



Release Notes for Cisco Internet Streamer CDS 2.5.9

These release notes cover Cisco Internet Streamer CDS Release 2.5.9-b130.



Note

Release 2.5.9-b130 obsoletes all previous Release 2.5.9 builds.

Revised: May 2011, OL-22793-04

Contents

The following information is included in these release notes:

- [New Features, page 2](#)
- [Enhancements, page 2](#)
- [System Requirements, page 21](#)
- [Limitations and Restrictions, page 22](#)
- [Important Notes, page 22](#)
- [Open Caveats, page 23](#)
- [Resolved Caveats, page 35](#)
- [Upgrading to Release 2.5.9, page 108](#)
- [Documentation Updates, page 111](#)
- [Related Documentation, page 111](#)
- [Obtaining Documentation and Submitting a Service Request, page 112](#)



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

© 2011 Cisco Systems, Inc. All rights reserved.

New Features

Release 2.5.9 of the Cisco Internet Streamer CDS introduces the Multiple Logical IP Addresses feature.

Multiple Logical IP Addresses

The Multiple Logical IP Addresses feature allows for the configuration of multiple logical IP addresses for each gigabit Ethernet interface, port channel, or standby interface on an SE. Each logical IP address can be assigned to a delivery service.

The Multiple Logical IP Addresses feature supports up to 24 unique IP addresses within the same subnet for the same interface. Up to 24 unique IP addresses are supported in the SE to SR keepalive messages.

To configure multiple IP addresses on an interface use the **ip address** command multiple times in the config-if mode, or use the range keyword option (**ip address range**).

```
(config-if)# ip address <ip_addr> <subnetmask>
(config-if)# ip address range <lower_ip_addr_range> <upper_ip_addr_range> <subnetmask>
```

To view configured IP address for an interface, use the **show interface** command or the **show running-config** command. The IP address assignments for each SE can also be displayed in the CDSM GUI by viewing the Network Interfaces page (**Devices > Devices > General Settings > Network > Network Interfaces**).



Note

SNMP traps are still per interface; not per IP address. However, transaction logs include the server IP address.

After assigning the SEs to a delivery service, you can assign one of the IP addresses for that SE to the delivery service by using the Assign IP Address page (**Services > Service Definition > Delivery Services > Assign IP Address**).

If a delivery service is mapped to a specific IP address, the SR does not perform load balancing to any other IP address. If the delivery service is not mapped to an IP address, load balancing is performed.



Note

Removing an IP address from a delivery service interrupts the service. Changing an IP address for a delivery service causes all new requests to use the new IP address.

If using Device Groups for delivery services, assigning IP addresses to the SE interfaces must happen before assigning the device to the device group.

Enhancements

The enhancements section has the following subsections:

- [Enhancements in Release 2.5.9-b126](#)
- [Enhancements in Releases 2.5.9-b5, 2.5.9-b6, and 2.5.9-b18](#)

Enhancements in Release 2.5.9-b126

This section describes the enhancements to Release 2.5.9-b126 and includes the following subsections:

- [Alarm Filtering](#)
- [Web Engine Ingest Transaction Logs](#)
- [Transaction Log Enhancements](#)
- [Web Engine Range Request Behavior](#)
- [CLI Enhancements](#)
- [Other Enhancements](#)
- [Troubleshooting Utilities](#)

Alarm Filtering

In Release 2.5.9-b126, the CDSM GUI now has the capability to filter alarms and mark alarms as acknowledged. Alarms can be filtered based on alarm severity and device type. Alarms can be marked as acknowledged and are then moved to the Acknowledged Alarms table. Alarms listed in the Acknowledged Alarms table can be marked unacknowledged and are then moved back to the Troubleshooting table.



Note

If there is more than one alarm for a device, and the Troubleshooting table is sorted by device, then the device is only listed once for multiple alarms associated with it. The same is true for service alarms and license alerts.

Web Engine Ingest Transaction Logs

Release 2.5.9-b126 introduces ingest transaction logs for the Web Engine. Ingest transaction logs are used to log details of every upstream request sent by the Web Engine to the upstream SEs and origin servers. Ingest transaction logs only stores request details of cache-miss content and cache-hit content with a revalidation request; details of prefetched content are not stored in the ingest transaction logs.

To enable the Web Engine ingest transaction logs, enter the **web-engine http-ingest-logging enable** command.

The Web Engine ingest transaction logs are located in the `/local/local1/logs/webengine_ingestlog_clf` directory.

The ingest log file format is as follows:

```
Time URL FailOverSvrList ServerIP BytesRead BytesToRead AssetSize %DownloadComplete
Status-Returned MIME-Type Revalidation-Request
```

An ingest log file example for a cache-miss looks like this:

```
[17/Feb/2011:17:55:51+0000] http://4.0.1.6/sam.html 4.0.1.6/ 4.0.1.6 45 45 45 100 200
text/html; charset=utf-8 No
```

An ingest log file example for a cache-hit with a revalidation request looks like this:

```
[17/Feb/2011:17:59:15+0000] http://4.0.1.6/sam.html 4.0.1.6/ 4.0.1.6 0 0 0 0 304 -
Yes[If_None_Match: "1d58ac1-2d-230b4c40"]
```

Transaction Log Enhancements

The ^M character in the header field for all protocol engines has been removed. A new line character has been added to the footer for all transaction logs. (CSCti22224 and CSCti21625)

Web Engine transaction logs enhancements include the following:

- Changing the unit of measure for the Extended Squid Current-Time (Request_Received_Time in squid format) from seconds to milliseconds. (CSCtj34708)
- The following custom tokens were added:
 - %M—MIME type of the requested asset.
 - %R—Request description (Squid description codes).
 - %Z—Print the request received time stamp in milliseconds; otherwise, the request received time stamp is in seconds.
 - %{Header}i—Any request header. All client request headers are only logged on the edge SE.

Web Engine Range Request Behavior

During cache-miss scenarios, the **web-engine range-cache-fill enable** command enables the Web Engine to cache the full content when a client requests a content range where the first byte of the range is zero (0). The full content is cached and only the requested range is sent to the client.

If the first byte of the range is not zero (0), the content is not cached and the client receives only the requested content range from the content origin server.

If this configuration parameter is not enabled and the range request is specified with the first byte of the range being zero and the last byte not specified, the full content is cached on the SE and served to the client.



Note

Multiple sub-ranges are not supported. The **range cache fill enable** command is only for the Service Engine to cache the complete file when the range request starts with zero (0). The client is only served the requested byte range.

The range request has the following behavior when there is no active cache-fill session at the time of the request:

- If the SE has already cached the full file, the range request is served from the local cache.
- If the SE does not have the file being requested, and **web-engine range-cache-fill** is enabled and the requested range starts with 0 (zero), a full file download is cached on the SE and served to the client.
- If the SE does not have the file being requested, and the **web-engine range-cache-fill** is enabled and the requested range does not start with 0, the file is sent by way of bypass (downloaded from the origin server directly and not cached on the SE).
- If the SE does not have the file being requested, and the **web-engine range-cache-fill** is disabled, and the requested range starts with 0 (zero) and has no finite end point, the file is cached on the SE and served to the client. However, if the request range starts with 0 and ends with a finite end point, the requested range is served by way of bypass (downloaded from the origin server directly and not cached on the SE).

- If the SE does not have the file being requested, and the **web-engine range-cache-fill** is disabled, and the requested range does not start with 0 (zero), the file is served by way of bypass (downloaded from the origin server directly and not cached on the SE).

The request bundling has the following behavior during an active cache-fill session:

- If a content is not cached, the first client accessing that content goes to the origin server to download the full content. This is the *cache-fill period*.
- During the cache-fill period,
 - If other clients request the same content in a GET of the full object, those clients do not go to the origin server, but feed off of the "cache-fill" session.
 - If there are clients requesting the same content in a range-request (a portion of the file), those clients go to the origin server directly to fetch that range.

For small files, when there is a cache-fill in progress that could satisfy the subsequent request, the clients are served the ongoing cache-fill without initiating a range request to the upstream device.

For large files, if the ongoing cache-fill has not yet been cached, a new feed is immediately initiated for the request range and for subsequent range requests.

- After the object is fully cached, all future requests (both GET and range request) are served from the local cache.

Request bundling was introduced in Release 2.5.7. If the range request portion is already cached, it is served out of the local cache, even if the full file is not finished downloading yet. Only when a portion of the range requested is not yet all on disk will the request follow the CDS hierarchy to locate the cached content, ending at the origin server. In contrast, Release 2.5.3 always sends range-requests to the origin server until the entire file is fully cached.

CLI Enhancements

The following command enhancements have been made in this release:

- Enhanced routing statistics—Statistics to show which routing method is used in redirection to Service Engines (**show statistics service-router routing**).
- Enhanced transaction logs—Addition of routing-method field to show which routing method was chosen. The routing methods displayed are: Last-Resort, Network, Proximity, Zero-Network, Geo-Location
- Enhanced proximity statistics—Addition of proximity-related statistics to show number of cache hits, cache misses, and errors (**show statistics service-router routing proximity**).
- Enhanced geo-location statistics—Addition of geo-location related statistics to show number of cache hits, cache misses, and errors (**show statistics service-router routing geo-location**).
- Command to view proximity cache—**show service-router proximity-based-routing cache ip <ip address_or_subnet>**, where IP address or subnet is the client IP address or subnet of the proximity cache information to be displayed.
- Allow the Service Router to subscribe to specific domains—Ability to specify domains that the Service Router should subscribe to. By default, the Service Router takes all the domains specified in the CDSM. With this enhancement, the Service Router only takes the list of domains configured through the CLI. Following is an example of the configuration and show commands for this enhancement:

```
SR(config)# service-router subscribe domain test1.com
SR(config)# service-router subscribe domain test2.com
```

```
SR(config)# service-router subscribe domain test2.com

SR# show service-router subscribe domain
Domains subscribed:
test1.com
test2.com
test3.com
```

- Enhanced Web Engine detailed statistics—**show statistics web-engine details** command output has been enhanced to include the following information highlighted in bold:

```
Web-Engine Detail Statistics
-----
Active HTTPSession           : 0
Active DataSource            : 0
Active HTTPDataFeed          : 0
Active HTTPDataFinder        : 0
Memory Hit                   : 0
Cut-Thru Counter             : 124616
Memory Usage                  : 146415616
Outstanding Content Create Requests: 0
Outstanding Content Lookup Requests: 0
Outstanding Content Delete Requests: 0
Outstanding Content Update Requests: 0
Statistics was last cleared on Friday, 24-Sep-2010 10:57:32 UTC.
```

The Content Abstraction Layer (CAL) helps with asset placement across various disks and also helps to translate a URL to a disk location. In addition, CAL also helps manage the eviction and for inter cache routing.



Note All output field data on the CAL operations are from the perspective of the Web Engine and are only incremented when the Web Engine initiates a CAL operation.

The new output fields descriptions are as follows:

- Outstanding Content Create Requests—This operation allocates a disk and a file path for a given URL. The protocol engine uses this location to store the downloaded content. The number of Outstanding Creates reflect the number of such requests to the CAL module that have been submitted but were not completed.
- Outstanding Content Lookup Requests—This operation translates the URL from an end client into a disk path in the case of a cache hit (based on a previous create). In the case of cache miss, it would give the route from where the content can be found. The counter number of outstanding lookups reflects the number of pending requests.
- Outstanding Content Delete Requests—This operation deletes a file created by CAL. The number of outstanding deletes reflects the number of pending delete requests.
- Outstanding Content Update Requests—This operation updates the Content metadata CAL. The number of outstanding updates reflect the number of pending update requests submitted to CAL.



Note If there is a back log of 1000 CAL create operations, the cut-through mode is used (but only for small files). The Cut-Thru Counter is incremented. For large files, the create operation proceeds and waits until the back log is cleared, in which case there might be a latency in the large file download start.

- Following new CLI commands were added:
 - debug authsvr
 - debug authsvr trace
 - debug authsvr error
 - show statistics authsvr
 - show web-engine cache-route <URL>
 - debug all has default logging level of ERROR
 - web-engine revalidation must-revalidate enables revalidation for all dynamic cached content.
- New **web-engine transaction-monitor** command monitors the transaction logs and publishes the statistics and information regarding latency. For this command to work, transaction logs have to be enabled and must be in Apache format or Extended Squid format. There should be at least one transaction every 10 second, and the output of the command can be logged to a file or printed in the console.

New **web-engine realtime-monitor** command monitors the transaction logs and statistics every interval and publishes information about the requests received, such as response codes, cache access status, and memory utilization.

The logs are written to /local/local1/<dirname>. The logs are consumed by a GUI that displays this information as charts. There should be at least one transaction every interval.
- New **interface portchannel** keywords have been added. The following new keywords have been added to the interface PortChannel command:
 - autosense—Interface autosense
 - bandwidth—Interface bandwidth
 - description—Interface specific description
 - full-duplex—Interface full duplex
 - half-duplex—Interface half duplex
 - ip—Interface Internet Protocol configuration commands
 - ipv6—Interface IPv6 configuration commands
 - shutdown—Shutdown the specific portchannel interface

Other Enhancements

This section describes the following enhancements:

- [ucache Enhancements](#)
- [New Service Monitor Alarm](#)
- [No Cache Service Rule Supported for Web Engine](#)
- [Burst Streaming License Control](#)
- [Temperature Alarm](#)
- [Replication Status Alarm](#)
- [Flash Media Streaming Query String](#)
- [Exclude Domain from URL Signing](#)

ucache Enhancements

The ucache process, also known as the cache content manager, manages the caching, storage, and deletion of content.

Previously, the Internet Streamer CDS software did not restrict adding new content to CDS network file system (CDNFS) as long as there was enough disk space for the asset. The **cache content max-cached-entries** command restricted the number of assets, but it was not a hard limit. New content was always added and the CDS would delete old content in attempt to keep within the limits configured. The CDS could actually have more content than the configured limit, because the process to delete content is slower than the process to add content. The same situation applies to disk-usage based deletion, where deletion occurs when 90 percent of the CDNFS is used.

In Release 2.5.9-b126, content addition is stopped at 105 percent of the maximum object count or 95 percent of the CDNFS capacity (disk usage). For example, if the maximum number of objects has been configured as 3,000,000 (which is the default value), the CDS starts deleting content if the object count reaches 3,000,000, but adding content is still allowed. Adding content stops when the maximum number of content objects reaches 3,150,000 (105 percent of 3,000,000), which allows time for the content deletion process to reduce the number of objects in the CDS to the configured limit. Adding content resumes only after the number of objects is 3,000,000 or less. The same logic applies to disk usage. The deletion process starts when disk usage reaches 90 percent, adding content stops when disk usage reaches 95 percent, and adding content resumes only after the disk usage percentage reaches 90 percent or less.

If adding content has been stopped because either the content count reached 105 percent of the limit or the disk usage reached 95 percent of capacity, a UCACHE BUSY error message is sent to the Web Engine, Windows Media Streaming, or Movie Streamer, and the protocol engine performs a cut-through or a bypass.

The **show cdnfs usage** command shows the current status of whether the content is able to be cached or not. Following is an example of the output:

```
# show cdnfs usage
Total number of CDNFS entries : 2522634
Total space                   : 4656.3 GB
Total bytes available         : 4626.0 GB
Total cache size              : 2.4 GB
Total cached entries         : 2522634
Cache-content mgr status      : Cachable
Units: 1KB = 1024B; 1MB = 1024KB; 1GB = 1024MB
```

If the maximum object count is reached, the following is displayed:

```
Cache-content mgr status      : caching paused[ max count 105% of configured reached ]
```

If the disk usage reaches more than 95 percent, the following is displayed:

```
Cache-content mgr status      : caching paused[ disk max 95% of disk usage reached ]
```



Note

When the CDS is just started or the ucache process (which is the cache content manager) is just restarted, it performs a scan of the entire CDNFS. During this period, the deletion starts at 94 percent (not 90 percent) and adding content stops at 95 percent.

Eviction Protection

The ucache eviction algorithm is triggered when the disk usage reaches 90 percent or when the cached object count reaches the configured maximum object count. The eviction algorithm assigns a priority number to each content object based on the greedy-dual-size-frequency (GDSF) algorithm. The priority number is based on the size, usage, and the last evicted object priority (relative) of the object. Small objects are given preference over large objects; that is, they are less likely to be deleted.

To protect incoming large objects from getting a low priority and being deleted, use the **cache content eviction-protection** global configure command. The **cache content eviction-protection** command allows you to set the minimum content size (100 MB, 500 MB, 1 GB, and 4 GB) and the minimum age (1–4 hours for 500 MB size, 1, 4, 8, or 24 hours for all other sizes) of the content object to be protected from deletion. For example, to set the eviction protection for content objects larger than 100 MB that were ingested in the last two hours, you would enter the following command:

```
#(config) cache content eviction-protection min-size-100MB min-duration-2hrs
```

If the content object being cached is larger than the configured size, it is inserted into a protection table along with the current time stamp. If the difference between the object's time stamp and the current time is greater than the configured time duration, the object is removed from the protection table. If the eviction algorithm is triggered, before it selects an object for deletion, it first looks at the protection table, and if the object is found, it is skipped for that iteration. Both the **clear-cache-content** and **clear-cache-all** commands also check the protection table before deleting an object. As for relative cache content, content in the protection table might still be deleted if the relative content that is not protected is deleted. The eviction protection is disabled by default.

If the ucache eviction algorithm is not able to find any content to delete, a syslog message is sent to notify the administrator to revisit the configuration. Changing the settings of the **cache content eviction-protection** command only affect the content that are currently in the protection table and any new content that will be added. Any object that is removed from the protection table prior to the configuration change is not brought back into the protection table.

Reloading the SE or entering the **no cache content eviction-protection min-size-xx duration-xx** command removes all entries in the eviction protection table.



Note

Changing the time on the SE affects the ucache eviction process. If the time is set forward, content is deleted sooner than expected. If the time is set back, content is protected longer.

The **show cache content** command displays the eviction protection status and the number of elements in the eviction protection table.

New Service Monitor Alarm

A major alarm is raised for a port channel if an interface within the port channel has a different negotiated data rate than the rest of the interfaces in the port channel.

Following is an example of the output for the **show alarms** command that has this alarm:

Major Alarms:

```
-----
Alarm ID           Module/Submodule   Instance
-----
1 speed_mismatch   nic                PortChannel 1
```

Following is an example of the **show alarms history detail** command:

```
Op Sev Alarm ID           Module/Submodule   Instance
-----
1 R Ma speed_mismatch     nic                PortChannel 1
```

Oct 21 13:58:03.682 UTC, Environment Alarm, #000056, 5500:540003
 Speed mismatch among interfaces assigned to portchannel.

Following is an example of the **show alarms details support** command:

```
Critical Alarms:
-----
None
Major Alarms:
-----
      Alarm ID                Module/Submodule      Instance
-----
1 speed_mismatch            nic                   PortChannel 1
Oct 21 13:58:03.682 UTC, Environment Alarm, #000056, 5500:540003
Speed mismatch among interfaces assigned to portchannel.
```

A speed mismatch has occurred among the interfaces assigned to a portchannel. Check the switch settings and cable connections.

No Cache Service Rule Supported for Web Engine

In Release 2.5.7, the Service Rule XML file for the Web Engine did not support the no-cache element. In Release 2.5.9-b126, the Web Engine supports the Rule_NoCache element. Following is an example of the no cache element (Rule_NoCache):

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
  <Revision>1.0</Revision>
  <CustomerName>ATT</CustomerName>
  <Rule_Patterns>
    <PatternListGrp id = "grp1">
      <Domain>www.rfqdn.com</Domain>
    </PatternListGrp>
  </Rule_Patterns>
  <Rule_Actions>
    <Rule_NoCache matchGroup = "grp1" protocol = "http" />
  </Rule_Actions>
</CDSRules>
```

If no cache is configured, the content is served by way of bypass (downloaded from the origin server directly and not cached on the SE).

The output for the **show statistics web-engine detail** command displays the no cache scenario as a cache bypass use case.

