Engine has been idle for a long period of time.
  c. The client machine has some malfunctioning program (for example, spyware or a virus) and is sending HTTP requests to the Content Engine along with the first request from the browser. The user agent is named Tioga, and the request is as follows:

     ```
     GET http://somehostname/Zone-UVWXYZ/config.cfg HTTP/1.0\r\n
     Request Method: GET
     Accept: */*\r\n
     User-Agent: Tioga\r\n
     Host: somehostname\r\n
     Pragma: no-cache\r\n
     ```

     where *somehostname* is a hostname.

     The user will be authenticated after waiting approximately two minutes. After reporting a failure to the browser, the Content Engine uses the same credential and retrieves the group information for that user from its HTTP authentication cache.

  Workaround: On the Content Engine, configure a rule to either reject requests from the user agent named Tioga, or configure the **no-auth** rule to bypass authentication for this user agent.

- CSCeg86386

  Symptom: In a Content Router environment, users are not able to choose RTSPU (UDP) or RTPST(TCP) by requesting with rtspu:// or rtspt:// from their Windows Media players. Another symptom is that an RTSPT stream is returned when an RTSPU stream is requested. A third symptom is that even though you specified the **wmt disallowed-client-protocols rtspu** global configuration command, it is not preventing clients from being served for a request rtspu://crfqdn/file.asf, which will return an RTSP stream instead of an error.

  Condition: This problem can occur if a Content Router is being used for RTSP redirection.

  Workaround: There is no known workaround.

- CSCeh20906

  Symptom: Even though you have the transaction log sanitize feature enabled on the Content Engine, the RealProxy or RealServer access logs still display the client IP address even though it should be hidden.

  Condition: This problem is caused because the **transaction-logs sanitize** CLI command is not working properly for the RealProxy and RealServer. Even though you have entered the **transaction-logs sanitize** global configuration command, the RealProxy or RealServer access logs still display the client IP address even though it should be hidden.

  Workaround: There is no known workaround.

- CSCeh23466

  Symptom: The table of contents and the index of the ACNS Content Distribution Manager online help are not functioning. When you open the online help window, the left pane, which contains the table of contents and index, appears blank.

  Condition: This problem is caused by the Windows Security Update MS05-001. This security patch prevents the creation of an instance of the HTML Help ActiveX control that is served in HTML content from outside the Local Machine zone.

  Workaround: Because the ACNS Content Distribution Manager is part of your internal network, you may modify the Windows registry to allow execution of ActiveX controls that are served from within the intranet zone. For more information on modifying the registry to workaround this issue, refer to Microsoft Knowledge Base article 892675, which is available at this URL: http://support.microsoft.com/kb/892675.

- CSCeh34004

  Symptom: When connected to an external ICAP server, the Content Engine may stop forwarding data. After the ICAP server timeout occurs, an error is reported to the HTTP client.

  Condition: This problem can occur because of the timing of server responses.

  Workaround: There is no known workaround.

- CSCeh34292

  When the WMT player is being proxied to the Content Engine, the player stops and starts buffering several times when it is playing a media file.

  Condition: This problem can occur under the following condition:

  a. WMT is disabled on the Content Engine.
  b. The media file is located on the Windows Media Series 9.1 server that will send back a keepalive header without a content-length header.

  Workaround: Enter the **http ignore-resp-len-conn-hdr-check** global configuration command, which is a hidden CLI command, on the Content Engine.

- CSCeh35923

  Symptom: When you are trying to install the ACNS software on a Content Engine, DMA errors are displayed.

  Condition: This problem only occurs under the following condition:

  a. You are trying to install the ACNS software image on a CE-7326.

  b. You select Option 7 from the Installer main menu as follows:

```
Installer Main Menu:
    1. Configure Network
    2. Manufacture flash
    3. Install flash cookie
    4. Install flash image from network
    5. Install flash image from cdrom
    6. Install flash image from disk
    7. Wipe out disks and install .bin image
    8. Exit (and reboot)
Choice [0]: 7
```

  Workaround: The DMA errors are displayed four to five times in sequence and then the normal operation of the Content Engine continues without any user intervention.

- CSCeh38741

  Symptom: The Windows Media player is not able to stream content for more than one hour in the case of a cache hit.

  Condition: This problem can occur when the Limit Player Timeout Inactivity value in the origin Windows Media server is set to the default value of 3600 seconds.

  Workaround: Increase the Limit Player Timeout Inactivity value in the origin Windows Media server.

- CSCeh73477

  Symptom: The acquirer experiences a problem with a samba crawl. The acquirer is recrawling the same crawl job.

  Condition: This problem can occur if both of the following conditions exist:

  1. A channel contains a samba crawl from a Network Appliance file server, which contains such media files as .wmv files.
  2. The time to live (TTL) is set to recrawl the file at a fixed interval that is specified by the TTL attribute.

  Workaround: There is no known workaround.

- CSCeh93212

  Symptom: The Websense Manager cannot connect to the local (internal) Websense server that is running on the Content Engine, and clients receive the following error: “Failed to connect, the server is not yet fully started. please try again in a little while”.

  Condition: This problem can occur if a standby IP address is used on both the primary and secondary interfaces, which prevents the Websense Manager from connecting to the Content Engine.

  Workaround: Disable the standby IP group and use a single IP address on the interface.

- CSCei01668

  Symptom: The firewall shows that there is an excessive amount of traffic coming from the Content Engine over TCP port 8999.

  Condition: This problem can occur if the Content Engine is on the outside of the firewall (connected to the internet gateway router). The Content Engine is constantly attempting to reset the connections to the inside with a source port of TCP 8999 going to the NAT address of the clients.

  Because the port translation timer has expired on the Content Engine, the Content Engine uses port 8999 to return the message to the client. Because there is no NAT address configured on the firewall with the TCP port 8999, these messages/requests fail at the firewall.

  Workaround: Configure the following global configuration CLI commands on the Content Engine:

  ```
  ContentEngine(config)# http tcp-keepalive enable
  ContentEngine(config)# tcp keepalive-timeout 60
  ContentEngine(config)# tcp keepalive-probe-interval 60
  ```

- CSCei06964

  Symptom: The Windows Media player is not able to play the URL.

  Condition: This problem can occur if the Content Engine is in between the Windows Media player and an ISA proxy, and NTLM authentication is enabled on the ISA proxy.

  Workaround: There is no known workaround.

- CSCei18400

  Symptom: There is a problem with playing high definition/high bit rate video on-demand streams.

  Condition: This problem can occur if there are more than 14 unique 2-Mbps streams with two clients per stream (28 connections).

  Workaround: There is no known workaround.

- CSCei28716

  Symptom: The system crashes and there are kernel core dumps.

  Condition: This problem occurs very rarely.

  Workaround: No workaround is required because the Content Engine will reboot and the system will work normally after the reboot.

- CSCin54434

  Symptom: Websense Manager cannot connect to the local Websense server (the Websense server runs as a separate process on the Content Engine instead of running on a separate system).

  Condition: This problem occurs if an external IP address is used from Websense Manager to connect to the local Websense server that is running on the Content Engine.

  Workaround: There is no known workaround.

- CSCin59462

  Symptom: An FTP client application stops receiving data for a data transfer operation such as a directory listing (ls) or file transfer (GET). The same symptom can occur for FTP-over-HTTP data transfers from the FTP server to the Content Engine.

