Release Notes for Cisco Internet Streamer CDS 2.6.1

These release notes cover Cisco Internet Streamer CDS Release 2.6.1-b21.

Note Release 2.6.1-b21 obsoletes all previous builds of Release 2.6.1.

Revised: April 2012, OL-23610-05

Contents

The following information is included in these release notes:

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

New Features

Release 2.6.1 of the Cisco Internet Streamer CDS introduces the following features:

NAS

Network-attached Storage (NAS) is supported as a read-only storage respository at the root location (Content Acquirer) in the CDS. Content is written to the NAS by an external agent, such as the Origin Server, a publishing subsystem, or a data storage application. The NAS offers a "new content category," similar in characteristics to dynamically-cached content, which does not require metadata attachment.

Note NAS is only supported in lab integrations as proof of concept.

The following rules apply to NAS support in Release 2.6.1:

- NAS cannot be used as a source for prefetched or hybrid content.
- Only content serviced by the Web Engine is supported (HTTP content and Flash Media Streaming).

  Note NAS for Windows Media Streaming and Movie Streamer is not supported.

- Only Network File System (NFS) mounts are supported for acquiring content from the NAS.
- Content acquired from the NAS is not written to local storage on the SEs at the root location; when reading content, NAS is considered an extension of the local file system.
- If there is more than one SE in a root location for a delivery service, then the SE that acquires the content from NAS is based on a hash of the content URL (similar to dynamically-cached content).
- NFS share can be mounted from multiple IP addresses simultaneously.
- Multiple mounts for the same volume on a NAS is supported.
- NAS should be colocated with the SEs at the root location; if WAN link is used, then WAN link failover scenario should be provided.
- IP address failover by the NAS should be implemented to avoid service disruption.
- NAS is not applicable to live streaming
- NAS lookup is tried before pulling content from the Origin Server
- When Web Engine performs FastCAL lookup, NAS file lookup is performed first; followed by cached content, then prefetched content.
- In a cache-miss scenario, the Origin Server is queried last.

Note Ingress traffic from NAS mounts is not distributed evenly over port channels. Separate interfaces can be used for NAS outside of the port-channel configuration to achieve better load balancing. Ingress traffic to the CDS is determined by the switch, this applies to all application traffic over port channels.

Network traffic performance can be impacted by too small a value for the TCP parameter: net.inet.tcp.rexmit_slop. If it is determined that network throughput performance is impacted, the net.inet.tcp.rexmit_slop value on the NAS server should be reviewed.

The permissions for directories on the NAS-mounted file system should be a minimum of "read" and "execute" by *others*, and files on the NAS-mounted file system should be a minimum of "read" by *others*.

For example, a directory permission at a minimum should be:

```
dr-xr-xr-x
```

and a file permission at a minimum should be:

```
-r--r--r--
```

If access to a NAS-mounted content results in a 500 error, the permissions of the files should be verified.

Configuring NAS

Configuring NAS in the CDS consists of the following tasks:

1. Create a NAS XML file.
2. Register the NAS XML file with the CDSM by uploading or importing the file.
3. Associate the NAS XML file with a Content Origin.

For information on these tasks, see the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide*.

NAS Mount Removal

When removing NAS mounts, the SE configuration should be updated before the NAS IP addresses are removed.

Note Any NAS mount changes should be performed in a maintenance window to avoid service disruption.

To remove NAS mounts, do the following:

Step 1 Remove from the NAS XML file the IP addresses that are to be removed from the NAS server.

Step 2 Update the NAS XML configuration file in the CDSM GUI.

a. Register the updated NAS XML file with the CDSM by choosing **System > Configuration > NAS File Registration**.

b. Associate the NAS file with the Content Origin of the delivery service by choosing **Services > Service Definition > Content Origins**.

Step 3 Verify the configuration has been propagated to each SE in the delivery service by entering the **show content-origin** command on each SE in the delivery service.

Step 4 Remove the IP addresses on the NAS server.

Monitoring NAS

NAS share states are checked every few seconds. If NAS mounts fail, alarms and syslog messages are generated. The CDS supports failure-retry of the NAS.

CLI show Commands

The following CLI show commands provide information about the NAS state:

- **show content-origin** [**request-fqdn** <*domain*>]—Displays information about the NAS mount
- **show statistics web-engine**—Displays NAS hit count as "External Hit"
- **show statistics flash-media-streaming**—Displays NAS hit count as "External Hit"

Alarms

Alarms are viewable through the CDSM GUI Alarms table or through the SE CLI.

The following alarms are displayed in the **show alarms** command:

```
Minor Alarms:
-------------
     Alarm ID             Module/Submodule     Instance
     -------------------- -------------------- ------------------------
   1 nas_offline          sysmon               14.1.2.12:/data
   2 nas_offline          sysmon               14.1.2.12:/data@10.11.12.13
Major Alarms:
-------------
     Alarm ID             Module/Submodule     Instance
     -------------------- -------------------- ------------------------
   1 nas_failure          sysmon               14.1.2.13:/data
   2 nas_failure          sysmon               14.1.2.14:/ifs/data
   3 nas_failure          sysmon               14.1.2.15:/data
```

Syslog

The following syslog messages are displayed if the NAS mount fails:

```
Cds Origin Manager writes syslog messages when NAS mount fails. Below are some sample
syslog messages:
Apr 28 04:25:26 nas-se CdsOriginMgr: %SE-CdsOriginMgr-3-802100: Failed to mount NFS vod/0
for NAS share 14.1.2.12:/ifs/data
```

FastCAL

The Content Abstraction Layer (CAL) library provides an interface to the Content Delivery Network File System (CDNFS). The CAL library monitors the content in the CDNFS and communicates with the Ucache process to evict less popular content. In Release 2.6.1, the Ucache process is replaced with the Content Manager process for all protocol engines and modules. See the "Content Manager" section on page 5 for more information.

Release 2.6.1 introduces the Fast Content Abstraction Layer (FastCAL) library to provide quick response time for high-performance Web Engine create, update, lookup, and delete operations. All other protocol engines and modules, including live streaming for Flash Media Streaming and RTSP gateway,

continue to use the CAL library and Unified Namespace (UNS) process. Flash Media Streaming VOD (prefetched, hybrid and dynamically cached content) use FCAL by way of the Web Engine. FastCAL communicates with the Content Manager for popularity tracking. Lookup notifications are also sent from FastCAL to the Content Manager.

Note As part of the upgrade to Release 2.6, all disks (including CDNFS disks) are reformatted. For information on the upgrade procedure, see the *Cisco Internet Streamer CDS 2.6 Software Upgrade Guide*

FastCAL also supports the Network-Attached Storage (NAS) feature. See the "NAS" section on page 2 for more information about this feature.

For more information about the FastCAL disk path, disk allocation, and bucket allocation, see the "FastCAL" section in the "Product Overview" chapter of the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide*.

CLI Changes

The following commands change for the Web Engine with the introduction of FastCAL and Content Manager:

- **cdnfs browse**—Used to browse the CDNFS directories and files, no longer displays cached content for the Web Engine or for Flash Media Streaming in Release 2.6.1. Instead, only cached content for Windows Media Streaming and Movie Streamer, and prefetched content are displayed. To display cached content, use the **show cache content** command.

  Note The **show cache content** command output does not display priority (also known as popularity) of cache content in Release 2.6.1 To see popularity ranking, use the **show content-mgr content cache** command or view the content-manager transaction log.

- **cdnfs cleanup**—Used to cleanup unwanted entries in CDNFS, is deprecated in Release 2.6.1 in the following manner. When an SE is removed from a delivery service, Content Manager removes all cache content for that delivery service. All prefetched content for that delivery service is removed by the Acquisition and Distribution process. However, if the Acquisition Distribution process fails because of an SE being offline or for any other reason, then the **cdnfs cleanup** command is still required to remove the prefetched content.

Content Manager

As part of FastCAL, the Content Manager module is introduced, which replaces the Ucache process. Content Manager keeps track of all the files in CDNFS, and maintains all content popularity information and stores it in a snapshot file. Content Manager includes the following enhancements:

- Improve cache content storage from 10 million to 20 million content objects
- Increase maximum length of URL to 2048 characters
- Continue to manage cache content objects for all protocol engines
- Maintains share memory containing disk related information
- Monitors disk usage periodically and starts eviction when usage exceeds threshold
- Receives updates on disk information based on CMGRSlowScan process, which scans the entire system over a 12-hour period
- Receives updates on each disk during start-up from CMgrSnapshotReader

In Release 2.6.1, the upper limit of the maximum number of content objects on the SE has increased from 10 million objects to 20 million objects. The default value has increased from 3 million to 20 million. If the maximum number of content objects was configured using the **cache content max_cached_entries** command in Release 2.5.9 or later, this value is retained in Release 2.6.1. If the maximum number of content objects was not configured, the default value of 20 million content objects is applied.

For more information about the Content Manager, see the "Content Manager" section in the "Product Overview" chapter of the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide*.

Transaction Log

The Content Manager transaction log filename has the following format:

content_mgr__<*ipaddr*>_*yyyymmdd_hhmmss*_<>, where:

- <*ipaddr*> represents the IP address of the SE, SR, or CDSM.
- *yyyymmdd_hhmmss* represents the date and time when the log was created.

The Content Manager transaction log file is located in the /local1/logs/content_mgr directory.

Table 1 describes the fields for the Service Monitor transaction log on an SE.

Table 1 Content Manager Transaction Log Fields

Field	Description
Date	Date of log entry.
Time	Time of log entry.
ContentType	Type of content, which is either cached or prepos-content (prefetched).
Operation	Content Manager operation, which is addition, deletion, update, or eviction.
Priority	Prefetched content always has a priority of 0, which means ignore. The lower the number, the lower the priority.
CreationDate	Date the content object was created.
CreationTime	Time the content object was created.
FileSize	File size, in bytes, of the content object.
HitCount	Number of times the content object was accessed.
URL	URL of the content object. If Content Manager cannot retrieve the URL by using the FastCAL lookup of the disk path, then the ContentType field has a value of "unknown-content" and the URL field displays "-."
Path	Disk path of the content object.

CLI Changes

The following commands have been added or modified for Content Manager:

```
# content-mgr disk-info force-reset
(config)# cache content max-cached-entries <1-20000000>
(config)# cache content eviction-preferred-size
(config)# cache content eviction-protection
(config)# contentmgr hitcnt-decay-half-life
```

The following show commands have been added or modified for Content Manager:

```
# show cdnfs usage
# show cache content
```

```
# show content
# show content-mgr
# show content-mgr health-info
# show content-mgr disk-info
# show content all
# show content url
# show content diskpath
# show content last-folder-url
# show statistics content-mgr
# clear content last-folder-url
# clear content url
# clear cache content
# clear content
# clear cache all
```

For information about the changed commands, see the *Cisco Internet Streamer CDS 2.6 Command Reference*.

CDSM GUI Changes

To configure the Content Manager settings through the CDSM GUI, choose **Devices > Devices (SE) > General Settings > Content Management**. The Content Management page is displayed with the following fields:

- Max Cache Content Entries—Range is 1–20,000,000, default is 20,000,000
- Cache content eviction preferred size—Drop-down list options are: large or small
- Enable Eviction Protection check box—Unchecked (disabled) by default
  - Minimum cache entry size to protect—Drop-down list options are 100 MB, 500 MB, 1 GB, and 4 GB
  - Minimum duration to protect the content from eviction—Drop-down list options are: 1, 2, 3, or 4 hours
- Hit Count Decay Half Life—Range is 1–30, default is 14 days
- Threshold of Disk Failures Per Bucket—Range is 1–100 percent, default is 30 percent

Error Logs

The following error logs have been added or modified for Content Manager:

- ContentMgr process errorlog—Directory path is ~/errorlog/content_manager.current
- CMGRSlowScan process errorlog—Directory path is ~/errlog/cmgr_slow_scan.current
- CMgrSnapshot process errorlog—Directory path is ~/errlog/cmgr_snapshot.current
- Command errorlog—Directory path is ~/errlog/fcal_util.current

Web Engine Integration with FastCAL

Web Engine calls FastCAL directly for content creation, lookup, update, and deletion. See the "Web Engine" section on page 9 for information on Web Engine and Windows Media Streaming requests, and other new features of Web Engine.

Alarms

Web Engine generates the cal_diskwrite_exceed minor alarm if the outstanding writes are greater than the threshold, which is set to 3000 for the CDE250-2S6 and CDE250-2M0, and 1500 for all other CDEs.

Web Engine generates the cal_lookup_exceed minor alarm if the outstanding lookups are greater than the threshold, which is set to 25,000 for the CDE250-2S6 and CDE250-2M0, and 15,000 for all other CDEs. The Service Router does not redirect any HTP requests to an SE with this alarm raised. The alarm is cleared when the number of lookups is reduced to 24,000 for CDE250s and 14,000 for all other CDEs.)

UNS Integration with FastCAL

UNS is the process that is called by other modules like CMS, Acquisition and Distribution, and Streamscheduler to access the CDNFS content by way of the CAL–UNS client library. UNS still handles Movie Streamer and Windows Media Streaming content (both prefetched and cached), and live streaming content for Flash Media Streaming.

UNS uses FastCAL for any disk-based operation. Content Manager and FastCAL now handle accounting of disk usage and new content allocation to the disks for all modules.

Batch deletion using the CDSM GUI or the **clear content url** command uses FastCAL to delete the asset.

