Release Notes for Cisco TV CDS 2.0

These release notes cover Cisco TV CDS Release 2.0.0.

Revised: March 4, 2009 OL-17355-01

Contents

The following information is in the release notes:

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

New Features

Release 2.0 of the Cisco TV CDS introduces the following new features:

- Media Scheduler
- Support of the next generation appliances (CDE110, CDE220, and CDE420)

Media Scheduler

The Media Scheduler features aids content ingest workflow and scheduling tasks for both asset-based and real-time content. The Media Scheduler allows you to schedule real-time ingests by specifying the data feed import type and the transformer type (used to process the ADI metadata). You can upload an EPG file to populate the Media Scheduler or manually enter each timeslot. Input channels are mapped to a multicast group IP address and port, where scheduled content are ingested.

Next Generation Appliances

The Cisco TV CDS Release 2.0 supports the next generation appliances, which consist of the following:

- CDE110
- CDE220
- CDE420

The CDE110 is used to run the Content Delivery System Manager (CDSM) Content Delivery Application (CDA). The CDE220 can be used to run the Streamer, Vault, or Integrated Streamer Vault (ISV) CDAs. The CDE420 is used to run the Vault CDA.

Enhancements

Table 1 describes the enhancements to Cisco TV CDS 2.0.

Table 1 Enhancements in TV CDS 2.0

Enhancements	Descriptions	Category	Supported CDEs[1]
Single software image	Combines support for the ISA and RTSP environments into a single software release. The environment is selected during the software installation.	Serviceability	Generation One and Generation Two CDEs
Software installation	Improves procedures for software installation and deployment of new CDEs, as well as improved software upgrade for pre-Release 2.0 hardware (Generation One CDEs).	Serviceability	Generation One and Generation Two CDEs
Preinstallation of software	Simplifies initial installation of next generation appliances by shipping them with the operating system and CDS software preinstalled.	Serviceability	Generation Two CDEs
Cisco Unique Device Identifier (UDI)	Supports electronic retrieval of product type, serial number, and hardware information on the next generation appliances.	Serviceability	Generation Two CDEs

Table 1 Enhancements in TV CDS 2.0 (continued)

Enhancements	Descriptions	Category	Supported CDEs[1]
Stream resiliency in RTSP environment	Supports stream failover capability in the RTSP environment.	Resiliency	Generation One and Generation Two CDEs
Network failures	Enhances handling of network partitioning failures.	Resiliency	Generation One and Generation Two CDEs
Database replication	Improves database replication across the Content Delivery System by enhancing the database architecture.	Resiliency	Generation One and Generation Two CDEs
Content mirroring failures	Introduces detection of mirroring failures and corrective action to prevent loss of content.	Resiliency	Generation One and Generation Two CDEs
New VOD environments	Extends integration with leading backoffice vendors, by adding support for the following: • NGOD architecture, with SeaChange Axiom backoffice • EventIS • Minerva • Quative • Myrio • Onewave • Eyeka	Extensibility / Integrations	Generation One and Generation Two CDEs
User Generated Content (UGC) for Eyeka backoffice	Adds the ability to integrate CDS with Eyeka backoffice to ingest User Generated Content (UGC)	Extensibility / Integrations	Generation One and Generation Two CDEs
Time-shifted TV services for Coship backoffice	Supports integration with Coship backoffice system to enable advanced video services such as TV on demand, and Time-shifted TV services such as Start Over, Look Back and Catch up to live.	Extensibility / Integrations	Generation One and Generation Two CDEs
SNMP monitoring capabilities	• Enhances MIB support on CDS Streamers to allow real-time monitoring of total active streams, unique streams, streams served from disk, and streams served through cache-fill • Additional SNMP Traps to notify application-level events and failures (MSA events)	Manageability	Generation One and Generation Two CDEs

Table 1 Enhancements in TV CDS 2.0 (continued)

Enhancements	Descriptions	Category	Supported CDEs[1]
CDSM	• Offers configurable system monitoring thresholds (port loss, disk loss, disk capacity and file system usage) • New report and Server Level monitoring that shows cache-fill bandwidth by server • New monitoring report that shows content titles and number of copies across all Vault servers • Usability enhancements	Manageability	Generation One and Generation Two CDEs
MediaPublisher (Ingest Manager [AIM])	Supports simultaneously ingesting content and publishing metadata to multiple backoffice instances	Extensibility	Generation Two CDEs

[1] Generation One CDEs are the CDE100, CDE200, CDE300, and CDE400 that use the Lindenhurst chipset. Generation Two CDEs are the next generation appliances, which are the CDE110, CDE220, and CDE420.