  Condition: For FTP client applications, the Content Engine must be using the FTP proxy through WCCP redirection, configured for following the FTP client's mode for establishing a data connection. The FTP client application must have also been set to use active mode to the FTP server.

```
ContentEngine(config)# wccp ftp router-list-num number
ContentEngine(config)# wccp version 2
ContentEngine(config)# ftp proxy active-mode enable
```

  For FTP-over-HTTP data transfers, the Content Engine must be configured for an FTP incoming proxy and configured to use active mode to the FTP server. The client browser must be configured to use the Content Engine FTP proxy for FTP URLs.

```
ContentEngine(config)# ftp proxy incoming port
ContentEngine(config)# ftp proxy active-mode enable
```

  The symptoms can occur with the configurations described above and when the FTP server starts sending data packets that are received out of order by the Content Engine before the Content Engine sends the TCP connection establishment SYN-ACK packet to the FTP server.

  Workaround: Remove the Content Engine active mode configuration by entering the following global configuration command:

```
ContentEngine(config)# no ftp proxy active-mode enable
```

  When this symptom occurs on an FTP client application, press **Ctrl-C** simultaneously to stop the partial data transfer operation.

  When this symptom occurs on a browser configured for FTP-over-HTTP, click the **STOP** button to stop the partial data transfer operation.

- CSCsb61528

  Symptom: The Content Engine sends the redirect assign message before it receives the "I see you" message from the router.

  Condition: Because the Content Engine sends the redirect assign message before it receives the "I See You" message, the redirect assign message will always have a bad rcv-id. This problem occurs because the rcv-id is incremented as part of the router processing the "Here I am" message. Consequently, the value in the redirect assign message will be behind by 1.

  Workaround: No workaround is required because although the redirect assign message will have a bad rcv-id (it will be behind by 1), the redirect assign message is resent by the Content Engine and is accepted by the router without affecting the WCCP service.

- CSCsb65952

  Symptom: There is a local Network Agent core file on the Content Engine. (The local Network Agent is one of the services of the local Websense server and runs on the Content Engine.)

  Condition: This problem can occur when the local Network Agent is enabled on the Content Engine.

  Workaround: There is no known workaround.

- CSCsb69794

  Symptom: There is not an option in the Websense GUI for configuring the Winix NTLM Settings (Windows NT Directory/Active Directory [Mixed Mode]).

  Condition: The problem can occur in the following situation:

  – The Content Engine is running the ACNS 5.3.1.5 software or a later release and the integrated Websense software.

  – More than 24 hours have elapsed since you originally configured the Winix NTLM setting.

  Workaround: Reinstall the user service component of Websense on the Content Engine. For example, enter the following two global configuration commands:

```
ContentEngine(config)# no websense-server service user activate
ContentEngine(config)# websense-server service user activate
```

- CSCsb72030

  Symptom: The Content Engine is returning a 200 OK response when it should be returning a 304 message.

  Condition: This problem can occur when the content has been pre-positioned on the Content Engine.

  Workaround: There is no known workaround.

- CSCsb79685

  Symptom: When a WMT stream is pre-positioned, the audio works but the playback of embedded slides in the pre-positioned WMT stream are not displayed.

  Condition: This problem occurs if Microsoft presenter was used to create a WMT stream that has embedded slides. When this content is pre-positioned, WMT opens and the audio works but the slides never appear.

  Workaround: When you are using Microsoft producer to publish the content, select publish to **My Computer** and when you select the **Choose publish settings for different audiences** option do not check the **Enable rich-media Streaming** option. When the content is pre-positioned, all content that is created in publishing should be pre-positioned.

- CSCsb81163

  Symptom: The browser displays an error message that the requested URL could not be retrieved.

  Condition: This problem can occur when the clients are browsing HTTPS sites that require a login.

  Workaround: Because this is an intermittent problem, try to log in to the HTTPS site at a later time.

- CSCsb95697

  Symptom: The SNMP client is experiencing counters and gauge values of zero.

  Condition: This problem can occur if the Content Engine is running the ACNS 5.2.7 software or a later release, and it has not been rebooted for several weeks.

  Workaround: There is no known workaround.

- CSCsc00804

  Symptom: When the primary Content Distribution Manager is upgraded to the ACNS 5.3.3 software or a later release, the WCCP service to all of the registered Content Engines is interrupted. Only some of the Content Engines recover from this interruption in the WCCP service.

  Condition: This problem can occur if all of the registered Content Engines are running the ACNS 5.3.3 software or a later release, and then you upgrade the Content Distribution Manager to the ACNS 5.3.3 software or a later release.

  Workaround: There is no known workaround.

- CSCsc05348

  Symptom: During ICAP REQMOD precache processing, a significant amount of server errors occur.

  Condition: The server errors are being generated because the existing connections are closed when the internal connection to the Content Engine receives an error.

  Workaround: No workaround is required because even though the clients whose requests are going through the Content Engine will experience one failure to load a page, their attempt to reload a page will succeed.

- CSCsc07702

  Symptom: A PacketVideo player cannot play back a Helix Mobile Producer-encoded media file.

  Condition: This problem occurs when the files are pre-positioned. This problem does not occur if the QuickTime player (Version 6.0.5 or Version 7.0.2) is used to play back the files.

  Workaround: There is no known workaround.

- CSCsc13494

  Symptom: A disk is marked as “bad” when a disk error threshold is reached after a transient disk failure.

  Condition: This problem occurs only rarely and can only occur if the Storage Array device is attached to a model CE-7325 that is running the ACNS 5.3.3.8 software or a later release.

  Workaround: After the disk is marked “bad,” you can enter the **disk mark *diskname* good** EXEC command on the Content Engine to mark the disk as “good.”

- CSCsc14022

  Symptom: The Windows Media player reports an error when the user attempts to play a URL that requires authorization by the Camiant ICAP server.

  Condition: This problem occurs in the following situation. A request fail authorization with the ICAP server occurs, and the Camiant ICAP server has its alternate URL configured as a content-routed FQDN (for example, http://<cr-fqdn>/filename.asf).

  Workaround: The Windows Media player will not report an error and will successfully play the alternate URL that is configured on the Camiant ICAP server if you configure the alternate URL in one of the following formats:

  – A Windows Media player meta file that will be content routed to a Content Engine (for example, http://<cr-fqdn>/filename.asf.asx). This URL can also be specified using the RTSP protocol.

  – A file that resides on an external Windows Media server (a Windows Media server that does not reside on a Content Engine).

- CSCsc15499

  Symptom: HTTP POST requests, which are received through HTTP1.0, can fail and a 400 Bad request error message is generated.

  Condition: This problem can occur if the POST request contains an additional CRLF pair following the announced Content-Length. There are certain clients that are known to append this data to a request.

  Workaround: Disable HTTP 1.0 at the client.

- CSCsc19566

  Symptom: A Content Engine can hang or go into kernel debug mode if the kernel debug feature is enabled on the Content Engine.

  Condition: This problem can occur with a model CE-7325 that is running the ACNS 5.2.7.7 software or a later release.

  Workaround: Reload the Content Engine.

- CSCsc25501

  Symptom: After you remove the **no-auth** rule on the Content Engine, the Content Engine continues to apply the rule even if you enter the **no rule enable** command and then remove all of the pattern lists.

  Condition: This problem occurs if the **no auth** rule has been configured and then you remove it from the Content Engine.

  Workaround: Reboot the Content Engine.

- CSCsc26852

  Symptom: There is a cache assert in the icap_in_pending_list.

  Condition: This problem can occur if the Content Engine is running the ICAP process.

  Workaround: No workaround is required because the cache process automatically restarts on the Content Engine.

- CSCsc42786

  Symptom: Websense logging on the Content Engine does not show the usernames for queries that are made through LDAP/NTLM.

  Condition: This problem can occur if the Content Engine is running the ACNS 5.3.x software release or a later software release.

  Workaround: Downgrade the Content Engine to the ACNS 5.2.x software or an earlier software release.

- CSCsc44106

  Symptom: The configured rules for a device group are randomized when they are applied to the Content Engine that joins the device group.