Flash Media Streaming

The following features are supported for Flash Media Streaming:

- Service Rules Using the XML File
- Support for SWF Validation

Service Rules Using the XML File

In Release 2.5.7 and Release 2.5.9, service rules for the Web Engine were configured per-delivery service by using the Service Rule XML file, and service rules for Windows Media Streaming, Movie Streamer, and Flash Media Streaming were configured per-device either by using the CDSM or by using the **rule** command in the CLI.

In Release 2.6.1, service rules for Flash Media Streaming are now configured using the Service Rule file. By associating the Service Rule file with a delivery service, all service rules defined in the file are applied to all SEs in the delivery service.

The following rule actions are supported for Flash Media Streaming:

- Allow (Rule_Allow)
- Block (Rule_Block)
- URL signature validation (Rule_Validate)
- SWF file validation (Rule_SwfFileValidate)

The maximum number of rule actions allowed in a Service Rule file is 100. The file also allows the use of Boolean AND and OR functions. For more information, see the *Cisco Internet Streamer CDS 2.6 Software Upgrade Guide*.

Note All per-device service rules configured for Flash Media Streaming in previous releases must be converted to the per-delivery service Service Rule files in Release 2.6.1.

Rule_SwfFileValidate is introduced in Release 2.6.1.

Support for SWF Validation

Small Web Format (SWF) file validation is supported by using the Service Rule XML file. A client player generates the signature for an SWF file and the signature is sent to the Flash Media Streaming engine. The client SWF file is validated against the SWF file on the SE. If the subscriber edits the SWF file or uses a malicious SWF file, the signatures differ and the request is rejected.

For more information, see the "SWF Validation Process" section in the "Creating Service Rule Files" appendix of the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide*.

Monitoring

To monitor Flash Media Streaming requests, use the **show statistics flash-media-streaming swf** command.

Web Engine

The following features are supported for Web Engine:

- Content Flow Trace
- Windows Media Streaming Request Handling and Statistics
- HTTP Error Response Caching
- Rule Actions for Web Engine in Service Rule XML File

Content Flow Trace

Content Flow Trace is a new feature of the Web Engine in Release 2.6.1 and is used to track the flow of HTTP messages through the CDS and the HTTP response from the Origin Server.

To accomplish this, custom HTTP headers are used for both the requests and the responses. Every tier adds information to the HTTP headers before sending it to the next SE. The custom headers added by the SEs are stripped by the Content Acquirer before the request is sent to the Origin Server. Similarly, the custom headers are stripped from the response before sending it to the client, unless the **Enable Filter Trace Flow to Client** option is enabled for the delivery service (**Services > Service Definition > Delivery Service > General Settings**).

Note The Content Flow Trace is used for debugging potential issues in the CDS and should not be used during high traffic loads.

For more information, see the "Content Flow Trace" section in the "Monitoring the Internet Streamer CDS" chapter of the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide*.

Windows Media Streaming Request Handling and Statistics

This section describes how Web Engine handles Windows Media Streaming requests and the associated new statistics.

ASX Request Handling

Web Engine generates meta responses for the following ASX requests:

- Requested Windows Media Streaming asset is prefetched
- Unicast (.asx) request for Windows Media Streaming live program is scheduled
- Multicast (.nsc.asx) request for live program is scheduled

When the **wmt disallowed-client-protocols** command is configured, Web Engine generates the meta response based on the protocols enabled. When both RTSPU and RTSPT are disabled, only the HTTP URL is generated in the meta response. However, when HTTP is disabled, the generated ASX file still contains the HTTP URL, so that the content can be served by the Web Engine as a progressive download (as opposed to live streaming by Windows Media Streaming). For .nsc.and asx files, only the HTTP URL is generated.

VOD ASX Request

Web Engine does lookups for incoming ASX requests in the following manner:

- If the ASX asset is cached or prefetched, the asset is served.
- If the ASX asset is not found, Web Engine strips the .asx extension from the URL and performs the lookup again.
  - If the asset is found (after stripping the .asx from the URL), Web Engine generates the meta response for the requested Windows Media Streaming ASX request.
  - If the asset is not found (after stripping the .asx from the URL), no meta response is generated and the request is treated as a cache miss.

Live ASX Request

In the case of a unicast live request or a multicast live request, Web Engine generates the meta response for found assets. If the asset is not found, Web Engine generates a "403 Forbidden" error message and sends it to the client.

NSC Request Handling

An NSC request is a managed live streaming request. When the live program schedule is started, the NSC content is created by Windows Media Streaming.

For Web Engine lookups of NSC files, CAL returns the NSC file location where the content can be served from, or returns "Not in Schedule."

Statistics

New statistics for meta responses generated by Web Engine have been added to the **show statistics web-engine** command, the **show statistics web-engine detail** command, and the **show content url <*url*> detail** command. Following are example outputs of these commands with the new information in bold.

```
# show statistics web-engine
HTTP Request Info Statistics
----------------------
Num Lookups                   :                          1
Preposition Hit               :                          0
Alien Hit                     :                          0
Cache Hit                     :                          0
Cache Miss                    :                          1
Partial Cache Hit             :                          0
Cache Bypass                  :                          0
Live Miss                     :                          0
Live Hit                      :                          0
ASX Meta Response             :                          0

# show statistics web-engine detail
Web-Engine Detail Statistics
---------------------
Active HTTPSession            :                          0
Active DataSource             :                          0
Active HTTPDataFeed           :                          0
Active HTTPDataSourceFinder   :                          0
Active HTTPTransaction        :                          0
Pending HTTPTransaction       :                          0
Active ServerXact             :                          0
Total HTTPConnection          :                          0
Active HTTPConnection         :                          0
Idle Proxy HTTPConnection     :                          0
Idle Origin HTTPConnection    :                          0
Memory Hit                    :                          0
Cut-Thru Counter              :                          0
Memory Usage                  :                 1164374016
WebEngine Trickle Status      :                          0
Outstanding Content Create Requests:                     0
Outstanding Content Lookup Requests:                     0
Outstanding Content Delete Requests:                     0
Outstanding Content Update Requests:                     0
Outstanding Content Popularity Update Requests:                    0
Statistics was last cleared on Tuesday, 05-Apr-2011 01:10:29 GMT.

# show content url http://192.168.54.5/diff.new detail
CAL content object attributes:
        URL: http://192.168.54.5/diff.new
        Status is 3 (Servable)
        Content is Complete
        File size is 0 Bytes
        Playable by WebEngine
        Content is CACHED
        Start Time : Not present
        End Time : Not present
        Internal path to data file
[/disk00-01/c/192.168.54.5/66/66/6666cd76f96956469e7be39d750cc7d9/diff.new.http]

Web Engine attributes:
        Date: Mon, 07 Mar 2011 19:23:43 GMT
        Request time: Tue, 05 Apr 2011 01:10:36 GMT
        Content-length: 205
```

```
Content-Type: text/html; charset=iso-8859-1
Cache-Control:Max Age= 1000
IsErrorResponse: Yes
HTTP Status Code: 404
Keep-Alive:timeout=5, max=100
My-Header:haha
```

HTTP Error Response Caching

Caching HTTP error responses from the Origin Server provides the Web Engine with the ability to validate incoming requests faster and reduce unnecessary access to the Origin Server.

As an example, the Origin Server sends back a response with the status "503 Service Unavailable" and includes the *maximum age* in the response. The Web Engine caches the response locally, and for any subsequent client requests for the same content, the Web Engine compares the cached response age with the maximum age returned in the response. If the cached response is expired, the Web Engine rechecks the Origin Server; otherwise, the Web Engine sends the cached response to the client.

The HTTP response headers must include the max-age, expiry, etag, and other fields that are required to determine whether the responses can be cached.The HTTP response headers that can be cached are those that indicate some error has occurred with respect to the client request (4xx or 5xx status codes).

Note Error response 416 is not cached when the origin server responds with Transfer-Encoding:Chunked header. Whenever the origin server sends chunked encoding, whatever status is returned, the response is not cached.Configuring HTTP Response Caching.

The HTTP Response Caching feature is enabled on a per-delivery service basis (**Services > Service Definition> Delivery Service > General Settings**).

Monitoring HTTP Response Caching

Two output fields are added to the **show statistics web-engine** command:

- Error Response Miss—Normal cache-miss case. The Origin Server sends back the response with the status code that is configured to be cached, and a file is created locally to store the cache response headers.
- Error Response Hit—Locally stored cached HTTP response gets hit, it is not expired, and the client response is generated from it.

The Request-Desc/Status-Returned field in the Web Engine client transaction log includes the error status code for both TCP_MISS and TCP_HIT. A TCP_HIT with an error status code means the HTTP response was served from cache. The meaning of a TCP_MISS with an error status code has not changed.

Rule Actions for Web Engine in Service Rule XML File

The following new rule actions have been added to the Service Rule XML file for Web Engine:

- URL Resolve
- URL Redirect
- Force Revalidation
- URL Generate Signature

Multiple Rule Actions in Web Engine

Previously, only Rule_UrlRewrite was supported. With the introduction of Rule_UrlRedirect and Rule_UrlResolve in Release 2.6.1, it is important to note that the Web Engine only applies one of these rule actions. These rule actions are applied in the following order:

1. Rule_UrlRedirect
2. Rule_UrlResolve
3. Rule_UrlRewrite

If more than one rule action is returned from the Authorization Server, only the one with the higher priority is chosen.

URL Resolve

In many content delivery cases, URLs are not just used as unique identifiers of the content, but they are also used to transfer specialized information from the client to the Origin Servers (for example, client IP addresses and special tags for video identification) in the form of query strings.

The URL Resolve rule action (Rule_UrlResolve) provides a way to take a client's incoming URL (known as the Intercept URL) and resolve it into other URLs that can be used for caching (known as the Storage URL) and ingesting (known as the Source URL) the content.

In Release 2.6, the default behavior of the Web Engine is to cache the content when the request URL has a query string, which results in multiple copies of the same content being stored. Release 2.5.9 supported the Rule_NoCache rule action in the Service Rule file, which offered a way to not cache content with query strings; however, this meant the content was served by way of bypass (downloaded from the Origin Server directly), which resulted in more connections to the Origin Server. With the Rule_UrlResolve rule action, the Storage URL provides a way to address any URL uniqueness that complicates caching, so long as the uniqueness can be removed by parsing the URL and replacing parts of the URL with regular expressions.

For more information about the URL Resolve rule action, see the "URL Resolve" section in the "Creating Service Rule Files" appendix of the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide.*

URL Redirect

The URL Redirect (Rule_UrlRedirect) rule action is supported in the Service Rule XML file for the Web Engine. Following is an example of the Rule_UrlRedirect rule action:

```
<Rule_UrlRedirect matchGroup = "grp4" protocol = "http" redirect-url = "http://www.google.com" />
```

The *matchGroup* attribute value is the list of PatternListGrp *id* attributes. The *protocol* attribute value must be http. The *redirect-url* attribute value is the URL used to redirect the original request.

Note Only http is supported as the *protocol* attribute value. All other values have no affect.

Whether a Rule_UrlRedirect pattern is matched or not, rule processing continues to the next configured rule. If the Rule_UrlRedirect pattern is matched, the request is redirected. If the Rule_UrlRedirect pattern is not matched, the request is not redirected.

The **show statistics web-engine** command has a new counter, Authorization Redirect, which keeps track of the number of URL Redirect hits.

Force Revalidation

The Force Revalidation (Rule_ForceReValidate) action rule forces revalidation of cached content. The freshness of content algorithm and the comparison between the Origin Server expiry time with the max age value are ignored if this rule action is invoked.

If the Rule_ForceReValidate rule action is configured as part of Service Rule file, the Authorization Server responds to the Web Engine with the Rule_ForceReValidate directive. This enables the Web Engine to take appropriate revalidation action.

For more information about the URL Resolve rule action, see the "Force Revalidation" section in the "Creating Service Rule Files" appendix of the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide.*

URL Generate Signature

The URL Generate Signature (Rule_UrlGenerateSign) rule action is supported in the Service Rule XML file for the Web Engine. The Rule_UrlGenerateSign is a rule action for generating the URL signatures in the Windows Media metafile (ASX file) response associated with prefetched content, based on the SE configuration for the URL signature and this rule action.

The Windows Media player receives the ASX file containing the signed URL, parses it, and send out the request again with the signed URL. The SE receives the signed URL and performs the URL validation with the internally signed URL. If the validation is successful, the content is served to the client.

For more information about the URL Resolve rule action, see the "URL Generation Signature" section in the "Creating Service Rule Files" appendix of the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide.*

Authorization Server

The Authorization Server has been enhanced in the following ways:

- Support for Flash Media Streaming
- Rule Actions Added for Web Engine
- CDSM GUI Changes for Authorization Server
- Statistics Enhancements
- Service Rule File Changes

Support for Flash Media Streaming

The Authorization Server supports Flash Media Streaming in Release 2.6.1. For more information, see the "Flash Media Streaming" section on page 8.

Rule Actions Added for Web Engine

The Authorization Server supports new rule actions for Web Engine. For more information, see the """Rule Actions Added for Web Engine" section on page 14.

Apply to All Tiers Element

The Apply to All Tiers (ApplyAllTier) element has been added. The ApplyAllTier element has the following effect:

- If the ApplyAllTier is set to yes, then the Rule_UrlResolve rule action is applied to all SEs in the delivery service.
- If the ApplyAllTier is no or if it is absent, and Rule_UrlResolve is included in the Service Rule file, then the Rule_UrlResolve does not work properly.
- If the ApplyAllTier is no or if it is absent, and Rule_UrlResolve is not included, then the Service Rule file is only applied to the edge tier, as was the behavior before Release 2.6.1.