```
HTTP Request Info Statistics
-----
Num Lookups                : 1
Preposition Hit            : 0
Cache Hit                  : 0
Cache Miss                 : 0
Partial Cache Hit         : 0
Cache Bypass               : 1 <---bypass gets incremented
Live Miss                 : 0
Live Hit                   : 0

Impact: None
```

Burst Streaming License Control

Previously, the license limit was set to 500 Mbps and each protocol engine had a maximum number of sessions allowed. In Release 2.5.7, the base license limit was set to 200 sessions and 200 Mbps bandwidth.



Note

This feature only applies to the Windows Media Streaming engine, the Flash Media Streaming engine, and the Movie Streamer engine.

Configure Burst Count

The protocol engines can trigger multiple minor alarms for session and bandwidth exceeded threshold conditions. If multiple minor alarms are triggered for a protocol engine in a single day (24-hour interval), they are recorded as a single alarm.

The burst count, which indicates the number of days after which a major alarm is raised, is configurable. On the Service Engine, use the **service-router service-monitor threshold burstcnt** command to configure the burst count. The default setting is one (1), which means all the minor alarms that occur in a single day (24-hour interval) are counted as one single alarm. If the **service-router service-monitor threshold burstcnt** command is set to two, all minor alarms that occur in two days (48-hour interval) are counted as a single alarm.

Configure Universal License

A universal license is similar to a regular license, except it has a higher bandwidth and applies to all protocol engines (except Web Engine). When a universal license is purchased and configured, the alarm data for all protocol engines are cleared. Thereafter, the monitoring of the protocol engines continues as usual for any future alarms.

On the Service Engine, use the **service-router service-monitor license-universal enable** command to enable the universal license. The **service-router service-monitor license-universal** command is disabled by default.

SNMP Traps

The Service Engine generates the following SNMP traps when a new major alarm is triggered:

- WMT_ALMID_LICENSE_OVERLOAD
- FMS_ALMID_LICENSE_OVERLOAD
- MS_ALMID_LICENSE_OVERLOAD

Temperature Alarm

In Release 2.5.9-b126, the temperature alarm support is disabled by default on the CDE100 and CDE200. The alarm temperature enable command has been added and is only applicable to the CDE100 and CDE200. When the alarm temperature enable command is entered on the CDE100 and the CDE200, the temperature alarm is visible and "alarm temperature enable" is displayed in the output for the show running-config command. When no alarm temperature enable command is entered on these platforms, there is not temperature alarms. (CSCt172788)

The temperature alarm on the CDE200-2G2 and the CDE205 continues to be supported as in previous releases.

Replication Status Alarm

The `rep_status_failed` alarm is triggered if the replication misses three times in a row. You can configure a lower value for the `System.repstatus.updateRateSec` to have the alarm trigger sooner. The `rep_status_failed` alarm is raised only once after three times the `System.repstatus.updateRateSec` seconds.

For example, if the `System.repstatus.updateRateSec` value is set to 10 minutes (600 seconds) and the `System.datafeed.pollRate` is set to 2 minutes, when the SE fails to send a datafeed in the next 2 minutes (120 seconds), `device_offline_alarm` is raised. However, the `rep_status_failed` alarm is not raised just because the `device_offline_alarm` has been raised. The offline issue could be transient and cleared in the next two minutes. There may be multiple SEs with offline and online states being triggered multiple times during this period because of network issues and so on.

Flash Media Streaming Query String

Previously, if an RTMP request had a query string in the URL for VOD, the Web Engine could decide whether or not to cache the content based on the Web Engine configuration. However, if the query string in the RTMP URL included the end-user specific parameters and not the stream name, every request would have a different URL because every user has a different query string. This leads to the same content getting cached multiple times.

In Release 2.5.9-b126, the **flash-media-streaming ignore-query-string enable** command has been added, which tells Flash Media Streaming to remove the query string before forwarding the request to the Web Engine in the case of VOD, or before forwarding the request to the forwarder SE in the case of live streaming.

If URL signature verification is required, the sign verification is performed before the query string check is invoked. The URL signing and validation, which adds its own query string to the URL, continues to work independently of this enhancement.

When the **flash-media-streaming ignore-query-string enable** command is entered, for every request in which the query string has been ignored, a message is written to the FMS error log, and the Query String Bypassed counter is incremented in the output of the **show statistics flash-media-streaming** command. The FMS access log on the edge SE contains the original URL before the query string was removed.

The **flash-media-streaming ignore-query-string enable** command affects every VOD and live streaming request and is not applicable to proxy-style requests.

Exclude Domain from URL Signing

The URL Signing and Validation feature has been enhanced with the ability to exclude the domain from the URL signing and validation.

The Python URL Signing script has been updated with the `exclude-domain` parameter. If the `exclude-domain` parameter is set to 1, then the domain is excluded from the URL signature. If the `exclude-domain` parameter is set to 0, then the domain is included in the URL signature.

If the domain is excluded from the URL signature, then the domain must be excluded from the URL validation. To exclude the domain from URL validation for the Web Engine, use the **exclude-domain** option for the `exclude-validate` attribute of the `Rule_Validate` element. For more information, see the “Creating Service Rules Files” appendix in the *Cisco Internet Streamer CDS 2.5 Software Configuration Guide*. To exclude the domain from the URL validation for any other protocol engine, use the **exclude domain-name** keyword for the **validate-url-signature** command. For more information, see The “Configuring Devices” chapter in the *Cisco Internet Streamer CDS 2.5 Software Configuration Guide*.

Troubleshooting Utilities

Release 2.5.9-b126 provides the following CLI troubleshooting utilities:

- [ss](#)
- [tcpmon](#)
- [netmon](#)
- [netstatr](#)
- [gulp](#)

SS

The `ss` utility is used to dump socket statistics. It shows information similar to `netstat` and displays more TCP information than other tools.

When specifying the options and filters, you can use the short form of the option (a single dash followed by a character) or the long form of the option (two dashes followed by the whole word). To view the list of options and filters, enter `ss -h` (or `ss --help`) and the list of options and filters are displayed along with descriptions.

```
# ss -h
Usage: ss [OPTIONS]
      ss [OPTIONS] [FILTER]
  -h, --help            this message
  -V, --version         output version information
  -n, --numeric         does not resolve service names
  -r, --resolve         resolve host names
  -a, --all             display all sockets
  -l, --listening      display listening sockets
  -o, --options         show timer information
  -e, --extended       show detailed socket information
  -m, --memory         show socket memory usage
  -p, --processes      show process using socket
  -i, --info           show internal TCP information
  -s, --summary        show socket usage summary

  -4, --ipv4           display only IP version 4 sockets
  -6, --ipv6           display only IP version 6 sockets
  -0, --packet         display PACKET sockets
  -t, --tcp            display only TCP sockets
  -u, --udp            display only UDP sockets
  -d, --dccp           display only DCCP sockets
  -w, --raw            display only RAW sockets
  -x, --unix           display only Unix domain sockets
  -7, --filter         display when tcp rqueue threshold meet
  -8, --filter         display when tcp wqueue threshold meet
  -9, --filter         display when tcp retransmit threshold meet
  -W, --filter         display only window scale disable
  -B, --background    display output in new format
  -L, --no_loop_back  display without loopback interface
  -S, --basic_output  display basic information
  -f, --family=FAMILY display sockets of type FAMILY

  -A, --query=QUERY
      QUERY := {all | inet | tcp | udp | raw | unix | packet | netlink}[,QUERY]

  -F, --filter=FILE   read filter information from FILE
      FILTER := [state TCP-STATE] [EXPRESSION]
```

With the **-A** query option, you list the identifiers (all, inet, tcp, udp, and so on) of the socket tables you want displayed, separated by commas.

With the **-F** filter option, you can filter by TCP state, or using a boolean expression you can filter by IP addresses and ports.

The default output does not resolve host addresses (IP addresses) and does resolve service names (usually stored in local files). To resolve host addresses, use the **-r** option. To suppress resolution of service names, use the **-n** option.

Usage Examples

The following command displays all TCP sockets:

```
ss -t -a
```

The following command displays all UDP sockets:

```
ss -u -a
```

The following command displays all established SSH connections and displays the timer information:

```
ss -o state established '( dport = :ssh or sport = :ssh )'
```

The following command displays all established HTTP connections and displays the timer information:

```
ss -o state established '( dport = :http or sport = :http )'
```

tcpmon

The **tcpmon** utility is a script that constantly calls the **ss** utility at specified intervals. The **tcpmon** utility searches all TCP connections every 30 seconds and displays information about any socket that meets the search criteria. To view the list of options, enter **tcpmon -h**.

```
# tcpmon -h
```

```
Usage: Tcpmon [-N] [-R <Recv-Q-Threshold> | -S <Send-Q-threshold> | -T
<Retransmit-threshold>]
        [<loop-time-in-seconds>] [<iterations>]
        (runs every 30 sec forever by default)
```

Usage Examples

The following command sets the polling cycle to 30 seconds and the recover-queue threshold to 100:

```
# tcpmon -R 100 30
```

The following command sets the polling cycle to 30 seconds and displays only the sockets with window scaling disabled:

```
# tcpmon -N 30
```

Output Example

The following example shows the output for the **tcpmon** utility:

State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Rtt/var	Swnd	Retrans
ESTAB	0	257744	10.3.5.2:80	10.3.5.137:32963	530/15	13	0
ESTAB	0	861560	10.3.5.2:80	10.3.5.137:32849	545/24	4	0
ESTAB	0	234576	10.3.5.2:80	10.3.5.122:32979	547/22.2	6	0
ESTAB	0	254848	10.3.5.2:80	10.3.5.103:32909	531/14.8	10	0
ESTAB	0	231680	10.3.5.2:80	10.3.5.135:32925	532/11.5	9	0

ESTAB	0	224440	10.3.5.2:80	10.3.5.133:33057	550/32	7	0
ESTAB	0	267880	10.3.5.2:80	10.3.5.135:32985	530/18.2	7	0
ESTAB	0	291048	10.3.5.2:80	10.3.5.113:32909	539/12.2	6	0
ESTAB	0	249056	10.3.5.2:80	10.3.5.103:32903	520/23.2	8	0
ESTAB	0	218648	10.3.5.2:80	10.3.5.132:33069	522/14.5	16	0
ESTAB	0	702280	10.3.5.2:80	10.3.5.100:32829	539/24.5	5	0
ESTAB	0	412680	10.3.5.2:80	10.3.5.110:32992	546/22.8	7	0
ESTAB	0	254848	10.3.5.2:80	10.3.5.115:33136	552/37.2	5	0

Table 1 describes the tcpmon output fields.

Table 1 tcpmon Output Fields

Field	Description
State	One of the following TCP connection states: ESTAB, SYN-SENT, SYN-RECV, FIN-WAIT-1, FIN-WAIT-2, TIME-WAIT, CLOSE-WAIT, LAST-ACK, LISTEN, and CLOSING.
Recv-Q	Number of bytes in the receiving queue.
Send-Q	Number of bytes in the sending queue.
Local Address: Port	Source address and port.
Peer Address: Port	Destination address and port.
Rtt/var	Average round-trip time (in seconds) and the deviation.
Send	Current sending rate (in Mbps).
Retrans	Number of retransmit timeouts.

netmon

The **netmon** utility displays the transmit and receive activity on each interface in megabits per second (Mbps), bytes per second (Bps), and packets per second (pps). To view the list of options, enter **netmon -h**.

```
# netmon -h
Usage: netmon [<loop-time-in-seconds>] [<iterations>]
        (runs forever if iterations not specified)
```

netstatr

The **netstatr** utility displays the rate of change, per second, of netstat statistics for a given period of time. The average rate per second is displayed, regardless of the sample period. To view the list of options, enter **netstatr -h**.

```
# netstatr -h
Usage: netstatr [-v] [<loop-time-in-seconds>] [<iterations>]
        -v verbose mode
        (default is 3 sec loop time, run forever)
```

gulp

The **gulp** utility captures lossless gigabit packets and writes them to disk, as well as captures packets remotely. The **gulp** utility has the ability to read directly from the network.

To view the list of options, enter **gulp --h**.

```
#gulp --help
```

```
Usage: /ruby/bin/gulp [--help | options]
--help      prints this usage summary
supported options include:
-d          decapsulate Cisco ERSPAN GRE packets (sets -f value)
-f "... "   specify a pcap filter - see manpage and -d
-i eth#|-   specify ethernet capture interface or '-' for stdin
-s #        specify packet capture "snapshot" length limit
-r #        specify ring buffer size in megabytes (1-1024)
-c          just buffer stdin to stdout (works with arbitrary data)
-x          request exclusive lock (to be the only instance running)
-X          run even when locking would forbid it
-v          print program version and exit
-Vx...x    display packet loss and buffer use - see manpage
-p #        specify full/empty polling interval in microseconds
-q          suppress buffer full warnings
-z #        specify write blocksize (power of 2, default 65536) for long-term capture
-o dir      redirect pcap output to a collection of files in dir
-C #        limit each pcap file in -o dir to # times the (-r #) size
-W #        overwrite pcap files in -o dir rather than start #+1
-B          check if select(2) would ever have blocked on write
-Y          avoid writes which would block
```

For more detailed information about the **gulp** options, see

Table 2 *gulp Options*

Option	Description
-d	Decapsulates packets from a Cisco Encapsulated Remote SPAN Port (ERSPAN). Sets the pcap filter expression to "proto gre" and strips off Cisco GRE headers (50 bytes) from the packets captured. (If used with -f option note that arguments are processed left to right).
-f	Specify a pcap filter expression. This may be useful to select one from many GRE streams if using -d, or if not using -d, because filtering out packets in the kernel is more efficient than passing them first through the gulp utility and then filtering them out.
-i eth#	Specify the network interface to read from. The default is eth1 or the value of the environment variable \$CAP_IFACE, if present. Specifying a hyphen (-) as the interface will read a pcap file from the standard input instead. (If you forget the -d option during a live capture, you can decapsulate offline this way.)
-r #	Specify a ring buffer size (in megabytes). Values from 1–1024 are permitted. The default is 100. If possible, the ring buffer is locked into RAM.
-c	Copy and buffer bytes from stdin to stdout—do not read packets from the network and do not assume anything about the format of the data. This may be useful to improve the real-time performance of another application.
-s #	Specify packet capture snapshot length. By default, complete packets are captured. For efficiency, captured packets can be truncated to a given length during the capture process, which reduces capture overhead and pcap file sizes. (If used with the -d option, it specifies the length after decapsulation.)

Table 2 *gulp Options (continued)*

Option	Description
-x	Use file locking to request (by way of exclusive lock) that this is the only instance of the gulp utility running. If other instances are already running, they must be stopped before the gulp utility can start with this option.
-X	Override an exclusive lock (-x option) and run anyway. An instance of gulp started this way holds a shared lock if no exclusive locks were broken; otherwise, it holds no locks at all (causing a subsequent attempt to get an exclusive lock to succeed).
-v	Print program version and exit.
-V xxxxxxxx	If the string of Xs is wide enough (10 or more), it is overwritten twice per second with a brief capture status update consisting of one digit followed by two percentages. The digit is the number of decimal digits in the actual count of lost packets (0 indicates no drops). The two percentages are the current and maximum ring buffer utilization. The updated argument string can be seen with the "ps -x" option (or equivalent). If the string of Xs is too short to hold the information above, a more verbose status line is written, twice per second, to standard error instead. The first method is probably more useful to occasionally check on long captures and the second is more convenient while experimenting and setting up a capture.
-p #	Specify the thread polling interval (in microseconds). The reader and writer threads poll at this interval when the ring buffer is full or empty. Polling (even frequently) on modern hardware consumes immeasurably few resources. The default interval is 1000.
-q	Suppress warnings about the ring buffer being full. If input is not from a live capture, no data is lost when the ring buffer fills so the warning can be safely suppressed. If stdin is actually a file, warning suppression happens automatically.
-z #	Specify output write blocksize. Any power of two between 4096 and 65536. The default is 65536.
-o dir	Redirects pcap output into a collection of files in the specified directory. Pcap files are named pcap###, where ### starts at 000 and increments. The directory must exist and be writable by the user running the gulp utility.
-C #	When using the -o option, start a new pcap file when the old one reaches about # times the size of the ring buffer. The default value is 10 and the default ring buffer size is 100MB; so by default, pcap files grow to about 1000 MB before a new one is started. Since some programs read an entire pcap file into memory when using it, splitting the output into chunks can be helpful.
-W #	Specifies a maximum number of pcap files to create before overwriting them. The default is to never overwrite them. This option allows capturing to occur indefinitely with finite disk space.
-B	This option enables the code to check before each write whether the write would block. When the gulp utility exits, it announces whether any writes would have been blocked.
-Y	This option writes which ones would be blocked, but are deferred until they will not be blocked.

Usage Examples

The following command provides a basic capture on eth1 with a pcap filter:

```
# gulp -i eth1 -f "..." > pcapfile
```

The ellipsis (...) refers to the Berkeley Packet Filter (pcap) expressions, such as “host foo.”

The following command provides a capture of the 10 most recent files of a 200 MB ring buffer to 1000 MB files:

```
gulp -i eth1 -r 200 -c 10 -w 10 -o pcapdir
```

Enhancements in Releases 2.5.9-b5, 2.5.9-b6, and 2.5.9-b18

Table 3 describes other enhancements to Internet Streamer CDS 2.5.9.

Table 3 *New Features in Internet Streamer CDS 2.5.9*

Enhancement	Description
Weight parameter added for Proximity Engine BGP location community	Weight field is added to the BGP Location Community page in the CDSM GUI and the weight keyword is added to the location-community command. The assigned weight of a location community is considered in the proximity ranking algorithm.
BGP location community maximum	Maximum number of location communities allowed for each SR is 128. The show running-config command displays the location communities in ascending order.
Windows Media Streaming transaction logs generated by SE in case of client disconnect.	Transaction logs are generated by the client or the downstream SE and sent to the upstream SE, unless there is a disconnect before the log is sent. In those cases, the upstream SE can generate the transaction log based on the client information sent at the beginning of the session and information gathered by the SE. In this way, a Windows Media Streaming transaction log always exists for every client session.
Proximity Engine on CDE220-2G2	Proximity Engine supported on the CDE220-2G2.
Date and time display in CDSM GUI alarms window	Date and time are now displayed when the alarms window displays. (CSCte03118)
CDSM GUI does not display last login session information	CDSM GUI now does not display last login session information (date/time, host, and terminal type was previously shown in System home page). (CSCte10661)
Web Engine transaction log entry change	Timestamp for Web Engine transaction log entry no longer has a space between the date and the time.

Table 3 *New Features in Internet Streamer CDS 2.5.9 (continued)*

Enhancement	Description
Web Engine cache-fill for range requests	<p>During cache-miss scenarios, the web-engine range-cache-fill enable command enables the Web Engine to cache the full content when a client requests a content range where the first byte of the range is zero (0). The full content is cached and only the requested range is sent to the client.</p> <p>If the first byte of the range is not zero (0), the content is not cached and the client receives only the requested content range, which is served from the content origin server.</p> <p>If this configuration parameter is not enabled and the range request is specified with the first byte of the range being zero and the last byte not specified, the full content is cached on the SE and served to the client.</p> <p>The show running-config command and the show web-engine all command display the configuration state of this parameter.</p>
Delivery service naming convention.	Spaces are no longer allowed in delivery service names.
Service Rule file supports multiple instances of same action.	There is no limit to the number of rule action instances. For example, there can be multiple Rule_Allow elements. However, if multiple rule actions of the same type exist, the last rule action with a matched pattern has precedence over any of the preceding rule actions of the same type. For example, if there are multiple Rule_Rewrite elements, the final rewrite URL is from the last rule subelement match found.

Request Routing Engine API

The Request Routing Engine API allows another platform's software client to make queries to the Request Routing Engine, in the form of an HTTP request, about which Service Engine the Request Routing Engine selects.



Note

The Request Routing Engine API does not support service-aware routing.

The HTTP request to the Request Routing Engine must have the following format:

```
http://ServiceRouterIP/routeURL?CDNURL=<Requested URL>&ClientIP=<ClientIP>
```

The Request Routing Engine returns an HTTP response with an XML payload that has the primaryContentRoutedURL, which contains the selected Service Engine.

Disk Latent Sector Error Handling

Latent Sector Errors (LSEs) are when a particular disk sector cannot be read from or written to, or when there is an uncorrectable ECC error. Any data previously stored in the sector is lost. There is also a high probability that sectors in close proximity to the known bad sector have as yet undetected errors, and therefore are included in the repair process.

The syslog file shows the following disk I/O error message and smartd error message when there are disk sector errors:

```
Apr 28 21:00:26 U11-CDE220-2 kernel: %SE-SYS-4-900000: end_request: I/O error, dev sdd,
sector 4660
Apr 28 21:00:26 U11-CDE220-2 kernel: %SE-SYS-3-900000: Buffer I/O error on device sdd,
logical block 582
Apr 28 21:04:54 U11-CDE220-2 smartd[7396]: %SE-UNKNOWN-6-899999: Device: /dev/sdd, SMART
Prefailure Attribute: 1 Raw_Read_Error_Rate changed from 75 to 73
Apr 28 21:04:54 U11-CDE220-2 smartd[7396]: %SE-UNKNOWN-6-899999: Device: /dev/sdd, SMART
Usage Attribute: 187 Reported_Uncorrect changed from 99 to 97
Apr 28 21:04:54 U11-CDE220-2 smartd[7396]: %SE-UNKNOWN-2-899999: Device: /dev/sdd, ATA
error count increased from 1 to 3
```

The **disk repair** command repairs the bad sector, including the proximal sectors and then reformats the drive. All data on the drive is lost, but the sectors are repaired and available for data storage again.



Caution

The device should be offline before running the **disk repair** command. Because this command involves complex steps, we recommend you contact Cisco Technical Support before running this command.

The **disk repair** command not only repairs the bad sectors, but reformats the entire drive, so all data on the drive is lost. The difference between the **disk repair** command and the **disk reformat** command is that the **disk format** command only reinitializes the file system and does not repair bad sectors.

The **disk repair** command has the following syntax:

```
# disk repair disk_name sector sector_address_in_decimal
```

For example, the following command repairs the sector 4660 on disk 02:

```
# disk repair disk02 sector 4660
```

A minor alarm is set when an LSE is detected. After the sector is repaired with the **disk repair** command, the alarm is turned off.

Minor Alarms:

```
-----
Alarm ID           Module/Submodule   Instance
-----
1 badsector        sysmon             disk11
May 19 20:40:38.213 UTC, Equipment Alarm, #000003, 1000:445011
"Device: /dev/sdl, 1 Currently unreadable (pending) sectors"
```

Service-Aware Routing Enhancement

Prior to Release 2.5.9 the following user agents are served by the Windows Media Engine:

- Natural Selection (NS) player and server
- Windows Media player and server

The following user agents are served by the Movie Streamer Engine:

- Quicktime player and server
- RealOne player
- RealMedia player

In Release 2.5.9, in addition to redirecting requests based on the above user agents, requests for content with the following file extensions are served by Windows Media Engine (both HTTP and RTSP requests):

- wma
- wmv
- asf
- asx

In Release 2.5.9, requests for content with the following file extensions are served by the Movie Streamer Engine:

- 3gp
- 3gp2
- mov
- mp4

System Requirements

The Internet Streamer CDS runs on the CDE100, CDE200, CDE205, and the CDE220 hardware models. [Table 4](#) lists the different device modes for the Cisco Internet Streamer CDS software, and which CDEs support them.

Table 4 Supported CDEs

Device Mode	CDE100	CDE200	CDE205	CDE220-2G2	CDE220-2S3i
CDSM	Yes	No	Yes	No	No
SR	Yes	Yes	Yes	Yes	No
SE	Yes	Yes	Yes	Yes	Yes
SR—Proximity Engine standalone	No	No	Yes	Yes	No

Release 2.5.9 supports the CDE220-2S3i platform. There are 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 CDE205/220/420 Hardware Installation Guide* for set up and installation procedures for the CDE220-2S3i and the *Cisco Internet Streamer CDS 2.5 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 CDE205/220/420 Hardware Installation Guide* for set up and installation procedures for the CDE220-2G2.

The CDE100 can run as the CDSM, while the CDE200 can run as the Service Router or the Service Engine. See the *Cisco Content Delivery Engine CDE100/200/300/400 Hardware Installation Guide* for set up and installation procedures for the CDE100 and CDE200.

The CDE205 can run as the CDSM, Service Router, or Service Engine. See the *Cisco Content Delivery Engine CDE205/220/420 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.

Important Notes

To maximize the content delivery performance of a CDE200, CDE205, or CDE220, 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 2.4 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 CDE200, 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 CDE200 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 a full CDE200, CDE205, or CDE220 capacity, we recommend that you provision a dedicated CDE200 to handle WMT; and likewise for HTTP. In such cases, we do *not* recommend that you mix the two traffic types on all CDE servers which could result in suboptimal aggregate performance and require more CDE200, CDE205, or CDE220 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

The open caveats section has the following subsections:

- [Open Caveats in Release 2.5.9-b130](#)
- [Open Caveats in Release 2.5.9-b126](#)
- [Open Caveats in Releases 2.5.9-b5, 2.5.9-b6, and 2.5.9-b18](#)

Open Caveats in Release 2.5.9-b130

This release contains the following open caveats:

Windows Media Streaming

- CSCto92496
Symptom:
After five days load testing, core.wmt_be found on device.
Conditions:
It happens for Windows Media Streaming five, when a pause event happens in a live program.
Workaround:
None.
- CSCto41489
Symptom:
The cs-url process logs the original URL for the request, not the SR redirected URL.
Conditions:
When the request is redirected from an SR.
Workaround:
The IP address of the host is in the transaction log filename. This information can be used instead of the SE name in the SR redirected URL.
- CSCtn93441
Symptom:
The cs-uri-stem limit is 128 bytes, so long string values are truncated.
Conditions:
When cs-uri-stem is longer than 128 characters.
Workaround:
None.

Authorization Server

- CSCto80450
Symptom:
Changing the primary or secondary Geo-location servers configuration does not take affect immediately.
Conditions:
Change primary or secondary Geo-location IP address on the SE configuration.
Workaround:
Restart authsvr process.

Acquisition and Distribution

- CSCto91729
Symptom:
MetaReceiver process core dumps.
Conditions:
Because of a timing issue, the resources being accessed unsafely within MetaReceiver process.
Workaround:
None. However, node-mgr restarts the meta-receiver smoothly after the core dump. Minimum impact to the service.

Network

- CSCto32852
Symptom:
The error condition triggers the core dump and causes the dataserver become out of sync.
Conditions:
The condition happens when the **interface portchannel 1 bandwidth 100** command and the **interface portchannel 1 bandwidth 1000** command are entered, and then the SE is rebooted.
Workaround:
Configure the port channel bandwidth, save the configuration, and then reboot the SE. Do not change the bandwidth back and forth and then the condition will not get triggered.

HTTP Core

- CSCtn50177
Symptom:
HTTP connection is closed after the content gets served, even if there is "Connection: Keep-Alive" in HTTP/1.0 request.
Conditions:
 - HTTP/1.0 and "Connection: Keep-Alive" exists
 - Large content gets served successfully
Workaround:
N/A. Impact on client side.

HTTP Stress

- CSCto27256
Symptom:
Total memory of process stays at 2GB after stopping longevity test.
Conditions:
At the end of longevity test total memory of process stays at 2 GB.

Workaround:

No workaround now. Platform team is investigating more into the glibc[malloc] library.

URL Manager

- CSCto84838

Symptom:

URL signature validation fails since the client browse; that is, the android, cannot understand a colon (:).

Conditions:

When a signed UEL contains a colon (:), the android browser cannot handle it.

Workaround:

Do not use an android browser. Other players handle this correctly.

CDSM

- CSCtn30873

Symptom:

Java core dump found on the CDSM.

Conditions:

Logging into the CDSM and password not provided.

Workaround:

None.

Stream Scheduler

- CSCto43865

Symptom:

The **show programs** command reports the wrong live program status.

The **show programs** command reports “Failed to start program (UNS resolve fails)” or “Failed to start program (WMT API failed to start program).”

Conditions:

When the live program is working correctly.

Workaround:

None.

Transaction Logs

- CSCto55259

Symptom:

For transaction logs, the rotation does not work for compressed files.

Conditions:

When configuring the transaction-logs export compression.

Workaround:

None.

Unified Kernel Streaming Engine (UKSE)

- 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.

Workaround:

None. Low impact, a few stale session hang around for an extra 15 to 20 minutes.

UNS

- CSCto99601

Symptom:

The alarm “unsinconsistentetries” has been raised. It can be seen in the output of **show alarms** command.

Conditions:

This alarm is generally raised when an internal UNS journal file used by UNS process gets corrupted when UNS starts. It can also be caused when there is an inconsistency between total content count between two internal processes: UNS and Ucache.

Workaround:

The **cdnfs database recover** command should be run to remove the inconsistency and the device should be reloaded afterwards. The device should be in the “Offloading” state when this is done.

Geo-Location Server

- CSCtn58091

Symptom:

The core.service_router generated on the Service router.

Condition:

Number of errors("QUOVA_RETURN_FAILURE") being returned from the quova server.

Workaround:

None.

Open Caveats in Release 2.5.9-b126

This release contains the following open caveats:

Web Engine

- CSCtn04535
Symptom:
Duplicate entries found in the output of the **show content** and **show cache** commands, but the disk maintains only a single copy of the content.
Conditions:
Content cached in Release 2.5.3 Web Engine if requested in Release 2.5.9 results in duplicate entries for ucache process.
Workaround:
Enter the **clear cache all** command before upgrading to Release 2.5.9.
- 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.
Workaround:
With SR in the scenario and the Web Engine threshold set appropriately the service threshold alarm is raised, and no more request reach the SE. In this case, this issue would not be seen.
- 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.
Workaround:
Use Apache or Extended-Squid transaction logging formats, or configure custom transaction logging with either %r or %U (including both %r and %U prints redundant information).
- CSCtj71416
Symptoms:
Client receives a “500 Internal server” error, and the errorlog has a “Content Lookup Failed” entry.
Conditions:
If CAL lookup takes more than 200 milliseconds or if CAL lookup fails for any other reason, it times out causing the Web Engine to send back a:”500 Internal server” error.

Workaround.

The next request attempt should work once the lookup is successful. No other workaround.

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

Workaround:

This happens under stress and a long longevity test. Current read time is two seconds and Web Engine treats it as an internal error.

Cache Router

- CSCtj19955

Symptom:

Cache Router goes into core dump.

Conditions:

When under stress testing, by using the siege tool to issue 200 concurrent requests to VOD content on the origin server. The siege tool was configured to issue RFQDNs to the edge SE. (www.<EDGE-SE-NAME>.se.<OFQDN>/<content>) Occurred in Release 2.5.3, as well as Release 2.5.9.

Workaround:

No service impact. Self-correcting in seconds.

This happens very rarely under prolonged stress testing using all cache-miss traffic, without SR load balancing. When it core-dumps, the Web Engine still proceeds and serves the client requests successfully, despite not getting the route information from the cache-router module. Just the route information the Web Engine uses will be from its own memory cache, and not the latest from the cache-router module. If the Web Engine's cached routes do not contain any upstream SEs, the Web Engine fulfills the client request from the origin server. If there is no connectivity to the origin server, a "504 Gateway Timeout" error is returned to the client. While the cache-router is core-dumping or restarting and is not available, the SR does not direct further traffic to this SE until the cache-router is back up and running. The cache router restarts within a matter of seconds and all normal operations resume. So this is self-correcting within a few seconds.

- 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.

Workaround:

Minimal service impact. Self-correcting in seconds.

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.

SNMP

- CSCtj85882

Symptom:

Some invalid SNMP query messages can cause the SNMP daemon to go into core dump.

Conditions:

Invalid SNMP messages are sent to the device. Occurred in Release 2.5.3, as well as Release 2.5.9.

Workaround:

Use the CDSM or CLI to retrieve system information and healthy status.

Content Cache Manager (Ucache)

- CSCti46019

Symptom:

The ucache process goes into core dump when the memory usage reaches close to 4 GB, no service failure occurs during this period, just a core file is generated on the SE.

Conditions:

The core dump happens when the ucache process memory usage reaches close to 4 GB. This can happen for the following reasons:

- SE has large amounts of content with large URLs.
- The **clear cache all** command was entered when there are many content files.

Occurred in Release 2.5.3, as well as Release 2.5.9.

Workaround:

If the number of content objects in the SE is not large and the URL size is small, then this core dump can be avoided. Maximum cache object count can be set by using the **cache content max-obj-count** command.

- CSCtj76113

Symptom:

The error messages logged in the ucache logs when there is stress and eviction in progress.

Conditions:

The error message occurred when the ucache process was in a stressed environment with eviction in progress. The eviction resulted in sending an RPC to itself during the eviction. When there are many RPC messages coming into the ucache process, the RPC can time out.

Workaround:

Too many deletion operations are the root cause for this error message. If the maximum object count is small, this issue can be avoided.

Service Router

- CSCtl93373

Symptom:

The fmsdge process core dumps sometimes on the SR when a stress test using RTMPT is running.

Conditions

When a very high or uncontrolled ramp up rate is used in the load tool and more RTMPT connections are sent than what is the maximum configured, the extra connections are rejected. As a result the tool tries to send more connections leading to more connections getting rejected. As this happens the memory usage of the fmsdge process keeps increasing and it coredumps at 4GB. Occurred in Release 2.5.3, as well as Release 2.5.9.

Workaround:

If a controlled ramp up rate is used which is not very high (less than 10 users per second) then this issue is not seen.

- 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.

Workaround:

Reduce one of the three: number of Coverage Zone file entries, number of delivery service, or number of SEs per location.

Flash Media Streaming

- CSCtk12424

Symptom:

Sometimes more connections are served than the maximum configured connections on the server.

Conditions:

If a maximum number of connections (e.g. X connections) is configured on the server and more connections are requested at nearly the same instant (more than X connections) then all of them may be served successfully by the server. This is because it takes some time for the server to record a new connection and enforce access control policies before which the next subsequent connection comes in. Occurred in Release 2.5.3, as well as Release 2.5.9.

Workaround:

No workaround at this point, however this issue will not be seen if the connections are separated by a few seconds.

- CSCtk18297

Symptom:

When RTMPT stress test is running, fmsedge process memory keeps growing and reaches 4 GB. Finally, a 4 GB core-dump file is generated.

Conditions:

Configure 1400 concurrent VOD sessions, all unique, cache-miss RTMPT stress traffic. Monitor the memory usage for two to three hours. The memory usage for the fmsedge process keeps increasing. When the memory reaches 4 GB, the process goes into core dump. Occurred in Release 2.5.3, as well as Release 2.5.9.

Workaround:

Setting the SR Burst Control feature monitors the memory usage and SR stops sending any further requests to the SE. Currently, 10 users per second ramp-up rate is a reasonable value.

Service Monitor

- CSCtj81042

Symptom:

Service Monitor goes into core dump.

Conditions:

During stress test. Occurred in Release 2.5.3, as well as Release 2.5.9.

Workaround:

Service Monitor process restarts by itself.

UNS Server

- CSCtf37689

Symptom:

The UNS server goes into core dump after a device reload (after running Flash Media Streaming mixed traffic).

Conditions:

When running Flash Media Streaming mixed performance testing(70-20-10: 70percent all unique, 20 percent single unique, 10 percent cache-miss) traffic. Occurred in Release 2.5.3, as well as Release 2.5.9.

Workaround:

This core dump happens at random when the UNS process starts. This could be while SE is reloading, and it should not affect any customers because it is not service impacting.

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.

Workaround:

Web Engine restarts by itself.

Platform

- CSCtn64252

Symptom:

SE fails to upgrade to new image via CDSM device group.

Conditions:

Traffic was running while upgrade is in progress.

Workaround:

The Internet Streamer CDS software does not currently support the upgrading of live devices. Prior to upgrading a device, one should first offline the device to ensure no traffic is actively reaching the device.

Open Caveats in Releases 2.5.9-b5, 2.5.9-b6, and 2.5.9-b18

These releases contain the following open caveats:

Windows Media Streaming

- CSCtg55017

Symptom:

When setting up a live program with multiple bit rate (MBR) content as the source, the stream freezes.

Conditions:

When setting up a live program with MBR content as the source, lots of different bit rate requests for the live program cause this issue. Occurred in Release 2.5.3, as well as Release 2.5.9.

Workaround:

Do not set up live program with MBR content as the source.

- CSCtf74656

Symptom:

After run a certain long time SE can not server any requests in Longevity test.

Conditions:

In longevity tests with mixed heavy traffic and "cache revalidate for each request" enabled, after running a certain period of time (duration depends on the test profile), the SE cannot serve requests. The following is an example of the profile:

```
1200 all-unique 100kbps sessions -prepositioned length : 30mins
```

```

1200 all-unique 300kbps sessions -prepositioned      length : 30mins
600 all-unique 700kbps sessions - cache hit         length :30mins
800 all-unique 1mbps sessions - cache hit           length :1hr
200 all-unique 2mbps sessions - cache hit           length :30mins
100 long url single-unique 700kbps sessions - prepositioned      length : 30mins
600 single-unique 1mbps sessions - cache hit         length : 1hr
Total : 4700 concurrent requests

```

Occurred in Release 2.5.3, as well as Release 2.5.9.

Workaround:

Disable cache revalidate for each request."

Flash Media Streaming

- CSCta44470

Symptom:

This issue is seen when the client requests a live stream to the SE and after about eight hours, the client stream is stopped and the connection gets closed.

Conditions:

This issue occurs only when playing a live stream continuously for more than eight hours to a single client. If the clients keeps connecting to the live stream and disconnecting from the live stream, this issue does not occur.

Workaround:

No workaround, however the next click does work.

Web Engine

- 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.

Workaround:

Increase the pacing to 50 or 100 Mbps.

Resolved Caveats

The caveats listed in this section have been resolved since Cisco Internet Streamer CDS Release 2.5.9. Not all the resolved issues are mentioned here. The following list highlights the resolved caveats associated with customer deployment scenarios. The resolved caveats section has the following subsections:

- [Resolved Caveats in Release 2.5.9-b130](#)
- [Resolved Caveats in Release 2.5.9-b126](#)
- [Resolved Caveats in Releases 2.5.9-b5, 2.5.9-b6, and 2.5.9-b18](#)

Resolved Caveats in Release 2.5.9-b130

The following caveats have been resolved since Cisco Internet Streamer CDS Release 2.5.9-b130.

Windows Media Streaming

- CSCto48858
Symptom:
Using the fast-forward or rewind functions on a stream being played in the player can cause the stream playback to fail.
Conditions:
Fast-forward or rewind happens at the time when an internal data keepalive is triggered.
- CSCto43673
Symptom:
The wmt_be process core dumped when the Windows Media Streaming server was serving live requests for server-side playlists.
Conditions:
This occurred when many media clients frequently opened and closed the server-side playlist live sessions.
- CSCtn72856
Symptom:
Windows Media Streaming ml memory leaking, 104 byte for every WMT live request from SE to client.
Conditions:
The memory leak happens for each new live broadcast request; that is, once the wmt_ml process starts playing a new live program, there will be approximately 104 bytes leaked in the memory.
Under high-stress conditions while testing live program s, with play-teardown-play-tear down occurring within a short time (3 second-span), this leak occurs at a faster rate.
- CSCtn89388
Symptom:
From the view of the client side, no media traffic is received; that is, all of the RTSP negotiation procedures work well, but no media data is sent from the SE to the client. From the view of the SE, there is no incoming statistics entry for the program, but the outgoing statistics show Playing.
Conditions:
Many new incoming requests for the program are on going and the connection between the Content Acquirer and the Encoder or origin server is broken.
- CSCtn94772
Symptom;
When there are a lot of requests for a single Windows Media Streaming MBR file, some of the requests can not be served and playback fail.
Conditions:
A lot of requests are sent for a single MBR content.

- CSCt151661
Symptom:
Playback fail for a cache hit MBR VOD content.
Conditions:
Windows Media Server does not send the same set of packets for the same pair of streams during stream switch.
- CSCto46694
Symptom:
The wmt_be process core dumped when the Windows Media Streaming server was serving live requests for server-side playlists.
Conditions:
This occurred when many media clients frequently opened and closed the server-side playlist live sessions.
- CSCto50433
Symptom:
The wmt_be process generated a core dump.
Conditions:
Rare conditions.
- CSCto79284
Symptom:
A wmt_be core dump is found.
Conditions:
When the WMT ASF parser receives a corrupted data packet.
- CSCto79808
Symptom:
A wmt_be core dump generated on the SE.
Conditions:
It occurs during a live request. The client sends a request with stream-offset. Because it is a live stream, there is no offset. This request causes the wmt_be process core dump.
- CSCto82311
Symptom:
Windows Media Streaming FE sessions keep in play state for a long time before exit even BE connections to outside are closed.
Conditions:
System under Windows Media Streaming VOD stress test in pass-through mode.

Movie Streamer

- CSCti41776
Symptom:

Movie Streamer engine is unable to serve live requests for a certain handset, like Nokia E71.

Conditions:

The User-Agent media player contains “RealPlayer.”

UNS

- CSCtn41014

Symptom:

the show cdnfs usage command output shows that the total cached entries are greater than the total CSCtn58091CDNFS entries.

Conditions:

This is due to the UNS journal file getting corrupted when UNS is started. The UNS journal file can get corrupted when the system goes into kernel debugger (KDB) mode.

Web Engine

- CSCtn40476

Symptom:

Data sources hang.

Conditions:

This is a timing issue. Moving the tempfs directory to disk and reading the datafeed as completed before the net writing. Also, a particular net writing failure happened, which caused the data sources not to be moved to the eviction list.

- CSCtn54704

Symptom:

Web Engine keeps sending Authorization Server query for a request.

Conditions:

In VOD and live cases, Web Engine does retry with id auth server query. When delivery service id is not available, Web Engine will keep trying retry-with-id, and auth server will keep replying retry-with-id.

- CSCto75342

Symptom:

The Web Engine communicates to the Authorization Server to apply the service rule configuration and to determine whether to allow the client or not.

For the Authorization Server to identify which delivery service this request belongs to, the Web Engine passes it the delivery service ID. The Web Engine gets this ID based on the internal mapping it does for RFQDN/OFQDN/Delivery service ID for all VOD delivery services.

Because the Web Engine did not properly initialize the delivery service ID, under stress, this variable gets corrupted and sometimes has the delivery service ID which maps to an existing delivery service, even though the incoming domain does not match. This causes Authorization Server to allow those requests.

Conditions:

Seen only under stress.

- CSCto77258
Symptom:
Windows Media App does not support UserAgent = LAVF52.34.0.
Conditions:
Always.
- CSCtk09509
Symptom:
Web Engine crashes and all existing sessions are terminated. Service restarts immediately and continues to serve new requests.
Conditions:
Web Engine crashes when live and VOD delivery service share content origin while serving revalidation request in a stressed environment.

Service Router

- CSCto03562
Symptom:
User agent is logged with spaces in between.
Conditions:
Depends on the client player.
- CSCtk52746
Symptom:
Service Router CPU usage nears 100 percent and never comes down.
Conditions:
Service Router process running under high load for a longer time. SR socket leak issue reported. Corner case during high CPU, all sessions are terminated at the same time by the load tool. Occurred in Release 2.5.3, as well as Release 2.5.9.
- CSCto34695
Symptom:
An IP address with an invalid netmask is allowed in <Network> tag of Coverage Zone file.
Conditions:
Invalid netmask specified in <Network> tag of the Coverage Zone file.

Flash Media Streaming

- CSCtn76089
Symptom:
A Flash Media Streaming core dump is found on the Service Engine.
Conditions:
This occurs when an empty stream name is present in the URL. Following is an example of an empty stream name causing this issue:

```
rtmp://flv.csi.cds.cisco.com/vod/
```

Following is an example of a URL with a stream name where this does not occur:

```
rtmp://flv.csi.cds.cisco.com/vod/abc
```

CDSM

- CSCte45395

Symptom:

In CMS logs on SR, prints lots of error logs like:

```
... java: %SE-CMS-6-700001: error rc trying to retrieve global isis statistics
... ds_getStruct: unable to get `stat/sg/isis/statistics/global' from dataserver
```

Conditions:

CMS collects proximity statistics, but it forgets to check if the Proximity Engine is started or not.

Unified Kernel Streaming Engine (UKSE)

- CSCto77107

Symptom:

System hangs if KDB is enabled. If KDB is not enabled, the system automatically reboots after 30 seconds.

Conditions:

It is a very small corner case. It was happening only when we have a lot of clients joining and leaving the live delivery service in a stress environment.

Resolved Caveats in Release 2.5.9-b126

The following caveats have been resolved since Cisco Internet Streamer CDS Release 2.5.9-b126.

Windows Media Streaming

- CSCtn64286

Symptom:

The fd leak for wmt_ml process, WMT engine cannot serve any more requests after running a long time.

Conditions:

This happens when running MBR VOD cases.

- CSCtn10650

Symptom:

The wmt_be process goes into core dump.

Conditions:

This occurred for RTSP and MMS-over-HTTP mixed scenario. Windows Media Streaming received the RTSP/RTP data after sending an HTTP request to the upstream SE.

- CSCtI93018

Symptom:

Found one wmt_be process taking high CPU is stuck in below loop and flooding logs in unified_errlogd. This was happening when that wmt_be received a RTSP DESCRIBE request and was using MMS-over-HTTP to contact upstream SE.