  Condition: This problem occurs because the Content Distribution Manager GUI sorts the configured device group rules by the name of the rule. When you use the Content Distribution Manager GUI to configure rules for a device group, you cannot specify the precedence of a configured rule.

  Workaround: There is no known workaround.

- CSCsc45058

  Symptom: The Windows version of the PacketVideo player does not display video output. The player indicates that buffering is occurring but no video or audio is rendered.

  Condition: This problem occurs if the client is a PacketVideo player (a Windows simulator) and the source is a PacketVideo server. (The actual mobile phone-based PacketVideo client plays video/audio properly for the same program.)

  Workaround: Use the QuickTime player or a VLC client to view the content from a Microsoft Windows computer.

- CSCsc49144

  Symptom: The SmartFilter URL filtering feature is unexpectedly disabled on the Content Engine.

  Condition: This problem can occur in the following situation:

  – An external IP address is not configured on the Content Engine.

  – The interface IP address of the Content Engine is removed. (The Content Engine is left without an IP address.)

  Workaround: Reassign the IP address and reenable the SmartFilter URL filtering feature on the Content Engine.

- CSCsc71576

  Symptom: The Content Router does not redirect requests to Content Engines in less specific network routes when all Content Engines in the more specific network routes have reached their load threshold.

  Condition: This problem occurs when all of the following conditions exist:

  – The Content Router is configured to redirect requests based on the load of the Content Engines.

  – The coverage zone file has some Content Engines serving a more specific network route and some Content Engines serving a less specific network route, as shown in the following example:

```
<coverageZone>
<network>10.86.0.0/16</network> -----> More specific network route
<CE>ce1</CE>
<metric>10</metric>
</coverageZone>

<coverageZone>
<network>10.77.0.0/16</network> -----> More specific network route
<CE>ce2</CE>
<metric>10</metric>
</coverageZone>

<coverageZone>
<network>10.0.0.0/8</network> -----> Less specific network route
<CE>ce3</CE>
<metric>10</metric>
</coverageZone>

ce3 is configured to serve the network 10.0.0.0/8 which is less specific to the
network 10.86.0.0/16 served by ce1 and 10.77.0.0/16 served by ce2.
```

  – All the Content Engines serving the more specific network have reached their load threshold.

  – The Content Router receives a request from a client in the more specific network.

Workaround: The coverage zone file should be reconfigured in such a way that all Content Engines serving the less specific network route should be configured for the more specific network route with a higher metric value, as shown in the following example:

```
<coverageZone>
<network>10.86.0.0/16</network> -----> More specific network route with lower metric
<CE>ce1</CE>
<metric>10</metric>
</coverageZone>

<coverageZone>
<network>10.77.0.0/16</network> -----> More specific network route with lower metric
<CE>ce2</CE>
<metric>10</metric>
</coverageZone>

<coverageZone>
<network>10.86.0.0/16</network> -----> More specific network route with higher metric
<CE>ce3</CE>
<metric>20</metric>
</coverageZone>

<coverageZone>
<network>10.77.0.0/16</network> -----> More specific network route with higher metric
<CE>ce3</CE>
<metric>20</metric>
</coverageZone>
```

In this example, ce3 (initially configured for the 10.0.0.0/8 network route) is now configured for both the more specific network routes 10.86.0.0/16 and 10.77.0.0/16 with a metric value 20, which is higher than the metric value of 10 configured for ce1 and ce2.

If the Content Router receives a request from network 10.77.0.0/16, and if Content Engine ce2 has reached its load threshold, the Content Router will redirect the request to Content Engine ce3.

Similarly, if the Content Router receives a request from network 10.86.0.0/16, and if Content Engine ce1 has reached its load threshold, the Content Router will redirect the request to Content Engine ce3.

- CSCsc72072

  Symptom: With MMS URLs, WCCP hits for pre-positioned WMV files fail.

  Condition: This problem occurs because UNS resolution fails.

  Workaround: Substitute an IP address for the fully-qualified domain name (FQDN).

- CSCsc75289

  Symptom: Usernames are not being used by the Websense Network Agent for user-based policy filtering.

  Condition: This problem occurs if the Websense Network Agent is configured on the Content Engine.

  Workaround: There is no known workaround.

- CSCsc81316

  Symptom: At the Content Engine, the client is refused access to the RealProxy client. The Content Engine is also logging the following types of error messages:

  ```
  Sep 2 11:50:30 prx03 wccp: %CE-WCCP-3-500001: RTSP Proxy may be down, keepalives
  halted!
  Sep 2 11:50:30 prx03 rtspd: %CE-WCCP-3-500057: wccp_liveness_update(): Could not send
  alivemessage (tries 1). Success
  Sep 2 11:50:38 prx03 MCM: Plugin MC_REAL_ERRORPLUGIN: 72: Error retrieving URL
  `broadcast/.../reflector:35134' (Invalid path)
  Sep 2 11:50:39 prx03 MCM: Plugin MC_REAL_ERRORPLUGIN: 74: Error retrieving
  URL`broadcast/.../reflector:35137' (Invalid path)
  ```

  Condition: This problem can occur if RealProxy is enabled on a Content Engine that is running the ACNS 5.x software.

  Workaround: Reload the Content Engine.

- CSCsc81507

  Symptom: The Content Engine may lose the configured routes.

  Condition: This problem can occur if you have manually entered the routes.

  Workaround: Reenter the routes.

- CSCsc83129

  Symptom: ACNS pre-positioned downloads are slower than downloads from the origin server. For example, if you download a pre-positioned file from a Content Engine, the maximum download speed is 3.5 Mbps. If you download the same file directly from the origin server, the maximum download speed is 10 Mbps.

  Condition: This problem can occur in the following situation. A Content Engine model CE-7305 is running the ACNS 5.3.5 software or a later release and the pre-positioned file is downloaded over a Gigabit Ethernet interface with an HTTP bit rate set to 0 (unrestricted).

  Workaround: There is no known workaround.

Resolved Caveats—ACNS 5.4.1 Software

This section lists the caveats that have been resolved in the ACNS 5.4.1 software release. The resolved caveats are grouped into the following categories:

AAA Accounting

- CSCeg90529

  No command information is being received under the standard Cisco ACS TACACS headers.

Acquisition and Distribution Resolved Caveats

- CSCeh06795

  A live channel may fail to be played from the clients. The replication fails as indicated by the output from the **show programs** EXEC command. This problem can occur in the following condition:

  a. You are running the ACNS 5.2.1b7 software and later releases.

  b. You configure a live channel and then schedule it through the Content Distribution Manager GUI.

  c. You use uppercase letters when specifying the program name.

  Because uppercase letters are sometimes rejected, you need to avoid using uppercase letters when specifying the program name in the Content Distribution Manager GUI. This problem was fixed in the ACNS 5.4.1 software release.

- CSCeh40754

  The root Content Engine cannot acquire content. The Content Distribution Manager GUI replication status window indicates that the Content Distribution Manager has no content, and the receiver Content Engines indicate “No Status Reported.” This problem can occur if the root Content Engine has recently experienced a failure that took it down, or it required a hard reboot that caused a database corruption on the root Content Engine, which in turn prevented the acquirer from acquiring the content.

- CSCeh44689

  The acquirer fails to load or start if the origin server requires NTLM authentication and the NTLM credentials are not provided to the acquirer.

- CSCei48756

  Content Engines that are running the ACNS software may bypass TCP segments that have a multicast destination MAC address.

- CSCei64591

  The Windows Media player cannot play a URL that involves redirection by a Content Router. The Content Engine’s IP address is being resolved to the standby IP address instead of the interface IP address.