Note The ApplyAllTier element must be set to yes for the Rule_UrlResolve to work properly. For more information, see the "URL Resolve" section in the "Creating Service Rule Files" appendix of the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide.*

CDSM GUI Changes for Authorization Server

The changes to the CDSM GUI for Authorization Server consist of the following:

- Uploading or Importing a Service Rule File
- Uploading or Importing an Authorization Service FIle

Uploading or Importing a Service Rule File

The **System > Configuration > Service Rule File Registration** page has been changed to the **System > Configuration > Authorization File Registration** page. The Authorization File Registration page is used to upload a Service Rule file into the CDSM and register it to the CDSM. The import method has been added to this page.

In previous releases, you can upload the Service Rule file from any location that is accessible from your PC by using the **Browse** button. In Release 2.6.1, you can also import the Service Rule file from an external HTTP, HTTPS, FTP, or CIFS server.

For more information on registering a Service Rule file with the CDSM, see the "Creating Delivery Service—Authorization Plugins" section in the "Configuring Delivery Services" chapter of the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide*.

Uploading or Importing an Authorization Service FIle

The **Services > Service Definition > Delivery Services > Authorization Service** page has been changed to the **Services > Service Definition > Delivery Services > Authorization Plugins** page. The Authorization Plugins page offers the option to select a Service Rule file for the delivery service or to add an Authorization Service file (now referred to as the Geo/Ip File) for the delivery service.

Note Because both the Service Rule file and the Authorization Service file use the Authorization Server to allow or deny requests, and process the service rules, the Authorization Service file is now referred to as the Geo/IP file in the CDSM GUI.

For more information on uploading or importing a Geo/IP file for a delivery service, see the "Creating Delivery Service—Authorization Plugins" section in the "Configuring Delivery Services" chapter of the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide*.

Statistics Enhancements

Previously, statistics reported the total number of requests that were allowed or blocked by the Authorization Server. In Release 2.6.1, the statistics now report the number of requests allowed and blocked for each delivery service and for each rule.

The statistics are cleared when the configuration is updated. If the Authorization Service (Geo/IP) file is updated, the IP and Geo statistics are cleared. If the Service Rule file is updated, the Service Rule statistics are cleared. If the Authorization Server is restarted, all statistics are cleared.

The show statistics authsvr command has the following syntax:

```
show statistics authsvr global
show statistics authsvr delivery-service-id <delivery-service-num> [detail | geo | ip |
rules]
```

The **show statistics authsvr global** command displays the same information as previous releases; that is, the number of allowed and blocked requests for both known and unknown servers, and the number of errors.

The **show statistics delivery-service-id** command displays the allowed and blocked statistics for the specified delivery service and requires one of the following keywords:

- **detail**—Lists the statistics for IP network blocking, geographical region blocking, and service rules
- **geo**—Lists the statistics for geographical region blocking
- **ip**—Lists the statistics for IP blocking
- **rules**—Lists the statistics for the service rules

Service Rule File Changes

The following configuration changes have been added to the Service Rule file:

- Rule Pattern SrcIP
- Multiple Action Rules

Rule Pattern SrcIP

In Release 2.5.7 and later releases, the SrcIP pattern does not support classless inter-domain routing (CIDR) format. The client IP address from the incoming request is compared against a single IP address without taking the CIDR format into consideration.

In Release 2.6.1, the SrcIP pattern requires the IP address be specified in the CIDR format. The Service Rule XML file validation fails if the IP address is not in CIDR format.

Multiple Action Rules

In Release 2.6.1, the maximum number of rule actions allows is 100. If the number of rule actions exceeds 100, then the Service Rule XML file validation fails. Only the following rule actions are allowed to have multiple entries:

- Rule_Rewrite
- Rule_UrlResolve

- Rule_UrlGenerateSign

All other rule actions can only have a single entry.

Kernel and Platform

Release 2.6.1 introduces the following kernel and platform features:

Support for the CDE250

CDE250-2S6 and CDE250-2M0 are supported in this release, which includes four interfaces at 10 gigabit Ethernet speeds and four interfaces at gigabit Ethernet speeds (plus an two additional gigabit ethernet interfaces for management).

GRUB Bootloader and File System

In previous releases, the rescue image was invoked on an SE, SR, or CDSM by entering *** at the bootloader prompt. In Release 2.6.1, a new bootloader menu is introduced that allows you to either boot from the most recent pending software image stored on flash, or to invoke the rescue image from an FTP server.

The software partition size has increased from 1 GB to 5 GB. The **show disk detail** command output displays the new sizes for the file systems.

Note When downgrading a device from Release 2.6.1 back to Release 2.5.x, compact flash content is restored to 2.5.x format, but the software partition remains at 5 GB.

For information about the software upgrade procedure, see the *Cisco Internet Streamer CDS 2.6 Software Upgrade Guide*.

LACP Support

Link Aggregation Control Protocol (LACP) provides functionality for better port channel link detection. If incorrect configuration on a port channel decreases the available bandwidth, LACP sends an alarm notification. Additionally, when LACP is enabled, a link could be considered LACP inactive if it is plugged into the wrong port channel; however, the physical layer still considers it active. Without LACP, a link within a port channel could be configured incorrectly and decrease available bandwidth; however, there is no easy way to detect this is happening.

LACP has the intelligence to send packets only on active links to keep the network traffic moving and raise alarms for inactive links. It also provides the following load-balancing algorithm for the port channel:

- dst-ip
- dst-mac
- dst-port

- src-dst-ip
- src-dst-mac
- src-dst-port
- src-port
- src-mixed-ip-port
- dst-mixed-ip-port
- src-dst-mixed-ip-port

Note LACP must be enabled on the participating devices, including the switch, to work properly.

CLI Changes

LACP is enabled at the interface configuration mode.

```
interface PortChannel <1-4> lacp
```

The following command is used to configure load balancing:

```
port-channel load-balance ?
  dst-ip        Dst IP Addr (default)
  dst-mac       Dst Mac Addr
  dst-mixed-ip-port Destination IP Addr and TCP/UDP Port
  dst-port      Dst Layer 4 port
  round-robin   Round robin
  src-dst-ip    Source and Dst IP Addr
  src-dst-mac   Source Dest Mac address
  src-dst-mixed-ip-port Source Destination Ip and Source Destination Port
  src-dst-port  Source and Destination Layer 4 port
  src-mixed-ip-port Source Ip and Source Destination Port
  src-port      Source Layer 4 port
```

The round-robin load-balancing mode is not supported in the LACP.

Alarms and show Commands

The **show lacp internal** command and the **show lacp counters** command have been added for LACP. Following is an example of the **show lacp internal** command:

```
# show lacp internal
Interface PortChannel 1 (4 physical interface(s)):
Protocol: LACP
Mode:     src-dst-port
Port                    Admin-State Link-State     LACP-State     Aggregate id
------------------------------------------------------------------------------
GigabitEthernet  3/0           up         up         bndl              21
GigabitEthernet  4/0           up         up         bndl              21
GigabitEthernet  5/0           up         up         down              22
```

The Aggregate ID and LACP-State provide a way to tell if the link belongs to the same port channel. If state is “bndl,” then the CDS is sending and receiving state information from the LACP. If the state is “down,” then the port channel is incorrect, or the interface speed is a mismatch from other interfaces. If the state is “no_neighbor,” then the CDS cannot communicate with LACP.

A link status, LACP link status, alarm is raised if the LACP-state status is “down.”

The **show alarms** command displays any LACP alarms. Following is an example of the LACP alarms:

The alarm format will be in the following

```
# show alarms

Major Alarms:
-------------
     Alarm ID             Module/Submodule     Instance
     -------------------- -------------------- -------------------------
   1 lacp_link_down       nic                  GigabitEthernet 3/0
   2 lacp_no_neighbor     nic                  GigabitEthernet 4/0
```

Service Monitor polls the LACP link status every 60 seconds. If the LACP link is down, an alarm is raised; otherwise, the alarm is cleared. LACP alarm is raised if speed or duplex mode mismatch is detected. If an LACP alarm is raised, a log entry is added to the syslog file (/local/local1/syslog.txt).

APIs

Release 2.6.1 introduces the File Management API. The File Management API can be used to manage the following XML files registered to the CDSM:

- Coverage Zone files
- NAS files
- Service Rule files
- CDN Selector files

Enhancements

The following enhancements have been added in Release 2.6.1-b21:

- Service Router
- Proximity Engine
- AAA Support for TACACS+
- CDSM GUI—XML Schema Files
- SNMP
- Interface Alarms
- Windows Media Streaming User Agent
- Support for Non-Paced HTTP Sessions
- Skip Location Leader Selection for Edge SE
- Other Enhancements
- Other CLI Changes

Service Router

The following Service Router features have been added to Release 2.6.1:

- Per-Domain Content-Based Routing
- Show Proximity Cache Information
- Geo-Location Cache Disable and Timeout Information

Per-Domain Content-Based Routing

When content-based routing is enabled the service router redirects the request based on the request URL. The requests for the same URLs are redirected to the same Service Engine in order to optimize performance. This helps in optimizing disk usage and improves cache-hit ratio.

Previously, the content-based routing can be enabled or disabled on the SR; that is, content-based routing is enabled or disabled for all the domains. In Release 2.6.1, content-based routing can be enabled or disabled on a per-domain basis.

Content-based routing per-domain is enabled by checking the **Enable Content Based Routing** check box on the **Services > Service Definition > Content Origins** page. **Enable Content Based Routing** is checked by default. This feature requires that content-based routing be enabled on the SR.

To show content-based routing states, log in to SR and enter the **show service-router content-based routing** command.

Show Proximity Cache Information

A show command has been added to Release 2.6.1 to show whether a particular IP address or subnet is present in the cache for proximity-based routing, and if so, information about the corresponding Service Engines, their ratings, and the time the entry was cached are displayed. The show command is as follows:

```
show service-router proximity-based-routing cache ip <ip address/subnet>
```

where *ip address/subnet* is the client IP address or subnet for which the proximity cache information needs to be displayed.

Geo-Location Cache Disable and Timeout Information

The Service Router (SR) caches information from Geo-Location server during the first request so that further requests can be served from cache instead of contacting the Geo-Location server.

Previously, there was no way to disable this caching mechanism if the SR performance needed to be measured without geo-location cache.

A new command has been added to disable geo-location cache and also to configure geo-location cache timeout to purge the entry in cache after the configured timeout period. The command is as follows:

```
service-router location-based-routing location-cache timeout <timeoutvalue>
```

where *timeoutvalue* is the time interval, in seconds, in which the cache is purged. The range is 0–864000. The default value is 691200.

If timeoutvalue is 0, the response from the Geo-Location server is not cached in the SR. For other values of timeoutvalue, the response from Geo-Location server is stored in the SR cache for the first time and expires after timeoutvalue.

The following command disables the Geo-Location cache in the SR:

```
service-router location-based-routing location-cache timeout 0
```

The following command configures Geo-Location cache timeout of 5 seconds so that entries in the cache are cleared after 5 seconds.

```
service-router location-based-routing location-cache timeout 5
```

The **show service-router location-based-routing** command displays the configured cache timeout value.

Proximity Engine

The following features are supported for Proximity Engine:

- BGP show Command Enhancement
- Location Community Enhancement
- Static Routes

BGP show Command Enhancement

Previously, the **show ip bgp community** command output displayed the same information as the **show ip bgp all** command.

The **show ip bgp community** command output has been modified to display the origin AS and community values. Following is an example of the new output for the **show ip bgp community** command:

```
# show ip bgp community
    sh ip bgp community
    BGP table version is 32, local router ID is 1.100.9.206
    Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
    Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
    Community: @ - source, # - target

       Network          Next Hop        Origin AS  Community List
    *>e2.4.1.0/24       192.168.82.2    33
    *>e3.1.4.0/24       192.168.82.2    23         @23:999
    *>e5.5.5.5/32       192.168.82.2    23         @23:999
    *>e12.1.1.0/24      192.168.82.1    23
    *>e12.1.1.1/32      192.168.82.2    23         @23:100 @#44:100
    *>e13.1.1.0/24      192.168.82.1    23
    *>e13.1.1.1/32      192.168.82.2    23         @#44:100
    *>e14.1.1.1/32      192.168.82.2    23         @#44:100
    *>e40.1.1.0/24      192.168.82.2    23         @23:999
    *>e41.1.1.0/24      192.168.82.2    23         @23:999
    *>e42.1.1.0/24      192.168.82.2    33
    *>e43.1.1.0/24      192.168.82.2    33
    *>e44.1.1.0/24      192.168.82.2    33
    *>e45.1.1.0/24      192.168.82.2    33
    *>e46.1.1.0/24      192.168.82.2    33
    *>e50.1.1.0/24      192.168.82.2    23         @23:999
    *>e51.1.1.0/24      192.168.82.2    23         @23:999
    *>e52.1.1.0/24      192.168.82.2    33
    *>e53.1.1.0/24      192.168.82.2    33
    *>e54.1.1.0/24      192.168.82.2    33
    *>e55.1.1.0/24      192.168.82.2    33
    *>e62.1.1.1/32      192.168.82.2    23         @23:999
    *>e62.62.62.0/24    192.168.82.2    23         @23:999
    *>e108.0.32.0/24    192.168.82.2    33
    *>e171.70.0.0/16    192.168.82.2    33
    *>e171.71.0.0/16    192.168.82.2    33
    *>e172.20.0.0/16    192.168.82.2    33
    *>e192.168.81.0/24  192.168.82.2    23
    *>e203.0.0.205/32   192.168.82.2    23         @23:999
```

Note The Community List column uses the @ symbol to denote the source community value and the # symbol to denote the target community value that is location specific.