Supported Environments

Release 2.0 of the Cisco TV CDS supports the following environments and associated backoffice integrations:

- ISA environment
  - Tandberg OpenStream backoffice
  - Onewave backoffice
- RTSP environment
  - SeaChange Axiom backoffice (NGOD architecture)
  - EventIS
  - Minerva
  - Quative
  - Myrio
  - Coship
  - Eyeka

System Requirements

The Cisco TV CDS Release 2.0 runs on the CDE110, CDE220, and CDE420. See the *Cisco Content Delivery Engine110 Hardware Installation Guide*, and the *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide*.

The Cisco TV CDS Release 2.0 also runs on the CDE100, CDE200, CDE300, and CDE400 hardware models that use the Lindenhurst chipset. See the *Cisco Content Delivery Engine CDE100/200/300/400 Hardware Installation Guide* for set up and installation procedures.

Release 2.0 does not support the CDEs with the ServerWorks chipset. All CDEs with the ServerWorks chipset need to be replaced with the CDEs with the Lindenhurst chipset or the Next Generation Appliances (CDE110, CDE220, andCDE420) before upgrading to Release 2.0.

See the "Related Documentation" section on page 21 for links to the documentation online.

Limitations and Restrictions

There are no limitations nor restrictions in Release 2.0.

Open Caveats

This release contains the following open caveats:

CDSM

- CSCsu67090

  Symptom:

  When the DNS settings are configured and then deleted in the CDSM, the settings are not removed from the hosts line in the /etc/resolv.conf file.

  Condition:

  Use the CDSM, configure the DNS settings and delete them through one of the following pages:

  - **Configure > System Level > DNS**
  - **Configure > Array Level > DNS Binding**
  - **Configure > Server Level > DNS Binding**

  Workaround:

  The statsd process regenerates these configurations when it is restarted. Log into the server as *root* and use the **/home/stats/statsd** command.

- CSCsv28319

  Symptom:

  In the CDSM, when host entries are created and then deleted, they are not removed from the /etc/hosts file.

  Condition:

  Use the CDSM, choose **Configure > System Level > Host Service** to configure the hosts and delete them.

  Workaround:

  Edit the /etc/hosts file manually.

- CSCsv29715

  Symptom:

  The Services Monitor page shows the Cisco SNMP Server when it was unchecked in the System Threshold page.

Condition:

In the CDSM, choose **Maintain > Servers > System Thresholds**, uncheck the Cisco SNMP Server check box, and click **Submit**. The **Monitor >Server Level > Services Monitor** page for each server shows the Cisco SNMP Server process.

Workaround:

There is no workaround.

- CSCsw18466

  Symptom:

  The ASM Audit Log archival is not generating.

  Condition:

  Choose **Report > Archived Data** and select **Audit Logs**. There are no Audit Log files listed.

  Workaround:

  Audit logs are available for 60 days through the **Report > System Level > CDSM Audit Logs** page.

- CSCsx23575

  Symptom:

  The SNMP trap destination cannot be configured in the CDSM.

  Condition:

  Use the CDSM and configure the SNMP trap station. An error message stating there was a failure to configure the SNMP Trap and a javascript error may appear on the browser.

  Workaround:

  Trap destinations can be configured in the /usr/local/share/snmp/snmpd.conf file. However the snmpd.conf file is regenerated any time the statsd process on the server is restarted.

- CSCsx63348

  Symptom:

  In CDSM, when a disk threshold is equal to the actual percentage available, the overall status stays green, whereas clicking the disk results in a warning that the threshold has been exceeded.

  Condition:

  When the actual usage is equal to the threshold crossing alert (TCA).

  Workaround:

  To have the overall indicator turn yellow, set the TCA to one percent lower than the actual TCA percentage.

- CSCsx63423

  Symptom:

  The disk threshold settings for the CServer usage do not turn the disk overall status to yellow or red based on the disk capacity notify or warning.