- CSCej02204

  The ACNS acquirer repeatedly attempts to acquire files that have been removed from the origin server. This problem only occurs when a schedule is used within the manifest file.

- CSCsb73083

  For the same content, pre-positioned files are being served slower than if the content is served from the Content Engine’s web cache as a result of a cache hit.

- CSCsb76407

  The multicast receiver is unable to receive any files that are sent from the multicast sender. This problem can occur if the multicast sender and the multicast receiver both have two network interfaces, and multicast traffic is sent and received through the second network interface.

- CSCsc05453

  A coverage zone file import fails and the following warning appears in the system log (syslog):

```
08/25/2005 05:51:53.721(Local) [W] cdm(FileManager):
com.cisco.unicorn.util.SystemCommandTimeoutException: Timeout error:
com.cisco.unicorn.ut
il.SystemCommandTimeoutException: Timeout error
       at com.cisco.unicorn.util.Utils.SystemExec(Utils.java:728)
       at com.cisco.unicorn.controller.ComplexUrlFile.get_(ComplexUrlFile.java:273)
       at com.cisco.unicorn.controller.ComplexUrlFile.fetch(ComplexUrlFile.java:135)
       at
com.cisco.unicorn.controller.FileManager.checkIfModified(FileManager.java:456)
       at com.cisco.unicorn.controller.FileManager.runImpl(FileManager.java:289)
       at com.cisco.unicorn.server.AModule.run(AModule.java:177)
```

  The problem can occur if the download of the coverage zone file takes more than 60 seconds because of the size of the coverage zone file and the network bandwidth.

- CSCsc39071

  If MMS acquisition is used, the asfduration process generates a core file during the acquisition of Windows media files.

- CSCsc44863

  In rare situations, the CleanupAD process can generate a core file.

- CSCsc49571

  Multicast distribution cause files to be retransmitted to Content Engines that have already replicated the files.

- CSCsc67608

  The multicast distribution balance of the priority-based queue versus the ime-based queue is not in line with the configured multicast distribution priority weight. This problem can occur when files, which are larger than 1GB, have been transmitted or are in the queue.

- CSCsc67631

  The multicast distribution priority weight balance may be skewed from day to day. This problem can occur because the scheduler is tracking the statistics for one day only. If there are large files being transferred over a low bandwidth, the scheduling could be skewed for the day.

- CSCsc83680

  New files cannot be pre-positioned and older files cannot be deleted because UNS fills up. This problem occurs because the file system has filled up to the point that UNS cannot even rewrite the required journal files.

- CSCsc83687

  Under the ext2 file system, cdnfs corruption causes a UNS directory to be assigned a regular filename, which takes up disk space that is not cleaned up by a cdnf clean up. This problem can occur if the Content Engine is running the ACNS 5.2.x or an earlier release.

- CSCsc83707

  All pre-positioned content is lost throughout the content distribution network. This problem occurs in the following situation. The root Content Engine fails and the temporary root takes over. However, the temporary root either cannot access the manifest file or cannot access the origin server (or both). Consequently, the temporary root deletes all of the content it previously had pre-positioned from the root Content Engine. Eventually all of the other Content Engines also delete all of their content.

DNS Resolved Caveats

- CSCeh41983

  The DNS process can stop responding after a corrupted DNS response is received.

- CSCeh82112

  The DNS service can crash or stop responding when it receives a certain type of maliciously coded DNS request from a client.

ICAP Resolved Caveats

- CSCeh96632

  The connection to the ICAP server is not terminated for up to 1.5 minutes after the server is unreachable. This problem occurs regardless of the keepalive timer setting.

- CSCei44203

  If you remove (unconfigure) the primary IP address of the ICAP server on the Content Engine, and then configure the backup IP address and attempt to add (configure) the primary IP address back, an error message is displayed:

  ```
  ContentEngine(config-icap-service)# server icap://x.x.x.x:1344/SWFICAP
  Error setting ICAP server (/cfg/gl/icap/servers/surfcontrol:icap:;;x.x.x.x.x:
  ```

- CSCei55485

  A TCP connection to the origin server is opened before the request is sent to the ICAP server. The origin server times out before the data transfer to the ICAP server and processing is completed.

- CSCei61774

  The ICAP process generates a core file if you delete the ICAP service from the Content Engine. This problem can occur if the Content Engine is running the ACNS 5.3.1 software or a later release. This problem was fixed in the ACNS 5.4.1 software release.

- CSCei83038

  If the Content Engine is running the ACNS 5.3.1 or ACNS 5.3.3 software, the ICAP daemon is logging errors and generates a core file. This problem was fixed in the ACNS 5.4.1 software release.

Management Resolved Caveats

- CSCeg59411

  To facilitate device group usage, the Contact and Location fields in the SNMP General window of the Content Distribution Manager GUI were moved to a new window under the Pages Configured for This Device Group.

- CSCeh19042

  In the HTTP Statistics window of the Content Distribution Manager GUI, the Hit Rate column can display a negative number for the device group even though the window displays the correct statistics for the individual Content Engines in the device group.

- CSCeh19440

  If you try to enter a value for the maximum group cached authenticated entries settings that is out of range for the specified hardware platform, the Content Distribution Manager GUI does not display a warning message that Content Engine's local settings will override the device group setting for the maximum HTTP authenticated caching setting if the specified setting exceeded the platform limit for a particular Content Engine that was assigned to that device group. In the ACNS 5.4.1 software release, this problem was fixed; in this situation, the Content Distribution Manager GUI now displays an icon to indicate that some of the Content Engines in this device group are using local settings.

- CSCeh48631

  The LocationApiServlet fails with a constraint exception when the name is not set.

- CSCeh55264

  The DeviceGroup TimeZone Settings with summertime set are overridden by each device in the device group. This problem can occur if the CMS agent that is running on the Content Engine fails to properly parse the time zone configuration on the device and reports the time zone as having been changed from that of the Content Distribution Manager configuration. This situation causes the values to be overridden. This problem only occurs for the default time zone of UTC.

- CSCeh57366

  If you are running the ACNS 5.0 or 5.1 software on the Content Distribution Manager and one or more of the registered Content Engines are running the ACNS 5.2.x or 5.3.1 software, the NTLM server may appear out of order when you check the running configuration on the Content Engine. This problem can occur if you have specified both the primary and secondary domain servers for one of these Content Engines (or for a group that contains one of these Content Engines) through the NTLM Server Settings window of the Content Distribution Manager GUI.

- CSCeh58488

  Clients receive a "Page cannot be displayed" error message when they access a site that requires NTLM authentication. This problem can occur with chunked-encoded responses and responses without a content length header.

- CSCeh60484

  If you perform a software download from the Content Distribution Manager GUI and the download file is larger than 1 MByte, the GUI displays an incorrect status message about the software download ("Download failed") while it is performing the software update.

- CSCeh60931

  If the CMS database tables are lost on a Content Engine that is registered with a Content Distribution Manager, the CMS service cannot start on the Content Engine even though the database and the acquisition and distribution tables still exist on the Content Engine.

- CSCeh83278

  When you configure an on-demand program for IP/TV-ACNS integration, the IP/TV Program Manager may issue an error message indicating that the manifest URL is invalid. This problem can occur if you enter a DNS name in the Manifest URL in the Channel Content section of the Content Distribution Manager GUI and the actual hostname of the IP/TV Program Manager does not match the specified DNS name.

- CSCeh89501

  A couple of misspelled words in the Content Distribution Manager GUI were fixed in the ACNS 5.4.1 software release. In the Channels Content window, “presedence” was changed to “precedence.” After you use the Capacity window to submit a change, “capcaity” was changed to “capacity” in the pop-up window that confirms that the specified change has been committed.