When the optional community value is specified (for example, **show ip bgp community 23:999**), the output displays only the information for that community value.

Location Community Enhancement

Previously, the algorithms used to determine preference and ranking of the SEs preferred Proximity Target Addresses (PTAs) that shared the same community attributes as the Proximity Source Address (PSA), to PTAs that did not share the same community attributes with the PSA.

However, in certain deployments it is advantageous to include certain PTAs even though the PTAs do not share any community attributes with the PSA. A common example is an SE in a city close to the client PC; in such case, the SE might not share any community attributes with the client PC, but should be preferred over another SE in a far-away city. Previously, to accomplish this, the network operator had to tag the BGP prefixes of the PTA (and sometimes even the PSA) with proper community values in the router and the Proximity Engine, while also configuring which community values are location specific in the Proximity Engine.

The Proximity Engine has been enhanced to allow the association of PSA and PTA community attributes with each other and assign the association a preference level.

CLI Changes

The following change has been made to the **location community** command:

location community <*community*> [**target** <*community*>] [**weight** <*weight*>]

The first community value is mandatory and denotes the PSA location-community. The target community (PTA location community) is optional, and if not specified, is the same as the PSA location community. So, if the target community is not specified, the PSA and PTA must have a common community for the PTA to be considered in the preference and ranking.

The weight field is optional and has a range of 1–7, with 7 being the best association (most preferred) and 1 being the default. An association weight of 0 implicitly means no association (least preferred).

The following command associates a PSA with a location community 1:1 with a PTA with a location community of 2:2 and a weight of 2:

```
SR(config-bgp)# location community 1:1 target 2:2 weight 2
```

The source and target community can also be a range. The following command associates the source community 1.:1 with all target communities in the range 2:0-2:10 and a weight of 2:

```
SR(config-bgp)# location community 1:1 target 2:0-2:10 weight 2
```

If multiple location community commands satisfy more than one matching criteria, the weight is based on the following preference level (most preferred to least preferred):

1. Specific source community—Specific target community
2. Specific source community—Range target community
3. Range source community—Specific target community
4. Range source community—Range target community

Note Source community ranges are not allowed to overlap. A maximum of 240 unique specific source or range source community configurations can be entered. Each unique specific source or range source community can be associated with a maximum of 240 unique specific target or range target communities.

Location community proximity algorithm is enabled by using the **proximity algorithm** command, and has been enhanced as follows:

```
SR(config-)# proximity algorithm bgp location-community [strict]
```

The optional **strict** keyword instructs the Proximity Engine to return UINT-MAX as the proximity rating for PTAs that are not associated with the PSA by way of any location-community attribute. This configuration is global and applies to all proximity requests. If PSA is BGP and has no community attributes, then all PTAs get UINT_MAX rating. If the PSA is IGP, then this configuration does not apply and other proximity algorithms, BGP best-path and IGP metric, are used to rate the PTAs in the proximity request.

The **show statistics ip proximity rib** command displays the number of Strict mismatch responses.

CDSM GUI Changes

The optional **Target Community** field has been added to the BGP Location Community page.

In the **Devices > Devices > Routing Settings > Proximity Server Settings > BGP** page in the Location Community for BGP table, click the **Create New** icon or the **Edit** icon next to an existing location-community configuration. The BGP Location Community page is displayed with the new **Target Community** field. The Target Community values have the same format and restrictions as the **Location Community** field, which are the following:

- Must match the pattern: <AS1>:<POP1>[-<AS2>:<POP2>]
- AS1 and AS2 must be in the range 1–65535.
- POP1 and POP2 must be in the range 0–65535.
- AS2 should be greater than AS1, or POP2 should be greater than POP1 if AS2 equals to AS1.
- New BGP community setting should make sure that target community and local community pair is unique and not existent.

The **Match mode** drop-down list with the strict option for the proximity algorithm has been added to the Proximity Routing General Settings page.

In the **Devices > Devices > Routing Settings > Proximity Server Settings > General Settings** page, the **Match mode** drop-down list has two options, normal and strict. Select **normal** for the **proximity algorithm bgp location-community** command, and select **strict** for the **proximity algorithm bgp location-community strict** command.

Static Routes

Unicast static routes can be configured for the Proximity Engine. Static routes provide the Proximity Engine the ability to resolve learned BGP route next hops without IGP routing information. The following new commands have been added:

```
ip rib route <destination prefix> <netmask> <nexthop ip>
ip rib route <destination prefix> <netmask> <interface>
ip rib route <destination prefix> <netmask> <interface> <nexthop ip>
```

Following are examples of the ip rib route command:

```
(config)# ip rib route 10.1.1.1 255.255.255.0 20.1.1.1
(config)# ip rib route 10.1.1.1 255.255.255.0 gigabitethernet1/0
(config)# ip rib route 10.1.1.1 255.255.255.0 gigabitethernet1/0 20.1.1.1
```

This command allows static route configuration where the next-hop resolution depends on other static route configuration, The maximum number of static routes that can be configured is 200. The maximum number of equal cost multiple path (ECMP) static routes is 16.

When the next hop cannot be resolved, the static route configuration is not rejected, but the static route is not installed in Routing Information Base (RIB). When the next hop is resolved, the static route is installed automatically.

The **show ip rib route static** command displays the static routes.

The new **show ip static route** command displays the static route configured and stored in the RIB table.

AAA Support for TACACS+

Authentication, authorization, and accounting (AAA) have been added for the Terminal Access Controller Access Control System Plus (TACACS+) authentication server.

Note Authentication and authorization are supported for local, RADIUS, and TACACS+; however, accounting is only supported for TACACS+.

CLI Changes

The following commands have been added for authentication:

- **aaa authentication login** {**local** |**radius** | **tacacs+**} {**primary** | **secondary** | **tertiary**}
- **aaa authentication login fail-over server-unreachable**
- **aaa authentication enable** {**enable** | **radius** | t**acacs+**} {**primary** | **secondary** | **tertiary**}

The following commands have been added for authorization using the TACACS+ server:

- **aaa authorization commands** {**0** | **15**} **tacacs+** [**if-authenticated**]
- **aaa authorization config-commands**
- **aaa authorization consol**e
- **aaa authorization exe**c {**local** |**radius** | **tacacs+**} {**primary** | **secondary** | **tertiary**}

The following commands have been added for accounting using the TACACS+ server:

- **aaa accounting commands** {**0** | **15**} {**start-stop** | **stop-onl**y} **tacacs+**
- **aaa accounting exec** {**start-stop** | **stop-only**} **tacacs+**
- **aaa accounting system** {**start-stop** | **stop-onl**y} **tacacs+**

The password keyword has been added to the enable command.

- **enable password** {**0 plainword** | **1 cryptoword** | **clear-text**}

The following show commands have been added for AAA:

- **show aaa commands** [**authorization** | **accounting**]
- **show aaa enable** [**authentication**]
- **show aaa exec** [**authorization** | **accounting**]
- **show aaa login** [**authentication**]
- **show aaa system [accounting]**
- **show statistics aaa**

The following debug command has been added for AAA:

- **debug aaa** {**authentication** | **authorization** | **accounting**}

The **aaa authentication login** commands and the **aaa authorization** commands in Release 2.6.1 correspond to the **authentication login** commands and the **authentication configuration** commands in previous releases. Table 2 describes the changes between previous Internet Streamer CDS software releases and Release 2.6.1.

Table 2 Changes to Commands for AAA

AAA Services	Before Release 2.6.1	In Release 2.6.1
Login authentication	[no] authentication login {local | radius | tacacs} enable [primary | secondary | tertiary]	[no] aaa authentication login {local | radius | tacacs+} {primary | secondary | tertiary}
Exec authorization	[no] authentication configuration {local | radius | tacacs} enable [primary | secondary | tertiary]	[no] aaa authorization exec {local | radius | tacacs+} {primary | secondary | tertiary}
Login fail-over	[no] authentication fail-over server-unreachable	[no] aaa authentication login fail-over server-unreachable

For information about the changed commands, see the *Cisco Internet Streamer CDS 2.6 Command Reference*.

CDSM GUI Changes

This section describes the changes to the CDSM GUI to support AAA.

Note Authentication and Authorization are supported for local, RADIUS, and TACACS+. Accounting is only supported for TACACS+.

Authentication Configuration

To configure the login and enable authentication for the device, choose **Devices > Devices > General Settings > Login Access Control > Login Authentication**. The Login Authentication page is displayed.

Note You must configure TACACS+ server settings for the device before you apply TACACS+ Server for login and enable authentication.

The Login Authentication page has the following fields:

- **Enable Failover Server Unreachable**—To query the secondary authentication database if the primary authentication server is unreachable, check this box.

  Note To use this option, you must set TACACS+ or RADIUS as the primary authentication method and local as the secondary authentication method.

- **Authentication Login Servers**—Check this option and set one or more AAA servers for login authentication. By unchecking this option, local authentication is used by default. Three servers can be configured.
- **Authentication Enable Servers**—Set one or more AAA servers for enable authentication. Three servers can be configured.
- **Password**–Set the local enable password.

Authorization Configuration

To configure the authorization for the device, choose **Devices > Devices > General Settings > Login Access Control > Exec Authorization**. The Exec Authorization page is displayed.

Note You must configure TACACS+ server settings for the device before you apply TACACS+ Server for authorization.

The Exec Authorization page has the following fields:

- **Authorization Exec Servers**—Check this option, and then set one or more AAA servers for Exec authorization. By unchecking this option, local authorization is used by default. Three servers can be configured.
- **Normal User Commands**—Enable or disable authorization for Exec (shell) commands for normal users.
- **Super User Commands**—Enable or disable authorization for Exec (shell) commands for super users.
- **Enable Config Commands**—Enable or disable authorization for configuration mode commands.

  Note To use this option, you must set normal or super user commands first.

- **Enable Console Config**—Enable or disable authorization for all configurations on console line.

Accounting Configuration

To configure the accounting for the device, choose **Devices > Devices > General Settings > Authentication > AAA Accounting**. The AAA Accounting page is displayed.

Note You must configure TACACS+ server settings for the device before you apply TACACS+ Server for accounting.

The AAA Accounting page has the following fields:

- **System Events**—Set record type for system events.
- **Exec Shell Events**—Set record type for starting an Exec (shell).
- **Normal User Commands**—Set record type for Exec (shell) commands for normal users.
- **Super User Commands**—Set record type for Exec (shell) commands for super users.

CDSM GUI—XML Schema Files

The XML schema files are now available for viewing or downloading through the CDSM GUI. All XML files can be validated through the CDSM GUI by clicking the Validate button; however, if you want to use an external XML validation program, you can save the XML schema file to use for that purpose. The following XML schema files are available:

- CDSAuthorization.xsd—Authorization Service file (also known as the Geo/IP file) is used to specify the geographic regions and IP networks that are allowed or denied access to a delivery service.
- CDSRules.xsd—Service Rule file used by a delivery service to specify the service rules for all SEs in a delivery service.

- CdsCoverageZone.xsd—Coverage Zone file is used to customize the networks and geographic regions each SE services.
- CdsOrigin.xsd—NAS file used for defining a NAS device.
- CDNSelector.xsd—CDN Selector file is used for third-party streaming service selection. The CDN Selector is an early field trial (EFT) feature.
- CdnManifest.xsd—Manifest file is used to specify the content to be prefetched and to control the delivery of the prefetched content for a delivery service.

To open or download an XML schema file, do the following:

Step 1 Choose **System > CDS-IS Files > XML Schema Files**. The CDS-IS XML Schema page is displayed with a link to each XSD (schema) file.

Step 2 Click the link for the file. Depending on the browser program used, one of the following or something similar happens:

- File is displayed in a new window and the File Download dialog box is also displayed
- Opening dialog box is displayed
- File is displayed in a text editor program.

SNMP

The CISCO_CDS_SERVICE_ROUTING_MIB.my has been added to the supported MIBs and included as downloadable file in the CDSM GUI.

The Service Router MIB provides some object identifiers (OIDs) for Service Router statistics. All the OIDs in the MIB are only for querying purposes; no traps have been added to this MIB.

The Service Router MIB provides two groups, cdssrStatsGroup and cdssrServiceMonitorGroup, which contain OIDs for the statistics from the s**how statistics service-router summary/dns/history/se/content-origin** command and the **show service-router service-monitor** command.

The MIB can be downloaded from the CDSM GUI by going to **System > CDS-IS Files > SNMP MIB** and clicking the link for the CISCO_CDS_SERVICE_ROUTING_MIB.my file.

Interface Alarms

The following changes have been made for interface alarms in Release 2.6.1:

- Configurable alarm shutdown for an interface
- LACP alarm raised or cleared if port channel is in LACP mode
  - LACP no neighbor alarm
  - LACP link down alarm
- Link speed mismatch alarm
- Link down alarm generated, if applicable, when the interface is stabilized (not transition mode)

The **alarm admin-shutdown-alarm enable** command shuts down the alarm. If there is already an alarm raised when the **alarm admin-shutdown-alarm enable** command is entered, disabling the alarm shutdown command does not clear the outstanding alarm. There are two ways to avoid this situation:

1. Clear the outstanding alarm first before disabling this option.
2. Disable this option and reboot. The alarm is cleared during reboot.

Note The **alarm admin-shutdown-alarm enable** command should entered before any of the above for the alarm to take affect.

