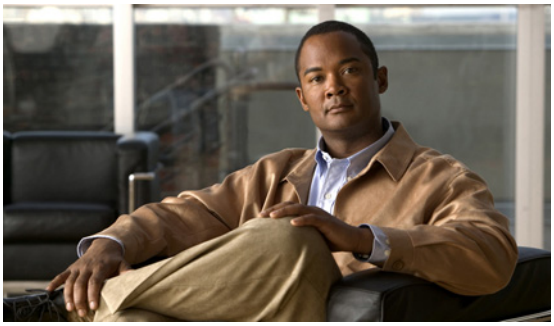

Release Notes for Cisco Videoscape Distribution Suite, Internet Streamer 3.2

These release notes cover Cisco Videoscape Distribution Suite, Internet Streamer Release 3.2.

Revised: March 2013, OL-29020-01

Contents

The following information is included in these release notes:

- New Features in Release 3.2, page 2
- System Requirements, page 3
- Limitations and Restrictions, page 4
- System Limits and Thresholds, page 5
- Important Notes, page 8
- Open Caveats, Resolved Caveats and Enhancements Added in Release 3.2., page 9
- Upgrading to Release 3.2, page 12
- Documentation Updates, page 14
- Related Documentation, page 14
- Obtaining Documentation and Submitting a Service Request, page 15

Note The HTTPS feature and Session-Based Encryption feature are released as general availability (GA) features in Release 3.2. For more information on these features, see the Release Notes for 3.0.0 (http://www.cisco.com/en/US/docs/video/cds/cda/is/3_0/release_notes/CDS_RelNotes3_0_0.html).

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

New Features in Release 3.2

The Release 3.2 of the Cisco VDS Internet Streamer introduces the following features:

- Origin Server Failover
- Generic Session Logging
- Support for UCS M3 platforms

Origin Server Failover

The Content Acquirer can failover to an alternate Origin server if the primary Origin server fails. The alternate Origin server is configured on the Services > Service Definition > Content Origins > Failover Settings page in the CDSM GUI. The Content Acquirer detects Origin Server failure using timeout or other mechanisms. When an Origin Server failure is detected, an alarm is generated to CDSM. The alarm is cleared automatically after a configurable period of time. Meanwhile, the Content Acquirer switches to the secondary Origin Server seamlessly. When all of the Origin Server fails, a 504 response will be generated and sent to client. The operator then manually switches working server among primary OS and any alternate OS. Transaction logs are generated to log these events.

Note The OS Failover feature is only available for HTTP/webEngine.

Generic Session Logging

In Release 3.2, CDS-IS supports Generic Session Tracking and Logging. Generic Session Tracking is used to track the HTTP user session based on session id which is a unique id during the entire session life circle.

This tracking is not ABR protocol specific, the mechanism is generic. All the session information elements can be retrieved from incoming request URL (Intercept URL) and cookie. New and existing SBE rules are configured to retrieve this kind of session information. The requests that cannot be tracked will still be served. Generic Session Tracking does not support Session based encryption.

Note If both Generic Session and ABR Session tracking are enabled in CDSM GUI, the ABR session tracking will get the priority and track the session.

Support for UCS M3 platforms

In Release 3.2 of the Cisco VDS Internet Streamer introduces six UCS M3 configurations. The new UCS M3 HW configurations are to replace UCS M2 HW in the near future.

The following six configurations are being introduced:

- UCS C220 M3 - Mgr/SR Common configuration for Enterprise and Service Providers
- UCS C220 M3 - Enterprise Low
- UCS C220 M3 - Enterprise High
- UCS C240 M3 - Service Providers SAS Vod

- UCS C240 M3 - Service Providers SAS Live
- UCS C240 M3 - Service Providers SATA

For more information about the supported UCS M3 configurations and ordering info please send an e-mail to ask-cds-pm@cisco.com or contact the Cisco support organization

System Requirements

The Internet Streamer CDS runs on the CDE205, CDE220, and the CDE250 hardware models, as well as four UCS models.

Table 1 lists the different device modes for the Cisco Internet Streamer CDS software, and the supported platforms.

Table 1 Supported Hardware Platforms

Device Mode	CDE205	CDE220-2G2	CDE220-2S3i	CDE250 (all models)	UCS C200	UCS C210	UCS C220	UCS C240
CDSM	Yes	No	No	No	Yes	No	Yes	No
SR	Yes	Yes	No	No	Yes	No	Yes	No
SE	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
SR—Proximity Engine standalone	Yes	Yes	No	No	No	No	Yes	No

The new CDE250 models (CDE250-2S8, CDE250-2S9, and CDE250-2S10) have four interfaces at 10 gigabit Ethernet speeds and four interfaces at gigabit Ethernet speeds (plus two additional gigabit ethernet interfaces for management).