- CSCeh96563

  Because of insufficient error handling, the CMS service reconnects to the data server if the requested information (for example, the WMT license) is not found in the data server. (The data server is the service that maintains the current device configuration.) In this situation, the system log contains messages such as the following:

  ```
  May 6 13:52:50 P9ISCEN01 java: %CE-CMS-6-700001: ce(DataFeedPoll): Reconnecting to
  dataserver
  ```

- CSCei05765

  When you use the Content Distribution Manager GUI to view any of the statistics graphs (for example, Bytes Served, Bandwidth Efficiency Gain, Streaming Sessions, and CPU Utilization), the time axis is inaccurate. The reading is off by the UTC time of the local Content Engine or the Content Distribution Manager. This problem can occur if the Content Distribution Manager is configured to use a nonstandard time zone.

- CSCei26550

  Every 2 minutes, a registered ACNS device sends an RPC request to the Content Distribution Manager. When you enable a debug on the primary Content Distribution Manager, the debugging shows that these alarm updates are empty (the updated size is zero [0]):

  ```
  06/14/2005 05:39:20.849(Local) [D] cdm(RpcWorker-1): Processing partial alarm update
  from device ... events size 0
  ```

- CSCei44218

  A standby Content Distribution Manager goes offline when statistical records are being consolidated daily. This problem occurs only if the Content Distribution Manager is managing a large number of Content Engines (for example, a deployment of 1,400 Content Engines).

- CSCei47490

  The Content Engine fails to process an update that it received from the Content Distribution Manager and the errorlog/cms_log.current file contains a null pointer exception message.

- CSCei91572

  The order of the access control lists (ACLs) appear out of order in the Content Distribution Manager GUI after changes are made to the order of the ACLs even though the configuration on the device is correct. This problem occurs rarely.

- CSCsc29404

  The STATEFS fills up and causes the Content Distribution Manager to go offline. This problem can occur if the primary or standby Content Distribution Manager is part of a large network and the registered Content Engines are sending monitoring statistics, but the Content Distribution Manager is not effectively cleaning up the database. Those monitoring statistics bloat the database, fill up the STATEFS, and cause the Content Distribution Manager to go offline.

- CSCsc42378

  The Content Distribution Manager GUI shows a significant number of Content Engines that are offline. This problem can occur if there is a very large number of Content Engines deployed (over 1,400 Content Engines) and the Content Engines and the ACNS 5.2.3.9 software release is running on the Content Distribution Manager.

- CSCsc44742

  When a customized time zone and summertime zone have been configured, and then you attempt to delete this configuration from the Content Distribution Manager GUI, only the summertime zone configuration is deleted; the customized time zone is not deleted.

- CSCsc64327

  The Content Distribution Manager GUI does not respond. On rare circumstances, the internal system log processes will operate concurrently. This situation causes a deadlock, which causes the Content Distribution Manager GUI to become unresponsive.

Media and Streaming Resolved Caveats

- CSCef07860

  If you have used the **rtsp server cisco-streaming-engine broadcast id** global configuration command to configure an RTPS broadcast, and then you attempt to disable the broadcast by entering the broadcast ID (for example, iptv) as part of the **no rtsp server cisco-streaming- engine broadcast id** global configuration command, this message is displayed:

  ```
  ContentEngine(config)# no rtsp server cisco-streaming-engine broadcast id iptv
  ```

  In the ACNS 5.4.1 software release, you can now disable a CLI-configured RTSP broadcast by entering the broadcast ID as part of the **no rtsp server cisco-streaming- engine broadcast id** global configuration command.

- CSCeh20894

  The Content Engine cannot play a media file from a Windows Media Series 9.1 server. When the WMT Media player plays a media file from a Windows Media Series 9.1 server through the Content Engine, one of the following problems can occur:

  – The player will not play the media file from the Windows Media Series 9.1 server and enters into a buffer mode.

  – The Content Engine plays the media file partially and then enters into buffer mode repeatedly while it is playing the file.

- CSCeh40432

  When the source of a WMT alias is changed to another source URL, the clients do not reflect the changes. The client is still connected to the old source stream even though the changes have been made. The user is viewing a completely different stream than the one that is being sourced to the originating Content Engine. When using Windows media streams in a cascaded hierarchy (one Content Engine that is retrieving a stream from another and so on), if a client is retrieving a stream from an alias and the alias that it is pointing to is changed to a different source, the client stream is not updated.

- CSCeh41537

  The Windows Media player enters into a buffering state for managed live programs that are created with a broadcast publishing point as the source. This problem occurs with files that contain a large number of script events that are used as the source for creating the publishing point in a Windows Media server.

- CSCeh43420

  The cache process can crash and a core file can be generated on a Content Engine during a chunk-encoded object data transfer. When this problem occurs, the cache process is automatically restarted.

- CSCeh68970

  When the location leader for a WMT live multicast program fails, the other Content Engine (for example, CE2) in the same location does not start multicasting; however, it does serve the unicast request from the forwarder location.

- CSCeh72679

  Even though all of the NTLM credentials are provided, the proxy still fails authentication because the acquirer always uses unicode for the credentials.

- CSCeh79582

  The play duration is not available for pre-positioned media files. This problem can occur if the acquirer is used to acquire the media files and the play duration is not shown in the replication status and in the cdnfs lookup in the Content Engine.

- CSCeh94630

  The RealProxy administrator GUI shows garbled content. This problem can occur if you change the RealProxy configuration through the administrator GUI. A new window opens and displays garbled content.

- CSCei10904

  The output of the **show statistics wmt streamstat** EXEC command shows that the fast-cache acceleration bandwidth is being allocated for live HTTP requests. This problem can occur if the fast cache feature is enabled on the Content Engine for WMT request.

- CSCei24143

  The Windows Media player displays the following error message when a WMV file is requested: “Windows Media Player cannot connect to the server. The server name may be incorrect or the server is busy. Try again later.” The directory core_dir on the Content Engine contains a mms_server process core file. The Windows Media player might play the file if the cache is bypassed but the play duration might be incorrect.

  This problem can occur if the following situation exists: the Windows Media services is enabled on the Content Engine and the WMV file has incorrect ASF header information (for example, files that are encoded with “Flip4Mac WMV Export Component for QuickTime (Mac) Ver.1.0.3”).

- CSCei27384

  The ISO-MPEG4 compression uses more bandwidth than is necessary. A conditional check ensures the minimum quality of video by increasing the video bandwidth, irrespective of the value configured in the IP/TV Program Manager.

  The **Enforce ISO-MPEG4 Minimum Video Quality (BCS corrects Bandwidth for Best Results)** option has been added to the IP//TV Program Manager page. This new option allows you to specify whether or not the Broadcast Server should follow the user-specified bandwidth settings. If this new option is disabled, the Broadcast Server will use the user-specified bandwidth settings.

- CSCei31433

  The Cisco Streaming Engine crashes on the Content Engine. This problem can occur if the Content Engine is booted and has been configured to use the Cisco Streaming Engine in its bootup configuration (the **rtsp server cisco-streaming-engine enable** command has been specified on the Content Engine).

- CSCei52366

  When multiple users play the WMT VoD content and continuously press their player control buttons (for example, the rewind and forward button), the data server can exit and cause the Content Engine to restart.

- CSCsb81485

  Files that are part of an asx playlist file can be truncated. This problem can occur when HTTP is the protocol used to play the asx playlist file.

- CSCsc45064

  By default, the ACNS 5.x software distributes Session Description Protocol (SDP) content using HTTP to dynamically generate subsequent SDP over RTSP. In the ACNS 5.4.1 software release, the Cisco Streaming Engine can now retrieve SDP content using HTTP for CLI-based programs.