  Condition:

  Disk capacity notify and warning do not turn the overall status yellow or red.

  Workaround:

  There is no workaround.

- CSCsx98619

  Symptom:

  The CDSM reported active stream count is different from the cserver alloc count.

  Condition:

  This occurs when streams are allocated, but are not playing.

  During periods of high churn, the stream counts can be different because of polling intervals of the data.

  Workaround:

  There is no workaround. The two statistics are similar, but not exact representations of each other.

- CSCsy03309

  Symptom:

  The CDSM only allows EPG files up to 2MB in size to be uploaded.

  Condition:

  When importing an EPG file larger than 2MB, an error states that the upload failed with filesize = 0.

  Workaround:

  Separate the EPG file into smaller size files. Change the upload_max_filesize parameter in the /arroyo/www/conf/php.ini file to 5M. The upload_max_filesize cannot be larger than 5MB.

- CSCsv16883

  Symptom:

  Several warning messages display when clicking the last page of the Stream Monitor search results.

  function on the page

  Condition:

  From the M**onitor > System Level > Stream Monitor** page, set the search criteria and click **Search**. Clicking the last page of the report displays the warning messages.

  Workaround:

  Click **New Report**, or the **Back** icon in the browser, to return to the Stream Monitor page.

CServer

- CSCsu01226

  Symptom:

  The content being ingested was stopped in the middle of ingesting. Because the CDS software registered these content objects as being in the middle of ingest, the content could not be deleted.

  Condition:

  Content is being ingested when, probably, the FTP connection broke and was never reestablished. This caused the content to get stuck in the middle of ingesting.

  Workaround:

  Restart the ContentStore Slave service. This flushes the ingest queue, which is stored in memory.

- CSCsw80147

  Symptom:

  The message in the protocoltiming.log file does not reflect the correct state of Vaults that are switched to offloading.

  Condition:

  When Vaults are placed in the offload state (that is, they are not ingesting any new content) by the TRICKLE_DOWN command or by the CDSM GUI Server Offload page, the protocoltiming.log file is not updated.

  Workaround:

  No workaround required. The system functions properly and ingests take place correctly, the message is just not updated correctly.
- CSCsx04305

  Symptom:

  Video content files over 11 GB in size are not handled well.

  Condition:

  When ingesting content (including live content) that results in a single 1x file being over 11 GB in size, it may not be handled correctly.

  Workaround:

  Limit the size of content to six hours of standard-definition (SD) content or three hours of high-definition (HD) content.
- CSCsx93294

  Symptom:

  Null streams may occur when more than 2,432 streams are played on one Streamer

  Condition:

  If more than 2,432 streams are played, in some cases, those streams may play null streams.

  Workaround:

  Do not play more than 2,432 streams per Streamer. This problem does not occur in all cases, but if it does, reduce the number of streams to less than 2,432.

Streaming

- CSCsx18109

  Symptom:

  When a network error occurs and connectivity between servers (Vault, Streamer, and so on) is lost, the network becomes partitioned and error recovery begins.

  Condition:

  If routers fail, networks go down, cables fail, NICs fail, and so on, then errors occur. Streams begin to fail and the system tries to recover those streams so they continue playing.

  Workaround:

  When the administrator discovers that a network problem occurred, they should begin to reassign the failed streams to other Streamers.

- CSCsw87225

  Symptom:

  An error message states that "Fill content failed, Fill IGate failed."

  Condition:

  This error message can occur on Vault Lindenhurst CDEs (CDE400s) that are overloaded. Overloading a CDE400 could occur when ingesting over a 150 content objects, generating over five trick files for over 150 content objects, or a combination of the two.

  Workaround:

  This is a limitation on the CDE400. For higher performance requirements, the Next-Generation Content Delivery Engine (CDE), CDE420, is required.
- CSCsw87409

  Symptom:

  If a Streamer is out of capacity for live content streaming, the number of active streams may not be reported correctly in protocoltiming.log

  Condition:

  If over 160 channels of live content is played for 480 streams on 2 Streamers, this error may occur.

  Workaround:

  Increase the number of Streamers that stream live content.

Network

- CSCsy00879

  Symptom:

  A CPU lockup can occur if the server is overrun with network traffic when initializing.