```
01/21/2011 04:01:22.181(Local) (23750)ERRO:httpfe.cpp:596-> Connecting to same host :
10.148.158.66 This IP is the SE itself, means it tries to connect to itself
01/21/2011 04:01:22.181(Local) (11334)ERRO:httpfe.cpp:595-> Possible loop detected.
01/21/2011 04:01:22.181(Local) (11334)ERRO:httpfe.cpp:596-> Connecting to same host :
10.148.158.66
01/21/2011 04:01:22.181(Local) (23750)ERRO:httpfe.cpp:595-> Possible loop detected.
01/21/2011 04:01:22.181(Local) (23750)ERRO:httpfe.cpp:596-> Connecting to same host :
10.148.158.66
01/21/2011 04:01:22.181(Local) (11334)ERRO:httpfe.cpp:595-> Possible loop detected.
01/21/2011 04:01:22.181(Local) (11334)ERRO:httpfe.cpp:596-> Connecting to same host :
10.148.158.66
01/21/2011 04:01:22.181(Local) (23750)ERRO:httpfe.cpp:595-> Possible loop detected.
01/21/2011 04:01:22.181(Local) (23750)ERRO:httpfe.cpp:596-> Connecting to same host :
10.148.158.66
01/21/2011 04:01:22.181(Local) (11334)ERRO:httpfe.cpp:595-> Possible loop detected.
```

Conditions:

Occurred in Release 2.5.3 and possibly Release 2.5.9.

- CSCtn10583

Symptom:

The wmt_be process goes into core dump.

Conditions:

This occurred when there was mixed traffic stress testing.

- CSCtj69901

Symptom:

When sending a request from a client for a live program, the program cannot play. The **show statistics wmt streamstat** command output on the SE shows the stream is in PLAY, but no data is being sent out.

Conditions:

The SE has found a nonentity front-end as the data fetcher, and cannot get packets from upstream SE.

- CSCth58862

Symptom:

Video hang issue seen in a specific scenario, when seek to a time point, the player hang there for several minutes

Conditions:

The request is going through three tiers. Seeking to a point and close the player. And then start another player, seek to the same time point. After repeating the above steps several times, the end user might see the hang issue.

- CSCti52364
Symptom:
SE has generated core-dumps.
Conditions:
When the first request is OPTION and no subsequent requests come in, SE will timeout and generate the core-dump.
- CSCti20636
Symptom:
While requesting for a live program a core-dump is generated and the request fails.
Conditions:
The live program is configured by way of manifest file.
- CSCth32290
Symptom:
wmt_be core dumped for memory logic error.
Conditions:
When running under stress for long term, wmt_be maybe core dump. But do not find in which explicit condition this will happen.
- CSCti92019
Symptom:
When request for a content (*.asf) it generate a wmt_ml core dump.
Conditions:
Request for the same content (*.asf) several times continuously.
- CSCtj38623
Symptom:
WMT MBR, when seek backward, it stops playing
Conditions:
Under two tier topology.
 - 1) create a VOD delivery service.
 - 2) request for an MBR preposition content and play it for sometime.
 - 3) seek it backward and the streaming stops.
- CSCtj27672
Symptom:
After configure wmt outgoing proxy all other wmt configuration is lost.
Conditions:
Configure wmt outgoing proxy.

- CSCtj61353/CSCtj61321/CSCti52358

Symptom:
WMT want to post a log to up-level SE with deleted libwww objects in some specific conditions, this will cause WMT core occurs.

Conditions:
Client send a PLAY request to edge SE -> Mid SE -> up-level SE. Client data being response back half way through. However, under stress condition, WMT internally kill all libwww objects and in process of posting a log to up-level SE for the very sam object and it will end up core.
- CSCtj36490

Symptom:
When SE is streaming a cache miss MBR content, client failed to fast-forward or rewind.

Conditions:
The content is cache-miss and then try to do fast-forward or rewind.
- CSCtk62383

Symptom:
WMT Streaming stopping prematurely.

Conditions:
Cache miss scenario.
- CSCtk31079

Symptom:
WMT session is still seen in 'show wmt stats' even after client disconnects.

Conditions:
The client request HTTP streaming for WMT. Then it happens randomly.
- CSCth84349

Symptom:
When config WMT Rules - No-cache action, exceed-max size counter is getting incremented instead of cache bypass counter which should be incremented.

Conditions:
When configure the rules for No-cache action and run WMT client request.
- CSCtk64806

Symptom:
When playing WMT stream and it is a VOD cache miss, client sometimes receives a 504 error and quits before the end.

Conditions:
It must be VOD cache miss.
- CSCtk83097

Symptom:
In multiple tier cache miss scenario, many users watch the same content and do extensive trick operations may cause a race condition and packet delay, which may cause the downstream SE session timeout then cause the play failed.

Conditions:

In some specific multiple tier cache miss scenario.

- CSCtk64570

Symptom:

When playing WMT stream and it is a VOD cache miss, and client uses RTSP interleave mode, it sometimes freeze for several minutes before resume playing.

Conditions:

It must be VOD cache miss and client must use RTSP interleave mode.

- CSCtk65149

Symptom:

During a cache fill progress, multiple BE may attach to the same bufobj, if one of the users do a seek, which may cause the block range of bufobj change, then cause other users freeze.

Conditions:

During cache fill progress, multiple users view the same content, during the time, they do some trick operations.

- CSCtk31094

Symptom:

In some VOD cache miss scenario, a non-extracted idle-to-be-released FE could be picked up to fetch the content for other BE, if during the serving time, the FE exited due to its BE timeout, a video freeze could be seen.

Conditions:

In some specific cache miss scenario.

- CSCtj96549

Symptom:

The error message about the live source being dead is not displayed in the syslog.

Conditions:

When a managed live program is scheduled for a live source (Windows Media Encoder/Windows Media Publishing point).

- CSCtj40968

Symptom:

WMT core dumps when parsing ASF header and ASF header itself is corrupted.

Conditions:

When the message body size value in the ASF header and the actual message body size does not match.

- CSCtk12244

Symptom:

The data of the linked list corrupted and cause the endless loop when traverse this list.

Conditions:

Once happened in a location leader when upgrade from 2.5.3 b34 to 2.5.3 b35.

- CSCtj41000
Symptom:
When play a stream by way of HTTP, WMT core dumps. It was occurred when requests for session coming but the internal data structure maintaining the session already being terminated.
Conditions:
This occurs when Edge streamer or client has not received termination notification but upstream SE has already terminated session.
- CSCtk95283
Symptom:
On a race condition of MBR cache miss scenario, FE and BE may not sync with each other promptly for the bitmap file, which could cause a BE wait for a data block until timeout, during this time, video freeze happened.
Conditions:
In some specific MBR cache miss scenario.
- CSCtk34460
Symptom:
Transaction logs are not working with XBOX in WMT over HTTP cases.
Conditions:
WMT does not parse XBOX logging header correctly.
- CSCtl19905
Symptom:
The wmt_be process goes into core dump.
Conditions:
Invalid translog message is included in RTSP SET_PARAMETER request from player.
- CSCtl08716
Symptom:
408 error sent to client.
Conditions:
Pause or resume from i-player.
- CSCtl08861/CSCti08844
Symptom:
WMT : core.wmt_ml.2.5.9.b118.ipvbuild.19739 found on Root SE stress testing
Conditions:
Under 2-tier topology
 - 1) Create a VOD DS and LIVE DS.
 - 2) Using Ixia requested both the content for 1000 requests each.
 - 3) Using Wmload tool requested both MBR and SBR content.
 - 4) Core found.

- CSCtg52228

Symptom:

Enhancement need as following: when client does not send a translog entry to SE we will generate one according to the collected data by SE.

Conditions:

When client does not send translog, there's no translog generated by SE. add the feature to replace the space with underscore in user-agent field.
- CSCtj88924

Symptom:

When the wmt process exit, the wmt share mem slot for it is not properly cleared and end up steamstats is not cleared.

Conditions:

Under the condition When user run the CLI "clear wmt stream-id". and after the WMT processes getting stopped, then corresponding WMT streamstats still shows up in the system.
- CSCtk15963

Symptoms:

The wmt_be process core dumped during stress in a 3 tier setup.

Conditions:

 - 4000 requests of single unique file + 400 all unique requests
 - topology has EdgeSE1 -> MiddleSE1 -> Acq1 -> OS
 - Have been running this stress for more than 10 days and observed these coredumps today.
- CSCtl22175

Symptoms:

While doing seek operation each time, session counter gets increment when issuing an HTTP cache miss requests

Conditions:

 - Assign Root, Middle and Edge to DS
 - Disable both fast cache and fast start on all SE's
 - Set the max concurrent sessions as -4
 - Enable the MMS over Http
 - Request a fresh content and do seek operation, 4 to 5 times
 - Check the stats and alarms.
 - Could find number of sessions gets incremented in each seek operation
- CSCtj41132

Symptom:

The following message is displayed when running multiple bit rate (MBR) longevity and stress:

```
WMT:core-dump "core.wmt_m1.2.5.9.b110"
```

Conditions:

This occurred when running a long MBR stress test on a Windows Media Streaming VOD delivery service.

- CSCtj42783/CSCtl57849

Symptom:

Delete the one of the uns entries for a content and then request for this content, SE failed to server it.

Conditions:

One of uns entries is deleted for a content.

Flash Media Streaming

- CSCth28786

Symptom:

Flash Media Streaming core process takes more memory and finally result in a core dump. Because of the core dump, some connections (a third of the connection for each process core dump) get disconnected and the next click results in playing fine.

Conditions:

Under heavy stress, when cache revalidation is enabled on the Web Engine and the Authorization Server is enabled on the SE, more requests are processed. This results in many items getting queued for Flash Media Streaming, which takes more memory and causes a core dump.

- CSCth99727

Symptom:

Request failing for files with large ASF header when given HTTP requests.

Conditions:

The content has a large asf header which is more than 32K.

- CSCtk67534

Symptom:

Compared to earlier builds, an extra field "c-proto-ver" has been added at position 19 in the FMS transaction logs, however the log header has not been updated to reflect this.

Consequently, the values for "s-uri" (which used to be in position 19) are now in position 20, but the header still shows it in position 19, and similarly all further fields have also shifted one place to the right compared to their position in the header.

Conditions:

This defect is only present in 2.5(9) build 117.

Under b118, by adding a new field name 'c-proto-ver' in the header so that the header and log entries are consistent in number. The field names and field values will also be consistent.

- CSCtj56543

Symptom:

WE Core dump on executing FMS Cache miss scenario and dies

Conditions:

- Execute FMS all unique 1mbps files 1000 concurrent RTMPT sessions.

- When the FMS sessions configured as less than 200 and the requests being pumped in is much higher, WE core-dumps.

- CSCtj43903

Symptom:

The fmsedge process core dumps in an RTMPT all unique vod stress test after few hours

Conditions:

Because of a null pointer exception in Adobe code, the process fmsedge core dumps.

Such core can happen occasionally.

- CSCtk65734

Symptom:

Compared to earlier builds, an extra field "c-proto-ver" has been added at position 19 in the FMS transaction logs, however the log header has not been updated to reflect this.

Consequently, the values for "s-uri" (which used to be in position 19) are now in position 20, but the header still shows it in position 19, and similarly all further fields have also shifted one place to the right compared to their position in the header.

Conditions:

This defect is only present in 2.5(9) build 117.

- CSCtj98800

Symptom:

FMS 3.5.5 brings critical security fixes along with other generic fix, there are no existing CDS-IS FMS implementation changes.

Conditions:

New binary available from 2.5.9-b118 and above.

- CSCtn12712

Symptom:

Adding "ignore query string CLI" enhancement.

Conditions:

In 2.5.9 if a web engine request has a query string in it, its treated as cache bypass by default and file is not cached on disk. FMS treats this has a proxy response. If you enable the ignore query string CLI, FMS does not send query string to web engine hence web engine response can be cache miss / cache hit.

Web Engine

- CSCtl07928

Symptom:

HTTP files are corrupted when files are downloaded partially on the Content Acquire and edge SE.

Conditions:

This issue is seen in Release 2.5.3-b36 with the following sequence of events:

1. Issue a request to the Content Acquirer.
2. Issue a request to the edge SE.

3. Terminate the session on the edge SE. The edge SE still continues to cache content from the Content Acquirer despite terminating the client request.
 4. Terminate the session on the Content Acquirer. The file continues to be cached on both SEs and completes on the Content Acquirer, but there is some delay in the completion on the edge SE.
 5. Send a new request to the edge SE and terminate it. The edge SE cached the content completely.
 6. Check the file size, UNS lookup, and the MD5 checksum.
 7. Observe the MD5 check sum on the edge SE is incorrect.
- CSCt117888

Symptom:
Incorrect file size and MD5 check sum reported by the edge SE during a repeated client abort.

Conditions:
This occurred in a two-tier topology when the edge SE was stressed with 100 cache-miss requests, repeated client aborts were issued by using a Spirent client, and the connections were retried a number of times. The Web Engine pacing settings were changed frequently in the interim, the file size reported on the edge SE was bigger than the file size on the origin server and this led to data corruption as well as an incorrect MD5 checksum. The particular configuration change was Web Engine pacing changes; however, this defect is also applicable for other configuration changes.
 - CSCtj72121

Symptom:
Web Engine does not respect If-Match header processing. This fails RFC compliance.

Conditions:
When sending an If-Match request, a “412 Precondition Failed” response is expected.
 - CSCth53387

Symptom:
In the Squid transaction logging format, the method is shown as NONE in particular scenario.

Conditions:
When the SE is unassigned from the delivery service while Zeri live playback is happening.
 - CSCth23130

Symptom:
Web Engine core dumps in a particular scenario.

Conditions:
This happens when the incoming URL is corrupted.
 - CSCti07849

Symptom:
The middle SE is bypassed and request directly goes to the acquirer SE for some cases.

Conditions:
Happens when there are quite a many ABR request streams. Exact root cause and reason is still unknown.
 - CSCtg66031

Symptom:

Web-Engine will core dump if two delivery services are configured with the same origin server (one for VOD and one for Live).

Conditions:

Same as above.

- CSCtn59480

Symptom:

The Web Engine crashes on route failure on free of route context in stress environment.

Conditions:

Under cache-miss stress testing.

- CSCtn49035

Symptom:

Web Engine process crashes and any existing connections are terminated. Process is restarted immediately and further connections continue to be served.

Conditions:

When the incoming request has a cache-control header with max-age, min-fresh, or max-stale configuration parameters with values greater than 50 digits, it causes the web-engine process to crash.

- CSCtn24334

Symptom:

Web Engine goes into a core dump because the data feed pause logic did not come into the picture when Web Engine tried to create file. This caused the Web Engine to try to write the content into a file that had not been created yet. The reason why Web Engine failed to pause the HTTP data feed is because there was no Content-Length header in the response from upstream.

Conditions:

When there was no Content-Length header in the response from upstream.

- CSCth75132

Symptom:

HTTP requests with a cookie large enough to cause packet segmentation will fail: the client does not receive the requested content.

Conditions:

The HTTP request packet is segmented (at TCP level) into two or more IP packets, with the cookie spanned across multiple segments.

- CSCti37365/CSCti37380

Symptom:

Bytes recorded are not incremented for error cases.

Conditions:

Bytes recorded are not incremented for error cases.

- CSCti39153

Symptom:

SE generates a web-engine core dump while running traffic under stress for Head and Get Request.

- Conditions:
Head and Get Request sent for the same content under stress conditions.
- CSCti27454
Symptom:
Bytes Transferred is not updated for HEAD requests and error response.
Conditions:
Error response is sent to client. This could be a 4xx or 5xx.
 - CSCti30714
Symptom:
When stress is done with HEAD request there is memory leak that happens which results in number of HTTP session does not get cleaned up.
Conditions:
Happens when only head request is sent to WE under stress.
 - CSCti21813
Symptom:
In the middle tier or acquirer streamer the transaction log description in case of revalidation request with 304 response is incorrect. Revalidation request sent statistics in not incremented.
Conditions:
Happens only on revalidation request with 304 response.
 - CSCti31102
Symptom:
Transaction log entry is wrong for no-store.
Conditions:
When no-store is used this is seen.
 - CSCti07849
Symptom:
Some HTTP requests are not getting service and will time out. SR does not notice this problem and requests are continuing to be directed to this Streamer.
Conditions:
This happens with a very low probability, whenever the Web Engine is parsing the admin configuration. This is especially prone to happen, when configurations were changed while Web Engine is already up and running. Roughly 1 out of 10 times.
 - CSCth57065/CSCti68361
Symptom:
You might see the alarm:
SE# **show alarm history detail**
Op Sev Alarm ID Module/Submodule Instance

1 R Mi memory_exceed web-engine
Jun 28 07:49:11.203 EST, Processing Error Alarm, #000006, 7000:900001
Web Engine process exceeds memory threshold

This is mostly for idle systems, for non-idle systems you might see that the process "web-engine" is taking a lot of CPU in "top", but not in "show processes details."

You might also see issues with streaming from the relevant SEs.

Conditions:

Running 2.5.9.

- CSCth25341

Symptom:

Eighty-seven percent chance that Web Engine stops when HTTP Request sent with a corrupt URL. All existing session currently held by web-engine gets disconnected. Web Engine process restarts within approximately 30 seconds and continues to serve subsequent request.

Conditions:

Request with corrupt URL pattern like the below causes web-engine stops.

- [http://]
- [http://:password@domain/path]
- [http:///path]
- [http://?/domain]

- CSCti49243

Symptom:

Web Engine goes into core dump. Through stack back tracing, HTTPHeader in HTTPRequest got corrupted with error "address out of bounds".

Conditions:

The issue is really hard to hit. So far it was only found in the scenario below:

- Two tier setup: client<->SE<->AC<->OS
- Cache miss & cache hit

- CSCti66218

Symptom:

HEAD requests going as cache bypass result in memory leak.

Conditions:

These are seen during HEAD requests.

- CSCti36203

Symptom:

In Heavy stress scenario, once in a while there is a request which fails due to Tmpfs file creation, as can be seen in log file.

Conditions:

This Tmpfs file creation was result of multiple thread hitting the same code block and trying to get temporary file name from Temfs module, which. returns the same value for both, 1 which is first succeeds in creating file, while other 2nd fails

- CSCti80240

Symptom:

The issue was caused when fail over server connection failed while making connection. Error response was being set to the WEHTTPClient and hence DataFeed was hanging and all associated HTTPSessions or all future Sessions with the same URL.

Conditions:

End user will see a 504 instead of the Session hanging.

- CSCth75966

Symptoms

HTTP Request sending Bad request.

Conditions:

The request URI has a domain with port in it. Ex `http://cisco.com:80/index.html`.

- CSCti70778

Symptoms:

Client receives a 504 gateway timeout or long time to serve the file.

Conditions:

Under stress sometimes SE are unable to make connection to OS.

- CSCti23800

Symptoms:

The parsed header in WE is only a reference to the buffer in libevent. That buffer is fully controlled by libevent, and will be reallocated by libevent based on the incoming requests, which caused the parsed header to be invalid.

Conditions:

Performance impact. Did performance testing, under stress, from speed point of view, the impact is very small, within microsecond level; from throughput point of view, there is almost no difference; from memory and cpu usage, there is more memory and cpu usage, but it is still in acceptable range.

- CSCti26222

Symptoms:

When you perform netstat you see a lot of FD's in Established state but the count in HTTPSession in HTTP statistics is 0.

Conditions:

Clients connection to the SE but not sending any request. The timer didn't get activated until we read the first byte.

- CSCti37182

Symptom:

Cache-control:no-cache and Pragma:no-cache header in the response chain returned by Origin server is not respected by Web-engine. Web-engine continues to cache the content

Conditions:

When Cache-control:no-cache and Pragma:no-cache header is returned by Origin server in its response header.

- CSCti44461

Symptom:

Mime type on the transaction logging is logged as application/octet-stream for .asx file type.

Conditions:

For TCP_MISS HEAD request, mime type on the transaction log record is logged incorrect for .asx file type.

- CSCti47058

Symptom:

Response code on transaction log file incorrect for Gateway time out error.

Conditions:

In case of CAHE MISS HEAD request, incorrect response code 500 is set on the transaction log record.

- CSCti47528

Symptom:

Incorrect Transaction log desc TCP_REFRESH_HIT set on log record HEAD request.

Conditions:

In case of Cache hit HEAD request, with revalidation request for the same to the origin server returning 200 response, the transaction log has incorrect description instead of TCP_REFRESH_MISS.

- CSCti79475

Symptoms:

Web Engine core dumps.

Conditions:

Under heavy stress the Web Engine Core dumps as it cannot open a file in tmpfs as it already exists.

- CSCti62977

Symptoms:

The Server is reaching a malicious OS or contents not in the delivery service are being cached and served.

Conditions:

A client send a request adding the internally used Cds_Hcache_Header that the Service engines use to determine the route that is taken through the system. The user can use this information and ask the Service Engine to fetch information directly from a malicious OS, to replace valid data.

- CSCti95606

Symptom:

AuthServ rule engine only allow Web Engine rule, the other rule being denied.

Conditions:

This happens when running WMT/MS or FMS.

- CSCti30795

Symptom:

There is memory leak in Datasourcefinders for certain scenarios.

Conditions:

Cache bypass data source, head request.

- CSCti75394
Symptom:
The SE returns a 400 Bad Request to the client.
Conditions:
The client send an HTTP Request greater than 4k in size. Generally due to cookie headers.
- CSCti66866/CSCti68430
Symptom:
 - NONE/500 with the Range-cache-fill case after OS restarted
 - CPU Threshold exceeded with only 200 requests
 Conditions:
When OS is disabled, the corresponding datasource in Web-Engine will be marked as complete with an error. Any future request to the same URL will be simply closed.
- CSCth25341
Symptom:
A specially crafted URL may cause the web engine to stop and restart; for example:
`GET http://4.0.2.41/Big_Buck_Bunny/default.html HTTP/1.1`
Conditions:
Affects all versions of software prior to first fixed release after release 2.5.7.
- CSCtj18635
Symptom:
Web Engine has changed FD limitation to 10000, while glibc has a limitation of 65536. So back down Web Engine FD limitation to 65536.
Conditions:
Very stressed system using more than 65536 file descriptors.
- CSCti71770
Symptom:
Request that is sent as Header:[space] is treated as a bad request even though it \ is a valid request as per RFC.
Conditions:
When request has Header:[space]
- CSCti97215
Symptom:
At WE startup, config values are not loaded and junk values are returned to applications. DataServer error 63 returned on query to DataServer.
Conditions:
When web-engine starts and stops frequently, the config values from dataserver were not loaded properly.
- CSCti74744
Symptom:

When the client set SE as proxy and send a cache request for a content which is not present in OS. Under the 404 response, it is showing as TCP_MISS, instead it should be TCP_ERROR.

Conditions:

When content is not present in OS and 404 response seen.

- CSCti99255

Symptom:

WE core-dump seen when second ip address is configured.

Conditions:

When second ip address is added to port channel interface.

- CSCtj14208

Symptom:

After reboot, Ext-squid transaction logging does not continue to log.

Conditions:

After transaction logging format configuration change and reboot.

- CSCti89308

Symptom:

HTTPMessage does not allow Files greater than 10 GB to be downloaded.

Conditions:

If we send a request for a file that is greater than 10 GB in size the Web-Engine will just return back an error saying file is too big.

- CSCti99015

Symptom:

WE does not accept new connection saying resource constraint with no load.

Conditions:

Shared memory corruption which end up make WE think it's over the resources limit.

- CSCti87169

Symptom:

WE should serve request in bypass mode when WE serving large file and encounter disk creation failure.

Conditions:

When serving a large file and Calcreate fails.

- CSCtj22139

Symptom:

Web Engine core dump after VM reaches 4 GB.

Conditions:

Stress Tested with 30000 clients all cache miss, and see after 4G of VM reached,

- CSCtj05074/CSCtl01319

Symptom:

WE core dump seen on HTTP client side during cache-miss case.

Conditions:

A wrong memory deletion piece of code during a cache-miss case and the cache-miss requests with same URL are abort during Web-engine restart.

- CSCtg66031

Symptom:

WE core dumps in particular scenario.

Conditions:

When VOD and live delivery service share the same Content Origin and auth server enabled and stress is run.

- CSCti56202

Symptom:

In case of error response, client response is not created from OS response header.

Conditions:

During send error response back to client.

- CSCti80235

Symptoms:

While getting a 404 not found from OS the Persistent Connection is getting disconnecting.

Conditions:

If the request is a CacheBypass request we close the connection as soon as it is complete.

- CSCtj13086

Symptom:

Transaction log record has missing fields and negative time to serve field.

Conditions:

When transaction logging is enabled in the streamer at the time of a request being processed, transaction log record for that request may have incomplete values.

- CSCti79753

Symptom:

Time-to serve logged negative value after stopped the stress testing using siege tool.

Conditions:

Turnaround time values logged in the translog is overflowed.

- CSCtj14530

Symptom:

Web Engine coredumps when sending requests.

Conditions:

The request being sent is a POST request with 0 length content-length

- CSCtj14537

Symptom:

Web Engine Core dumps when Serving request.

Conditions:

The Host Header has a space between the Host and port for example, Host :port or Host: port.

- CSCtj22500

Symptoms:

Client receives a 500 Internal server error.

Conditions:

URL being sent in the request has non escaped characters; for example, "%2e%2f"

- CSCti66322

Symptom:

Web-engine Range-cache-fill does not work in specific case.

Conditions:

- For the first request, it will go through CacheBypassDataSource and the DataSource will be valid for 4 seconds even after the request is completed.
- When the second request arrives with CacheFillRange Enabled, it will still find the same CacheBypassDataSource. As a result, it will be served by cachepass.

- CSCtj07631

Symptom:

TCP_MISS/0 o seen in transaction log record.

Conditions:

When the streamer handles a request for zero byte file, the transaction log record for that request is not populated with the correct response code 200(TCP_MISS/200).

- CSCtj07589/CSCti90526

Symptoms:

Browser hangs when requesting for content.

Conditions:

Transfer Encoding is used to serve the file and the length of the file is 0.

- CSCtj19833

Symptom:

WE HTTP Cache App attempting to serve POST request.

Conditions:

When the request is POST for HTTP.

- CSCtj22758

Symptom:

Custom transaction logging does not log all the fields if %{HEADER}i is configured on the custom log format pattern.

Conditions:

If %{HEADER}i is configured on the format pattern along with other custom format string, some fields mentioned in the format pattern, would be missing in the transaction log record created.

- CSCtj36500
Symptom:
Transaction logs show 504 or a SE bypass for request to Valid OS with no overload on the SE or SE's. Error logs show the read error with ev_buffer_empty.
Conditions:
While doing cache miss to the same content origin over a persistent connection. ABR case or small file cache miss care.
- CSCtj46273
Symptom:
Web Engine was adding the HTTP connection to its idle queue for persistence, even when there is packet drop during body download causing read time out. Such an HTTP connection should not get re-used for another request and has to be deleted.
Conditions:
When HTTP body was downloaded partially and read timeout happens over HTTP persistent connection.
- CSCtj33760
Symptom:
IMS request for Prefetched content always get the 200 OK response instead 304.
Conditions:
When send the request from Client with IMS header option.
- CSCtj09429
Symptom:
WE virtual memory does not raise alarm and threshold before it reach 4 GB.
Conditions:
Send traffic in 3000 connections and with a file size of 80 KB.
- CSCtj25938
Symptom:
TCP_HIT with long serve time seen in customer lab after 2.5 hr. load test.
Conditions:
The timeout for ucache lookup was 2seconds. Now it's being changed to 200milliseconds.
- CSCti68475
Symptom:
Web Engine return wrong content type "application/octet-stream" for WMV.
Conditions:
After a WMV video is prefetched, then use wget to get the video from SE. The content type returned by SE is wrongly as "application/octet-stream". It should be "video/x-ms-wmv" instead.
- CSCtj44117
Symptom:
Liveliness query returns the CDS-IS version in the 200OK.

Conditions:

HTTP request sent, awaiting response...

HTTP/1.0 200 OK

Server: Content Delivery System Software 2.5.9

- CSCti84697

Symptom:

WE asserts (core dump) when nhm library communication fails after 3 tries.

Conditions:

Race condition in alarm area during "show alarm".

- CSCtj57409

Symptom:

During mixed stress (WE small objects/FMS cache-miss/WMT cache-miss), the WE processes getting stuck at CAL update. This will lead to WE max sessions reach its limit(30000) and no more requests getting served.

Conditions:

Latency in serving request during CacheHit with Re-validation. Latency caused by operations performing CAL operations (lookup, update, popularity update).

- CSCtj34371

Symptom:

Web-Engine does not have the support on the services restart CLI.

Conditions:

As above.

- CSCtj34030

Symptom:

The transaction logging request description field displayed on ext-squid format does not reflect the exact status of the request. And it is also not in sync with statistics.

- Most of error response cases and cases in which a request piggy-backs with the already existing datasources the were differences in handling the request decs field
- TCP_MEM_hit was not supported
- NONE/(4xx-5xx) is corrected to reflect the cache status
- Statistics needs to be in sync with the request desc field of the log file

Conditions:

- CSCtj52419

Symptom:

"Request per Second" displayed on the web-engine statistics (show statistics web-engine) is not accurate.

Conditions:

The "request per sec" field on the statistics is an average requests over the last statistics cleared time to current time. If the last statistics cleared time is far behind, the displayed request per second is not accurate.

- CSCtj57668

Symptom:
Client and Server Error Statistics not incremented.

Conditions:
For requests marked as 'Bad Requests' by web-engine, the corresponding client / server Error statistics is not updated.
- CSCtj60176

Symptom:
In custom transaction log format %T should log turn around time in seconds.

Conditions:

 1. Created a custom transaction log format as the following:
Custom format is "%a %{User-Agent}i %A %b %T %U %r %m"
 2. %T should log turn around time in seconds.
 3. Currently it is logging wrong value.
- CSCtj34708/CSCtj54596

Symptom:
The request received time stamp on the extended squid log file does not have millisecond granularity.

Conditions:
When extended squid is made the logging format for Web Engine.
- CSCtj75754

Symptom:
Bytes_out in statistics & xact log does not reflect actual bytes sent to client, in cases where client closed the connection (or other failures) before the WE could write all response bytes.

Conditions:
When client close the connection before all bytes being responded.
- CSCtj73312

Symptom:
Custom translog not correct for "%X" formatter.

Conditions:
%X - Connection status when the response is completed
When custom translog is enable, and formatting & configure as such.
Custom format is "%{User-Agent}i %{Host}i %a %b %r %m %>s %U %X %q"
Expected Output: the possible values for the field are,
X =connection aborted before the response completed.
+ =connection may be kept alive after the response is sent.
- =connection will be closed after the response is sent.
- CSCtj73298

Symptom:

Custom logging not correct for the format %U.

Conditions:

%U - URL path requested, not including query strings.

When custom translog is enable, and formatting & configure as such.

Custom format is "%{User-Agent}i %{Host}i %a %b %r %m %>s %U %X %q"

Expected Output

The URL query string to be ripped down for the format %U

- CSCtj60166

Symptom:

SE ip against %A of custom log format not logging correctly.

Conditions:

[1] Created a custom log format as

Custom format is "%a %{User-Agent}i %A %b %T %U %r %m"

[2] Against %A (SE Ip) it always logs the loop back ip