- CSCsc49964

  When streaming with the MMS protocol, the mms_server generates a core file if it receives an unusual port string (for example, a port string of "\\0.0.43008.3221225472\TCP\0" instead of "\\10.40.1.20\UDP\2488") from the client.

- CSCsc45089

  An ACNS 5.x RTSP PacketVideo stream expires after 3 hours and cannot reconnect.

- CSCsc46435

  When the MMS protocol is used, the **block** rule action does not work for pre-positioned content.

Proxy and Caching Resolved Caveats

- CSCef90286

  The Content Engine returns HTTP 1.1 content instead of HTTP 1.0 content to HTTP 1.0 client browsers. This problem occurs because the Content Engine cannot recognize the difference between HTTP 1.1 and HTTP 1.0 client requests. The Content Engine sends HTTP 1.1 content in response to HTTP 1.0 requests.

- CSCeg27152

  The clients of HTTP or streaming services may see broken pages or broken connections. This problem can occur because the Content Engine enters or exits a WCCP cache farm, which can result in inconsistent views of bucket ownership on the Content Engines in the cache farm.

- CSCeg36621

  File transfers of large files fail and connection reset error messages are generated. This problem occurs with HTTP, native FTP, and FTP-over-HTTP proxies (Content Engines) that are running the ACNS 5.2.x and 5.1.x software. This problem was fixed in the ACNS 5.4.1 and 5.2.7 software releases.

- CSCeh00314

  In the case of WMT live and content routing, the HTTP failover URL does not work. In the case of a WMT live using content routing, the client is redirected to the Content Engine after the initial communication between the client and the Content Router. When the Content Engine receives this request, it sends the client an .asx file that contains two URLs (an MMS URL and an HTTP URL). In the case of WMT live, this HTTP URL is not valid. If the client fails over to this HTTP URL if the MMS URL fails, the stream will not be served by the Content Engine. This problem was fixed in the ACNS 5.4.1 software release.

- CSCeh02627

  If a POST request includes an “Expect: 100 Continue” response, the Content Engine can experience problems in processing these POST requests properly.

- CSCeh15968

  The client receives an unexpected 400 bad request HTTP response from the origin server when the request is going through a Content Engine. This problem can occur if the client sends an unnecessary carriage return/line feed (\r\n) in between the end of one request and the beginning of another request. These extra characters have been seen using the following version of the browser: Internet Explorer Version 6.0.2800.1106.xpsp2.040919-1003, Cipher Strength: 128-bit, Update Versions: SP1, Q832894, Q837009, Q831167, Q823353, and Q871260.

- CSCeh30618

  The **ip domain name** *domain name* global configuration command does not allow the domain name to start with a number. The command requires that the domain names begin with a letter and then only contain numbers and letters. An example is as follows:

  ```
  ContentEngine(config)# ip domain name 123abc.mydomain.com
  Illegal domainname 123abc.mydomain.com.
  Valid domainname can contain only alphanumerics, hyphen and dot.
  ```

  In the ACNS 5.4.1 software release, the **ip domain name** *domain name* global configuration command was modified to allow domain names that begin with a number.

- CSCeh31352

  The cache process generates a core file. This problem can occur under the following situation:

  a. The Content Engine has NTLM request authentication enabled.
  b. One client (client A) requests an NTLM protected object from an origin server.
  c. Another client (client B), whose user belongs to 500 groups, requests a plain object such as www.yahoo.com.
  d. While client B is still waiting for all the groups to be retrieved, client A sends a request to www.google.com for plain objects.

- CSCeh48360

  The **rewrite** rule action fails for WMT requests if the **no-proxy** rule action is also configured for a matching pattern. This problem causes the **no-proxy** rule action to be executed first instead of the **rewrite** rule action. An example is shown as follows:

```
ContentEngine# show rule all
Rules Template Configuration
----------------------------
Rule Processing Enabled
Actions :
rule action rewrite pattern-list 5
rule action no-proxy pattern-list 7
Pattern-Lists :
rule pattern-list 5 group-type or
rule pattern-list 5 url-regsub (mms.*://www.wm-server-1.com).* \1/pinball.wmv rule
pattern-list 7 group-type or rule pattern-list 7 dst-ip 10.77.157.169 255.0.0.0
```

  In this case, 10.77.157.169 is the IP address of the www.wm-server-1.com.

  If a request is given for mmst://www.wm-server-1.com/100kbs.wmv, it must be rewritten to the URL mmst://www.wm-server-1.com/pinball.wmv. However, because the no-proxy action is executed first, such a rewrite does not occur.

- CSCeh55335

  If the **http cache-vary-user-agent enable** global configuration command has been entered on the Content Engine, the cache process can crash on the Content Engine.

- CSCeh69442

  The Content Engine does not cache the content and does not receive any requests even though the router is redirecting traffic to the Content Engine. This problem can occur if the request header line in the packet is greater than 8 KB. This problem causes the Content Engine to reset the connection, and an entry is created for the bypass list.

- CSCeh73714

  The cache process stops and the output of the **show tech-support** EXEC command shows a back trace.

- CSCeh90745

  WCCP goes into bypass mode and bypasses a large number of connections. This problem can occur in the following situation. The Content Engine receives a large number of connections over WCCP, and a substantial number of these connections are proxy-style requests. If the **http proxy incoming 80** global configuration command has not been entered on the Content Engine, these connections result in “wrong destination address in proxy mode” errors. If too many of these errors occur, the Content Engine goes into overload bypass mode because it assumes that there is an overload situation.

- CSCei04882

  Certain requests (for example, when you click on links from the results of a Goggle search) to the Content Engine time out without any response from the Content Engine. This problem can occur if all of the following conditions exist:

  a. The server response is noncacheable.

  b. The server transfer encoding is chunked.

  c. The Content Engine is configured to keep a persistent connection with the server.

  This problem was fixed in the ACNS 5.4.1 software release.

- CSCei13929

  Websense configurations (for example, the downloaded database and license information) are lost. This problem occurs only if you use the Content Distribution Manager GUI to perform the Websense configuration.

- CSCei17023

  More than a 60-second delay occurs before the LDAP prompt is sent to a client.

- CSCei54044

  When the ACNS web proxy is being used, users cannot successfully authenticate themselves with internal websites that use NTLM authentication.

- CSCsb50371

  The Content Engine may stop authenticating users if there is a heavy load of LDAP authentication requests.

- CSCsb60793

  When users initially open their browsers, they can experience more than a 60-second delay before they are able to browse. This problem can occur if the proxy autoconfiguration feature is enabled on both the browser and the Content Engine and the client points to a DNS name that resolves to multiple Content Engines. This situation can cause a looping between the Content Engines before the client will receive the proxy.pac file.

- CSCsb69744

  The caching application on the Content Engine experiences critical memory shortfalls that can cause the Content Engine to enter into an overload bypass condition. In the errlog-cache-* files, there are messages that indicate the Content Engine has experienced “desperate” low memory conditions.

- CSCsb81144

  The cache process generates a core file and then restarts. This problem can occur with certain pass-through NTLM requests.

- CSCsb83342

  The Content Engine hangs and does not authenticate NTLM users or pass-through traffic. The command output of the **show statistics ntlm** EXEC command shows the state of the NTLM servers as “DEAD.” This problem can occur if the Content Engine is running NTLM or some other type of authmod authentication.

- CSCsc04029

  The syslog on the Content Engine contains numerous occurrences of the following error messages:

  ```
  %CE-UNKNOWN-3-899999: Failed to get client name: error 18
  %CE-UNKNOWN-3-899999: Failed to initialize request info
  ```

  This problem can occur if SmartFilter is enabled on the Content Engine.

- CSCsc06687

  A user with the username of “root” is not allowed FTP access to the Content Engine. This problem occurs if the username “root” is used when the user sends an FTP request to the Content Engine.