To use the CDSM GUI to enable or disable Alarm shutdown for an interface, choose **Devices > Devices > General Settings > Notification and Tracking > Alarm Settings**. The Alarm Settings page is displayed with the **Alarms for Admin Shutdown Interface** check box.

For more information on LACP alarms, see the "LACP Support" section on page 17.

Windows Media Streaming User Agent

The following user agents are supported for Windows Media Streaming:

- NSPlayer
- WMServer
- WMPlayer
- NSServer
- Windows Media Player

In Release 2.6.1, Windows Media Streaming has been enhanced to support custom user agents that are configured through the CDSM GUI (**Services > Service Definition > Delivery Services > General Settings**.).

Support for Non-Paced HTTP Sessions

The support for non-paced HTTP sessions is applicable to VOD-only delivery services and is ideal for adaptive bit rate (ABR) clients. This feature allows the session to pace itself with the client's speed.

To configure a delivery service for non-paced HTTP sessions, choose **Services > Service Definition > Delivery Services > General Settings**, set the **Maximum bitrate limit per session for HTTP** field to 0, and click **Submit**. This setting provides best-effort behavior and sessions use the available bandwidth.

Skip Location Leader Selection for Edge SE

When the **Skip Location Leader Selection for Edge SE** option is enabled, the location leader selection is skipped at the edge location, and the edge SE directly contacts the location leader of the upstream tier. None of the other edge SEs are contacted.

When the **Skip Location Leader Selection for Edge SE** option is disabled, the location leader selection takes place at the edge tier. The edge SE may or may not directly contact the location leader of the upstream tier, and may or may not contact any SEs in the edge tier based on the location leader selection.

To configure the delivery service to skip the location leader selection for the edge SE, choose **Services > Service Definition > Delivery Services > General Settings**, check the **Skip Location Leader Selection for Edge SE** check box, and click **Submit**.

This feature is mainly used to improve the edge-tier caching efficiency to avoid content duplication at the edge-tier SEs.

Other Enhancements

Table 3 describes the other enhancements to Internet Streamer CDS 2.6.1.

Table 3 Other Enhancements in Internet Streamer CDS 2.6.1

Enhancement	Description
Proximity Engine—show proximity cache and hit count	The s**how service-router proximity-based-routing cache ip** <*ipaddress/subnet*> command was added, where "ip address/subnet" is the client IP address /subnet for which the proximity cache information needs to be displayed. The output displays the SE name, rating and cached time.
Flash Media Server 3.5.5	The Flash Media Streaming protocol engine has been upgraded to support the Flash Media Server 3.5.7 r7009. The supported Flash Media Server version that is supported can be displayed by viewing the access.00.log file.
Web Engine—show statistics	New counters have been added to the show statistics web-engine command output. For more information, see the *Cisco Internet Streamer CDS 2.6 Software Upgrade Guide*.
Live Programs—Block per schedule	When the Block per Schedule option is enabled, the live program stops all active streams when the scheduled playtime ends. To enable Block per Schedule, choose **Services > Live Video > Live Programs > Definition**, check the **Block per Schedule** check box, and click **Submit**.
Service Monitor threshold and augmentation threshold alarms	Following new Service Monitor alarms have been added: • Alarm 900003 (WebCalLookupThreshold) • Alarm 900004 (WebCalDiskWriteThreshold) • Alarm 9000013 (WebCalLookupAugThreshold) • Alarm 9000014 (WebCalDiskWriteAugThreshold)
REA removed	The Remote Execution Agent (REA) has been removed.
Web Engine transaction log (CSCtr53860)	The following format token has been added to the custom log format: %C—Records AuthLOOKupTime|CALLOOKuptime|CacheRouterTime|OSDownloadTime in microseconds granularity. CacheRouterTime displays only on revalidation scenario. In normal cache-miss use case, the CALLOOKuptime| includes the time taken by cache route lookup as well.
Web Engine Ingest transaction log (CSCtr39460)	Spaces removed from MIME-Type and Revalidation-Request fields. If the Revalidation header is an etag, the space between the header and colon (If-none-match: "etag ") is removed. If the revalidation header is a date header, the space is replaced by an underscore (_) for readability.
Web Engine transaction log message size	Web Engine transaction message log size increased from 8 KB to12 KB.

Table 3 Other Enhancements in Internet Streamer CDS 2.6.1 (continued)

Enhancement	Description
Web Engine Ingest transaction log—New fields	The following fields have been added to the Ingest transaction log: • DownloadTime(Seconds) • ReadCallBack • CDSDomain • ConnectionInfo(LocalPort| ConnectTime|Retry|Reuse) • IngestStatus
Service Router transaction log	The route-path field has been added to the Service Router transaction log.
CDSM GUI—Request Routing Engine	Add **Location Cache Timeout** field to **Devices > Devices (SR) > Request Routing Settings > General Settings** page. For more information, see the "Turn Off Caching of Geo-Location Servers" section on page 31.
CDSM GUI—Core Dump File	**Devices > Devices > Monitoring > Core Dump Files** page has been added and lists the core dump files for the device. If a core dump file is created, a major alarm is raised, and the Troubleshooting Menu for the Alarms table provides a link to the Core Dump Files page.
CDSM GUI—Alarms for Admin Shutdown Interface	Add **Alarms for Admin Shutdown Interface** check box to **Devices > Devices > General Settings > Notification and Tracking > Alarm Settings** page. For more information, see the "Interface Alarms" section on page 27.
Device Offline Detection	Device Offline Detection uses UDP to detect the device is offline instead of TCP 443 (System.datafeed.pollRate).
Content Removal	Content removal returns the details for each content removal request. This change is in both the CDSM GUI and the API.

Transaction logs—software header	Each transaction log includes a header line that provides the Cisco Internet Streamer CDS software version. Following is an example of the Web Engine Extended Squid-style header:
	`#Software: (CDS 2.6.1 b13)`
	`Current-Time Time-to-Serve Client-IP Request-Desc/Status-Returned Bytes-Xferred Method URL MIME-Type`

Other CLI Changes

In addition to the new commands and command changes that are described in the "New Features" section on page 2 and the "Enhancements" section on page 19, this section includes changes to other commands. For information about the changed commands, see the *Cisco Internet Streamer CDS 2.6 Command Reference*.

ip dscp all

The **ip dscp all** <*value*> command has been added to provide a way to mark DSCP bits on all out going IP packets on the SE. The DSCP bits can be set as follows:

```
SE(config)# ip dscp all ?
  <0-63>   Set DSCP value
  af11     Set packets with AF11 dscp (001010)
```

```
af12     Set packets with AF12 dscp (001100)
af13     Set packets with AF13 dscp (001110)
af21     Set packets with AF21 dscp (010010)
af22     Set packets with AF22 dscp (010100)
af23     Set packets with AF23 dscp (010110)
af31     Set packets with AF31 dscp (011010)
af32     Set packets with AF32 dscp (011100)
af33     Set packets with AF33 dscp (011110)
af41     Set packets with AF41 dscp (100010)
af42     Set packets with AF42 dscp (100100)
af43     Set packets with AF43 dscp (100110)
cs1      Set packets with CS1(precedence 1) dscp (001000)
cs2      Set packets with CS2(precedence 2) dscp (010000)
cs3      Set packets with CS3(precedence 3) dscp (011000)
cs4      Set packets with CS4(precedence 4) dscp (100000)
cs5      Set packets with CS5(precedence 5) dscp (101000)
cs6      Set packets with CS6(precedence 6) dscp (110000)
cs7      Set packets with CS7(precedence 7) dscp (111000)
default  Set packets with default dscp (000000)
ef       Set packets with EF dscp (101110)
```

After configuring the **ip dscp all** <*value*> command, the DSCP field on the IP header is set on every outgoing IP packet. The configuration overrides previous individual DSCP values set by other applications; this includes the delivery service-based QoS setting and the system-wide settings for QoS for unicast data.

There can only be one configuration of the **ip dscp all** command. Adding a second configuration fails if a configuration already exists.

To remove a DSCP setting, use the **no ip dscp all** <*value*> command. The value of the no form of the dscp all command must match exactly the configured setting. For example, to remove **ip dscp all cs1**, you must enter the **no ip dscp all cs1** command. If you entered **no ip dscp cs5**, the removal fails because the value does not match the existing setting.

Note The following commands have been removed:

ip dscp {**client** {**cache-hit** {**match-server** | **set-dscp dscp-packets** | **set-tos tos-packets**} | **cache-miss** {**match-server** | **set-dscp dscp-packets** | **set-tos tos-packets**}} | **server** {**match-client** | **set-dscp dscp-packets** | **set-tos tos-packets**}}

Turn Off Caching of Geo-Location Servers

The following command sets the timeout for caching the response from the Geo-Location server:

service-router location-based-routing location-cache timeout *<value_in_secs>*

The <value_in_secs> must be in range 0-864000 and 691200 is the default value.

If <value_in_secs> is 0, the response from the Geo-Location server is not cached on the SR.

For other values of <value_in_secs>, the response from the Geo-Location server is stored in the SR cache for the first instance and expires after <value_in_secs> seconds.

clear cache

When **clear cache content** command is entered, by default the system tries to evict 1000 MB of content from all the disks. If the SE model has 12 disks, then 1000 MB/12 = ~83 MB of content from each disk is slated for eviction.

This is because of the new FastCAL and Content Manager, where each disk has its own eviction tree, and content has to be evicted from each disk separately.

disk repair

The **repair-disk** utility provides progress indicators and displays a log of repaired sectors; it also provides more robust sector error detection, repair, and validation.

In Release 2.6, the **disk repair** command has been enhanced to provide equivalent functionality as the **repair-disk** utility.

show service-router

The **service-router subscribe domain** command provides a way to specify domains that the Service Router should subscribe to. By default, the Service Router takes all the domains specified in the CDSM. With the **service-router subscribe domain** command, even if only one domain subscription is configured subscription through the CLI, the service router takes the list of domains subscribed through the CLI to be complete list.

Following is an example of the **service-router subscribe domain** command:

```
(config)# service-router subscribe domain test3.com
```

Following is an example of the show service-router subscribe domain command:

```
# show service-router subscribe domain
    Domains subscribed:
        test1.com
        test5.com
        test4.com
        test3.com
```

service-monitor

In previous releases, a major alarm was raised when the number of failed CDNFS disks exceeded a threshold. The threshold was set using the **service-router service-monitor threshold failcntdisk <***number_of_CDNFS_disks***>** command on the SE. The default value was 1.

In Release 2.6, the keyword has been changed from **failcntdisk** to **faildisk** and the definition of the keyword has been changed to the overall percentage of CDNFS disk failures. In the current implementation, a major alarm is raised if the percentage of CDNFS disk failures exceeds the threshold value. The default value is 75 percent.

Table 4 describes the differences in the disk failure threshold between previous releases and Release 2.6.1.

Table 4 Disk Failure Threshold Differences in Release 2.6.1

Disk Failure Threshold in Previous Releases	Disk Failure Threshold in Release 2.6.1
Disk Fail threshold configuration is the number of CDNFS disks that can fail before raising the threshold alarm.	Disk threshold configuration is the overall percentage of CDNFS disk failure for raising the threshold alarm.
The range for configuration is <1-15>	Range is <1-100>, independent of hardware.

Table 4 Disk Failure Threshold Differences in Release 2.6.1 (continued)

Disk Failure Threshold in Previous Releases	Disk Failure Threshold in Release 2.6.1
Depends on CDNFS disk fail alarms to calculate the number of failed disks (false disk fail alarms can add to the disk fail threshold and raise the alarm)	The service monitor looks for active CDNFS volumes and calculates the percentage failure. Hence, no dependency on disk failure alarms. If a disk does not have a CDNFS mount point, then it is considered in-to the threshold value.
If the service monitor failcntdisk threshold is configured, upgrade to 2.6.0 (after CSCtr08547) will cause the configuration to be lost. The Configuration needs to be re-done after the upgrade.	The same behavior applies to downgrade of software. If the faildisk is configured before downgrade, it will be lost after downgrade. The configuration needs to be re-done after the downgrade.

Note Software upgrade leads to configuration loss of this setting. The configuration must be reset if you want something other than the default setting of 75 percent.

System Requirements

The Internet Streamer CDS runs on the CDE205, CDE220, and the CDE250 hardware models.

Note Release 2.6.1 does not support the CDE100 and CDE200.

Table 5 lists the different device modes for the Cisco Internet Streamer CDS software, and which CDEs support them.

Table 5 Supported CDEs

Device Mode	CDE205	CDE220-2G2	CDE220-2S3i	CDE250-2S6	CDE250-2M0
CDSM	Yes	No	No	No	No
SR	Yes	Yes	No	No	No
SE	Yes	Yes	Yes	Yes	Yes
SR—Proximity Engine standalone	Yes	Yes	No	No	No

CDE250-2S6 and CDE250-2M0 platforms have four interfaces at 10 gigabit Ethernet speeds and four interfaces at gigabit Ethernet speeds (plus two additional gigabit ethernet interfaces for management).

The CDE220-2S3i platform has a total of 14 gigabit Ethernet ports in this CDE. The first two ports (1/0 and 2/0) are management ports. The remaining 12 gigabit Ethernet ports can be configured as two port channels. See the *Cisco Content Delivery Engine CDE205/220/250/420 Hardware Installation Guide* for set up and installation procedures for the CDE220-2S3i and the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide* for information on configuring the Multi Port Support feature.

The CDE220-2G2 platform has a total of ten gigabit Ethernet ports. The first two ports (1/0 and 2/0) are management ports. The remaining eight gigabit Ethernet ports can be configured as one port channel. See the *Cisco Content Delivery Engine CDE205/220/250/420 Hardware Installation Guide* for set-up and installation procedures for the CDE220-2G2.