```
2.224.22.20 Wget/1.10.2 127.0.0.1 46 2262 http://3.22.0.10/erro.txt GET http://3.22.0.10/erro.txt
HTTP/1.0 GET
```

Expected: It should log the receiving interface of the SE.

- CSCtj60940

Symptom:

The 'dsdaemon" service disabled after reload w/ custom transaction format configured.

Conditions:

1. Enabled Transaction log and configured custom format as the following

```
transaction-logs format custom "%{User-Agent}i %{host}i %{Accept}i %{User-Agent}i
%a %A %b %D %h %I %m %O %q %r %t %T %U %V"
```

2. After reload service disabled for dsdaemon

```
# show alarms
```

```
Critical Alarms:
```

```
-----
```

Alarm ID	Module/Submodule	Instance
1 svcdisabled	nodemgr	dsdaemon

- CSCti82005

Symptom:

The threshold alarm generated by the upstream streamer is not respected by the downstream streamer in a specific scenario.

Conditions:

When the request is cache bypass request (pure proxy and no caching), and if the same request is issued continuously, the alarm generated by the upstream is not respected by the downstream Streamer.

- CSCtj78863

Symptom:

Web Engine goes into core dump while browsing Fox news.

Conditions:

Using SE as a proxy and browse websites of foxnews.com. During the test, the core got generated. It is because of an internal error while ProcessQueryString.

- CSCtj60584

Symptom:

Sending a request with ? in the URL and no path after the query; for example, <http://sename.se.rfqdn/index.html?>

While running mixed small objects stress, tried query string requests in parallel. At a particular scenario, SE caches the content which has query string in the URL.

Conditions:

Under stress traffic, and when request query string with "?"

- CSCtj76377

Symptom:

Custom logging to be modified for the format %r

Conditions:

In current translog, it didn't handle %r - First line of the request correctly.

- CSCtj83446

Symptom:

Multiple WE core dump (content update) running all-unique smooth stress.

Conditions:

Internally the DataSourceFinder was kept active even after serving the data to the end client and future requests will come to this DataSourceFinder. This will lead to undesirable coredumps.

- CSCtj37227

Symptoms:

Extra port seen at URI in the error log of Web Engine.

Conditions:

While running HTTP/1.1 compliance by Co-Advisor tool, an extra port 8080 seen at URI in the error log of Web Engine.

- CSCtj50665

Symptom:

Request to web-engine results in 400 Bad request.

Conditions:

Valid request with URL with scheme being HTTP:// instead of http://

- CSCtj48056

Symptoms:

SE sends 400 bad request for valid request or gets a 500 internal server error.

Conditions:

The request sent by the client or response sent from the OS has version that has leading 0's. Ex. HTTP/001.1 or HTTP/001.001 and error log complains of version not supported exception.

- CSCtj75754

Symptoms:

Bytes out value displayed in the statistics and the bytes_out value in the transaction log holds incorrect values.

Conditions:

When client disconnects in-between data transfer or for other reasons where the client could not receive all the intended bytes, the statistics and the transaction logging bytes_out field would be incorrect.

- CSCti75312

Symptoms:

When URL Signing validation fails, the error-redirect-URL does not work.

Conditions:

When error-redirect-url is specified and request is failed to redirect to it after AuthServe deny the request.

- CSCtj59700

Symptoms:

The web-engine memory usage increases to very high value during stress - even though the memory is actually released by the web-engine it does not go back to the system due to glibc caching the freed memory.

Conditions:

After memory exceeded alarm is raised, the end user sessions using persistent connections will get terminated after servicing the current transaction. The end client has to retry the next request and potentially get routed to another Streamer.

- CSCtj78764

Symptoms:

For requests that gets revalidated and has a response code 304 from the upstream (revalidation and a hit), the transaction logging desc field was incorrect.

Conditions:

No functionality impact. Impacts transaction logging when the request is revalidated and hit.

- CSCtj72004

Symptoms:

Cache-Control:no-cache or Pragma:no-cache header is not respected.

Conditions:

If the requested asset has an expiry value (an expiry header for the asset sent from the Origin Server), the no-cache header sent in the HTTP request from client is not respected. The cached asset is revalidated based on the expiry time value and no-cache header is ignored.

- CSCtj88826

Symptoms:

Add must-revalidate CLI. the CLI syntax is:

web-engine revalidation must-revalidate ?

Conditions:

It forces revalidation for all requests when turned on.

- CSCtj63018

Symptoms:

Under "show tech", Web-engine service is not running and it uses HTTP.

Conditions:

Under display of "show tech"

- CSCtj96260

Symptoms:

Transaction-monitor throws error when filename with path is given.

Conditions:

Under 2.5.9-b115, when running transaction monitor.

- CSCtj91327

Symptoms:

When a failover to the OS from edge SE and it fails to resolve the OFQDN, then subsequent session will hang.

Conditions:

When the origin server domain name is not resolvable & the connection to the origin server fails, the connection object is not removed from the map - however the first client that initiated this connection will get a gateway timeout error.

When a subsequent request to the same origin server is made, the invalid connection object from the map is used and that causes the session hang - as the states inside this connection object is invalid.

It is triggered with failover to the OS from an edge SE when it cannot resolve the OFQDN.

- CSCtk00909

Symptoms:

When a failover to the OS from edge SE and it fails to resolve the OFQDN, then subsequent session will hang.

Conditions:

When the origin server domain name is not resolvable & the connection to the origin server fails, the connection object is not removed from the map - however the first client that initiated this connection will get a gateway timeout error. When a subsequent request to the same origin server is made, the invalid connection object from the map is used and that causes the session hang - as the states inside this connection object is invalid. It is triggered with failover to the OS from an edge SE when it cannot resolve the OFQDN.

- CSCtl04922

Symptoms:

Web Engine transaction log format changed between b117 and b118.

Change #1: timestamp is missing millisecond granularity

Change #2: the slash "/" is missing between result code and status code

Conditions:

This ONLY happens under 2.5.9-b118, and got fixed in b119.

- CSCtk97095

Symptoms:

As a regression due to CSCtk65932, the cache min-ttl, max-ttl commands were not being executed on the CLI prompt.

Conditions:

This ONLY happens under 2.5.9-b118, and got fixed in b119.

- CSCtj86878

Symptoms:

WE Statistics: Bytes Per Second need to be modified as Avg Bytes Per Sec.

Conditions:

This statistics field "Bytes per second" is also an average from the last stats clear time. Hence, it will be made as "Average Bytes Per Second"

- CSCtk54511

Symptom:

CA Web-Engine Location Leader core dumps.

Conditions:

This should be a rare problem - and when this core dump happens web-engine should restart and get back in service.

- CSCtk31236

Symptom:

If a request with a query string is issued, the URL logged in the transaction logs is stripped of the query string.

Conditions:

1. Create VOD delivery Service & assign Service Engines to the DS.
2. Enable transaction logging in SE. Set the logging format as extended squid.
3. Give GET request to the file using,


```
http://www.webengine2.com/746kbs.wmv?test
```
4. Check the WE statistics using `sh stat Web Engine`.
5. Check the transaction logging in SE under the directory,


```
/local/local1/log/webengine_extsquid.
```
6. In the transaction logging, the request method recorded as GET.
7. But the URL field does not show the query string.

- CSCtj96887

Symptom:

When a content of length 0 is requested through Flash Media Streaming, this condition gets hit and core-dump happens.

Conditions:

When a Flash request to flv file which is having file size 0 byte and the core dump occurs. It can happen using mp4,mp3 and mpeg files also.

- CSCtk35272

Symptom:

Content range calculation is wrong. This for large files greater than 1 GB when cache fill range enabled.

Conditions:

When request large size file greater than 1GB.

- CSCtk83794

Symptom:

Web Engine core dumped while running url-rewrite stress request

Conditions:

Web Engine 2 GB core dumped while running the mixed (url-rewrite request and normal) requests using ixia. It's under single tier topology.

- CSCtk56040

Symptom:

1 byte transactions to web-engine is causing it to exhaust all memory (too many transactions piled up) and WE end upl core.

Conditions:

SE running out memory on 30K sessions, There should be alarm raised to not accept new requests. However, due to nature of persistent Connections, it might would serve new request on same connection and try to Create new objects, which will fail. This is corner case for the very small file size with SE ignoring Alarm.

- CSCtl10377

Symptom:

Web Engine query string config is not retained after reload.

Conditions:

Web Engine query string config is not retained after reload and need to change the below config on show running from "cache-query-string" into "query-string-caching."

web-engine query-string-caching enable

- CSCtk62741

Symptom:

Web-Engine must revalidate configuration exists even if revalidation is disabled.

Conditions:

Must revalidation results in revalidation though revalidation is disabled.

- CSCtk35692

Symptom:

The rpc_httpd process generated a core on CDSM.

Conditions:

None.

- CSCtk82485/CSCtl05610

Symptom:

Web Engine goes into core dump in edge SE on running mixed profile stress.

Conditions:

1. Create a VOD delivery service and assign three SEs with one SE at each location.
2. Start the Spirent test.
3. After running the test for 10+ hours, core dump generated in edge SE.

- CSCtj71439

Symptom:

Upstream SE sends back "Error in parsing method" under stress.

Conditions:

This is caused when the child SE retries to send the request using a new connection to the upstream. In this case it adds an extra `\r\n` to the request, this causes the upstream SE to interpret the new `\r\n` as a new request which has invalid pattern. This results it trying to send 400 back to the child SE.

This 400 is not transaction logged as we do not right now log errors sent at the time of request parsing. On the child SE you do not see this additional request of `\r\n` is initiated by in the HTTP upstream facing module and hence not propagated to the rest of the code and not logged in the transaction logging.

- CSCtl50813

Symptom:

No Cache option for the XML service rule in 2.5.9 is NOT supported.

Conditions:

Rule actions does not work for Web engine requests in 2.5.9. Auth server XML file supports the no-cache option, however WE used to not respect this configuration.

- CSCtl69561

Symptom:

The Content Acquirer will truncate the first two characters of the URL when asking it to the origin server when the URL contains `:80`.

For example the client asks for URL `http://abc.example.com:80/title/bar.html` then the CA will ask for `http://abc.example.com/tle/bar.html`.

Conditions:

Using `:80` in the URLs.

- CSCtj83053

Symptom:

While Parsing Headers of each request and when splicing happens between `'\r'` and `'\n'` it could lead to the body reading `'\n'` as part of the body.

Conditions:

It's due to the character based parsing which looks for `'\r'` and assume it is followed by `'\n'`.

- CSCt159517

Symptom:

WE core dumped during small obj all unique cache-miss stress of 200 TPS.

Conditions:

This is rarest case Core Dump.

It happens when Retry mechanism comes in play for the re-used Connection, for which Upstream has timed out.

Cache Router

- CSCtj29148

Symptom:

A new CLI command was added, **show web-engine cache-route URL**, that shows the route taken to retrieve an asset from a given URL and cache the same.

Conditions:

Usages of this of the **show cache-route** command are the following:

Assuming the CDS network has following topology:

- Root location: A, B
- Middle: C, D
- Edge Location: E

and the operator runs this command on node E for a given URL, the cache route has the following path E->C->A -> OS for this URL.

The expected output would be:

The route: [C's IP/A's IP] is used to cache the asset for URL=http://www.lnos.com.

Depending on the hierarchy, the cache route displayed to cache this URL asset can contain one hop or more than one hop.

Following is an example of the output for this command:

```
# show cache-route web-engine http://www.lnos.com
The route: [ 7.8.0.5 ] will be used to cache the asset for URL=http://www.lnos.com
V6-CDE220-3#sh cache-route web-engine
http://171.70.77.61/vcn-u5/lnissank/Test/untitled.bmp
The route: [ 7.8.0.5 ] will be used to cache the asset for
URL=http://171.70.77.61/vcn-u5/lnissank/Test/untitled.bmp
```

- CSCtj56256

Symptom:

Added the show cache-router upstream-status command to display the liveness of upstream SE.

Conditions:

Liveness state of upstream SE.

- CSCtj61919

Symptom:

^M is seen at the end of Web Engine transaction log record.

Conditions:

When Web Engine transaction logging is enabled, ^M is seen at the end of Web-Engine transaction Log record, if log file is opened with editor.

- CSCtj94034

Symptom:

Cache route path not updated in the middle SE in particular scenario.

Conditions:

Three-tier topology. two SEs in each tier.

OS -> Tier -1 SE11 , SE12 -> Tier 2 - SE21, SE22 -> Tier 3 - SE31, SE32

- Give a cache miss request. Check the cache route path.
- Stop the Web Engine service in SE21.
- Cache route path is not updated in SE22 box, though it is selected by the edge SE in cache route path.

The root cause being when there is a connect() error, Web Engine still ends up adding the ID to the fdset for read, which is wrong. This causes select to return bad file descriptor and Web Engine exits out.

- CSCtl59576

Symptom:

This problem can happen if there is greater than 50 ms network delay from the edge tier to the Content Acquirer tier. The load on the acquisition tier might not be balanced evenly as the actual location leader for a given URL is not used (as it was marked as not-live by the liveness query). For requests coming in from the edge SEs. However, if the request was sent to the mid-tier SEs it might be able to balance the load based on the URL hash. This is because of the shorter latencies between the intermediate and the acquirer tier.

Conditions:

When not in auto-update mode and performing the request liveness query, the liveness query will times out prematurely - that causes a device this is live to be considered as not live.

It has the following impact. It increases the load on the origin server in cases of concurrent accesses across all geographies. But it should not be very high due to the request bundling features built in to the Web Engine.

CAL

- CSCti39062

Symptom:

Web Engine process goes into core dump for some of HTTP requests. These requests fails and also the current serving requests are all terminated because the process coredumps.

Conditions:

When the HTTP request URL has a query string.

- CSCtj22466

Symptom:

When the SE is reloaded, Web Engine core file may be seen.

Conditions:

This core dump can happen when there are a few million content objects in a device and the device is reloaded. When there are a large number of content objects in the device, ucache process takes more time to come up, meanwhile when Web Engine tries to connect, the connection fails. This results in Web Engine going into a core dump.

- CSCtj29106

Symptom:

Time estimated for clear cache all is ten times longer than actual time.

Conditions:

Corrected behavior as following:

1. Clear cache content does not show how many content objects getting deleted.
2. Clear cache all shows estimate deletion time, time stamp, and progress during deletion on CDE-220-2S3 and CDE200.
3. Clear cache all shows time stamp and progress during deletion for not (2S3 and 200) box.
4. The time estimation is approximate time measured on a device with no traffic.

- CSCtj50976

Symptom:

The following entries seen in ucache errorlog:

```
ERRO:ucache_monitor.c:92-> uc_is_too_many_deletion_in_progress: num outstanding
deletions
ERRO:ucache_monitor.c:555-> uc_threshold_monitor: outstanding deletions[904 MB]
```

Conditions:

Under latest image, ucache is now deleting 25000 files per eviction cycle (which is an interval of one second) versus earlier ucache was able to delete only 250 files per eviction iteration. A new timer event finds that too many deletion are in progress and the eviction is postponed. Changing the error log level from ERROR to Debug.

- CSCtj54989

Symptom:

Web Engine results in random coredumps getting created during stressed environment.

Conditions:

When there are many transaction happening with ucache is busy (either by executing clear cache all, or with too much of eviction in progress or too many transaction), ucache timeout of 200Ms or 2 seconds happens, that is when the core dump happens. The timeout happens for one connection but next transaction will result in core dump.

- CSCtj59754

Symptom:

User issues clear cache content and got 9005 error message.

Conditions:

During ucache-svr core dump because of high memory usage and in the process of core-dumping. A more meaningful message is printed on the screen when this error happens.

- CSCtj98955

Symptom:

Because of RPC deletion timeout, there are remaining items stay on the system but unknown to UCACHE. It results to show cdnfs usage statistics inconsistency and show cache content shows nothing but there are actual contents in the systems.

Conditions:

Users will see those recently lookup/refreshed URL on show command. There is one existing solution to this which is ucache sanity, however, it is happens every 24 hours.

- CSCtk07312

Symptom:

During the eviction or stress to disk in streamer device and executing the "show content all" may result in throwing up some error messages. This is nothing to worry case, but CLI prints some unlikely message on the console.

Conditions:

The condition is very rare situation, where eviction is happening and show content all is executed. The **show content all** command tries to scan through the disk, and when "show content all " accessing some content, which is also getting evicted. That time the CLI will throw some error messages in the console.

Content Cache Manager (Ucache)

- CSCtj24449

Symptom:

The "clear cache all" CLI will fail saying "Previous clear cache all not completed. Retry again later!!!", when eviction in progress

Conditions:

When eviction in progress, during this period, "clear cache all" cannot be executed, but the failure message says previous clear cache all is in progress

- CSCtj25742

Symptom:

Contents still being cleared even though answer "NO" to clear cache all.

Conditions:

When execute "clear cache all" CLI command.

- CSCtj76078

Symptom:

An issue with the ucache module which is in charge of managing object eviction in case of disk near full or hitting max # obj.

The following three combination causes ucache to be very busy & slow in restoring existing entries into its database, hence unable to catch up on the eviction timely while new objects keep on getting inserted. Eventually the disk will be full.

Conditions:

Under the following 3 conditions, the disk will reach full:

1. The disk is near full already and needed eviction.
2. The box is reloaded or ucache is restarted (manually or due to core dump).
3. Lots of cache-miss traffic arrives.

- CSCtj88766

Symptom:

When UCACHE debug errorlog enabled during stress, 5 second of the log data is missing. This is due to the feature in unified_log module that two log creation time is less than 5 second, unified_log daemon will suspend the service of that module for 5 second.

Conditions:

When UCACHE debug errorlog enabled during stress. Fix was put in to increase the size of the errorlog from 2MB to 20MB and log rotation from 15 to 20.

- CSCtj44843

Symptom:

Alarm gets raised in the SE saying A&D Database failure due to no disk space left for 1 svcclowdisk AD_DATABASE

Conditions:

The issue happens when there are many content get cached into CDS. When there are many contents, ucache writes huge database into /state which results in other modules to run out of disk space. One of the module which regularly uses the /state file system is A&D database.

- CSCtl74377

Symptom:

When a new content comes in, there is no guarantee for the new content to get average /middle of the priority. This causes the new content to get evicted immediately after ingestion sometimes for a larger object.

Conditions:

The following solution is added:

1. Priority queue is an associative db based database and every eviction cycle (once in a second), checks how many content it needs to evict, and walks through the adb from lowest priority to higher priority till the requirement is satisfied.
2. When ever new content comes in (where the size greater than the configured size), can be added to the new table (map or hash table) with cache_entry pointer as key and its TTL (life time in the new table).
3. For every iteration of eviction cycle can go and increase the TTL, and any entry in the new list reached the configured TTL can be removed from the table.
4. After the TTL update and scrapping the new table, the eviction process can continue to do the original operation of eviction list preparation with one extra operation that it will compare with the new table before adding it to the free_list (the list that needs to be evicted). This way it will take care that the content which is in new table are not added for eviction. An asset will be in new table only when its life is lesser than the configured minimum TTL.
5. The clock value will be updated only when the clock is lesser than the maximum priority value of free_list.

- CSCtn01244

Symptom:

In the syslog entries, cached entries/max-cache-entry config updated incorrectly.

```
cached entries [4294967298], max-cache-entries configured[-17193441280655360])
```

Conditions:

The following is seen in syslog:

```
Feb 1 14:49:13 DD7-2G2-3 ucache-svr: %SE-ucache-3-121002: Eviction not possible
because all contents are protected from eviction(Protected entries[2], cached entries
[4294967298], max-cache-entries configured[-17193441280655360]).
```

- CSCtn08608

Symptom:

A very small amount of memory leak is introduced in a periodic snapshot update operation.

Conditions:

Memory leak very slowly during ucache update operation.

CDSM

- CSCtn64632

Symptom:

If the KO or KN of a URL signature key configured for a device group is smaller than 10, the URL signature may be removed when a full database update is performed or a device upgrade is performed.

Conditions:

Configuring URL signature keys with a KO or KN size that is smaller than 10 characters.

- CSCtj97942

Symptom:

If a device generates alarms too quickly (greater than or equal to ten per second), the CDSM GUI alarm table may contain some invalid alarms, which cannot be seen in the output of the **show alarms** command.

Conditions:

Node Health Manager does not send notification to its listeners if the alarms were generated too quickly (greater than or equal to ten per second); instead, it raises an overload alarm. After the overload period, the Node Health Manager clears the overload alarm and starts to send notifications to its listeners. But it does not send alarm records during the overload period. So, if one alarm is generated before the overload time, but it is cleared during the overload period, the CDSM GUI does not receive the clear notification, and as a result, the alarm remains in the CDSM GUI alarm table.

- CSCtn01841

Symptom:

Unable to upload a 5-MB Service Rule XML file into the CDSM.

Conditions:

This is an internal error that occurs from a third-party software that the CDSM uses for file uploads.

- CSCti32062
Symptom:
TACACS+ user login CDSM GUI failed.
Conditions:
The issue happens when a TACACS+ user logs in CDSM GUI at its first time.
 - Further logging by those already logged users will not trigger the issue.
 - Issue does not happen when logging GUI with local users.This symptom was introduced after 2.5.9.b7, when nscd service is added in our system
- CSCth89496
Symptom:
NTP Server configuration is lost from GUI and CLI, when 'force full database update' in SE's device home page.
Conditions:
It happens on SE, when more than one NTP server are configured through Device Group.
- CSCti56480
Symptom:
Device may lose some configurations after reload, upgrade, or downgrade. Sometimes all configuration is lost.
Conditions:
Before the device reboots, the file /local/locla1/.running_backup file exists. If this file is not the same with running-config, or after reload, CLI format changed, it loses the configuration.
- CSCti96532/CSCtj10685
Symptom:
CMS unable to send config-change notification to auth-svr when secondary ip addr was added or changed, as result cache-fill requests will be denied by upstream SE.
Conditions:
When user adding secondary address for port-channel interface.
- CSCti58900
Symptom:
Custom report with last 2 days is not displaying in CDSM GUI.
Conditions:
Always happen.
- CSCtj10161
Symptom:
CDSM: device name is truncated if it is over 20 characters
Conditions:
When device name is longer than 20 characters

- CSCtj10171
Symptom:
CDSM network interface device view does not show link condition (up/down/speed/mode).
Conditions:
Link Information missing under GUI page.
- CSCtj20538
Symptom:
Rule actions configuration lost while click "Force full database update."
Conditions:
Clicking the 'force full database update' button in the Device Home page causes the rule actions configuration lost from CLI running_config and startup config.
- CSCti39847
Symptom:
The CDSM GUI shows blank navigation bar (the top area) after a TACACS+ user logs out and then logs in the GUI again.
Conditions:
It happens when Local is configured as primary server, while TACACS+ is the secondary server.
- CSCsk41969/CSCtj18085
Symptom:
FMS: on GUI, statistics chart cannot display the date correctly
Conditions:
In the CDSM GUI, Devices > Monitoring > Statistics > Streaming Sessions page
 - In **Time Frame** drop-down list, select "Last Week," then click **Update**. There is a note stating "Daily data is available from Thu, 6 Sep 2007 through Mon, 10 Sep 2007." But from the chart, the date is from 6 sep to 11 sep, and the result is not correct.
 - Select **Custom Date Range**, enter "Sep 6 " through "Sep 10," and click **Update**. There is a note stating "Daily data is available from Thu, 6 Sep 2007 through Mon, 10 Sep 2007" (the same time range), but the chart is different than the first one above.
- CSCtb82518
Symptom:
In Services->Service Definition -> Delivery Services -> Replication Status GUI page, the replication status toggles between "No Status Reported" and "Completed" even if the replicating is finished.
Conditions:
The interval for the replication status reporting between CDSM and SE is not consistent
- CSCtj17216
Symptom:
Telnet on "Devices" page does not work for IE7/8 for CDSM GUI.

Conditions:

In 2.5.9 image, if customer clicks telnet button with IE7/8, warning message will appear because IE7/8 no longer support telnet protocol by default.

- CSCti58603

Symptom:

1. Go to CDSM > System > Configuration.
2. Click Service Routing > Coverage Zone File Registration.
3. Select "Upload" and select a Coverage Zone XML file.
4. Click "Validate" button.

Internet Explorer 8 pops up a windows showing "cannot display the web page. It works on Firefox 3.6.

Conditions:

When using Internet Explorer 8 and trying to upload Coverage Zone XML file.

- CSCti17684

Symptom:

Just testing on a CDE220, in CDSM Device > Application Control > Default and Maximum bandwidth. When entering a value above 12.000.000 the CDSM returns an error that says "Maximum bandwidth for Windows Media Incoming exceeds the platform limit of 12.000.000." However the maximum that can be configured on the device is 8.000.000, not 12.000.000.

```
# show wmt
WMT bandwidth platform limit: 8000000 Kbits/sec
```

Conditions:

On CDSM, enter a value above 12.000.000 for bandwidth.

- CSCtj17246

Symptom:

From CDSM GUI --> Devices --> SE, "Free" always displayed as 0.

Conditions:

"Free" is free space shown in diskman, and the free is the disk space not parted/formatted. It is designed behavior but looks confusing,

- CSCtj19989

Symptom:

GUI: need modify the default pacing to 0 from DS - General settings.

Conditions:

Change default value for Maximum Bitrate Limit per Session for HTTP from 1000 to 0.

- CSCtj05482

Symptom:

From the CDSM UI --> Devices --> SE, "Local Disks" always shown as 1 on CDSM GUI.

Conditions:

Because output format of CLI "diskman" changed. The perl script cannot parse it correctly and result in misbehavior.

- CSCti75725/CSCtj33246
Symptom:
False alarm for 80% local1 disk usage after user shell is installed
Conditions:
The /local1 usage alarm is a false one. It's caused by user shell User shell mount on /local/local1/rootfs/local1 and it breaks the grep pattern in log_monitor.sh. As a result, log_monitor.sh always fails the disk usage evaluation
- CSCtj38736
Symptom:
Sometimes cms service would restart when scheduling a program in CDSM GUI (Live Programs -> Schedule), users will be logged out from GUI and need to re-login.
Conditions:
During scheduling a program, e.g., configure "Play Forever" for a program, or the issue can be seen by clicking the "Submit" button repeatedly.
- CSCtj65755
Symptom:
When navigating to System / AAA / Domains / Entity Management as a TACACS user, an access forbidden (403) message is presented.
Conditions:
Login as a TACACS user.
- CSCtj56230
Symptom:
CDM: 'ConcurrentModificationException' errors found in CMS Logs
Conditions:
The registered devices experiencing flapping between online and offline modes and an ERROR message in the logs which indicates ConcurrentModificationException will be seen.
- CSCtj79007
Symptom:
GUI: need modify the default pacing to 1000kbps from DS - General settings.
Conditions:
Change default value for Maximum Bitrate Limit per Session for HTTP to 1000.
- CSCtj69931
Symptom:
CDSM Authserver rule and Geo IP file validation not working in Internet Explorer 8.
Conditions:
Browser: Internet Explorer 8
 1. Go to CDSM > System > Configuration.
 2. Click Service Rules > Service Rule File Registration.
 3. Select "Upload" and select an valid XML file.

4. Click "Validate" button.

The Internet Explorer 8 pops up a windows showing "cannot display the web page. Same issue is observer for Geo ip file validation. Service -> Delivery service -> Authorization service.

- CSCtj69472

Symptom:

In CDSM GUI page, go to System->CDS-IS Well Known Ports, the unused TCP port 8090 for old HTTP on Service Router get displayed in "CDS-IS Well Known Ports" list.

Conditions:

In the release of 2.6.0-b203/cdsis_2.5.9-b112 or before.

- CSCtj67628

Symptom:

Current CDSM support Alarm Acknowledging but it does not affect the System Status displayed on the main page. Need to provide another view of system status, where suppressed alarms are not shown. The reason is customer want to be able to differentiate an all green status w/o any suppressed alarm from an all green status with suppressed alarms.

Conditions:

Currently, the system status bar on CDSM GUI page shows all alarms statistics. But some customers suggest we provide another view to suppress acknowledged alarms. The default view is ignoring the acknowledged alarms. The view is session dependent, different sessions can have different views.

- CSCtk6418

Symptom:

If set System.repstatus.updateEnable value as false, all service will raise critical alarm reporting no status report.

Conditions:

Missing System.repstatus.updateEnable value check.

- CSCtk95115

Symptom:

If configuring by way of CLI, sometimes the configurations will be lost and override by settings from cdsm.

Conditions:

CMS will exec all URL signature keys even if only one key is updated. So if configuring URL signature key by way of CLI while SE receives update from cdsm, conflicts will occur.

- CSCtj83443

Symptom:

Popped up window of "show command" will not be closed after user log out.

Conditions:

The sub-window for "show commands" isn't opened correctly.

- CSCtj80947

Symptom:

CDSM: need delete old XML file when upload, if not Authsvr will deny.

Conditions:

After removing the Geo/IP & authsvr XML file from the DS, the request still go through the Geo Plug-in & gets denied. This is due to old XML is not removed by CDSM.

- CSCtk31004

Symptom:

Port channel member interface autosense mode not displayed correctly.

Conditions:

When autosense is turned off on Port channel, it will impact on how the network interface info is collected and displayed on CDSM.

- CSCtj97502

Symptom:

When Delivery Service's configuration changed on CDSM, it is not taking effect on SR.

Conditions:

The Root Cause is that the database info on delivery service IP assignment did not get synced up with the generator for the file of the SE-Content Origin subscribe file(/state/routing/shr_ws.dat).

- CSCtk17840

Symptom:

The following known TCP port 443 is missing at System->CDS-IS Well Known Ports GUI page, which is used for inter-SE communication.

Conditions:

No conditions.

- CSCtk56405

Symptom:

SE reported as offline on the CDSM GUI.

Conditions:

Java exceptions seen in syslog.

- CSCtk10420

Symptom:

SR Registration issue with CDSM -device remains offline.

Conditions:

- CDSM in 2.4.5-b25 and SR in 2.5.9-b117
- SR remains offline in CDSM after upgrading the SR by CDSM method.
- CMS log from SR and CDSM are attached.

- CSCtk00351

Symptom:

When an SR, which is SR and Proximity Engine mode, get deactivated, it mentions the Location as the default value which is the text "Please make a choice," it was not accepted. However, even with the warning message, the mode of the device gets changed from SR & Proximity Engine to "Service Router only."

Conditions:

From CDSM, try to deactivate the device with the Location field changed from the existing one (say, Root) to "Please make a choice". Then, when you try to submit the changes, it throws a warning "Transaction not completed." But, mode being changed from SR & Proximity Engine mode to SR only.

- CSCti54931

Symptom:

After SE reload, the CDSM GUI always displays the gateway as 0.0.0.0.

Conditions:

When CMS is enabled, it collects network information before sending updates to the CDSM. But after the system boots up, the network is not ready, as a result, gateway information is lost.

- CSCtl22066

Symptom:

Uploading service rule.xml file to CDSM results in error.

Conditions:

User name anything other than "admin."

- CSCtk11839

Symptom:

After running some test cases with large Geo/IP XML. After some time, error msg thrown on uploading. It was found the /tmp file is filled & no space left to create a new file and image cannot be downloaded.

Conditions:

During Geo/IP and Rule file validation/upload, CDSM generate tmp files under /tmp, which are not deleted later. This will end up /tmp space to be depleted.

- CSCtl84876

Symptom:

Error occurs in Uploading Coverage file of size more than 500 KB

Conditions:

It is because of an internal error derived from third-party software that CDSM uses for file upload.

SNMP

- CSCtj15109

Symptom:

SNMP daemon core dumps.

Conditions:

It happens when SNMP receives alarm notifications without description information.

- CSCti05966
Symptom:
authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. Only SNMPv3 is impacted by these vulnerabilities.
Conditions:
Cisco Internet Streamer CDS SNMPv3 HMAC Authentication issue.
- CSCtj41997
Symptom:
SNMP Manager fails the timeliness check after the CDE is rebooted.
Conditions:
SNMPv3 is enabled and the device is rebooted.
After reloading the CDE, the snmpEngineBoots remains 1 while the snmpEngineTime is reset.
- CSCtj67697
Symptom:
CDE220-2S3: snmpwalk does not return all objects in a table
Conditions:
Seen on 2S3 only. On 2s3, SNMP get next does not correctly get the next object.

UNS Server

- CSCti60918
Symptom:
When CLI "clear cache all" is executed, the following user warning message with alternate option will be shown:

```
This operation tries to free up xxxMB cached content. yyy Content files to be
deleted. Approximate time for completion is XX hours YY minutes.
The device needs to be offline for the operation to complete.
Alternate option: Format CDNFS using "disk recover-cdnfs-volumes" CLI
Proceed? [Yes/NO]"
```


Conditions:
None. Enhancement is added on existing CLI "clear cache all".
- CSCtj04740/CSCti41362
Symptom:
The reason is memory corruption at a specific location. This particular location can cause UNS thread into an infinite loop, all other UNS threads can potentially block on waiting for this thread to finish. This causes high CPU usages for UNS process.
Conditions:
Various URL requests.

- CSCtj29122

Symptom:

ERROR seen in UNS and ucache error log during cache-miss test with 80 TPS.

Conditions:

UNS errorlog:

```
10/03/2010 13:40:37.001(Local) (7459)ERR:unslog.c:134-> ufs_chan_lock: failed[110] to
acquire the lock for uns namespace. Failing!!!
10/03/2010 13:40:37.001(Local) (7459)ERR:unslog.c:134-> Failed to acquired lock [56]
```

URL Manager

- CSCti85605

Symptom:

URL Signing CLI configs is lost after reloading SE

Conditions:

In recent release image, the boot up sequence is faster as a result the network is not ready before this CLI is executed.

- CSCtj30209

Symptom:

The characters "%20" in a URL lead to invalid signed URL, Wmt_be core dump in 2.5.3b34

Conditions:

When encoder make "space" encoded as %20 in the URL, in which it will lead to invalid signed URL. For example, 2%20RTSP/1.0

- CSCtj63802

Symptom:

Invalid client IP addresses were matched and validated because of strstr usage.

Conditions:

When a device has an external IP address of 172.22.28.75 and a different IP address for internal. Flash Media Streaming and Authorization Server are enabled, and the primary Geo-location server IP address is 172.22.30.240 and the port is 7000. The server URL is rtmp://RT-612-8.se.sree.spcdn.net/vod and the stream name is the following:

```
foo.flv?SIGV=2&IS=0&ET=1287584870&CIP=7.5.1.1540&KO=1&KN=2&US=1960c0844d72221494d0eb0f
d76dc3ba0805ccea
```

Service Router

- CSCtn20525

Symptom:

When a request is forwarded for a last-resort use case, the SR needs to remove the .asx in the URL; otherwise, the content fails to be served.

Conditions:

When the **http asx-302-redirect** command is enabled, last-resort routing redirects by way of a 200 HREF which triggered the STB to use the NSPlayer client that subsequently ignores all redirects.

- CSCth86190

Symptom:

SE does not get picked for routing even though it has a lower metric.

Conditions:

When the SE is offloaded before the routing.

- CSCti32189

Symptom:

Sysmon core dump on protocol robustness testing using codenomicon for HTTP and RTSP.

Conditions:

Send anomaly request using codenomicon for HTTP from test case. This will leads to infinite request for HTTP on port 80.

- CSCtj17154

Symptom:

Service Router backend does not use new proximity server configured.

Conditions:

When an invalid proximity server configuration is made, which is updated to a new proximity server config.

- CSCtj89982

Symptoms:

This feature allows us to specify domains that the service router should subscribe to. By default the service-router takes all the domains specified in the CDSM. With this feature even if we configure one domain subscription through the CLI mentioned below, The service router will take the list of domains subscribed through the CLI to be complete list.

Syntax for config:

```
Temp2(config)# service-router subscribe domain test3.com
Show command for config:
Temp2# show service-router subscribe domain
Domains subscribed:
    test1.com
    test5.com
    test4.com
    test3.com
```

Conditions:

Service Router takes all the domains specified in the CDSM. This new CLI allow SR only take the domain configured by way of this CLI.

- CSCti09375

Symptom:

No fields for proximity/geo-location info.

Conditions:

When an SE is picked using geo-location or proximity based routing.

The following enhancements were added:

1) Enhanced Routing Statistics

Statistics to show which routing method is used in redirection to service engines.