- CSCsc16232

  Some of the **show stat http** EXEC commands might return an error. This problem can occur because the cache process has been restarted.

- CSCsc19552

  If there are “Force pool type 2: desperate” error messages in the Content Engine’s cache error log, the Content Engine goes into cache bypass mode. After the Content Engine enters into cache bypass mode, the “WCCP: Overload message received by wccp” message is repeatedly sent to the Content Engine’s system log (syslog).

- CSCsc47814

  Requests for objects, which are not pre-positioned and are redirected by a Content Router, fail if you configure the IP address as “OriginServer in Website” in the Content Distribution Manager GUI.

- CSCsc49557

  If the LDAP server is unavailable and the LDAP allow mode is enabled on the Content Engine, the Content Engine fails to retrieve the requested objects and receives an authentication failure message.

- CSCsc56266

  The cache process generates a core file. This problem can occur if the Content Engine performs a lookup in the dfs - mem_hash_lookup list.

- CSCsc58252

  A mask is not assigned to a WCCP farm of Content Engines, and the WCCP view continuously changes. This problem can occur if the WCCP farm changes before a mask is assigned to any of the farm’s Content Engines.

Rules Resolved Caveats

- CSCee56298

  Blank spaces are not allowed in a rule group name even though a blank space is allowed in an access list group name (for example, the **access-lists 300 permit groupname "CNBU1.LOCAL\Domain Users"** global configuration command accepts the “Domain Users” as a group name even though it contains a blank space). In the ACNS 5.4.1 software release, support for a blank space in a rule groupname string was added.

- CSCeg50621

  If you use the Content Distribution Manager GUI to create a rule for the **use-proxy** rule action for a device group and you specify the hostname in the rule, the Content Distribution Manager GUI displays a new rule for the assigned Content Engine after the rule is processed on the Content Engine. In the hostname field, the hostname is replaced by the IP address because the specified hostname is translated to an IP address after the rule is processed on the Content Engine. The CMS Local Central Management reports this change in the CLI to the Content Distribution Manager as a different rules record. This problem was fixed in the ACNS 5.4.1 software release.

- CSCeh34039

  The **no proxy** rule action does not work for transparently redirected proxy-style requests. This problem occurs if a pattern has been configured for a domain name (for example, abccorp.com), and a request is given to a source that is not a fully-qualified domain name (for example, http://www). This problem was fixed in the ACNS 5.4.1 software release.

Software Upgrade and Downgrade Resolved Caveats

- CSCeh37469

  You cannot configure the Websense server because of a synchronization problem. The output of the **show running** EXEC command shows that there are not any websense server configurations on the Content Engine, but the output of the **show websense-server** EXEC command shows that several websense components are installed on the Content Engine.

  The problem can occur if you upgrade from the ACNS 5.2.x software to the ACNS 5.3.x software before there are any Websense server configurations on the Content Engine. This problem was fixed in the ACNS 5.4.1 software release.

- CSCei54938

  After you upgrade from the ACNS 5.1.x to the ACNS 5.3.x software, the multicast expert configuration files are lost. This problem was fixed in the ACNS 5.4.1 software release.

- CSCei75601

  If a registered Content Engine is running the ACNS 5.3.3 software, and you downgrade it to the ACNS 5.2.7 software, the Content Engine loses its standby configuration (its standby group configuration) and is reachable only through the console. This problem was fixed in the ACNS 5.4.1 software release.

Other Resolved Caveats

- CSCdy02581

  When GRE encapsulation or Layer 2 redirection is being used, the Content Engine can drop the redirected packets because it does not handle bypassed connections properly.

- CSCeg50167

  The Content Engine is not appending an “X-Forwarded-for:” header to the HTTP request. This problem can occur if the **http append x-forwarded-for-header** global configuration command has been entered on the Content Engine and the HTTP request already has an “X-Forwarded-for:” header.

- CSCeh13038

  When a range of multicast addresses is configured, the multicast range is not used correctly. A live program uses two multicast destination addresses instead of using only one multicast destination address.

- CSCeh19530

  In rare circumstances, the CE-511 and CE-566 models can lock up. The syslog does not indicate any kernel crash or other problems that might explain the cause of such lockups. In this situation, these Content Engines disconnect from the network and do not respond to the console. The Content Engine does come back up after a power cycle. This problem was fixed in the ACNS 5.4.1 software release.

- CSCeh29538

  In the ACNS 5.3.x software and earlier software releases, administrator-restricted APIs only considered the username and not the role of the user when determining if the user should be granted access to the API. In the ACNS 5.3.x and earlier software releases, only users who have the username of admin can access these administrator-restricted APIs. In the ACNS 5.4.1 software release, users who have “admin” as one of their roles can access these administrator-restricted APIs.

- CSCeh34279

  The Content Engine does not export the transaction logs when the transaction log export feature is enabled. This problem occurs only if Cisco Streaming Engine logs files are in the /local1/logs/cisco-streaming-engine directory.

- CSCeh48047

  The Content Engine stops responding or enters kernel debug mode when there is high memory usage for TCP.

- CSCeh48187

  In rare circumstances, the Content Engine may not let anyone log in. This problem occurs only if all of the following conditions exist:

  – The system file system (sysfs) is not mounted on the Content Engine.

  – TACACS or RADIUS is enabled on the Content Engine and is the primary authentication mechanism.

  – Authentication failover is configured on the Content Engine.

  – The network is up and the TACACS or RADIUS server is reachable.

  This problem was fixed in the ACNS 5.4.1 software release.

- CSCeh66703

  The CLI configurations that were specified through the **ip route** global configuration command are not retained on an NM-CE model after the device is reloaded.

- CSCeh69177

  A "Critical: Disk failure error occurred on *disk drive in Storage Array number*" alarm is displayed on the Content Distribution Manager even though the disk has not really failed. The syslog.txt shows that the disk is reset and has returned to normal operation shortly after the alarm is raised, but the alarm is not reset.

  If you enter a **show disks details** EXEC command, the command output shows the state of the drive as normal. If the drive is bad, the command output of the **show disks details** command would show that there is a problem with the disk. This problem occurs only on storage arrays that are attached to a model CE-7325 that is running the ACNS 5.2.3 software. This problem was fixed in the ACNS 5.4.1 software release.

- CSCeh90085

  The media file system (mediafs) is borrowing more file space from the ACNS network file system (cdnfs) disk space than it should. The mediafs and cdnfs statistics files indicate that the underlying file system (which is shared by cdnfs and mediafs) is 100 percent full. Even though mediafs should only be allocated approximately 20 GB of space, the output of the **show statistics mediafs** EXEC command shows that mediafs is consuming over 30 GB. This problem can occur when mediafs is configured to use unused cdnfs disk space.

- CSCei04025

  You cannot log on to the Content Engine and messages about mingetty being killed by signal 25 are being generated. This problem can occur if the debug authentication feature (you have entered the **debug authentication user** EXEC command) has been enabled and is not disabled.

- CSCei05034

  NTLM failover does not work properly. Client requests can take approximately 2 minutes to time out because of an authentication failure and the Content Engine never detects the domain controller (DC) failure.

  This problem can occur if both of the following conditions exist:

  a. NTLM request authentication is enabled on the Content Engine.

  b. The domain controller service hangs but the domain controller hardware is still operating.

- CSCei06416

  When a data server crash occurs, a core file is not generated.

- CSCei33461

  Certain network modules, which are running the ACNS software, do not respond to MIB queries.

- CSCei35930

  A higher than normal CPU utilization on multiple Content Engines in a WCCP farm occurs and the performance is slow because fragmented GRE packets are bounced between the two Content Engines (CE1 and CE2). The number of received GRE packets increases at a high rate and the amount of GRE traffic significantly increases between CE1 and CE2.