The new CDE250 models only support the SE device mode and have the following storage capacities:

- CDE250-2S8—24 x 300 GB 2.5 SSD
- CDE250-2S9—12 x 600 GB 2.5 SSD
- CDE250-2S10—24 x 600 GB 2.5 SSD

The Cisco UCS models (UCS C200, UCS C210, UCS C220 and UCS C240) and the Cisco Internet Streamer Release 3.2 software are sold separately and ship independently of each other.

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

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

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

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

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

Limitations and Restrictions

This release contains the following limitations and restrictions:

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

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

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

System Limits and Thresholds

This release has the following limits and thresholds:

- Service Router Limits and Thresholds
- Service Monitor Limits and Thresholds
- Web Engine Limits and Thresholds
- CDSM Limits and Thresholds
- RTSP Gateway and Movie Streamer
- Windows Media Streaming
- Flash Media Streaming

Service Router Limits and Thresholds

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

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

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

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

Service Monitor Limits and Thresholds

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

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

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

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

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

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

Web Engine Limits and Thresholds

The Web Engine has the following limits and thresholds:

- Memory Usage
- Session Limits
- CAL Limits

Memory Usage

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

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

Session Limits

Web Engine supports the following session-threshold limits:

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

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

CAL Limits

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

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

Other CAL thresholds are as follows:

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

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

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

CDSM Limits and Thresholds

The CDSM has the following limits and thresholds:

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

RPC Connections

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

File Synchronization

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

CDSM Availability (primary and standby)

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

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

SE Configuration Change Synchronization

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

RTSP Gateway and Movie Streamer

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

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

Windows Media Streaming

Windows Media Streaming has the following limits and thresholds:

- Windows Media Streaming recommended concurrent remote server sessions 300

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

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

Flash Media Streaming

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

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

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

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

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

Important Notes

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Open Caveats, Resolved Caveats and Enhancements Added in Release 3.2.

This section describes the most important changes made in the Cisco Internet Streamer CDS 3.2.

- Open Caveats in Release 3.2., page 10
- Resolved Caveats in Release 3.2., page 10
- Enhancement Features Added in Release 3.2, page 10
- Accessing Bug Tool kit, page 11

Open Caveats in Release 3.2.

Table 2 lists the issues resolved in the Cisco Internet Streamer CDS 3.2 release.

Click on the bug ID to view the bug details. This information is displayed in the Bug Toolkit.

Table 2 Open Caveats in Cisco Internet Streamer CDS 3.2 Release

Bug ID	Description
CSCue80613	Working server is not updated in CLI after SwitchTo operation
CSCue83134	wmt core seen on SE while running codenomicon
CSCue86012	Web-Engine core while running ABR traffic

Resolved Caveats in Release 3.2.

Table 3 lists the issues resolved in the Cisco Internet Streamer CDS 3.2 release.

Click on the bug ID to view the bug details. This information is displayed in the Bug Toolkit.

Table 3 Resolved Caveats in Cisco Internet Streamer CDS 3.2 Release

Bug ID	Description
CSCue34975	Device hangs at 100% CPU utilization
CSCue39358	Power supply unit fails post upgrade to 3.1.2 b11
CSCud86431	Authsvr does not support https Protocol
CSCue04774	SSL Version 2 (v2) Protocol Detection (SSL 2.0 needs to be disabled)
CSCud29094	CLI to disable/enable tcp_tw_recycle or tcp_tw_reuse when needed
CSCud31565	The SR takes \".sdp\" in the URL as a keyword and handles it incorrectly
CSCud57383	sysmon robustness against sdt hangs (system runs out of rootfs inodes)

Enhancement Features Added in Release 3.2

Table 4 lists the enhancement features added in the Cisco Internet Streamer CDS 8.1.2 release.

Click on the bug ID to view the bug details. This information is displayed in the Bug Toolkit.

Table 4 Enhancement Features added in Cisco Internet Streamer CDS 3.2 Release

Bug ID	Description
CSCue34975	Device hangs at 100% CPU utilization
CSCue07235	No auto changing of the “Force Quota Usage Reporting” check box

Accessing Bug Tool kit

This section explains how to use the Bug Toolkit to search for a specific bug or to search for all bugs in a release.

Step 1 Go to http://tools.cisco.com/Support/BugToolKit.

Step 2 At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Toolkit page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, click the **Search Bugs** tab, enter the bug ID in the Search for Bug ID field, and click **Go**.