```
Temp2# show statistics service-router routing
----- SR Routing Statistics -----
Network Redirects:      :           0
Proximity Redirects:   :           0
Geo Location Redirects: :           4
Zero Network Redirects: :           0
Last Resort Redirects: :           1
```

2) Enhanced Transaction logging. Addition of field "routing-method" to show which routing method was picked.

```
#Software: Cisco CDS Service Router
#Fields: c-ip user-agent date time url protocol server-picked status routing-method
3.1.5.13 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rvAccept 2010-10-25 21:08:32
http://pxe.spcdn.net/index.html HTTP cnn.com 302 Last-Resort
3.1.5.13 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rvAccept 2010-10-25 21:17:40
http://sree.spcdn.net/index.html HTTP DD10-2G2-2 302 Network
3.1.5.13 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rvAccept 2010-10-25 21:21:38
http://sree.spcdn.net/index.html HTTP DD10-2G2-2 302 Proximity
3.1.5.13 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rvAccept 2010-10-25 21:22:02
http://sree.spcdn.net/index.html HTTP DD10-2G2-2 302 Proximity
171.71.50.213 Wget/1.10.2 (Red Hat modified) 2010-10-25 21:24:32
http://sree.spcdn.net/index.html HTTP DD10-2G2-2 302 Zero-Network
171.71.50.213 Wget/1.10.2 (Red Hat modified) 2010-10-25 21:28:15
http://sree.spcdn.net/index.html HTTP DD10-2G2-2 302 Zero-Network
171.71.50.213 Wget/1.10.2 (Red Hat modified) 2010-10-25 20:04:17
http://test.com/index.html HTTP SD-CDE100-CE-2 302 Geo-Location
171.71.50.213 Wget/1.10.2 (Red Hat modified) 2010-10-25 20:07:47
http://test.com/index.html HTTP SD-CDE100-CE-2 302 Geo-Location
10.21.64.52 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rvAccept 2010-10-25
20:09:00 http://test.com/index.html HTTP google.com 302 Last-Resort
171.71.50.213 Wget/1.10.2 (Red Hat modified) 2010-10-25 18:19:59
http://test.com/index.html HTTP W14-2G2-1 302 Network
10.21.64.52 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rvAccept 2010-10-25
18:20:55 http://test.com/index.html HTTP google.com 302 Last-Resort
10.21.64.52 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rvAccept 2010-10-25
18:22:10 http://test.com/index.html HTTP - 404 -
10.21.64.52 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rvAccept 2010-10-25
18:22:15 http://test.com/favicon.ico HTTP - 404 -
10.21.64.52 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rvAccept 2010-10-25
18:22:20 http://test.com/favicon.ico HTTP - 404 -
```

3) Enhanced proximity statistics. Addition of proximity related statistics to show number of cache hits, cache misses and errors.

```
DD10-CDE205-1#show statistics service-router routing proximity
----- SR Proximity Routing Statistics -----
Cache Hits      :           2
Cache Misses    :           3
Errors          :           2
```

4) Enhanced geo-location statistics. Addition of geo-location related statistics to show number of cache hits, cache misses and errors.

```
Temp2#show statistics service-router routing geo-location
```

```

----- SR Geo Location Routing Statistics -----
Cache Hits           :           3
Cache Misses        :           2
Errors               :           1

```

- CSCtj52764

Symptom:

Service Router not picking the SE configured in the zero network.

Conditions:

When the same subnet is configured with different prefix lengths or when there are multiple subnet matches in the coverage zone for a given client IP address.

- CSCtj93775

Symptom:

Unable to turn off service-monitor debug traces after its enabled.

Conditions:

After enabled "service-monitor debug," it shows nothing.

```

debug service-router servicemonitor
V9-CDE220-1# show debugging

```

After disabled the debug trace, still the errorlog prints the traces and unable to stop it.

- CSCtg22960

Symptom:

Adding show command for displaying the SR proximity cached entry and the hit count.

Conditions:

Syntax Command:

```

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

```

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

```

SJ-612-CDM# show service-router proximity-based-routing cache ip 172.20.123.12
No proximity cache information available.

```

```

SJ-612-CDM# show service-router proximity-based-routing cache ip 171.70.219.116

```

```

----- Proximity cache information for 171.70.219.116 -----
Cached proximity information on Fri Jul 30 05:19:50 2010

```

```

SE Name: V8-CDE200-Fiber

```

```

Rating : 3758096385

```

```

SE Name: SD-CDE100-CE-2

```

```

Rating : 3758096385

```

```

SE Name: SSFT-SR

```

```

Rating : 3758096385

```

```

SJ-612-CDM# show service-router proximity-based-routing cache ip 171.70.219.116/16

```

- CSCtj39709

Symptom:

Service Router returns CDS version in HTTP response, which is not desirable.

Conditions:

"Cisco-CDS version number" was returned as the server for both HTTP and RTSP requests.

- CSCtk46337
Symptom:
Service Router module coredumps.
Conditions:
When the data server notifications are not received completely multiple times. :Likely to be seen in cases of stress or when large coverage zones are loaded.
- CSCtk06918
Symptom:
Memory usage of service router is really high.
Conditions:
When the coverage zone file has zero networks configured.
- CSCth86738
Symptom:
SR: 'sh service-router routes' does not display output with large CZ files.
Conditions:
When Large CZ file is assigned to SR, ' sh service-router routes ' does not display the routes.
- CSCtl47980
Symptom:
SE to SR Keepalive alarm raised and clear every few hours.
Conditions:
When using a script to execute "show service-router service-monitor" every few seconds. And Data server errors were also seen in the service engines.
- CSCtl50500
Symptom:
Service Router RES memory usage increased to 3.2 GB when it tried to assign and unassign the Coverage Zone file repeatedly.
Conditions:
Unassigning and reassigning the CZ File 3 times will increase the memory utilization even further to 3.2 GB. At the end, service_router process stopped, core dumped, and restarted.

Network

- CSCtj47362
Symptom:
Add CLI to disable/enable auto negotiation under port channel.
Conditions:

```
DD6-2G2-3(config-if)# no autosense
DD6-2G2-3# show running-config
interface PortChannel 1
no autosense
ip address 5.2.0.15 255.255.0.0
exit
```

```

DD6-2G2-3(config)# interface portChannel 1
DD6-2G2-3(config-if)# autosense
DD6-2G2-3# show running-config
interface PortChannel 1
ip address 5.2.0.15 255.255.0.0
exit

```

- CSCtk09422

Symptom:
SE goes to KDB mode when configuring new portchannel during WE traffic.

Conditions:
Configure (adding/deleting) port-channel ip-addr when 2000 requests per second load on the device ongoing.
- CSCtk14269

Symptom:
After changing autosense and bandwidth on a port channel back and forth, the show interface command starts to print an error message.

Conditions:
The show interface command prints error message after setting bandwidth on port channel.

Proximity Engine

- CSCti34970

Symptom:
When BGP is configured on the Proximity Engine, its Autonomous System cannot be changed later.

Conditions:
This problem was introduced in 2.5.9.b17.
- CSCti40892

Symptom:
Proximity Engine is running, show running shows BGP, but bgpd is not running after reload or protocol stop/restart.

Conditions:
Timing issue, happens if BGP comes up faster than RIB, happens consistently in 2.5.9 b24.
- CSCti41769

Symptom:
If BGP does not start after reload, and we deconfig/config it to make it start, then it crashes, none of the protocols are restarted as they should be.

Conditions:
Corner case - timing issue, happens only if BGP has not started after reload.
- CSCti58002

Symptom:
Client requests to proximity engine time out.

Conditions:

Timing issue, shows up sometimes.

- CSCtk13609

Symptom:

DHT ring cannot be form even though the NTP server has been configured.

Conditions:

DHT node is configured with NTP server where its clock source is from external sources, rather than its hardware clock; for example, GPS. CLI 'show ntp status' command display the clock source type in the 'refid' column.

- CSCtl80593

Symptom:

PTAs that are directly connected do not get preferred rating even though they are close to PSA. The reason is that they are considered a direct route and BGP communities are not used.

Conditions:

Occurs when Streamers and Proximity Engine are connected by way of same switch.

Platform

- CSCtl72788

Symptom:

Older CDEs (CDE100 and CDE200) create false Temperature alarms.

Conditions:

Normal working conditions.

- CSCti46994

Symptoms:

Disk usage goes up periodically while being mostly idle in between peaks.

Conditions:

HTTP cache miss small objects (< 2mbyte per file).

- CSCti29701

Symptom:

The nscd process goes into core dump after two days of stress traffic.

Conditions:

The nscd process is restarted right away after core dump. Service router would redirect the traffic, and streaming will continue without any impact.

- CSCti75269

Symptom:

The netstat -s utility gives output in cumulative numbers only.

- CSCti75287
Symptom:
The tcpdump has limited capture rate.
- CSCti75249
Symptom:
ARP queue is too small.
- CSCti75261
Symptom:
The netmon utility gives output in bytes, no systat options.
- CSCti86437
Symptom:
Add CLI commands for ss, tcpmon, netmon and netstartr.
- CSCti66740
Symptom:
Add tcpmon utility.
- CSCti94605
Symptom:
Create a new 'disk recover-cdnfs-volumes' CLI. User is informed of the nature of the operation (all services stopped / reload / all content erased) and is double prompted (are you really sure?) for confirmation. When executed, all services are brought down by way of nodemgr. Once brought down, all CDNFS partitions (and only CDNFS partitions) are formatted. The end result is that all files are erased on all CDNFS partitions very rapidly (within 1 min). The system is automatically rebooted
Conditions:
To supports volume recovery by way of CLI.
- CSCtj14569
Symptom:
Interface option for static route CLI should be removed.
Conditions:

```
(config)# ip route 1.1.1.1 255.255.255.255 4.5.0.1 ?
(config)# ip route 1.1.1.1 255.255.255.255 4.5.0.1 interface 4.5.0.2
% Invalid input detected at '^' marker.
```
- CSCsy56641
Symptom:
2G2: Device gone into kdb while loading .bin image from installer.
Conditions:
2G2 while loading .bin image.

- CSCti55123
Symptom:
Pull out 1 raid disk and the degraded raid alarm comes up properly. Pull out the 2nd raid disk and no further alarms show up.
Conditions:
Critical alarm 445005 should be raised when both disks are pulled out.
- CSCtj39696
Symptom:
The image running is 2.5.9.b111, core dump generated with this image is showing version 2.5.6.
Conditions:
When core generated, it will show different version sometimes.
- CSCti91239
Symptom:
Core files for the vi editor are seen on the SE and CDSM.
Conditions:
None.
- CSCti50286
Symptom:
Web Engine generates a core and comes up.
Conditions:
WE domain name resolution core dumps on the name resolution part which could happen if the domain name is not part of the delivery service.
- CSCtl86860
Symptom:
Some commands allow an authenticated administrator user to obtain root privileges on a CDS-IS system. The CLI fails to properly validate provided user input.
Conditions:

```
# netmon -h;/bin/sh
# ss -h;/bin/sh
# tcpmon -h;/bin/sh
```

Unified Kernel Streaming Engine

- CSCtj37857
Symptom:
ukse_wmt.c:1114 : SE restarting while running WMT stress
Conditions:
When WMT streaming under stress, observed both for SBR content and MBR content.

- CSCt120958
Symptom:
Service engine rebooted automatically.
Conditions:
Rare condition. cache-miss case.
- CSCt173331
Symptom:
Accept-filter mishandling space from android 2.2 flash VOD.
Conditions:
Android player is sending different content type, and there are 2 space char after colon (:).
user-agent: Shockwave Flash
content-type: application/x-fcs
The kernel accept-filter does not handle spaces between "Content-type:" and "application/x-fcs.
- CSCt184066
Symptom:
One of the CPU cores showing 99 percent CPU usage in wmt_be process. This process cannot be killed or attach gdb.
Conditions:
This can happen during an extremely small corner case; for example:
 1. Client has connected.
 2. Entered fast start. Timer is added to schedule packets out. Lets say the timer was still pending meaning, about to run.
 3. Client exits. so, we handle the exit path and turn off the running flag of the client. and we are about to turn on the exit bit to notify all other threads that this client has exited.
 4. Right after turning off running flag, we get a control back into main thread. This thread would always wait on running flag. So, it would proceed further to clean up client and realizes that still the exit flag is not turned off.
 5. At this point, main thread, would see that still there was a timer pending for the client and can never be invoked as the client is gone. so, will delete the timer. There is a bug right after this.

Authorization Server

- CSCtk83193
Symptom:
The client receives a 403 error "Auth Server Query Denied" response and the Authorization Server blocks the request when Geo-location server failed initialization.
Conditions:
The request is blocked by the Authorization Server when there is an error in initializing the Geo-location server.

- CSCti30585
Symptom:
The AuthServer stops because of a signal 6 and generates a core dump file.
Conditions:
A huge authorization XML is uploaded having repeating values of IP address and various combination of subnet mask.
- CSCti83014
Symptom:
The AuthServer process coredumps because of a lack of memory caused by a slow increase in the authserver process memory.
Conditions:
The AuthServer is configured with rules XML having pattern match expressions (regex operation). There is a memory leak, causing the memory to increase slowly. Eventually the authserver coredumps due to lack of memory.
- CSCti82275
Symptom:
Certain client Ip address blocked by Geo server.
Conditions:
Authorization Geo XML file with some specific country (for example, India) in configuration. Request client ip address does not have valid State & city returned from Quova location server.
- CSCth37786/CSCti26407
Symptom:
Occasional restart of Authorization server during delivery service configuration update.
Conditions:
Service Engines in a delivery service are added/removed in quick succession.
- CSCti73995/CSCti79929/CSCti53309
Symptom:
Under high traffic condition the Web-Engine sees occasional "deny" for valid requests made to AuthServer.
Conditions:
The Web-Engine is under high traffic stress condition with each requests passing to AuthServer. The UDP buffer overflow during the AuthServer communication causes packets to drop. This results in Web-Engine experiencing DENY for requests made to AuthServer.
- CSCtj07698/CSCtj83143
Symptom:
Geo-location based authorization denies requests coming from locations that are matching one Allow block in the XML configuration file.
Conditions:
The XML configuration file also contains a Deny block that matches the same request that should be allowed.

Normally the action should be determined by the first matching block, and the Order element. A typical case will be to have a Deny block that matches "ALL" for country -> requests that already matched one Allow block will also be matched to the Deny block, and be denied.

- CSCtj26142

Symptom:

Enabling trace level logging during stress test causes AuthServ mem leak.

Conditions:

When the trace level is turned on in authserver.

- CSCtj60539

Symptom:

When URL signing keys not configured on streamer or cdsm, Change the key id, ko, client ip of the URL in the browser & issue the request. The content is still served instead of getting blocked.

Conditions:

URL signing keys are not configured by way of SE or CDSM.

- CSCtj57181

Symptom:

WE core dumps at sipc library during mixed stress test.

Conditions:

The AuthServer is enabled and there is a high incoming traffic.

- CSCtj39353

Symptom:

It is not possible to specify a rule based on negation. The AuthServer regex pattern has a limitation to support [^] or [!] in the pattern match. Therefore, it is not possible to specify a rule to do URL validation based on regex pattern rejection.

Conditions:

UrlRegex pattern having a negation pattern i.e. [^] or [!] does not work - the regex library does not match the incoming URL correctly based on the negation pattern.

It is an enhancement (to support "negate" regex) that cannot be addressed in 2.5 or 2.6 release but can be put on the road-map for 2.7 for marketing to prioritize. Customer can put this into their customer-driven feature request list to work with Cisco on prioritization and timing.

- CSCtj44579

Symptom:

AuthServer core dumps due to memory leak. when large number of delivery services are configured and each delivery service has a huge Authorization XML file associated with it.

Conditions:

There is a memory leak when large number of delivery services are configured and each delivery service has a huge Authorization XML associated with it.

- CSCtk15496

Symptom:

Not able to turn-off authserver debugging.

Conditions:

After enabling debugging authsvr trace. When try to disable the debugging using "undebug all" no effect i.e debugs for authserver is not disabled. Tried "undebug authsvr trace" it enabled the error debugging of authsvr without giving "debug authsvr error." Still authsvr trace messages are coming in the errorlog of authsvr. The show debugging command displays --> "Debug Authsvr error is on."

- CSCtj21662

Symptom:

Undebug/no debug all did not disabled authsvr trace logs.

Conditions:

When AuthSrv has trace level log, "Undebug/no debug" cannot disable it.

- CSCtk83193

Symptom:

Client get 403 error "Auth Server Query Denied" response and Authsvr blocks the request when quova server failed initialization.

Conditions:

The request is blocked by authsvr when quova initialization failed and there is an error in initializing quova server.

CLI

- CSCtl58519

Symptom:

The **find** command allows the user to run UNIX commands as user *root*.

Conditions:

Using the **find** command, it is possible to run random UNIX commands from the normal shell of the CDE. Only the administrator with privilege level 15 should be able to do this.

- CSCti20552

Symptom:

Missing option to pipe "|" when running 'show' commands. Missing option to run 'show' command while in config mode. We need to have options as on other Cisco devices, example:

```
Switch# show run | ?
  begin      Begin with the line that matches
  exclude    Exclude lines that match
  include    Include lines that match
Switch(config)# do show clock
13:28:14.529 EST Tue Aug 3 2010
```

Conditions:

In this fix, we only add support for '|' for 'show commands', not provide 'do command ***' under configure mode.

- CSCti32270

Symptom:

The type command only allows "type working.log <cr>", need to support pipe | command for type.

Conditions:

For "type" command to get "include/exclude" support.

- CSCtj21698

Symptom:

Type-tail is not following the log file changes, need -F, not -f.

Conditions:

We pass option "-f" to the tail command, When we have "follow" key word. This will follow the tail end of the file (as it grows) if and only if the "file descriptor" is valid; that is, when working.log gets deleted / reassigned the tail will not follow the log.

We have to pass the option of "-F" (upper cases) (or) use "-follow=name" so that the filename is followed instead of the file descriptor. So even if working.log changes the tail command will continue to follow.

- CSCtg68295

Symptom:

Adding ntp.drfit file for better time sync.

Conditions:

The driftfile entry in /etc/inet/ntp.conf tells xntpd the name of the file where it can find and store the clock drift, also known as frequency error, of the system clock. If the file exists at startup, it is read and the value is used to initialize xntpd's internal value of the frequency error. The file is updated once every hour by xntpd. It usually takes a day or so after the daemon is started to compute a good estimate of the clock drift. Once the initial value is computed, it will change only by relatively small amounts during the course of continued operation. Because xntpd needs a good estimate to synchronize closely to its server, there should always be a driftfile entry in /etc/inet/ntp.conf.

- CSCth97786

Symptom:

At the CLI, when using term length 0, type-tail l, include the lines that does not contain the filtered search.

Conditions:

The term length is set to 0.

- CSCtj74232

Symptom:

Some commands need to be removed from user exec mode.

```
EE8-2G2-5>?
cd          Change directory
delfile     Delete a file
deltree     Delete directory
mkdir       Create a directory
mkfile      Create file
rename      Rename Oldfile to Newfile
rmdir       Delete a directory
```

Conditions:

Under CLI EXEC mode. Because, by definition, User EXEC mode gives you limited access to view basic device functionality. No configuration privileges.

- CSCtl41656
Symptom:
Translog file not logged on working.log after change the clock settings unless transaction logs restart the config.
Conditions:
After changed the clock, no logs are logged on working.log until transaction log disabled/enabled.

Service Monitor

- CSCtj36777
Symptom:
Need to raising an alarm for portchannel, if negotiated data rate for interface is different in the portchannel.
Conditions:
When interface within port-channel being negotiated to wrong bit-rate.
- CSCti43840/CSCtj81825
Symptom:
Redundant error messages seen in svmon alarm monitor.
Conditions:
On CDSM, service_monitor_errorlog.current has many ERRO message indicating "Cannot get alarm threshold exceeded". However, CLI "show alarms detail" did not show any threshold exceeded alarms.
- CSCtk60930
Symptom:
The svc-monitor fd leak during stress testing with 900 simulated users.
Conditions:
Service monitor Socket creation error code: 6 of the below logs keep printing on SE during stress traffic and after stopped the stress testing.