  This problem can occur in the following situation:

  – CE1 and CE2 are in a WCCP farm that is performing Layer 2 redirection or IP spoofing, and the slow-start or flow protection feature is enabled on CE1 and CE2.

  – CE1 and CE2 are running the ACNS 5.3.1 or ACNS 5.3.3 software, which introduced the ability to fragment GREs at the Content Engine, but which did not enable the Content Engine to receive GREs.

  – A large packet comes to CE1 or CE2 for a flow that the other Content Engine might be handling. CE1 fragments the GRE and sends it to CE2, which bounces it back to CE1. The fragmented GRE continues to bounce between CE1 and CE2.

- CSCei39177

  The SNMP agent on a Content Engine stops responding to MIB queries and the only workaround to this problem was to restart the snmpced process.

- CSCei45817

  The core file is generated by the dispatcher process.

- CSCei61443

  When you terminate a Telnet session, the “Hang up” notification or signal is not sent to all the processes that were started during the session. If a tcpdump process is started during the Telnet session, it is not terminated when you disconnect from the Telnet session.

  This problem was fixed in the ACNS 5.4.1 software release. The “Hang up” signal is now sent to all of the child processes that were started from the session. As a result, the tcpdump process that might have been started during a session is automatically terminated when you disconnect from the Telnet session.

- CSCei75386

  The Content Engine reloads within a few seconds to minutes after a lower MTU size is configured either manually or because the startup configuration is parsed.

- CSCei92552

  The transaction logs that reside in the directory that are at the leaf level cannot be accessed by nonroot users because these directories do not have permissions for nonroot users. Because WMT has its transaction logs inside a separate folder in logs/wmt/export, nonroot users cannot access the WMT transaction logs.

- CSCsb38357

  The Apache HTTP server versions 2.0 through 2.0.46 are vulnerable to a denial of service attack. By initiating multiple subsequent internal redirects and nested subrequests, a local attacker can cause the server to enter into an infinite loop and crash.

- CSCsb44655

  The Content Router's default coverage zone file contains a netmask of 0.0.0.0/0 for the Content Engine.

- CSCsb61576

  The netstat process crashes on the Content Engine and there are negative inode numbers (when you enter the **show tech-support** EXEC command, the command output for the netstat information shows negative inode numbers).

- CSCsb62511

  The Invalid request method (2/4) for the 100-Continue response informational message fills up the Content Engine's system log.

- CSCsb74965

  When using HTTP custom error pages to return specific values to a client, certain options do not work properly. Specifically, no values are returned to the client if you use the %h (cache hostname) and the %M (request method) argument specifiers for the error signature).

- CSCsb82347

  Users cannot access certain directories under the logs directory and the error log directory if they are trying to access the directories through nonadministrative secure FTP (SFTP). In the ACNS 5.4.1 software release, the proper permissions were added to allow nonadministrative users to access these directories.

- CSCsb85147

  Because the default logging level of the Content Engine is a warning, the AddedProp error message is filling up the system log (syslog) on the Content Engine. This problem was fixed in the ACNS 5.4.1 software release where the priority of the AddedProp error message was changed from a warning to a debug.

- CSCsb85415

  The values in the Monitoring graphs in the Content Distribution Manager GUI dip to a very low value even though all of the registered Content Engines are reporting statistics to the Content Distribution Manager.

- CSCsb86324

  If the Content Engine has been configured to use the default RADIUS authentication port, port 1645, the **show running** EXEC command does not show the configured RADIUS authentication port number.

- CSCsb91566

  If a user attempts to log in with an invalid username and TACACS+ is being used for user login authentication, a core file can be generated.

- CSCsc00862

  When an interface switchover occurs within a standby group, a transient minor alarm on the ex-active interface is generated and cleared when the switchover is successful. This problem was fixed in the ACNS 5.4.1 software release where an alarm is generated only when the switchover is not successful.

- CSCsc04930

  Certain warning messages about low memory can occur with normal usage and transient load spikes. In the ACNS 5.4.1 software release, the wording for these logging messages was modified.

- CSCsc13494

  A disk is marked as bad when a disk error threshold is reached after a transient disk failure. This problem occurs only rarely and can only occur if the Storage Array device is attached to a model CE-7325 that is running the ACNS 5.3.3.8 software or a later release. This problem was fixed in the ACNS 5.4.1 software release.

- CSCsc21712

  The Content Engine's system log contains numerous occurrences of the following illegitimate error message:

  ```
  %CE-WMT-2-512071: uns_uns_get_ServerFlags error case: server_flags: 128
  ```

  This problem can occur if you have enabled the URL case insensitivity setting for playback (you have enabled the setting that specifies that the case of the URL should be ignored when playing back content), or you have used the Content Distribution Manager to enable the pure DNS routing setting in the website for the channel. Although these two settings are legitimate settings, the error message is not legitimate. In the ACNS 5.4.1 software release, this illegitimate error message is no longer logged if either or both of these settings have been specified.

- CSCsc22370

  If your manifest file is a crawl and you change the website page setting that indicates whether the case of the URLs should be ignored during the playback of content (you set or clear this setting), when the manifest file is executed, all of your content will be replicated again and the Content Distribution Manager GUI does not display a warning that this replication has started.

- CSCsc38791

  The client browser receives an Unsupported Request Method error message page because of a 400 bad request. This problem can occur if NTLM authentication and persistent connections are enabled on the Content Engine and the Content Engine is running the ACNS 5.3.3 software release.

Related Documentation

Your product shipped with a minimal set of printed documentation. The printed documentation provides enough information for you to install and initially configure your product.

Product Documentation Set

In addition to these release notes, the following documents are included in the product documentation set:

- *Documentation Guide and License and Warranty for Cisco ACNS Software, Release 5.4.x*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*

Refer to the *Documentation Guide and License and Warranty for Cisco ACNS Software, Release 5.4.x* for a complete documentation roadmap and URL documentation links for this product.

Hardware Documentation

- *Cisco Wide Area Application Engine 511 and 611 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7326 Hardware Installation Guide*
- *Cisco Content Engine 7305 and 7325 Hardware Installation Guide*
- *Cisco Content Engine 511 and 566 Hardware Installation Guide*
- *Cisco Content Engine 510 and 565 Hardware Installation Guide*
- *Cisco Content Engine 500 Series Hardware Installation Guide*
- *Cisco Content Distribution Manager 4630 Hardware Installation Guide*
- *Cisco Content Router 4430 Hardware Installation Guide*
- *Cisco Content Networking Hardware Installation Guide for the Seven-Rack Unit Chassis*

Software Documentation

- *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x*
- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.4*
- *Cisco ACNS Software Command Reference, Release 5.4*
- *Cisco ACNS Software API Guide, Release 5.4*
- *Cisco ACNS software Program Manager for IP/TV User Guide, Release 5.4*
- *Release Notes for Cisco ACNS Software Program Manager for IP/TV, Release 5.4*

Online Help

- Content Distribution Manager GUI online help system for centrally managed ACNS networks
- Content Engine GUI online help system for locally deployed Content Engines

Note The term *locally deployed Content Engine* refers to a Content Engine that was initially configured with the autoregistration feature turned off so that the Content Engine would not automatically register with the Content Distribution Manager. Because the Content Engine did not register with the Content Distribution Manager, it can be individually managed through the Content Engine CLI or GUI as a locally deployed device. The Content Engine GUI allows you to remotely configure, manage, and monitor locally deployed Content Engines through your browser.

The Content Distribution Manager GUI and the Content Engine GUI both have context-sensitive online help that can be accessed by clicking the **HELP** button.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.