The CDE205 can run as the CDSM, Service Router, or Service Engine. See the *Cisco Content Delivery Engine CDE205/220/250/420 Hardware Installation Guide* for set-up and installation procedures for the CDE205.

Note For performance information, see the release-specific performance bulletin.

Limitations and Restrictions

This release contains the following limitations and restrictions:

- There is a 4 KB maximum limit for HTTP request headers. This has been added to prevent client-side attacks, including overflowing buffers in the Web Engine.
- Standby interface is not supported for Proximity Engine. Use port channel configuration instead.
- There is no network address translation (NAT) device separating the CDEs from one another.
- Do not run the CDE with the cover off. This disrupts the fan air flow and causes overheating.

Note The CDS does not support network address translation (NAT) configuration, where one or more CDEs are behind the NAT device or firewall. The workaround for this, if your CDS network is behind a firewall, is to configure each internal and external IP address pair with the same IP address.

The CDS does support clients that are behind a NAT device or firewall that have shared external IP addresses. In other words, there could be a firewall between the CDS network and the client device. However, the NAT device or firewall must support RTP/RTSP.

System Limits and Thresholds

This release has the following limits and thresholds:

Service Router Limits and Thresholds

The Service Router has memory-related limits and thresholds. Memory usage of the Service Router depends on the number of coverage zone entries, the number of Content Origin servers, the distribution of subnets in the Coverage Zone file, and the number of Service Engines in the CDS. From our tests using a sample Coverage Zone file, we have observed that we can support 20,000 Coverage Zone entries with 26 SEs, and 40 Content Origins servers.

Note The number of Coverage Zone entries, SEs, and Content Origin servers are subject to change depending on the Coverage Zone configured.

We recommend keeping the memory usage (both virtual and resident) below 1.5 GB.

Frequent configuration updates could cause memory fragmentation, which raises the memory usage.

Service Monitor Limits and Thresholds

When the Service Monitor thresholds are exceeded, an alarm is raised on the respective device and an SNMP trap is sent to the CDSM. The parameters monitored and thresholds for each component or protocol engine can be modified. The default thresholds are as outlined below.

Following are the parameters that are monitored on each device (SE, SR, and CDSM) and the default threshold setting of each parameter:

- CPU—80 percent
- Memory—80 percent
- Kernel memory—50 percent
- Disk usage—0 percent
- Disk failures—75 percent
- Augmentation alarms—80 percent

Following are the parameters that are monitored only on the SE, along with default threshold setting of each parameter:

- Windows Media Streaming thresholds—90 percent
- Flash Media Streaming thresholds—90 percent
- Movie Streamer—90 percent%

- Maximum number of concurrent sessions—200
- Maximum Bandwidth—200,000 kbps
- NIC bandwidth—90 percent
- Burst Count—1

Web Engine Limits and Thresholds

The Web Engine has the following limits and thresholds:

- Memory Usage
- Session Limits
- CAL Limits

Memory Usage

In Release 2.5.9, the memory threshold on each SE is 3.2 GB. If the threshold is exceeded, the memory_exceeded alarm is raised and trickle mode is enabled. In Release 2.5.9, the admission control is based on 30,000 session and 3.2 GB of memory.

In Release 2.6.1, the memory threshold on each SE is 3.2 GB. If the threshold is exceeded, the memory_exceeded alarm is raised. In cases where the memory reaches 3.7 GB, trickle mode is enabled and eventually the Web Engine is restarted. The above memory values, and the 20,000–60,000 sessions and 100,000 open file/socket descriptor (FD) limit are used for admission control in Release 2.6.1.

Session Limits

Web Engine supports the following session-threshold limits:

- 49,800 session count for the CDE250
- 15,000 session count for all other CDEs

The max_session_exceeded alarm is raised if the session-threshold limit is reached. If further requests are sent to the SE even when the session threshold is reached, the Web Engine attempts to process the requests but does not accept any more requests when the request count reaches 60,000 on a CDE250, and 20,000 on all other CDEs.

CAL Limits

Outstanding CAL Lookup threshold is 25,000 on the CDE250 and 15,000 on all other CDEs. The WebCalLookupThreshold alarm is raised on reaching this threshold limit.

Outstanding CAL disk Write threshold is 3,000 CAL requests (create, update, delete, popularity update) on the CDE250, and 1,500 on all other CDEs. The WebCalDiskWriteThreshold alarm is raised on reaching this threshold.

Other CAL thresholds are as follows:

- File Descriptor usage threshold is 85 percent
- TEMPFS usage threshold is 80 percent
- Active datasource threshold is 2,000

Note CAL-related thresholds and the File Descriptor-related thresholds are introduced in Release 2.6.1.

Web Engine thresholds are also applicable to adaptive bit rate (ABR) streaming.

CDSM Limits and Thresholds

The CDSM has the following limits and thresholds:

- RPC Connections
- File Synchronization
- CDSM Availability (primary and standby)
- SE Configuration Change Synchronization

RPC Connections

A maximum of 40 RPC connections are supported among the managed devices (SE, SR, standby CDSM, and primary CDSM). The RPC connection maximum is defined in the httpd.conf.rpc configuration file located in the /state directory.

File Synchronization

The primary CDSM checks for file updates and synchronization with the managed devices (SE, SR, and standby CDSM) every ten minutes.

CDSM Availability (primary and standby)

The SE and SR check for the availability of the primary and standby CDSM on a regular interval; however, if the CDSM does not respond, the SE and SR use an exponential-backoff call for retrying the connection.

The exponential backoff call means that if the CDSM does respond to the first attempt, the SE or SR sleep for ten seconds before trying again. If the second attempt does not succeed, the wait time doubles (20 seconds), if that attempt does not succeed, the wait time doubles again (40 seconds). The wait time doubles every attempt (10, 20, 40, 80, and so on) until the maxWaitingTime of 320 seconds.

SE Configuration Change Synchronization

The period of time before the local configuration manager (LCM) on an SE sends a configuration change to the primary CDSM is a maximum of 2.25 times the polling rate. The polling rate is configurable through the CDSM GUI (**System > Configuration > System Properties**, System.datafeed.pollRate).

RTSP Gateway and Movie Streamer

The default RTSP Gateway transactions per second (tps) is 40. There are no other limits to the RTSP Gateway.

The Movie Streamer default maximum concurrent session is 200 and the default maximum bandwidth is 200 Mbps.

Windows Media Streaming

Windows Media Streaming has the following limits and thresholds:

- Windows Media Streaming recommended concurrent remote server sessions 300

Note Regarding concurrent remote server sessions, if all requests are unique cache-miss cases, Windows Media Streaming can reach up to 1000 sessions of 1 Mbps file each. Windows Media Streaming can sustain 1000 remote server sessions at most if the Content Origin server can respond, but the recommended value is 300.

- Windows Media Streaming transactions per second is 40 (because of the RTSP Gateway limitation).
- Memory threshold 3 GB
- CPU threshold is 80 percent

Flash Media Streaming

With the basic license, Flash Media Streaming the default maximum concurrent sessions is 200 and the default maximum bandwidth is 200 Mbps.

Buying more licenses can increase the concurrent sessions and maximum bandwidth as follows:

- CDE220-2G2 and CDE220-2S3—15,000 concurrent sessions and 8 Gbps maximum bandwidth
- CDE250-2M0—40,000 concurrent sessions and 40 Gbps maximum bandwidth

We recommend that the Flash Media Streaming process memory usage not exceed 3 GB resident set size (RSS). If the memory usage for Flash Media Streaming exceeds 3 GB RSS, a threshold exceeded alarm is raised.

Note RSS is the portion of a process that exists in physical memory (RAM), as opposed to virtual memory size (VSIZE), which includes both RAM and the amount in swap. If the device has not used swap, the RSS number is equal to VSIZE.

Important Notes

To maximize the content delivery performance of a CDE205, CDE220, or CDE250, we recommend you do the following:

1. Use port channel for all client-facing traffic.

   Configure interfaces on the quad-port gigabit Ethernet cards into a single port-bonding interface. Use this bonding channel, which provides instantaneous failover between ports, for all client-facing traffic. Use interfaces number 1 and 2 (the two on-board Ethernet ports) for intra-CDS traffic, such as management traffic, and configure these two interfaces either as standby or port-channel mode. Refer to the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide* for detailed instruction.

2. Use the client IP address as the load balancing algorithm.

   Assuming ether-channel (also known as port-channel) is used between the upstream router/switch and the SE for streaming real-time data, the ether-channel load balance algorithms on the upstream switch/router and the SE should be configured as "Src-ip" and "Destination IP" respectively. Using this configuration ensures session stickiness and general balanced load distribution based on clients' IP addresses. Also, distribute your client IP address space across multiple subnets so that the load balancing algorithm is effective in spreading the traffic among multiple ports.

   Note The optimal load-balance setting on the switch for traffic between the Content Acquirer and the edge Service Engine is dst-port, which is not available on the 3750, but is available on the Catalyst 6000 series.

3. For high-volume traffic, separate HTTP and WMT.

   The CDE205, or CDE220 performance has been optimized for HTTP and WMT bulk traffic, individually. While it is entirely workable to have mixed HTTP and WMT traffic flowing through a single server simultaneously, the aggregate performance may not be as optimal as the case where the two traffic types are separate, especially when the traffic volume is high. So, if you have enough client WMT traffic to saturate the full capacity of a server, we recommend that you provision a dedicated server to handle WMT; and likewise for HTTP. In such cases, we do *not* recommended that you mix the two traffic types on all CDE servers which could result in suboptimal aggregate performance and require more servers than usual.

4. For mixed traffic, turn on the HTTP bitrate pacing feature.

   If your deployment must have Streamers handle HTTP and WMT traffic simultaneously, it is best that you configure the Streamer to limit each of its HTTP sessions below a certain bitrate (for example, 1Mbps, 5Mbps, or the typical speed of your client population). This prevents HTTP sessions from running at higher throughput than necessary, and disrupting the concurrent WMT streaming sessions on that Streamer. To turn on this pacing feature, use the HTTP bitrate field in the CDSM Delivery Service GUI page.

   Please be aware of the side effects of using the following commands for Movie Streamer:

   ```
   Config# movie-streamer advanced client idle-timeout <30-1800>
   Config# movie-streamer advanced client rtp-timeout <30-1800>
   ```

   These commands are only intended for performance testing when using certain testing tools that do not have full support of the RTCP receiver report. Setting these timeouts to high values causes inefficient tear down of client connections when the streaming sessions have ended.

   For typical deployments, it is preferable to leave these parameters set to their defaults.

5. For ASX requests, when the Service Router redirects the request to an alternate domain or to the origin server, the Service Router does not strip the .asx extension, this is because the .asx extension is part of the original request. If an alternate domain or origin server does not have the requested file, the request fails. To ensure requests for asx files do not fail, make sure the .asx files are stored on the alternate domain and origin server.

Open Caveats

This release contains the following open caveats:

Content Manager

- CSCtu32965

  Symptom:

  The Content Manager process creates a coredump file when the CLI timeouts while a delivery service with lots of contents gets removed.

  Conditions:

  The coredump happens whenever the main Content Manager thread is busy for a long a time and an edm message arrives to Content Manager at the same time.

  Workaround:

  None.

NAS

- CSCtt42310

  Symptom:

  CdsOriginMgr (cds-origin-mgr) process stops responding to operations.

  Conditions:

  Unknown

  Workaround:<

  Restart the process by entering the following command to correct this issue:

  ```
  service cds-origin-mgr restart
  ```

Movie Streamer

- CSCts99039

  Symptom:

  System runs into OOM kdb state.

  Conditions:

  MS VOD preposition or cache hit. More than 500 Simultaneous users. Rtsp gateway processes use too much memory and cause kernel not be able to allocate memory for new requests.

  Workaround:

  Set movie streamer concurrent session limit to 500.

Data Server

- CSCts74627

  Symptom:

  The system is running slow on login, cli, and other dataserver related actions.

  Conditions:

  Service router process on SR is using more than 65535 file descriptors, It issues new connection to data server.

  Workaround:

  Restart service router process.

Windows Media Streaming

- CSCts83930

  Symptom:

  WMT cached content is not removed from cache for revalidation request.

  Conditions:

  The content is removed on content origin.

  Workaround:

Delete the content via cli "clear content url xxx"

- CSCts41691

  Symptom:

  In VOD case, Fast Forward/Rewind (FF/RW) request from a WMT media client fails

  Conditions:

  If following 6 steps happens in order,

  1. WMT receives a FF/RW request (the play scale > 0), let's say this is in session 1.
  2. Client pauses the session 1.
  3. Client resume playing the session 1 in normal speed (scale == 0).
  4. WMT receives another FF/RW request (the play scale > 0) for the same content, let's say this is in session 2.
  5. Client pauses the session 2.
  6. Client seek playing the session 2 in normal speed (the play scale == 0) with same npt (normal play time) with step 3 of session 1.

  The subsequence FF/RW request issued in either session 1 or session 2 will fail.

  Workaround:

  Close the media client and issue the FF/RW request again.

Platform

- CSCts24450

  Symptom:

  Under rare circumstances, there are times when diskman will allow multiple SYSTEM drives to co-exist in the system indefinitely.

  Conditions:

  Consider the following use-case:

  1. Disk02 "pulled" without doing a **disk unuse** command.
  2. Disk03 was marked bad/good, then a "disk policy apply" performed.
  3. Disk02 was re-inserted.