Step 4 To search for bugs in the current release, click the **Search Bugs** tab and specify the following criteria:

- Select Product Category—**Video**.
- Select Products—**Videoscape Distribution Suite for Internet Streaming**.
- Software Version—**[3.2].**
- Search for Keyword(s)—Separate search phrases with boolean expressions (AND, NOT, OR) to search within the bug title and details.
- Advanced Options—You can either perform a search using the default search criteria or define custom criteria for an advanced search. To customize the advanced search, click **Use custom settings for severity, status, and others** and specify the following information:
  - Severity—Choose the severity level.
  - Status—Choose **Terminated**, **Open**, or **Fixed**.

    Choose **Terminated** to view terminated bugs. To filter terminated bugs, uncheck the Terminated check box and select the appropriate suboption (Closed, Junked, or Unreproducible) that appears below the Terminated check box. Select multiple options as required.

    Choose **Open** to view all open bugs. To filter the open bugs, uncheck the Open check box and select the appropriate suboptions that appear below the Open check box. For example, if you want to view only new bugs in Prime Optical 9.5, choose only **New**.

    Choose **Fixed** to view fixed bugs. To filter fixed bugs, uncheck the Fixed check box and select the appropriate suboption (Resolved or Verified) that appears below the Fixed check box.
  - Advanced—Check the **Show only bugs containing bug details** check box to view only those bugs that contain detailed information, such as symptoms and workarounds.
  - Modified Date—Choose this option to filter bugs based on the date when the bugs were last modified.
  - Results Displayed Per Page—Specify the number of bugs to display per page.

Step 5 Click **Search**. The Bug Toolkit displays the list of bugs based on the specified search criteria.

Step 6 To export the results to a spreadsheet:

a. In the Search Bugs tab, click **Export All to Spreadsheet**.

b. Specify the filename and location at which to save the spreadsheet.

c. Click **Save**. All bugs retrieved by the search are exported.

If you cannot export the spreadsheet, log into the Technical Support website at http://www.cisco.com/cisco/web/support/index.html or contact the Cisco Technical Assistance Center (TAC).

Upgrading to Release 3.2

Release 3.2 supports upgrades from Release 2.5.9, Release 2.5.11, Release 2.6.x, Release 3.0.x, and Release 3.1.x.

Note When upgrading from Release 2.x to Release 3.x, and the streaming interface IP address is set as the management IP address on the SE, the rpc_httpd process fails to start because of a port 443 binding issue. Before upgrading to Release 3.x., either check the **Use SE's primary IP address for management communication** check box on the Device Activation page for the SE, or use a separate IP addresses for the streaming traffic and the management traffic (primary interface).

Note If your CDS software is older than Release 2.6.1 and you have CDE205 and CDE220 platforms in your system, you must check that the partition size (specifically, disk 00/02), on each CDE205 and CDE220 in your system is larger than 0.5 GB. To check the partition size, enter the **show disks detail** command. If the disk00/02 partition is not larger than 0.5 GB, you must upgrade the CDE to Release 2.6.1 before upgrading to Release 3.x.

If your CDS is running an older release than Release 2.5.9, you need to upgrade to Release 2.5.9 or 2.5.11 before upgrading to Release 3.2.

When upgrading from Release 2.5.9 or 2.5.11, all content is erased. For Service Engines, this means that prefetched metadata and content need to be redistributed from upstream SEs after the upgrade, and that cached content is not preserved. Additionally, Flash Media Streaming service rules must be converted from device-based service rules to the Service Rule XML file. For more information on upgrading from Release 2.5.9 and 2.5.11, see the *Cisco Internet Streamer CDS 2.6 Software Upgrade Guide* (http://www.cisco.com/en/US/docs/video/cds/cda/is/2_6/upgrade_guide/upgrade.html).

We strongly recommend that you upgrade your CDS network devices in the following order:

1. Multicast sender Service Engines
2. Multicast receiver Service Engines
3. Edge Service Engines
4. Middle-tier Service Engines
5. Content Acquirers
6. Service Routers
7. Standby CDSMs (Upgrade before primary when using the GUI only.)
8. Primary CDSM

Note When using the CDSM GUI to upgrade from Release 2.5.9, 2.5.11, or 2.6.1 to Release 3.2, after you upgrade the standby CDSM, if you switch roles of the standby CDSM and primary CDSM to maintain an active CDSM, the old primary CDSM is now the standby CDSM, and the old standby CDSM is now the primary CDSM. At this point, you must use the CLI to upgrade the new standby CDSM. The primary CDSM GUI cannot upgrade the standby CDSM.

Alternatively, if you do not switch roles of the standby CDSM and primary CDSM, you can use the CDSM GUI to upgrade the primary CDSM. The primary CDSM loses connectivity with the CDS devices for a short time during the upgrade, but this is not service affecting.

When using the CDSM GUI to upgrade from Release 2.6.3 and later releases to Release 3.11, after you upgrade the standby CDSM, if you switch roles of the standby CDSM and primary CDSM to maintain an active CDSM at all times, the new primary CDSM GUI can be used to upgrade the new standby CDSM.