  Condition:

  If a Streamer or Vault is over run by network traffic at the same time it is booting up, the server may not handle the traffic correctly and a CPU lockup can occur.

  Workaround:

  The primary workaround is to not have the network cables plugged in when the server is brought up. This problem is very rare, but if it occurs, the server can be rebooted and typically comes up without a problem.
- CSCsv84325

  Symptom:

  When the default gateway on a server is misconfigured, the CServer responds with a trap message.

  Condition:

  When configuring the default gateway on the Streamer with the same IP address as one of the Ethernet ports, the Streamer cannot stream correctly.

  Workaround:

  Configure the correct default gateway IP address.

Drivers

- CSCsx63245

  Symptom:

  A zero-length track was found when creating the track map. This is only a warning.

  Condition:

  When a new disk in inserted into the drive, a map of the drive is created. Periodically, a zero-length track may inadvertently be found. This is very rare, and does not affect the operation of the system.

  Workaround:

  No workaround is required. The system will operate normally if this occurs.
- CSCsw65414

  Symptom:

  Streaming over a WAN connection with low bandwidth can cause packet loss.

  Condition:

  If the communication bandwidth between Vaults and Streamers does not have enough bandwidth, packets can be lost.

  Workaround:

  Ensure that there is enough bandwidth to handle the streaming load needed.
- CSCsw98312

  Symptom:

  A drive that has intermittent failures (goes bad, then comes back, then goes bad again), is not handled well.

  Condition:

  This could happen if a disk drive is pulled out and immediately re-inserted, then immediately pulled out again.

  Workaround:

  Do not remove and replace a drive quickly.
- CSCsx34800

  Symptom:

  An error occurred when more than 300,000 pieces of content were ingested.

  Condition:

  If more than 300,000 pieces of content are ingested into the CDS an error occurs.

  Workaround:

  Do not ingest over 300k pieces of content.

Vault

- CSCsv94139

  Symptom:

  Requesting more than ten simultaneous FTP out sessions results in an error.

  Condition:

  When more than ten simultaneous FTPout sessions are requested an error results.

  Workaround:

  The workaround is to limit the number of simultaneous FTPout sessions to ten or less.
- CSCsx17185

  Symptom:

  On live ingest, if a drive fails, some content may be lost.

  Condition:

  When ingesting live content and a drive fails where content is being written to, some holes in the content may occur.

  Workaround:

  If possible, re-ingest the content.

Ingest Manager

- CSCsx55568

  Symptom:

  While processing a schedule of 30 30-minutes recordings, AIM was stopped and restarted. After recordings completed, it was discovered that one recording was not provisioned.

  Condition:

  In a MediaX environment, while processing a large number of recording events, stop and restart the AIM process.

  Workaround:

  There are no known workarounds for this.
- CSCsx75311

  Symptom:

  In a MedaX environment, when schedules are being processed, if the Ingest Manager is stopped for an extended period of time and then restarted, the Ingest Manager attempts to republish events that are in the past.

  Condition:

  This occurs in a MediaX live capture environment when the Ingest Manager is processing the recording schedule. If Ingest Manager is stopped or is down for an extended period of time (specifically beyond the event time of the recording), and then restarted, expired events may get published.

Workaround:

There is no workaround for this issue. The events are expired out of the system naturally, based on the license window dates.

ISA

- CSCsx52937

  Symptom:

  In an ISA MediaX environment, currently active recordings (live captures) are not displayed on the CDSM GUI **Monitor > System Level > Active Ingest** monitoring page.

  Condition:

  This only occurs in an ISA environment when using MediaX live capture capability. Active captures are not listed in the Active Ingest monitor page.

  Workaround:

  There is no workaround.

- CSCsv55572

  Symptom:

  If real-time assets (RTAs) fail prematurely during the passive FTP (PASV) command, there is no way to figure out which RTA content it was for. So there is no way for the Vault to provide the information about failed ingests to the CDSM.

  Condition:

  The PASV command failed while ingesting RTAs.

  Workaround:

  Fix the problem that is causing the PASV command to fail. Typically, this problem is caused by the Vaults being full.

Platform

- CSCsq89113

  Symptom:

  System does not operate correctly and will not boot.

  Condition:

  After following the existing procedure for swapping RAID drives on the CDSM, the server does not function and needs on-site resource to restore it. A RAID rebuild does not solve the booting problem.

