Release Notes for Cisco Internet Streamer CDS 3.1.1

These release notes cover Cisco Internet Streamer CDS Release 3.1.1-b2.

Revised: October 2012, OL-27551-01

Contents

The following information is included in these release notes:

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

New Features

Release 3.1.1 of the Cisco Internet Streamer CDS introduces the Multicast Cloud feature.

Content Replication Using a Multicast Cloud

The Multicast Cloud feature is a group of multicast-enabled SEs configured to communicate multicast session information with one another. The Multicast Cloud feature is described in the following sections:

Introduction to Multicast Cloud

Content is forwarded (or replicated) either by unicast pull (transmission initiated by a client request for the content) or, if it is enabled, by multicast push (transmission initiated in accordance with a preconfigured program or schedule). Unicast content forwarding involves communication between a single sender and single receiver, whereas multicast replication involves communication between a single sender and a selected group of receivers.

Multicasting allows efficient distribution of content to multiple SEs and is useful when many end users are interested in the same content. CDS software supports Pragmatic General Multicast (PGM)-based multicast replication, using either satellite or multicast-enabled terrestrial infrastructures. (PGM is a reliable multicast protocol that enables PGM receivers to report loss of data and request retransmission by the PGM sender.)

In CDS software, the administrator configures the CDS network for multicasting by configuring a multicast cloud in the CDSM GUI. The multicast cloud consists of one sender SE, an optional backup sender for multicast-to-multicast failover, and at least one receiver SE. All the SEs in one cloud share a unique advertising address, allowing them to communicate multicast session information. SEs that are assigned to the multicast cloud must be enabled for multicasting. The multicast cloud is then associated with one or more multicast-enabled delivery services. The multicast-enabled SEs assigned to the multicast cloud are also assigned to the multicast-enabled delivery service.

The SEs that are receivers get their content from the multicast addresses associated with the cloud. The multicast cloud is an overlay topology on the location-based distribution tree structure. The clouds can be chained by making a receiver of one cloud the sender of another cloud. For best performance, the SEs in a multicast cloud should all be able to receive data at about the same rate. The slowest receiver determines the rate at which the sender pushes the files.

When configuring the multicast cloud, the administrator specifies a range of addresses by entering a start IP address and an end IP address. Once a multicast cloud is configured, the multicast address range is used to provide each delivery service associated with it a unique data delivery service multicast address. When a multicast cloud is assigned to a delivery service, an unused IP address is automatically selected from this range to ensure that the address is used by only one delivery service and by only one multicast cloud. Because different multicast clouds may be associated with the same delivery service, the multicast address used for each delivery service needs to be different in each multicast cloud.

Distributing Content Through Replication

After content is acquired from the Origin server by the Content Acquirer of a delivery service, it can be replicated through the delivery service either by unicast or multicast transmission.

The delivery service configuration offers content replication options:

- Multicast and unicast (multicast with failover to unicast)
- Multicast-only
- Unicast-only

Unicast Replication

The basic delivery service distribution architecture provides for unicast content replication using a hop-by-hop, store-and-forward methodology with the forwarder SEs systematically selected on the basis of the manually configured location hierarchy.

To distribute content through unicast, the CDS network automatically creates a unidirectional distribution tree for each delivery service. The root node of the tree is the Content Acquirer of the delivery service, and each SE subscribed to the delivery service is a node on the tree.

For each node, its parent node is also called its forwarder SE. The algorithm for automatically designating the forwarder SE is called the channel routing algorithm.

Three general rules in the current channel routing algorithm are as follows:

1. In each location for each delivery service, only one SE fetches content from another location for that delivery service. We call this SE the location leader of the delivery service. All other SEs in this location use the location leader as the forwarder for this delivery service. There can be only one location leader per delivery service per location. Note that within one location, different delivery services may have different location leaders.

   The location leader is computed automatically by the channel routing algorithm.

   Use the **show distribution delivery-service** command to see which SE is the current forwarder for a delivery service. The reason/status field in the command output shows why an SE is unable to find a forwarder. Use the **show distribution forwarder-list** command to see the forwarder selection order of an SE for a delivery service.

2. The location leader finds a subscribed SE from the closest location on the path toward the Content Acquirer as its forwarder. If all the potential forwarders in a parent location are down (or unreachable) the location leader skips to the next location level in the hierarchy (towards the Content Acquirer location) to find a forwarder.