For more information on the upgrade procedure, see the *Cisco Internet Streamer CDS 3.2 Software Configuration Guide.*

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

Downgrading from Release 3.2

Note When downgrading from Release 3.2 to Release 2.5.x, make sure the Coverage Zone file is less than 7500 lines. If the Coverage Zone file is 7500 lines or greater, reduce the number of lines before downgrading to Release 2.5.x. This is not an issue when downgrading to Release 2.6.x.

For software downgrades from Release 3.2 on systems with primary and standby CDSMs, you need to do the following:

Step 1 If you are using the CDSM GUI, downgrade the standby CDSM first, followed by the primary CDSM.

If you are using the CLI, downgrade the primary CDSM first, followed by the standby CDSM.

Step 2 After downgrading the primary and standby CDSMs, using the CLI, log in to each CDSM and run the following commands:

- To downgrade from 3.2 to 2.5.9 or 2.5.11

```
cms database downgrade script downgrade/Downgrade3_1_2_b20_to_3_1_2_b19
cms database downgrade script downgrade/Downgrade3_1_1_to_3_1
cms database downgrade script downgrade/Downgrade3_1_to_3_0
cms database downgrade script downgrade/Downgrade3_0_to_2_6
cms database downgrade
cms enable
```

Then, consult the "Downgrading the Internet Streamer CDS Software" chapter in the Cisco Internet Streamer CDS 2.6 Software Upgrade Guide for downgrading from Release 2.6.x to Release 2.5.9 or 2.5.11.

- To downgrade from 3.2 to 2.6.x

```
cms database downgrade script downgrade/Downgrade3_1_2_b20_to_3_1_2_b19
cms database downgrade script downgrade/Downgrade3_1_1_to_3_1
cms database downgrade script downgrade/Downgrade3_1_to_3_0
cms database downgrade script downgrade/Downgrade3_0_to_2_6
cms database downgrade
cms enable
```

After downgrade from 3.2.0 to 2.6.1, If SE does not come up in operational status in SR, restart the Service router and the operational state will be updated.

- To downgrade from 3.2 to 3.1.0

```
cms database downgrade script downgrade/Downgrade3_1_2_b20_to_3_1_2_b19
cms database downgrade script downgrade/Downgrade3_1_1_to_3_1
cms database downgrade
cms enable
```

- To downgrade from 3.2 to 3.1.1 or 3.1.2.bN(N<20)

```
cms database downgrade script downgrade/Downgrade3_1_2_b20_to_3_1_2_b19
cms database downgrade
cms enable
```

- To downgrade from 3.2 to 3.1.2.bN(N>=20)

```
cms database downgrade
cms enable
```

Step 3 Downgrade the software on the Service Routers, followed by the Service Engines.

Documentation Updates

The following document has been added for this release:

- *Release Notes for Cisco VDS Internet Streamer 3.2*

Related Documentation

Refer to the following documents for additional information about Cisco Internet Streamer CDS 3.2:

- *Cisco Internet Streamer CDS 3.2 Software Configuration Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/3_2/configuration_guide/icds3.2confg.html
- *Cisco Internet Streamer CDS 3.0–3.1 Quick Start Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/3_0/quick_guide/ISCDSQuickStart.html
- *Cisco Internet Streamer CDS 3.2 API Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/3_2/developer_guide/iscds32APIGuide.html
- *Cisco Internet Streamer CDS 3.2Command Reference Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/3_2/command_reference/Command_Ref.html
- *Cisco Internet Streamer CDS 3.2 Alarms and Error Messages Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/3_2/message_guide/message_guide.html
- *Cisco Internet Streamer CDS 3.0–-3.2 Software Installation Guide for non-CDEs*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/3_2/install_guide/Non_CDE_IS_3_2_Software_Install.html
- *Cisco Content Delivery System 3.x Documentation Roadmap*
  http://www.cisco.com/en/US/docs/video/cds/overview/CDS_Roadmap3.x.html
- *Open Source Used in Cisco Internet Streamer CDS 3.1*
  http://www.cisco.com/en/US/docs/video/videoscape/Media_Processor_Mgmt_Console/OL-27694-01_CDS-IS_3.1_Open_Source.pdf

- *Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide*

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

  http://www.cisco.com/en/US/docs/video/cds/cde/regulatory/compliance/CDE_RCSI.html
- *Cisco UCS C200 Installation and Service Guide*

  http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C200M1/install/c200M1.html
- *Cisco UCS C210 Installation and Service Guide*

  http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C210M1/install/C210M1.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

The Cisco UCS C-Series Rack Servers documentation is available on Cisco.com at:

http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.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.