  Workaround:

  Rebuild the RAID and manually run GRUB to install the bootloader onto "SDA" in order for the system to boot correctly.

RTSP

- CSCsx72598

  Symptom:

  Stopping recordings while they are in the process of being captured may result in a database record being left behind for the captured content.

  Condition:

  In an FSI live capture environment, with current recordings being captured, the operator issues a request to delete the recordings.

  Workaround:

  The workaround is to re-issue the delete recording request for the content record that did not get deleted originally.

- CSCsx93749

  Symptom:

  When tearing down 3500 sessions simultaneously, the RTSP server loses the ability to service other requests.

  Condition:

  While the RTSP server is servicing a large number of sessions, 3500 in this case, issue a teardown request for every session. This problem seems to only happen in an environment where each client has its own TCP connection for an RTSP session and stream control communications.

  Workaround:

  The RTSP server can be restarted in order to service other requests.

  ```
  # arroyo stop rtsp
  # arroyo start rtsp
  ```

Upgrade

- CSCsx60926

  Symptom:

  After upgrading from Release 1.5.1.x to Release 2.0, the starteth file is missing on the CDS server. If the server is not using all of its Ethernet ports, the ports display as the yellow warning status, instead of the black disabled status.

  Condition:

  After upgrading of any Streamer, Vault, or ISV from Release 1.5.1.x to Release 2.0.

  Workaround:

  In the CDSM GUI **Configure > Server Level > Server Setup** page, select the IP address from the drop-down list, and click **Submit**. The starteth file is regenerated from the CDSM to the server. Alternatively, save a copy of the starteth file before upgrading the server, and copy it back after the upgrade.

- CSCsx80826

  Symptom:

  The /var/tmp/TRICKLE_DOWN file is missing on the server after upgrading to Release 2.0.

Condition:

The upgrade from Release 1.5.1.x to Release 2.0 reformats the file system. When the server restarts, the TRICKLE_DOWN file is not rewritten, the CServer is notified that the server is offline, and the CDSM reports the server is still offline.

Workaround:

To use the CDSM to rewrite the file, do the following:

a. Choose **Maintain > Servers > Server Offload**.
b. From the **Server IP/Name** drop-down list, choose a server and click **Display**.
c. Make sure the **Disable** radio button is selected, and click **Submit**.
d. Choose **Maintain > Server s> Server Restart**,
e. From the **Server IP/Name** drop-down list, choose a server and click **Display**.
f. From the **Restart** drop-down list, select **yes**, and click **Submit**.

The server reboots, and is recognized by the CServer and CDSM as being online.

Video

- CSCsu83085

  Symptom:

  Fast-forward and fast-rewind do not run smoothly.

  Condition:

  This is only for Advanced Video Coding (AVC) high definition (HD) encoded content. It does not occur on all vendor STBs. Some STBs do not show any signs of poor Fast-forward or Fast-rewind.

  Workaround:

  When Instantaneous Decoder Refresh (IDR) is set to "Always," there is a big improvement. Try different STB vendors.

Resolved Caveats

The following caveats have been resolved since Cisco TV CDS Release 1.5.1.4.1 and Release 1.6.1. Not all resolved issues are mentioned here. The following list highlights associated with customer deployment scenarios.

CDSM

- CSCso12720

  Needed to kill off database PID and restart database after backing up .db files and scrubbing off .idx and replay logs. rtp.db file was over 5G in size. Not sure if this had anything to do with it.

- CSCsu99948

  MSA logs are not being generated. Need to manually change ownership of /arroyo/msa and /opt/msa folders and subfolders from root to msa:isa.

- CSCsu87741

  CDSM database increases to greater than 4 GB causing inability for CDSM to function.
- CSCsw79478

  Unable to run reports because the database has stopped and avsdb process caused a core dump. Btree corruption occurred because of improper shutdown.
- CSCsr81309

  Configuration of a new QAM in the CDSM is not getting to the Streamer.
- CSCso28059

  Missing entry in the configuration file causes a failure to load the service groups.
- CSCsr29873

  Cannot configure an Array name in the CDSM.
- CSCsx96159

  Report archiving does not delete reports older than 60 days.