3. If the location leader SE fails for some time, another SE in the location takes over as the location leader. If the Content Acquirer fails, another SE in the location takes over as the temporary Content Acquirer.

Multicast Replication

In multicast content distribution, the sender SE in a multicast cloud proactively pushes content into the cloud according to a preconfigured schedule.

The receiver SEs listen on the advertisement IP address for information on content to be replicated from the sender, and then the receiver SEs decide whether or not to accept an advertisement and receive the corresponding content.

Content metadata must be distributed to a receiver first before the content itself can be replicated. Content metadata helps to define what content to retrieve, how content will be retrieved, how recently content has been updated, how content is to be pre-positioned (for example, expiration time), and so forth. Metadata is always distributed using unicast. Content, however, can be replicated using either multicast or unicast. A multicast receiver rejects the multicast sender's advertisement of a file if the proper content metadata has not yet arrived.

Multicast and Unicast

When a delivery service is configured for multicast and unicast, the receiver SE uses unicast to download content only after all carousel passes have been exhausted and after the preconfigured multicast transmission fails. In a multicast cloud configuration that uses a backup sender, when the delivery service is enabled for multicast and unicast, the failover to unicast occurs when the current active multicast sender has exhausted all the carousel passes for the file.

If the administrator wants the SEs to fall back to unicast (for example, with a multi-tier unicast deployment using a terrestrial multicast medium), the multicast cloud should be configured for a low number of carousel passes (such as 1, 2, or 3).

Multicast Only

If only multicast replication is desired (for example, with a hub and spoke or star topology deployment using a satellite multicast medium), the delivery services should be configured as multicast-only, with a high number of carousel passes configured in the multicast cloud (such as 10 or more).

When a delivery service is configured to be multicast only (that is, when the delivery services are associated with a multicast cloud and the subscribing receiver SE has multicast service enabled), content replication takes place only through multicasting. No retransmission takes place in unicast at all. This prevents background unicast polls from happening and taking up bandwidth. However, if an SE in the multicast-only delivery service is not enabled for multicasting, it can continue to request all the content from a multicast-only delivery service through unicasting.

Configuring Multicast Distribution

To configure the CDS for multicast replication of content, the following tasks need to be performed:

1. Enabling multicasting on SEs
2. Creating a multicast cloud
3. Assigning SEs to a multicast cloud
4. Assigning multicast clouds to delivery services
5. Assigning SE members of the multicast cloud to the delivery service (**Services > Service Definition > Delivery Services > Assign Service Engines**)

For more information, see the "Content Replication Using a Multicast Cloud" section in the "Network Design" chapter of the *Cisco Internet Streamer CDS 3.1 Software Configuration Guide*.

Alarms

The following sender and receiver alarms are generated during different failures:

- Multicast Data Sender
  - svcdevfailover—Minor. Backup multicast sender takes over. (The alarm is cleared when a backup sender falls back).

  - svcnomcastenable—Major. Multicast is disabled although the SE is a multicast sender or receiver, or it is subscribed to multicast delivery services.
- Multicast Data Receiver
  - svcnomcastconnectivity—Minor. Multicast receiver has a connectivity problem on the multicast advertisement address and has failed to receive heartbeats from the multicast sender for a while.
  - svcnacksuppressed—Minor. Multicast Receiver has stopped NACKs because of heavy loss.

Commands Related to Multicasting

Table 0-1 lists and describes CLI commands that are related to multicasting. For complete descriptions of these commands, including usage guidelines and examples, refer to the *Cisco Internet Streamer CDS 3.1 Command Reference*.

Table 0-1 Multicast-Related Commands

Command	Syntax	Description
distribution multicast	**distribution multicast send-nack-now**	Generates a NACK for missing objects and sends them to the multicast receiver.
	distribution multicast resend	Resends an individual object (**object** option) or specifies that the first round of carousel passes be triggered by a NACK only (**on-demand-only** option).
	distribution multicast stop	Sets the number of carousel passes completed to the maximum value so that no more multicast carousels can be triggered.
multicast	**multicast sender-delay** *delay*	Changes the default sender delay interval of 16 minutes. The time delay between sending metadata and content.
	multicast connectivity-test	Verifies multicast connectivity between a sender and one or more receivers.
	multicast fixed-carousel enable	Enables fixed carousel sending, regardless of receiver feedback; NACK triggered carousel passes are disabled. Only applies to the primary sender and is disabled if the SE becomes a backup sender.
	multicast priority-weight	Sets the percentage of multicast bandwidth for priority-based scheduling. The remaining bandwidth is given to time-based scheduling of queued jobs. The default is 50%.
	max-concurrent-jobs *number*	Sets the maximum number of objects that can be concurrently scheduled. When networks are reliable or size of files are small, we recommend setting this command to 50; otherwise (unreliable network or small files), the recommended setting is 5. The default is 5.
show multicast	**show multicast**	Displays the current status of the multicast client.