  This resulted in disk00/disk01/disk02 all being "SYSTEM" disks.

  Workaround:

  Should this condition ever occur, the following workaround recovers the SYSTEM drives and resolve the RAID1 conflicts:

  1. Off-line the CDE.
  2. Enter the **disk recover-system-volumes** command.

     This erases all content on all SYSTEM drives.
  3. Re-install the desired CDE software release (for example, **copy http install** command).
  4. Reload the CDE.

- CSCts65440

Symptoms:

See following messages in /local/local1/var/log:

```
named[8890]: %SE-UNKNOWN-4-899999:
client 127.0.0.1#33208: RFC 1918 response from Internet for 145.59.152.10.in-addr.arpa
```

Conditions:

Internal calls to sshd or ntpd will trigger a reverse dns lookup through named. This lookup will fail with an external dns server.

Workaround:

Use internal DNS internal.

- CSCts96782

  Symptom:

  If the Conditions (please see below) are met, then the data of one or more SSDs may be partially corrupted / lost during I/O write activity.

  Conditions:

  Either an unplanned power-failure / power-cycle, or the user executing the "shutdown poweroff" CLI command. This only applies to the CDE220-2S3I platform.

  Workaround:

  The only known workaround is to avoid sudden power-failures / power-cycling to the system.

  Always attempt to execute the CLI "reload" command to cleanly shutdown the system.

CAL

- CSCts14836

  Symptom:

  Under stress condition of movie streamer, rtspd (rtspgateway) process coredumped with backtrace pointing to uns-client-library.

  Conditions:

  UNS clients does memory mapped IO to cdnfs partition. When the cdnfs partition goes bad (or that particular sector goes bad), during when if UNS clients tries to access those bad portion of the disk will result in IO error. In memory mapped IO case, when disk produces IO error will result in SIGNAL 7 (bus error) Hence this coredump.

  Workaround:

  None exist at this point.

Flash Media Streaming

- CSCtt97134

  Symptom:

  The fmsedge process creates a coredump file randomly in the SE when the SE is under stressed longevity. The coredump backtrace shows during the system monitoring check the core created.

  Conditions:

  The coredump happens after a week-long longevity stress environment.

Workaround:

None. The fmsedge process is only involved during the session setup (for all RTMP varieties, except RTMPT); so the coredump should not cause any service disruption except when RTMPT is used. The process gets restarted automatically and should not cause any other issue.

- CSCtr61896

  Symptom:

  The fmscore process coredumps seen under very high stress.

  Conditions:

  Under too much of stress (alarms generated before), fmscore process coredumps randomly

  Workaround:

  Nothing found at this point. But if SR is there in the deployment, then this issue should not be seen as there were alarms generated before this coredump

- CSCtr93692

  Symptom:

  The fmsedge process coredump is seen randomly, when fms was rejecting all the requests due to BW or connection is high.

  Conditions:

  In this particular case, the number of fms max con-current connection is set to 200 and 3000tps requests is been sent. The fmsedge tries to reject all those extra requests and spirent tries to catch up the number of active connections. During this heavy reject period, fmsedge coredumped randomly.

  Workaround:

  This issue should not be seen if SR is there in the picture

Authorization Server

- CSCtr45127

  Symptom:

  Under high load, when the Rules XML contains large number of URL_Resolve (or multiple Url_Rewrites) then AuthServer timeout is seen.

  Conditions:

  When the Rules XML contains large number of URL Rewrite's, the AuthServer becomes busy and causes timeouts. The rules re-write is a computation intensive operation. If we have large number of URL rewrites configured, the AuthServer process gets busy and is not able to respond to incoming request within the acceptable time. Therefore timeout is seen.

  Workaround:

  The Rules XML configuration needs to be changed to have one set of Rule_UrlResolve that matches one pattern group for an incoming request.

Proximity Engine

- CSCtc20212

  Symptom:

  The following messages can be seen on a neighbor router when the BGP password is unconfigured on Proximity Engine, after the BGP adjacency has been formed, but corresponding removal is not performed on the router:

  ```
  *Feb  7 03:32:14.861: %TCP-6-BADAUTH: No MD5 digest from 192.168.82.33(179) to
  192.168.82.2(24018)
  *Feb  7 03:34:00.573: %TCP-6-BADAUTH: No MD5 digest from 192.168.82.33(179) to
  192.168.82.2(24018) (RST)
  ```

  Conditions:

  This issue occurs when adjacency is established with a neighboring router and the password is removed from Proximity Engine configuration and not re-configured within the hold time. Occurred in Release 2.5.3, as well as Release 2.5.9.

  Workaround:

  When the password is unconfigured on the Proximity Engine side, the two peers cannot communicate with each other. This state is reported on the router side with the following repeated messages:

  ```
  *Feb  7 03:32:14.861: %TCP-6-BADAUTH: No MD5 digest from 192.168.82.33(179) to
  192.168.82.2(24018)
  ```

  This occurs until the TCP connection is closed on Proximity Engine side and enters TIME_WAIT state. While this state lasts, no messages are printed on the router. The router is still retransmitting TCP packets, but the Proximity Engine is ignoring them, as per TIME_WAIT state. After about 60–75 seconds, the following messages start to display on the router:

  ```
  *Feb  7 03:37:32.937: %TCP-6-BADAUTH: No MD5 digest from 192.168.82.33(179) to
  192.168.82.2(24018) (RST)
  ```

  These indicate that the TCP connection has been completely closed on the Proximity Engine side, which therefore no longer has any knowledge of the TCP connection and responds to each retransmitted packet with an RST packet, which does not have an MD5 signature. This situation is described in RFC 2385, section 4.1 (Connectionless Resets). The messages are logged as long as the router retransmits TCP packets of the lost connection, which has been observed to occur for up to ten minutes. This issue does not affect correct operation.

CDSM

- CSCtu51601

  Symptom:

  Content-based routing is enabled for the Service Router and also at the Origin server configuration from GUI perspective, but from Service Router perspective, the content-based routing is only enabled globally and disabled for all delivery services.

  Conditions:

  After upgrading to Release 2.6.1 from Release 2.5.x.

Workaround:

After upgrading to Release 2.6.1, resubmit each Content Origin configuration in the CDSM GUI by going to **Services > Service Definition > Content Origins**, editing the Content Origin, and clicking **Submit**.

Service Router

- CSCtu43262

  Symptom:

  When an SE is offloaded and brought back online, the **show statistics se** command output on the SR still shows it as down.

  Conditions:

  This happens when the status update from the CDSM reaches the SR before the status update from the SE reaches the SR.

  Workaround:

  Any dummy configuration update should fix the issue. A configuration update could be any of the following:

  1. 1Assigning and unassigning the SE from any delivery service.
  2. Any routing related changes on the SR (content-based-routing, location-based-routing, proximity-based routing changes, ACC policy enabled or disabled, DNS-based redirection changes, or last resort configurations).
  3. Addition or deletion of delivery services.
  4. Any changes to Coverage Zone file.
  5. Changes to domain subscription.

Resolved Caveats

The caveats listed in this section have been resolved since Cisco Internet Streamer CDS Release 2.6.1. Not all the resolved issues are mentioned here. The following list highlights the resolved caveats associated with customer deployment scenarios.

CDSM

- CSCts28866

  Symptom:

  Configuring access list involving network range is erased after a few seconds.

  Conditions:

  Always.

- CSCts21219

  Symptom:

  Through CDSM GUI, we can configure 2,107,483,647 bitrate for incoming and outgoing also shows the configured value in CDSM. When we check it in SE it shows configured value as 40,000,000 (Max bit rate the platform supports).

  Conditions:

  CDSM allows configuration greater than maximum allowed.

- CSCts05524

  Symptom;

  The Flash Media Streaming maximum bandwidth and maximum sessions in CLI setting is platform dependent. CDSM GUI needs to show and check different maximum values for them depending on the device hardware model.

  Conditions:

  CLI configuration change for Flash Media Streaming.

- CSCtq59730

  Symptom:

  SE goes offline when enabling Fast SE offline detection.

  Conditions:

  This issue can be triggered by changing the UDP port on the CDSM GUI page.

Unified Kernel Streaming Engine (UKSE)

- CSCts09633

  Symptom:

  Under huge stress (clients > 6k) for WMT live requests, CLI stream statistics show a huge value for the outgoing streams bytes sent field.

  Conditions:

  Under huge stress.

- CSCto75362

  Symptom:

  After Windows Media Streaming live client stops under stress conditions, the **show statistics wmt streamstat** command may show a few remaining session of incoming and outgoing for another 15 to 20 minutes.

  Conditions:

  It happens for Windows Media Streaming live, with lots of client coming and leaving quickly.

Web Engine

- CSCtz21525

  Symptom:

  The iostat.log file is not truncated, local/local1 disk space use at risk.

Conditions:

Normal use.

- CSCts99053

  Symptom:

  1. All the 4 SRs and 1 backup CDSM were reported to be down on the primary CDSM. Only these 5 devices were observed to flip between online and offline modes while the SE's status seem to be ok.
  2. There were no reported interruption to the end user. But the CDN monitoring system (CDSM) is reported to be unreliable.
  3. Huge /local/local1/logs/rpc_httpd/ssl_scache.pag file size (~44GB) on the primary CDSM.
  4. No core files observed.

  Conditions:

  SRs/SEs/backup CDSM send http[s] messages to the primary CDSM which is handled by the rpc_httpd process on the CDSM. These requests are the http[s] messages that report the health of the various nodes to CDSM.

  Apache(rpc_httpd) uses ssl_scache.pag file to speed up parallel request processing by avoiding unnecessary session handshakes. At every SSLSessionCacheTimeout interval the global/inter-process SSL Session Cache information is timed out, with the httpd process acquiring a lock and traversing the records. Due to the size of the file (44gb) this operation is taking excessively long time thereby blocking other processes from reading the file for session information.

  Since the customer enabled "Fast SE Offline Detection mode", the SEs health is communicated to the CDSM using UDP messages (and not the http[s] mechanism). This corresponds to what was observed, where only the backup CDSM and the SRs were offline, while the SEs were reported to be online.

  Happens once every 6 months (with 50+ SEs, 4SRs and 1 backup CDSM communicating with the primary CDSM using SSL.

- CSCts20324

  Symptom:

  WE core-dumped during stress.

  Conditions:

  1. Pragma: no-cache header

  2. 1 byte content

  3. Throughput objective: 40Gbps

  4. Single

- CSCtn74299

  Symptom:

  The Web Engine generates a core dump in a particular scenario.

  Conditions:

  High stress Windows Media Streaming HTTP traffic is running, and Windows Media Streaming threshold is exceeded. This causes the Windows Media Streaming process to not accept the Web Engine HTTP forwarded request, and can cause Web Engine to core dump.

- CSCtn70651

  Symptom:

  The Web Engine crashes and the existing sessions are terminated. The process is restarted immediately and subsequent requests are handled seamlessly.

  Conditions:

  This occurs when a URL request is 2048 characters or longer and the request is handled by the Web Engine custom log format with both %r (to print the request first line) and %U (to print the url) in the format string.

- CSCtj71423

  Symptoms:

  Web Engine experiences read time outs from the Authorization Server during an 8-hour, all unique, cache-fill test.

  Conditions:

  This occurred in a three-tier topology with a Content Acquirer, middle tier, and edge SE all configured on CDE220-2S3 platforms. The transactions per second were around 50 to 60. The testing used all unique cache-fill content with one Spirent client port and 1 Spirent Server port. The file size was set to 500 KB. The test lasted eight hours.

```
10/23/2010 16:25:31.207(Local)(8159)ERRO:AuthSvrQuery.cpp:30-> Time out occurred with
authsvr read
10/23/2010 16:25:31.207(Local)(8159)ERRO:HTTPCacheAppCtxt.cpp:1510-> WorkerPid[8454]
HTTPCacheApp[0xeef02968] :  AppCtxt(0xe86a2158) Auth Server Query Error (-1),
AuthSvrQuery(0xe869bc08)
10/23/2010 16:25:31.207(Local)(8159)ERRO:HTTPCacheAppCtxt.cpp:1633-> WorkerPid[8454]
HTTPCacheApp[0xeef02968] :  AppCtxt(0xe86a2158) - Received Error (500) - Complete
```

- CSCth22448

  Symptom:

  Zeri VOD playback fails in a particular scenario.

  Conditions:

  The per-delivery service pacing is set to 1 Mbps and there is two-tier setup for the SEs.

Cache Router

- CSCtr05823

  Symptom;

  Cache Router dumps core.

  Conditions:

  Happens sometimes when there is a connection issue with upstream device.

- CSCtj25001

  Symptom:

  The Cache Router goes into core dump during Web Engine small-objects stress testing.

  Conditions:

  This occurs in a two-tier setup (Client->Edge->Acq->OS) with all unique cache-miss stress, running for about a day. The transactions per second was 200.

Service Router

- CSCty99937

  Symptom:

  After upgrading to Release 2.6.1,certain SEs were not receiving any requests.

  Added ten new delivery services and associated SEs. Location-based routing was used to identify a particular POP (set of SEs provisioned to serve a certain region, for example, North East America).

  Content-based routing is enabled, which is used to identify a SE within the POP.

  Conditions:

  Release 2.6.1, 2.5.9, or 2.5.11.10.

  Service Router has content-based routing enabled.

- CSCtu00872

  Symptom:

  Service Router falling back to last resort in some cases

  Conditions:.

  When requests for Service Engine alias with a domain it is not subscribed to are received, after which requests are received, for which that Service Engine is chosen for a domain it is subscribed to. The requests fails over to last resort.