CServer

- CSCsq67510

  The Streamer goes into KDB mode because of “ObjectSegmentDir” and “MemoryPool.” This rarely occurs.
- CSCsq79389

  Using the CDSM to change the IP addresses on an active Streamer causes reachable/ unreachable messages to be delivered at such a high rate that other processes are starved, including disk drives. This causes cache drives to be removed from the server because they cannot be serviced. On a Vault, content is lost because new directories are written to based on the remaining cache drives.
- CSCsl19351

  When any disk partition fills up to 100 percent, the CDS goes into KDB mode. This specifically occurs when the replay log is around 2 GB in size on each server.
- CSCsl16045

  The Vault goes into KDB mode when trying to ingest H.264 content.
- CSCso62256

  When a misconfigured router drops packets, the CDS servers show reachable/unreachable messages, which results in remote mirroring to run and recover content.
- CSCso60458

  CALYPSO ASSERT. Vault goes out of service when there is excessive packet loss on the cache-fill network. This results in excessive logging on the Vaults for every fill request, which results in the Vault running out of memory.
- CSCso51792

  Network problem causes the Streamers to go into KDB mode.

  When a fill request is already canceled out, the remote fill continues. With packet loss, these packets are queued up, expecting the holes to be filled. The holes are not filled because the fill request was already canceled. The fix is to properly cancel out the request.

- CSCsx04705

  The WaitForFTPDataDone may occur before the AllocDataListener is setup, causing the WaitForFTPDataDone to be processed before there is a connection. This leaves the connection hanging. If enough connections are tied up, the maximum FTP sessions allowed is exceeded, which results in refusal of subsequent FTP out requests.
- CSCsw94184

  If the number of RTI threads increases to a high number, the run_isa script fails and the ns_log file stops updating because of "word too long error" message.
- CSCsw86946

  CALYPSO ASSERT. The stream application sent a destroy message for a stream that had not completed setup.
- CSCso46290

  The Streamer goes into KDB mode when there are 31 different content rates.
- CSCso24579

  The Vault goes into KDB mode when there are mixed content types (HD and SD).
- CSCsm11262

  No cache-fill. The Vault refuses cache-fill.
- CSCsw25143

  Bad pointer reference when deleting an object from cache, which causes the Streamer to go into KDB mode.
- CSCsk84874

  Vault goes into KDB mode if the content is deleted in a multi-Vault configuration.
- CSCsl82609

  Streamer cannot fill after 24 days of uptime.
- CSCsv11061

  TTL values in the CDSM are not propagating to the Streamers.
- CSCsv01674

  Number of mirrored copies configured on the Vaults is not getting enforced.
- CSCsu93982

  If one Vault goes out-of-service in a two-Vault system, the remaining Vault runs out of memory and goes into KDB mode when trying to communicate with the downed Vault.
- CSCsk08957

  Rebooting a switch used for cache-fill, or link loss on a switch port used for cache-fill, could cause the Vault to stop functioning and go into KDB mode.
- CSCsu03408

  When ingested content has a bad PMT, the PAT and PMT are replaced with standard ones. If subsequent PMTs for that content are not standard (for example, AC-3) and they are replaced with the standard one, there is no audio during playout.
- CSCsr05721

  The Vault goes into KDB mode when ingesting content that is missing a PMT.

- CSCsq23825

  The ISV is not able to catch-up-to-live (with a three-second delay).
- CSCsq18177

  Defective or misconfigured Ethernet interface on a Vault or Streamer causes inbound and outbound packet corruption.
- CSCso69291

  CALYPSO ASSERT on m_monitorPacketReceived. During mirroring, when packet loss occurs because of router misconfiguration, reachable and unreachable messages are sent and this message occurs.
- CSCsl82609

  A Streamer cannot accept fill content from a Vault after 24 days of uptime because of an error in the counter. The counter goes negative in about 24 days, and goes positive again 24 days later.
- CSCsw25528

  Streamer trapped because of inconsistent states between the Streamer and Vault. Just prior to the trap, a NIC port went down and could be a contributing factor.
- CSCsk87462

  Corner case. Error handling in WriteBuf uses the wrong deallocator.
- CSCsu29595

  Getting duplicate packets during Vault mirroring.