Table 0-1 Multicast-Related Commands (continued)

Command	Syntax	Description
show distribution	**show distribution mcast-data-receiver** **show distribution mcast-data-sender**	Shows information about the multicast receiver or the sender. Displays information about the multicast cloud.
show statistics distribution	**show statistics distribution mcast-data-receiver** **show statistics distribution mcast-data-sender**	Displays the content distribution statistics of the multicast data receiver or sender.
clear statistics distribution	**clear statistics distribution mcast-data-receiver** **clear statistics distribution mcast-data-sender**	Clears multicast statistics.

APIs for Multicast Cloud

The following APIs have been modified or added to support the configuration and monitoring of the Multicast Cloud feature:

- Multicast Cloud—MCastApiServlet API has been added with create, modify, and delete actions, as well as assign and unassign receiver SEs, and assign and unassign the multicast cloud to a delivery service
- Delivery Service—ChannelApiServlet API createDeliveryService and modifyDeliveryService actions have been modified with the ability to enable multicast for the delivery service
- Service Engine— CeApiServlet API seMulticast action has been added to enable an SE as a multicast sender and multicast receiver.

For more information, see the *Cisco Internet Streamer CDS 3.1 API Guide*.

Enhancements

The following enhancements have been added in Release 3.1.1:

- Assigned IP Addresses for Edge SEs of Delivery Service
- Session-Based ABR Performance Enhancement
- CDSM Reports Alarms to Prime Central

Assigned IP Addresses for Edge SEs of Delivery Service

You can assign an IP address to an SE in a delivery service (**Services > Service Definition > Delivery Service > Assign IP Address**). If the requesting IP address is not matched with assigned IP address for the edge SEs of the delivery service, the request will be denied. (CSCub59480)

Note The Assign IP Address option is not supported for Flash Media Streaming; even if the IP address does not match the assigned IP addresses for the edge SEs of a Flash Media Streaming delivery service, the request is still served.

Session-Based ABR Performance Enhancement

Enhancements to HTTP ABR performance have been made for ABR Session Tracking. (CSCub52931)

CDSM Reports Alarms to Prime Central

Cisco PRIME for service providers is an experience delivery management architecture that enables the integrated design, fulfillment and assurance of customer experiences such as video, mobility, and managed cloud services delivered on converged IP networks.

As part of Cisco PRIME, the CDSM forwards alarms as SNMP traps to Prime Central. The CDSM supports the following functionality to provide communication to Prime Central:

- CDSM configuration settings to allow communication with Prime Central
- Registration of the CDSM on Prime Central
- Sending SNMP traps to Prime Central

Registering and De-Registering with Prime Central

After the Prime Central configuration is made either through the CDSM GUI or the API, the CDSM registers with Prime Central.

The registration process takes about 10 to 20 seconds. After registration is complete, the CDSM updates the status (Registered or Registration Failed) of Prime Central.

If the configuration settings for communicating with Prime Central are modified, if the modified fields affect registration, the CDSM de-registers and re-registers with the new Prime Central settings.

If the configuration settings for communicating with Prime Central are deleted, the CDSM de-registers from the Prime Central.

Configuring the CDSM to Communicate with Prime Central

For information on configuring the CDSM to communicate with Prime Central, see the “Configuring the CDSM to Communicate with an External System” section in the “Configuring System Settings” chapter of the *Cisco Internet Streamer CDS 3.1 Software Configuration Guide*.

For information on using the External System API to configure the CDSM to communicate with Prime Central, see the “Provisioning APIs” chapter of the *Cisco Internet Streamer CDS 3.1 API Guide*.

The getExternalSystems action has been added to the ListApiServlet and can be used to get the external system configuration IDs. The syntax is the following:

https://<cdsmIpAddress>:8443/servlet/com.cisco.unicorn.ui.ListApiServlet?action=getExternalSystems&param=all | <external_system_ID>,<external_system_ID>...