```
12/02/2010 14:44:53.746(Local) (22577)ERRO:servicemonitor.c:804-> Failed not connect to the nodehealth dataserver. (6)
12/02/2010 14:44:53.756(Local) (22577)ERRO:sm_service.c:109-> Failed not connect to the nodehealth dataserver. (6)
12/02/2010 14:44:53.784(Local) (22577)ERRO:servicemonitor.c:804
```

Movie Streamer

- CSCti94906
Symptom:
The Movie Streamer process enters core-dump, terminating all Movie Streamer sessions from the downstream clients on this streamer.

Conditions:

This happens once a MS UIMO (Unicast In and Multicast Out) live program is configured and Movie Streamer fails to join the specified multicast group.

Transaction Logs

- CSCti92988

Symptom:

Non- standard Quicktime Streaming Server format appears. Sawmill recognizes QTSS by the W3C header:

```
#Software: QTSS
#Software: DSS
```

The following header will not work:

```
#Software: Cisco-CDS Version: 2.0.0 Remark: all time values are in GMT.
```

Conditions:

Anew format, not yet supported by Sawmill.

Unified Log

- CSCtk56581

Symptom:

The rtspg/stream-scheduler/live-routing module by default trace level is used in error log.

Conditions:

Normal working path.

Acquisition & Distribution

- CSCtl02993

Symptom:

When issuing cdnfs cleanup force start, the ucache-svr snapshot db entry is treated as garbage & removed.

Conditions:

1. Cached thousands of content in SE.
2. Clear the contents using "clear cache all" command.
3. Few contents will be retained in the disk due to RPC timeout.
4. The same contents being looked up again, ucache sanity retain them back to the front end.
5. The entry ucache_svr created during the process is seen in cdnfs browse.
6. When issuing cdnfs cleanup force, the entry is treated as garbage & removed.

Resolved Caveats in Releases 2.5.9-b5, 2.5.9-b6, and 2.5.9-b18

The following caveats have been resolved since Cisco Internet Streamer CDS Releases 2.5.9-b5, 2.5.9-b6, and 2.5.9-b18.

Windows Media Streaming

- CSCth10896
Symptom:
When requesting cache miss content, SE tries to create a very large size (for example, 12TB) cache entry, which causes UNS core-dump.
Conditions:
The content is corrupted and includes some invalid value in the file header.
- CSCth99148
Symptom:
Sometimes file system freezes and SE goes into KDB mode.
Conditions:
SE has cached many large MBR contents whose file size is more than 1 GB.
- CSCth74586
Symptom:
In a system with two tiers of SEs, a client sends a request to the edge SE for a content, which is immediately pauses and no stream occurs. When the **show stat wmt streamstate** command is entered on the edge SE, there is a PAUSE stream entry.
Conditions:
The requested content is corrupted.
- CSCtg96202
Symptom:
Some content cannot be served by the SE.
Conditions:
The content has a large ASF header that is more than 32K bytes.
- CSCth99233
Symptom:
When serving MBR contents, sometimes SE generate wmt_be core dump.
Conditions:
More than one request for same MBR content and some seek, pause, play operation.
- CSCtg91264
Symptom:
Sometimes when Windows Media Streaming fast cache is disabled, the SE still performs fast cache.
Conditions:
Conditions when this occurs are still being investigated.

- CSCtf07360
Symptom:
Multiple bit rate (MBR) VOD payback fails for a large file sometimes.
Conditions:
Happens when fast cache is turned on.
- CSCtc98771
Symptom:
Stale sessions are listed in Play state in the output for the **show stat wmt streamstat** command.
- CSCtf77234
Symptom:
The transaction log configuration from device group cannot apply to the SE in this special case.
Conditions:
If configure any value from CLI and negate it, a CLI with default value still shows in running config.

Flash Media Streaming

- CSCtg07042
Symptom:
Flash Media Streaming core dumps after ten days of stress testing manual requests.
- CSCte65508
Symptom:
The Flash Media Streaming processes take 100 percent of the CPU usage after changing the local time or possibly a negative NTP change. Mostly this would occur when the SE is reloaded.
Conditions:
The fmsadmin process and fmsedge process is at 100 percent of the CPU after the SE reloads.
- CSCtf94686
Symptom:
Cache miss request fails to stream, when the virtual application path map is configured. But the same request next click works fine, because it is cache hit.
Conditions:
During the cache miss request, when the virtual application path map is configured, virtual path map is applied to cache fill requests. But the following HTTP range requests are still sent without the virtual path map, which results in the origin server replying with a 404 error message and the Flash Media Streaming cache miss request failing.

Web Engine

- CSCtg48830
Symptom:
The root cause of this problem is that the resource limit in the system has been reached, but web-engine is not aware of the fact that the system has been reached.

Conditions:

SE raised memory high alarm during the small-obj (smooth vod) test.

- CSCth89963

Symptom:

URL validation not applied for WMT streaming HTTP scenario.

Conditions:

WMT streaming scenario with URL signature validation rules configured.

- CSCth81633

Symptom:

Rule "Rewrite action" is not functional.

Conditions:

When "Rule action rewrite" is configured.

- CSCti08311

Symptom:

When a middle SE is dead or connection to it times out, Client sessions hang and SE showing hung HTTP sessions. We also see Content Acquirer transaction logs sending requests to itself.

Conditions:

Incorrect HCache-Header sent to the Content Acquirer causes it to send a request to itself.

- CSCti09238

Symptom:

The player stops streaming and sessions hang on the SE. From the transaction logs it could be observed that there are multiple requests on the Content Acquirer to itself.

Conditions:

When the request from the Edge SE failover to the Content Acquirer (when middle tier SE failed to respond).

- CSCti16831

Symptom:

WMT Live playback takes 5–6 seconds before playback when HTTP is used.

Conditions:

Two-tier setup and liveness query goes between edge and root. Because the WMT live request, EDGE sends liveness query to ROOT which takes around 5 seconds to close connection.

- CSCth78953

Symptom:

Some CDEs, particularly CDE220-2G2 and CDE200, are getting into KDB mode after an hour of stress testing with all unique cache-miss cases, because slab memory usage goes over 10 GB. A file size larger than 1 MB is also not utilizing Persistent Connection and getting delayed occasionally.

Conditions:

Same test done on CDE220-2S3 worked fine. So, particular hardware is exposing the underlying problem.

- CSCth50555
Symptom:
Cds_Hcache_Header is not honored by upstream SE.
Conditions:
the upstream SE is looking for the Cache Route even when the Hcache_header is set.
- CSCth89963
Symptom:
URL validation not applied for WMT streaming HTTP scenario.
Conditions:
WMT streaming scenario with URL signature validation rules configured.
- CSCth59022
Symptom:
Partial response headers improperly appended and parsed.
Conditions:
Not available.
- CSCth81606
Symptom:
HTTP rules are still effective when rule processing is disabled.
Conditions:
Rule action blocks HTTP in pattern-list X.
- CSCth81633
Symptom:
Cache router log file size too small.
Conditions:
With current size, the log file wrapped too fast.
- CSCth85349
Symptom:
In Windows Media player, a URL with a query string is unable to play content.
Conditions:
URL needs query string.
- CSCth84308
Symptom:
WMT service rules; for example, src-ip pattern for HTTP, are working in reverse manner.
Conditions:
When defining a service rule that uses rule action block or allow with the src-ip pattern.
- CSCth73499
Symptom:
Rule action block does not work on HTTP. A player is able to play content from blocked domains.

Conditions:

Configure a service rule action block on HTTP in pattern-list x. An example follows:

```
rule action block pattern-list 20 protocol http
```

- CSCth23130

Symptom:

The Web Engine core dumps in a particular scenario.

Conditions:

When streaming available bit rate (ABR) content with a lot of trick modes and pacing value changes on the fly.

- CSCth24981

HTTP 504 errors are seen in transaction log every few hours when sending request from ABR clients.

Conditions:

No specific condition for causing this issue is identified.

- CSCth37775

Symptom:

Web Engine serving available bit rate (ABR) content for Windows Silverlight fails in particular scenario

Conditions:

When a lot of player controls are given (rewind, fast-forward, and seek) and there is two-tier setup with two SEs in the upper tier, the playback fails

- CSCth24970

Symptom:

Some Manifest files cannot be downloaded by way of the SE.

Conditions:

Using older Apache HTTP server. Transfer:Encoding encoding is sent for static length file with Connection: Close.

- CSCtg98195

Symptom:

Passwd file on the SE and SR is exposed.

Conditions:

Enter the **?etc/passwd** command and the file on the SE is sent out when the request is sent for /etc/passwd file in particular manner by security tool Nessus.

- CSCtg89961

Symptom:

Edge SE does not request content from direct upstream SE but tries to failover to origin server (OS).

Conditions

When delay of liveness query from upstream SE happens, the edge SE marks the upstream as dead.

- CSCtg59009
Symptom:
All head requests return with a 501 not implemented.
- CSCtg28997
Symptom:
TCP sessions hang when a very large (greater than 1.5K bytes) cookie header is sent.
Conditions:
Parsing error occurs in some scenarios when the whole cookie is not received and a read is performed.
- CSCtg22998
Symptom:
Client request for a movie freezes. All subsequent requests for the same movie to the same SE also result in the video freezing.
Conditions:
Manifest file on the SE is corrupted and stays that way in memory. Hence all subsequent requests are served from the same file. HTTP sessions and data sources hang on the SE side, which can be seen when the **show statistics web-engine command** is entered.
- CSCtg11200
Symptom:
Core dump on Web Engine pointing to multiple thread transfers with incorrect URL.
Conditions:
Request sent with the host appended with port 80 to it; for example, http://SEIP:80/index.html
- CSCtg07057
Symptom:
When an error code is sent to the end user it does not have content-length leading to the client waiting for timeout before connection is closed.
Conditions:
Client request results in an error and the response does not have a content length as Body is not sent.
- CSCte63002
Symptom:
For HTTP/1.1 clients the browser will look like its in hang state for some time, till the keep-alive connection times out from the server.
Conditions:
Happens when Server returns 302 redirect for HTTP/1.1 clients.

Cache Router

- CSCtg90162
Symptom:
Cache Router sometimes selects same parent for different URL when playing Smooth HD video.

Conditions:

The hash algorithm is always generating the even hash value for different URLs, which is in turn selecting the same parent for different URL

CAL

- CSCth88395

Symptom:

Web Engine will result in having 30K sessions hanging, UNS not creating any more new contents (for other protocol engines). If there is a manifest files mentioned to the delivery service and a periodic refresh is given, then alarm will be raised saying manifest file fetch error. Basically UNS process goes into a dead lock or some state like that, which prevents UNS from any create operation.

Conditions:

The actual root cause for this issue is not found. But this issue is seen on HTTP small objects creation environment.

CDSM

- CSCth31347

Symptom:

After assigning a Coverage Zone file to the SR, the service-routes are displayed for a few seconds when the **show service-router routes** command is entered and then the output stops.

Conditions:

The SR database is not yet synchronized with the Coverage Zone file that was recently added.

- CSCti02310

Symptom:

The system supports ten gigabit Ethernet network interface since 2.6.0.b42. So if the CDSM is higher and SR is lower than this version, the CDSM throws an exception when receiving ISIS statistic data sent by SR, and vice versa.

Conditions:

Java file IsisStats' serial version uid was changed when this file was updated in CSCth04776, which means the old system cannot read this object from stream.

- CSCth23025

Symptom:

The white space is allowed in the delivery service name when creating and modifying a delivery service. In this case, the PCM hook fails to execute the delivery service related CLI at SE box.

- CSCtf61997

Symptom:

On an SE, the delivery service related information stored in the /state/perdsvc.xml file cannot be removed as expected even if the SE is deregistered from the CDSM.

Conditions:

If the SE is assigned as the Content Acquirer of any delivery service, the perdsvc.xml file is not changed after the SE deregistered.

SNMP

- CSCtg93811
Symptom:
ifInOctects and ifOutOctects in MIB-II reach the maximum 32 bit number and no longer change.
Conditions
The system is a 64-bit system. The system has run for long enough time so that the traffic on the interface has exceeded the range of the 32-bit counter.

UNS Server

- CSCth04635
Symptom:
Core was generated by uns-server. Program terminated with signal 11. Segmentation fault.

URL Manager

- CSCth27308
Symptom:
Wrong error code returned results in URL being allowed.
Conditions:
The URL is allowed even though the correct error check is done. This is because wrong error code is returned.

Service Router

- CSCth91974
Symptom:
Configuring 0.0.0.0 in the Coverage Zone file does not work when proximity-based routing is enabled and no rating respond.
Conditions:
When 0.0.0.0 is included in the Coverage Zone file and proximity-based routing generates no rating response.
- CSCth14220
Symptom:
For requests with large cookie headers (greater than 1500 bytes), the Service Router drops the requests.
Conditions:
The request to the Service Router to be fragmented because it is too large.
- CSCth05856
Symptom:
SEs go intermittently offline and come back online. Alarms are generated.

Conditions:

Happens when a large Coverage Zone file is uploaded (4MB) with several thousand entries.

Network

- CSCth14181

Symptom:

Throughput of a session is limited and lower than the bit rate configuration.

Conditions:

Symptom becomes more serious and apparent as network latency (RTT) increases.

Proximity Engine

- CSCth07380

Symptom:

When entering the **no router bgp** command and followed immediately by the **router bgp** command using copy and paste, the CLI may respond with the following error message:

```
Verifier didn't respond. Need to re-register verifier. (Error number: 64)
```

Conditions:

This problem may only be seen when using copy and paste. Entering the command by typing it will likely not cause a problem.

Platform

- CSCth60992

Symptom:

A Content Acquirer always performs a DNS lookup for every connection to an origin server. The TTL in the DNS response is not honored.

Conditions:

A cache miss occurs on the Content Acquirer.

- CSCth79471

Symptom:

Alarms are raised for physical issues on the drives but not for logical at this stage. XFS errors are seen in syslog but no alarm is generated.

Conditions:

Normal operations.

Unified Kernel Streaming Engine

- CSCth46631

Symptom:

The **show statistics wmt st** command is locked up. Live stream is frozen.

Conditions:

Client sessions join and leave a live stream.

API

- CSCth44836

Symptom:

UNS-related errors occur because the program name and reference URL had uppercase and lowercase characters, but the API only allows lowercase characters for both the program name and reference URL.

Conditions:

Live programs with uppercase characters in the program name and reference URL (unicast or multicast) are not consistent with API calls, which expect only lowercase characters.

Upgrading to Release 2.5.9

The only supported upgrade paths are Release 2.5.x to Release 2.5.9. If you are running a release prior to Release 2.5.x, you must upgrade to at least Release 2.5.x before upgrading to Release 2.5.9.



Note

Before upgrading from Release 2.5.3 to Release 2.5.9, enter the **clear cache all** command.

Content cached in the Release 2.5.3 Web Engine, if requested in Release 2.5.9, results in duplicate entries in the ucache process. Duplicate entries were found in the output of the **show content** and **show cache** commands, but the disk maintains only a single copy of the content.

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



Note

Release 2.5.9 only supports one IGP (IS-IS or OSPF) for the Proximity Engine. When upgrading to Release 2.5.9 from Release 2.5.1 or Release 2.5.3, if both IGPs (IS-IS and OSPF) were configured for the Proximity Engine, then one of the configurations must be removed.



Note

The new Web Engine in Release 2.5.9 cannot be removed during downgrade to Release 2.5.3 because this configuration is still valid in Release 2.5.3 (the new Web Engine was supported as an EFT feature in Release 2.5.3). Therefore, both CLI commands are present after downgrading.

If user roles are defined in Release 2.5.9, and the system is then downgraded to Release 2.5.3, then the following menu options will not be accessible to the user with defined roles:

- Devices > Service Engines > Service Control > ICAP
- Devices > Service Engines > Service Control > ICAP Services
- Devices > Service Engines > Service Control > PCMM QoS Policy
- Devices > Service Engines > Application Control > Web > HTTP > HTTP Connections
- Devices > Service Engines > Application Control > Web > HTTP > HTTP Caching

- Devices > Service Engines > Application Control > Web > HTTP > Advanced HTTP Caching
- Devices > Device Group > Service Control > ICAP
- Devices > Device Group > Service Control > ICAP Services
- Devices > Device Group > Service Control > PCMM QoS Policy
- Devices > Device Group > Application Control > Web > HTTP > HTTP Connections
- Devices > Device Group > Application Control > Web > HTTP > HTTP Caching
- Devices > Device Group > Application Control > Web > HTTP > Advanced HTTP Caching
- Services > Service Definition > Delivery Service > PCMM Config

If any defined user with a defined role requires access to the above menu options, then the menu options must be added by choosing **System > AAA > Roles** and enabling the services for those menu options.

Source Policy Routes

Release 2.5.7 supported multiple IP addresses on the CDE220-2S3i, which included specifying the default gateway and IP routes. The IP routes, source policy routes, were added to ensure incoming traffic would go out the same interface it came in on. An IP route was added using the **interface** keyword, which was introduced in Release 2.5.7, and has the following syntax:

```
ip route <dest_IP_addr> <dest_netmask> <default_gateway> interface <source_IP_addr>
```

In the following example, all destination traffic (IP address of 0.0.0.0 and netmask of 0.0.0.0) sent from the source interface, 8.1.0.2, uses the default gateway, 8.1.0.1. This is a default policy route.

```
ip route 0.0.0.0 0.0.0.0 8.1.0.1 interface 8.1.0.2
```

A non-default policy route defines a specific destination (IP address and netmask). The following ip route command is an example of a non-default policy route:

```
ip route 10.1.1.0 255.255.255.0 <gateway> interface <source_IP_addr>
```

When upgrading to Release 2.5.9, any source policy routes configured using the Release 2.5.7 **interface** keyword are rejected and are not displayed when the **show running-config** command is used. However, because you had to define the default gateway for all the interfaces as part of the multi-port support feature, the equivalent source policy route is automatically generated in the routing table. The following example shows the output for the **show ip route** command after upgrading to Release 2.5.9 with the default source policy routes highlighted in bold and the non-default policy routes highlighted in italics:

```
# show ip route
```

Destination	Gateway	Netmask
172.22.28.0	8.1.0.1	255.255.255.128
6.21.1.0	0.0.0.0	255.255.255.0
8.2.1.0	0.0.0.0	255.255.255.0
8.2.2.0	0.0.0.0	255.255.255.0
171.70.77.0	8.1.0.1	255.255.255.0
8.1.0.0	0.0.0.0	255.255.0.0
0.0.0.0	8.1.0.1	0.0.0.0
0.0.0.0	8.2.1.1	0.0.0.0
0.0.0.0	8.2.2.1	0.0.0.0

```
Source policy routing table for interface 8.1.0.0/16
172.22.28.0      8.1.0.1      255.255.255.128
```

```

171.70.77.0      8.1.0.1      255.255.255.0
8.1.0.0         0.0.0.0     255.255.0.0
0.0.0.0       8.1.0.1     0.0.0.0
    
```

```

Source policy routing table for interface 8.2.1.0/24
8.2.1.0         0.0.0.0     255.255.255.0
0.0.0.0       8.2.1.1     0.0.0.0
    
```

```

Source policy routing table for interface 8.2.2.0/24
8.2.2.0         0.0.0.0     255.255.255.0
0.0.0.0       8.2.2.1     0.0.0.0
    
```

If you have a default source policy route where the gateway is not defined as a default gateway, then you must add it after upgrading to Release 2.5.9. For example, if you had a source policy route with a gateway of 6.23.1.1 for a source interface of 6.23.1.12, and you did not specify the gateway as one of the default gateways, you would need to add it.

If you have a non-default source policy route, then you must add it as a regular static route (without the obsoleted **interface** keyword) after upgrading to Release 2.5.9. This route is then added to the main routing table as well as the policy routing table.

URL Public Key Signing

Table 5 describes the compatibility and results when using a prior CDS software release to perform URL signing and the current software release to perform URL validation.

Table 5 Release Compatibility of URL Signing and URL Validation

Release Used for URL Signing	Release Used for URL Validation	Results
2.3.x	2.4.3, 2.4.5, or 2.5.x	Not supported because the Release 2.3.x URL signing uses the port and schema for signing, but the Release 2.5.9 URL validation removes the port.
2.4.3	2.5.9	Supported for all URL signing versions, except version 3 (CSCtb99898).
2.4.5	2.5.9	Supported for all URL signing versions, except version 3 (CSCtb99898).
2.5.1 or 2.5.3	2.5.9	Supported for all URL signing versions.

Documentation Updates

The following documents have been added for this release:

- *Release Notes for Cisco Internet Streamer CDS 2.5.9*

The following documents have changed:

- *Cisco Internet Streamer CDS 2.5 Software Configuration Guide*
- *Cisco Internet Streamer CDS 2.5 Command Reference Guide*
- *Cisco Internet Streamer CDS 2.4–2.5 API Guide*
- *Cisco Internet Streamer CDS 2.5 Alarms and Error Message Guide*

Related Documentation

Refer to the following documents for additional information about the Cisco Internet Streamer CDS 2.5:

- *Cisco Internet Streamer CDS 2.5 Software Configuration Guide*
http://www.cisco.com/en/US/docs/video/cds/cda/is/2_5/configuration_guide/is_cds25-cfguide.html
- *Cisco Internet Streamer CDS 2.4–2.5 Quick Start Guide*
http://www.cisco.com/en/US/docs/video/cds/cda/is/2_4/quick_guide/ISCDSQuickStart.html
- *Cisco Internet Streamer CDS 2.4–2.5 API Guide*
http://www.cisco.com/en/US/docs/video/cds/cda/is/2_4/developer_guide/is_cds_24_apiguide.html
- *Cisco Internet Streamer CDS 2.5 Command Reference Guide*
http://www.cisco.com/en/US/docs/video/cds/cda/is/2_5/command_reference/Command_Ref.html
- *Cisco Internet Streamer CDS 2.5 Alarms and Error Messages Guide*
http://www.cisco.com/en/US/docs/video/cds/cda/is/2_5/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
- *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide*
http://www.cisco.com/en/US/docs/video/cds/cde/cde205_220_420/installation/guide/cde205_220_420_hig.html
- *Cisco Content Delivery Engine 100/200/300/400 Hardware Installation Guide*
http://www.cisco.com/en/US/docs/video/cds/cde/installation/guide/CDE_Install_Book.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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.