Database

- CSCsx76140

  Symptom:

  The CDSM GUI can appear unresponsive. Attempting to connect a browser to the CDSM hangs, and eventually the browser times out.
- CSCsl28749

  Vault runs out of FillCB resources and the database process goes into KDB mode when ingesting content at the same time as writing replication log information.

  The replication thread attempts to update the content GOID index at the same time content records are being stored in the replay logs.

Ingest Manager

- CSCsx57512

  The **stunnel** command is not included. This is needed to establish encrypted SSH sessions between the Ingest Manager and Widevine.
- CSCsx45220

  The Ingest Manager fails when cleaning up the Widevine ADI. This occurs when “movie” is part of the movie filename

ISA

- CSCsk70743

  The Vault stream service is not working, which results in error message 232 codes.
- CSCsw19924

  The Motorola STB gets a 5070 error if the session is reinitiated within ten seconds.
- CSCsv55563

  Live ingest should not be sent to a slave Vault that has the avsdb process stopped.
- CSCsm01902

  The LSCP server should set the from NPT of the first play request to zero if it was sent from the set-top box (STB) with a value beyond the end of the playlist.
- CSCsv19210

  Barker streams do not work if LCSPClientProto is set to RTSP.

Video

- CSCsv38339

  If the server cannot figure out the frame size in a stream, then it cannot initialize the dummy P-frames that are used when splicing. This has occurred twice, one was because of an illegal frame size. and the other had bad encoding.
- CSCsx22125

  Bad content causes bursts of 232 errors.
- CSCsx04951

  Resume play is not working as expected on the RNG-200 STB.
- CSCsr68629

  Trick modes of Starz content show as no picture (black screen).
- CSCsl05140

  The Streamer goes into KDB mode when trick files are created from bad content, that is content containing several transport packets with blocks of zero.

Other

- CSCsr87476

  Database get out of synchronization among CDS servers when a server goes into KDB mode without committing to disk before returning success to the replication event.
- CSCsu42509

  Log archive for Arroyo and ISA conflict, removing all ISA logs.

Upgrading to Release 2.0

Note Release 2.0 supports upgrades from Release 1.5.1.4.1 and Release 1.6.1. If your CDS is running an older version, you need to upgrade to Release 1.5.1.4.1 for ISA environments and Release 1.6.1 for RTSP environments, before upgrading to Release 2.0.

Note Because the software upgrade to Release 2.0 includes upgrading the operating system, a Cisco technician will perform the upgrade. The procedures described in this section are informational only. (EDCS-760974)

Note Downgrading from Release 2.0 to Release 1.5.1.4.1 or Release 1.6.1 is a manual process, requiring a reload of the older operating system (OS) and a reload of the old database files. Any changes made to configuration or content after upgrading to Release 2.0 are lost.

A high-level view of the CDS software upgrade procedure is as follows:

1. Upgrade CDSM to Release 2.0
2. Upgrade one site at a time starting from the site with the Control server and ending with the site with the Setup server. Upgrade the Streamers in the “Control” sites first (sites that have Stream Groups with only a Control server), followed by the “Setup/Control” sites (sites that have Stream Groups with a Setup/Control server).

   Repeat for every Streamer on the site starting with the “Available” Streamers, followed by the “Backup” Streamer, and ending with the “Primary” Streamer.
3. Upgrade all the Vaults. Upgrade all slave Vaults and finish with the master Vault.

Caution Upgrading to Release 2.0 does not preserve reporting data. To keep existing reporting data, save the reports to a comma-separated value file (CSV) and copy them to a separate server.

Note Software upgrades should be performed during maintenance windows; that is, during off-peak hours when no new content is ingested into the CDS and stream demands are the lowest.

The Cisco technician will have the following items to upgrade your software to Release 2.0:

- DVD-ROM of Red Hat Enterprise Linux 5 (32-bit) for the CDS servers
- DVD-ROM of Red Hat Enterprise Linux 5 (64-bit) for the CDSM
- CD-ROM with a boot ISO image for the CDS servers (32-bit OS)
- CD-ROM with a boot ISO image for the CDSM (64-bit OS)
- CD-ROM with the CDS-TV-2.0.0.iso image
- USB DVD-ROM drive
- Linux server (SSH-reachable) used to store the backup files of the CDSM and CDS servers

Note Any CDS server or another Linux server on the network can be used as long as it has the /arroyo/backup directory and is accessible through SSH. The pre-upgrade and post upgrade scripts ask you for the backup server's IP address. The CDSM backup files require approximately 50MB of disk space. The backup files for each CDS server (Streamer, Vault, or ISV) require approximately 1MB of disk space. So, the backup server needs approximately 60-65MB of disk space for a site that has one CDSM and ten CDS servers.