The information of the external systems is returned.

SNMP Operations

For SNMP operations, the SNMP4J open source library is used. SNMP traps are sent to the defined Prime Central. The CISCO-EPM-NOTIFICATION-MIB.my, published by Cisco, is used for sending SNMP traps to the Prime Central.

To access the CISCO-EPM-NOTIFICATION-MIB.my, go to: ftp://ftp.cisco.com/pub/mibs/v2/

Note If your browser is located behind a firewall or you are connecting to the Internet with a DSL modem and you are unable to access this file folder, you must change your web browser compatibility settings. In the Internet Explorer (IE) web browser, choose **Tools > Internet Options > Advanced**, and check the Use Passive FTP check box.

System Requirements

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

Table 2 lists the different device modes for the Cisco Internet Streamer CDS software, and which CDEs support them.

Table 2 Supported CDEs

Device Mode	CDE205	CDE220-2G2	CDE220-2S3i	CDE250 (all models)	UCS C200	UCS C210
CDSM	Yes	No	No	No	Yes	No
SR	Yes	Yes	No	No	Yes	No
SE	Yes	Yes	Yes	Yes	No	Yes
SR—Proximity Engine standalone	Yes	Yes	No	No	No	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 and UCS C210) and the Cisco Internet Streamer Release 3.1 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

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

This release contains the following open caveats:

Content Manager

- CSCua08680

  Symptom:

  When the **clear-cache-all** command is entered, sometimes the content is not completely deleted. This is because the Content Manager is not aware of all the content cached by the Web Engine.

  Conditions:

  When the Web Engine creates more than three million objects and the slow scan (slowscan) process has just finished running, some content is not known by the Content Manager.

Workaround:

The next round of slowscan (every 12 hours) picks up the content that was unknown by the Content Manager. After that, the **clear-cache-all** command works.

CLI

- CSCuc00495

  Symptom:

  Cannot access server via console. Keep getting “Username” prompt and “System Initializing. Please wait.....”

  Conditions:

  Upgrade "failure" from Release 2.6.3 to Release 3.1.

  Workaround:

  Physically access server and reinstall from CD-ROM.

Multicast Distribution

- CSCuc14038

  Symptom:

  Sometimes the files are transferred by way of unicast when the delivery service is of the type Multicast Unicast.

  Conditions:

  When the backup Sender is in the same location as that of primary Sender. When an SE that is not assigned to the multicast cloud resides in any of the location as the Content Acquirer, primary Sender, or a middle-tier Receiver.

  Workaround:

  Assign the backup Sender to a new location. Assign the SE that is not part of the multicast cloud to a location that is not in the direct upstream path of the edge location. Content is distributed properly and no issues are observed.

Resolved Caveats

The following caveats have been resolved since Cisco Internet Streamer CDS Release 3.1.1. Not all the resolved issues are mentioned here. The following list highlights the resolved caveats associated with customer deployment scenarios.

Web Engine

- CSCuc24174

  Symptom:

  The **clear content last-folder-url** command cannot clear the specified contents.

Conditions:

When the **clear content last-folder-url** command is entered in the in exec shell.

- CSCub00586

  Symptom

  Session-based Encryption with a single key per session (default configuration) does not work for HLS use case. HSS use case has no impact because the manifest for HSS is out-of-band.

  Conditions:

  When HLS encryption is enabled with a single key for a session (user).

CDSM

- CSCub73729

  Symptom:

  When using the API to create a live program, the <attribute> element value contains an unreachable URL, which means the CDSM cannot get this SDP file defined within the URL. Following is an example of a URL that is unreachable, which causes the SR to go offline and the CDSM to hang for awhile:

  ```
  <attribute value='unicastPushSDP:http://172.17.39.107/broadcast.sdp'/>
  ```

  Conditions:

  This issue happens when the XML file defines an unreachable <attribute> URL.

Service Monitor

- CSCub77092

  Symptom:

  Service Monitor process coredumps because of memory overflow.

  Conditions:

  When downgrading the software image from Release 3.1 to Release 2.5.9.

Acquisition and Distribution

- CSCub52883

  Symptom:

  The correct play length is not displayed for .wmv files.

  Conditions:

  When .wmv files are prefetched, the play length is displayed as 00:00:00.