- CSCts32077

  Symptom:

  SR does not detect SE interfaces.

  Conditions:

  When SE is configured with 10 GE interfaces as streaming interfaces.

- CSCts24932

  Symptom:

  Coverage zone file takes along time to load.

  Conditions:

  When the size of the coverage zone file being uploaded is very large. It took multiple hours to load a coverage zone with 48,000 entries.

- CSCtf67735

  Symptom:

  Memory usage of service route increases a lot and leads to coredump.

  Conditions:

  We see the memory leak when both these conditions are true:

  - There is only one se assigned to the delivery service and the se becomes unavailable (reloaded/offloaded).
  - There are a lot of requests from http 1.1 where there are multiple requests within the same http session.

- CSCtj83262

  Symptom:

  The Service Router sometimes goes into a core dump after uploading 4 MB Coverage Zone file.

  Conditions:

  The Coverage Zone file is too large (28,000 entries), with 10 delivery services, and multiple SEs. Occurred in Release 2.5.3, as well as Release 2.5.9.

MP3 Live Streaming

- CSCtk66500

  Symptom:

  Web Engine goes into core dump on the edge SE or middle SE, when the origin server or the Content Acquirer restarts during playback.

  Conditions:

  During the MP3-live playback, restart the Web Engine on the Content Acquirer or stop the encoder process on origin server. When the origin server restarts, all the SEs go into core dump. When the Web Engine restarts on the Content Acquirer, the middle SE and edge SE go into core dump.

Content Manager

- CSCtu21656

  Symptom:

  High disk I/O is noticed when a device was unsubscribed from a delivery service and the device had a few million content objects for that delivery service. This high disk I/O caused the SR not to send any request to this SE for some time.

  Conditions:

  When a device is part of a delivery service and has a few million content objects, if the device is unsubscribed from that delivery service, after five minutes the Content Manager is triggered to delete the millions of cached content. This deletion triggers lots of I/O to the disk.

- CSCts21599

  Symptom:

  When ContentMgr knows the contents that are not on the CDNFS. During eviction or show content-mgr content CLI, ContentMgr needs to find the content URL by accessing the contents on the disk. Since there is no such content on the disk, ContentMgr will throw an error which stating "fail to stat content, no such file."

  During sanity, ContentMgr validates all the content it knows, hence it shows how many invalid entries there are and cleans up all of them.

  Conditions:

  In a race condition when content update right after content eviction, ContentMgr thinks the update as new content is added. Hence, it logged as added. In this situation, content is evicted but ContentMgr still think it's a newly added content.

The invalid entry can also happen during snapshot and eviction operation. Snapshot writer is a forked process which writes all the content ContentMgr know at the moment to the snapshot files on each disk. Right after the forked, if some contents are evicted will still be recorded in the snapshot file. If ContentMgr restarts/coredump for some reason, then after restarts, ContentMgr will receive invalid entry from Snapshot reader which reads snapshot files.

- CSCts16697

  Symptom:

  When disk bucket threshold reaches on multiple disk-buckets, only one alarm is shown (alarm must be shown for each failed disk-bucket).

  Conditions:

  If multiple CDNFS disk failures (or disk un-mounts) happen leading to multiple disk-buckets reaching the configured threshold fail percentage, this problem would be seen.

- CSCts14395

  Symptom:

  When current object count is more than "cache content max-cached-entries" configured, ContentMgr starts to evict contents. However, if ContentMgr evicts more than configured, it assert itself.

  Conditions:

  When ContentMgr evicts more than configured, it assert itself hence coredump.

- CSCtr58223

  Symptom:

  Content Distribution in disks was unbalanced when caching MS and WMT content.

  Conditions:

  After disk eviction ran for a long time, contents became poorly distributed among disks. This was caused by evicting parent content in one disk that would evict child content in another. Since we only tracked parent content, CotentMgr did not have accurate information as to the size of the content in each disk.

Movie Streamer

- CSCtr44103

  Symptom:

  Movie Streamer restarts and if restarts too often, it is disabled by nodemgr.

  Conditions:

  Mov/mp4 files for preposition are generated by mp4box. If concurrent session is high. Too many memory is used and ENOMEM happens.

NAS

- CSCts31937

  Symptom:

  Content streaming from NAS mount failed even though all NAS mounts are healthy.

  Conditions

This is a race condition. When this happens, FastCAL holds a copy of staled NAS configuration, and not syncing up with the changes in shared memory. This condition persist.

- CSCts33205

  Symptom:

  CLI does not provide enough information/feedback to user when using show content-origin command

  Conditions:

  When user input wrong OFQDN name from CLI, they can not tell it is invalid or nothing is configured for a valid content origin.

CAL

- CSCtr98018

  Symptom:

  When the device has millions of cached content and administrator executes "cdnfs cleanup start", it takes very long time to complete it.

  Conditions:

  CDNFS clean up is the CLI to sync content from CDNFS to database to make sure are they valid content. "cdhnrf cleanup start" will scan disk for doing this operation and if there are millions and millions of content, then this CLI takes long to precess all the contents.

Platform

- CSCtx49711

  Symptom:

  The rootfs process could reach greater than 90 percent and cause an alarm.

  Conditions:

  The MegaSAS.log file under root may increase to a huge size.

- CSCtu10985

  Symptom:

  After upgrade, timezone defaults to PDT, instead of UTC.

  Conditions:

  This happens after upgrading from Release 2.5.x to Release 2.6.1.

- CSCts68691

  Symptom:

  On the CDE250-2M0 and CDE250-2S6 platforms, a faulty HDD/SSD may (under very rare circumstances) cause either the boot process to hang, or cause CLI commands issued to the faulty drive to hang indefinitely.

  Conditions:

  While the exact condition(s) leading up to such a HDD/SSD drive failure is unclear, it is suspected that a sudden power-loss/power-cycle may induce such failures.

- CSCtt32765

Symptom:

No coredump alarm is generated even though there are coredump files.

Conditions:

When coredump file size is over 2 GB, CDS-IS software does not generate coredump alarm.

- CSCts30852

  Symptom:

  For the CDE250, processor hyperthreading may be inadvertently disabled. To detect this condition, enter the **show tech-support** command.

  Verify that the number of logical CPUs is 16 by looking for the following line:

  ... output omitted...

  Total 16 CPUs.

  If the above output indicates there are only 8 CPUs, then hyperthreading has been disabled.

  Conditions:

  The root-cause of this is a BIOS configuration issue during manufacturing.

- CSCts30808

  Symptom:

  On 2CDE220-S3I and CDE220-2S6 platforms, the WebBIOS may display the following error message:

```
LSI MegaRAID SAS-MFI BIOS
Version 2.03.00 (Build October 03, 2008)
Copyright(c) 2008 LSI Corporation
HA -0 (Bus 18 Dev 0) MegaRAID SAS PCI Express(TM) ROMB
FW package: 9.0.1-0042
```

  Memory/battery problems were detected. The adapter has recovered, but cached data was lost. Press any key to continue, or 'C' to load the configuration utility.

  Conditions:

  This occurs whenever there is a failing/failed MegaRAID battery backup unit (BBU), and the system is suddenly power-cycled.

Transaction Logs

- CSCts20146

  Symptom:

  Translog file name logged with vip address instead of SE ip.

  Conditions:

  On Se, configure the direct server return vip address as follows.

  direct-server-return vip 1.1.1.1

- CSCts01841

  Symptom:

  Transaction logs export to SFTP server fails.

  Conditions:

The SSH key of the SFTP server has changed (because of, for example, sw re-install, key regeneration, and so on).

UNS

- CSCts16752

  Symptom:

  UNS process coredump seen in the SE.

  Conditions:

  when content-mgr was restarting multiple times (due to another bug), which results in shared memory reset frequently, during the same time, when UNS starts, it fails to attach to shared memory which results in calling assert().

Windows Media Streaming

- CSCtu28774

  Symptom:

  Non-corrupted cached content was reported corrupt by asf_dump utility.

  Conditions:

  Content files larger than 2 GB.

- CSCts23924

  Symptom:

  For all unique cache-miss cases, during cache-fill stage, Windows Media Streaming can only sustain about 200 concurrent users.

  Conditions:

  All unique cache-miss cases.

- CSCts22407

  Symptom:

  Windows Media Streaming backend process caused a core dump file to be created during post-processing of a VOD fast-forward or rewind request.

  Conditions:

  Only happens in VOD pass-through logic when a client is sending a fast-forward or rewind request. Windows Media Streaming front-end process received an end-of-stream (EOS) message during the front-end process or post-process pausing message.

- CSCts20792

  Symptom:

  wmt augment alarm is not cleared if service monitor alarm is disabled.

  Conditions:

  Same as symptom. Wmt augment alarm is not cleared if service monitor alarm is disabled.

Data Server

- CSCtq78801

  Symptom:

  A core file is generated by the Web Engine.

  Conditions:

  In stress, there are many liveness queries simultaneously from other SEs.

  Workaround:

  No need to have a workaround, the Web Engine is restarted by the nodemgr automatically.

Live Routing

- CSCtu08478

  Symptom:

  Windows Media Streaming live stream request goes directly to Origin server from non-Content Acquirer Service Engines.

  Conditions:

  Primary Content Acquirer was reloading or down. Some liveness query to backup Content Acquirer returns failure on Windows Media Streaming engine alive.

CLI

- CSCty82644

  Symptom:

  The admin-shell process goes into core dump.

  Conditions:

  Log in using SSH or Telnet to SE, SR, or CDSM by using the “expect” script instead of manually, and disconnect the SSH or Telnet session immediately after sending the **exit** command.

Upgrading to Release 2.6.1

Release 2.6.1 supports upgrades from Release 2.5.9 and Release 2.5.11. If your CDS is running an older release, you need to upgrade to one of these releases before upgrading to Release 2.6.1.

Note CDE100 and CDE200 is end-of-life and Release 2.6.1 does not support the CDE100 and CDE200.

After the upgrade procedure starts, do not make any configuration changes until all the devices have been upgraded.

Note As part of the upgrade to Release 2.6.1, all disks (including CDNFS disks) are reformatted. All content is erased. For Service Engines, this means that prefetched metadata and content need to be redistributed from upstream SEs after the software upgrade is complete. Cached content is not preserved.

Log files and configuration files are saved to one of the disk drives on the device while the other drives are formatted, and then copied back over to the original location. With any sizable amount of logs this can take awhile (over 30 minutes on average).

For information on the upgrade procedure, see the *Cisco Internet Streamer CDS 2.6 Software Upgrade Guide.*

Note When upgrading the Content Acquirers in a delivery service, to avoid having a critical alarm generated while the Content Acquirer is being upgraded, temporarily set the System.datafeed.pollRate field to 200 seconds or higher. When the upgrade is complete, reset the field to the original value. See the "System Properties" section in the "Configuring the System" chapter of the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide* for more information.

Note If you downgrade from Release 2.6.1 to Release 2.5.9, you will see that the **show acquirer progress** command incorrectly shows the acquired crawl items count as the same as before upgrading to Release 2.6.1. This is incorrect because all disks were reformatted as part of the upgrade to Release 2.6.1. To correct this, restart the acquiring and distribution process.

Documentation Updates

The following documents have been added for this release:

- *Release Notes for Cisco Internet Streamer CDS 2.6.1*
- *Cisco Internet Streamer CDS 2.6 Software Upgrade Guide*

The following documents have changed:

- *Cisco Internet Streamer CDS 2.6 Software Configuration Guide*
- *Cisco Internet Streamer CDS 2.6 Command Reference Guide*
- *Cisco Internet Streamer CDS 2.6 Quick Start Guide*
- *Cisco Internet Streamer CDS 2.6 Alarms and Error Message Guide*
- *Cisco Internet Streamer CDS 2.6 API Guide*
- *Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide*

Related Documentation

Refer to the following documents for additional information about the Cisco Internet Streamer CDS 2.6:

- *Cisco Internet Streamer CDS 2.6 Software Upgrade Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_6/upgrade_guide/upgrade.html
- *Cisco Internet Streamer CDS 2.6 Software Configuration Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_6/configuration_guide/is_cds26-cfguide.html

- *Cisco Internet Streamer CDS 2.6 Quick Start Guide*

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_6/quick_guide/ISCDSQuickStart.html
- *Cisco Internet Streamer CDS 2.6 API Guide*

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_6/developer_guide/is_cds_26_apiguide.html
- *Cisco Internet Streamer CDS 2.6 Command Reference Guide*

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_6/command_reference/Command_Ref.html
- *Cisco Internet Streamer CDS 2.6 Alarms and Error Messages Guide*

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_6/message_guide/messages.html
- *Cisco Content Delivery System 2.x Documentation Roadmap*

  http://www.cisco.com/en/US/docs/video/cds/overview/CDS_Roadmap.html
- *Open Source Used in Cisco CDS-IS 2.6*

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_6/third_party/open_source/OL-25149-01.pdf
- *Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide*

  http://www.cisco.com/en/US/docs/video/cds/cde/cde205_220_420/installation/guide/cde205_220_420_hig.html
- *Regulatory Compliance and Safety Information for Cisco Content Delivery Engines*

  http://www.cisco.com/en/US/docs/video/cds/cde/regulatory/compliance/CDE_RCSI.html

The entire CDS software documentation suite is available on Cisco.com at:

http://www.cisco.com/en/US/products/ps7127/tsd_products_support_series_home.html

The entire CDS hardware documentation suite is available on Cisco.com at:

http://www.cisco.com/en/US/products/ps7126/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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