Upgrade the Software on the CDSM

Upgrading the software on the CDSM has the following main tasks:

1. Shut down the processes.
2. Run the preupgrade script. This creates a backup file with the configuration settings and databases, and stores it on another Linux server.
3. Connect the USB DVD-ROM drive, insert the bootable CD-ROM, and reboot the CDSM.
4. Install the Red Hat Enterprise Linux 5 (64-bit) operating system.
5. Insert the CD-ROM with the TV CDS Release 2.0 software.
6. Run the post-install script. This fixes the disk partitions.
7. Install the TV CDS Release 2.0 software and initially configure the CDSM.
8. Run the upgrade script. This retrieves the backup file from the other Linux server.
9. Log in to the CDSM and complete the configuration.

Upgrade the Software on Each Streamer and Vault

Note In a multi-site CDS, upgrade the Streamers in the "Control" sites first (sites that have Stream Groups with only a Control server), followed by the "Setup/Control" sites (sites that have Stream Groups with a Setup/Control server).

In a multi-site CDS, upgrade all the Vaults using the same procedural order as the Streamers (offload, upgrade, reboot, and online). Start the Vault upgrade at the Control sites, then finish with the Setup/Control site.

Upgrading the software on a Streamer or a Vault has the following main tasks:

1. Offload the server and shut down the processes on the server.
2. Run the preupgrade script. This creates a backup file with the configuration settings and databases, and stores it on another Linux server.
3. Connect the USB DVD-ROM drive, insert the bootable CD-ROM, and reboot the CDSM.
4. Install the Red Hat Enterprise Linux 5 (32-bit) operating system.
5. Insert the CD-ROM with the TV CDS Release 2.0 software.
6. Install the TV CDS Release 2.0 software and initially configure the CDSM.
7. Run the upgrade script. This retrieves the backup file from the other Linux server.
8. Log in to the CDSM and complete the configuration.

Documentation Updates

The following documents have been added for this release:

- *Cisco TV CDS 2.0 ISA Software Configuration Guide*
- *Cisco TV CDS 2.0 RTSP Software Configuration Guide*
- *Cisco TV CDS 2.0 API Guide*
- *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide*
- Cisco Content Delivery Engine 110 Hardware Installation Guide
- Cisco Content Delivery System 2.x Documentation Roadmap
- *Regulatory Compliance and Safety Information for Cisco Content Delivery Engines*

Related Documentation

Refer to the following documents for additional information about the Cisco TV CDS 2.0:

- *Cisco TV CDS 2.0 ISA Software Configuration Guide* (OL-15953-01)

  http://cisco.com/en/US/docs/video/cds/cda/tv/2_0/configuration/isa_guide/tv_cds_2_0_isa_cfguide.html
- *Cisco TV CDS 2.0 RTSP Software Configuration Guide* (OL-15954-01)

  http://cisco.com/en/US/docs/video/cds/cda/tv/2_0/configuration/rtsp_guide/tv_cds_2_0_rtsp_cfguide.html
- *Cisco TV CDS 2.0 API Guide* (OL-18909-01)

  http://cisco.com/en/US/docs/video/cds/cda/tv/2_0/developer/guide/tv_cds_2_0_apiguide.html
- *Cisco Content Delivery System 2.x Documentation Roadmap* (OL-13495-07)

  http://www.cisco.com/en/US/docs/video/cds/overview/CDS_Roadmap.html

- *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide* (OL-16887-01)

  http://www.cisco.com/en/US/docs/video/cds/cde/cde205_220_420/installation/guide/cde205_220_420_hig.html
- *Cisco Content Delivery Engine 110 Hardware Installation Guide*

  http://www.cisco.com/en/US/docs/video/cds/cde/cde110/installation/guide/cde110_install.html
- *Cisco Content Delivery Engine 100/200/300/400 Hardware Installation Guide* (OL-13478-02)

  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* (78-18229-02)

  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.

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.