Multicast Distribution

- CSCub60908

  Symptom:

  In Release 3.1, there is a Unicast Multicast Option field in Delivery Service Definition page. There are three options for it: Unicast Only, Multicast Only, and Multicast Unicast.

  In Release 3.0, there is no such field. The distribution type is always unicast.

  If Multicast Only is configured in Release 3.1 and the system is downgraded to Release 3.0, the distribution type is not automatically changed back to unicast.

  The svcnomcastenable alarm is raised on all SEs. This alarm is not valid in Release 3.0 and should not be raised. Deleting the delivery service clears this alarm.

  Conditions:

  This issue occurs when the Unicast Multicast Option field is set to Multicast Unicast or Multicast Only for a delivery service in Release3.1, then the system is downgraded to Release 3.0.

- CSCub65253

  Symptom:

  In Release 3.1, there is a Unicast Multicast Option field in Delivery Service Definition page. There are three options for it: Unicast Only, Multicast Only, and Multicast Unicast.

  In Release 3.0, there is no such field. The distribution type is always unicast.

  If Multicast Only is configured in Release 3.1 and the system is downgraded to Release 3.0, the distribution type is not automatically changed back to unicast.

  If the following command is entered on the SE:

  `show distribution delivery-service delivery-service-name` *`<delivery service name>`*

  The output shows that the distribution type is Multicast Unicast or Multicast Only.

  This is only a display issue. The distribution process still works in the unicast distribution way.

  Conditions:

  This issue occurs when the Unicast Multicast Option field is set to Multicast Unicast or Multicast Only for a delivery service in Release3.1, then the system is downgraded to Release 3.0 and the **`show distribution`** command is entered.

Network

- CSCub77171

  Symptom:

  The device goes into kernel debugger mode (kdb) during a stress test.

  Conditions:

  The device tries to assign the auto-configuration IPv6 ipaddress to the interface bond0, but the router complains that the IPv6 address is a duplicate.

Upgrading to Release 3.1.1

Release 3.1.1 supports upgrades from Release 2.5.9, Release 2.5.11, Release 2.6.x, Release 3.0.x, and Release 3.1.0.

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 3.1.1.

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 3.1.1, 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 3.1 Software Configuration Guide.*

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

Downgrading from Release 3.1.1

For software downgrades from Release 3.1.1 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 3.1.1 to 2.5.9 or 2.5.11

```
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 3.1.1 to 2.6.x

```
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
```

- To downgrade from 3.1.1 to 3.0.x

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

- To downgrade from 3.1.1 to 3.1.0

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

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

Note If you are downgrading the CDSM from Release 3.0.0 to Release 2.6.x, after running the cms database downgrade command, run the downgrade/Downgrade3_0_to_2_6 command.

Documentation Updates

The following document has been added for this release:

- *Release Notes for Cisco Internet Streamer CDS 3.1.1*
- *Cisco Internet Streamer CDS 3.1 Software Configuration Guide*
- *Cisco Internet Streamer CDS 3.1 Command Reference Guide*
- *Cisco Internet Streamer CDS 3.1 Alarms and Error Message Guide*
- *Cisco Internet Streamer CDS 3.1 API Guide*

Related Documentation

Refer to the following documents for additional information about Cisco Internet Streamer CDS 3.1:

- *Cisco Internet Streamer CDS 3.1 Software Configuration Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/3_1/configuration_guide/icds31confg.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 3.1 API Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/3_1/developer_guide/iscds31APIGuide.html
- *Cisco Internet Streamer CDS 3.1Command Reference Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/3_1/command_reference/Command_Ref.html
- *Cisco Internet Streamer CDS 3.1 Alarms and Error Messages Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/3_1/message_guide/message_guide.html
- *Cisco Internet Streamer CDS 3.0–-3.1 Software Installation Guide for non-CDEs*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/3_0/install_guide/Non_CDE_IS_3_0_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/cds/cda/is/3_0/third_party/open_source/OL-25149-01.pdf
- *Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide*
  http://www.cisco.com/en/US/docs/video/cds/cde/cde205_220_420/installation/guide/cde205_220_420_hig.html
- *Regulatory Compliance and Safety Information for Cisco Content Delivery Engines*
  http://www.cisco.com/en/US/docs/video/cds/cde/regulatory/compliance/CDE_RCSI.html
- *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.